softline direct

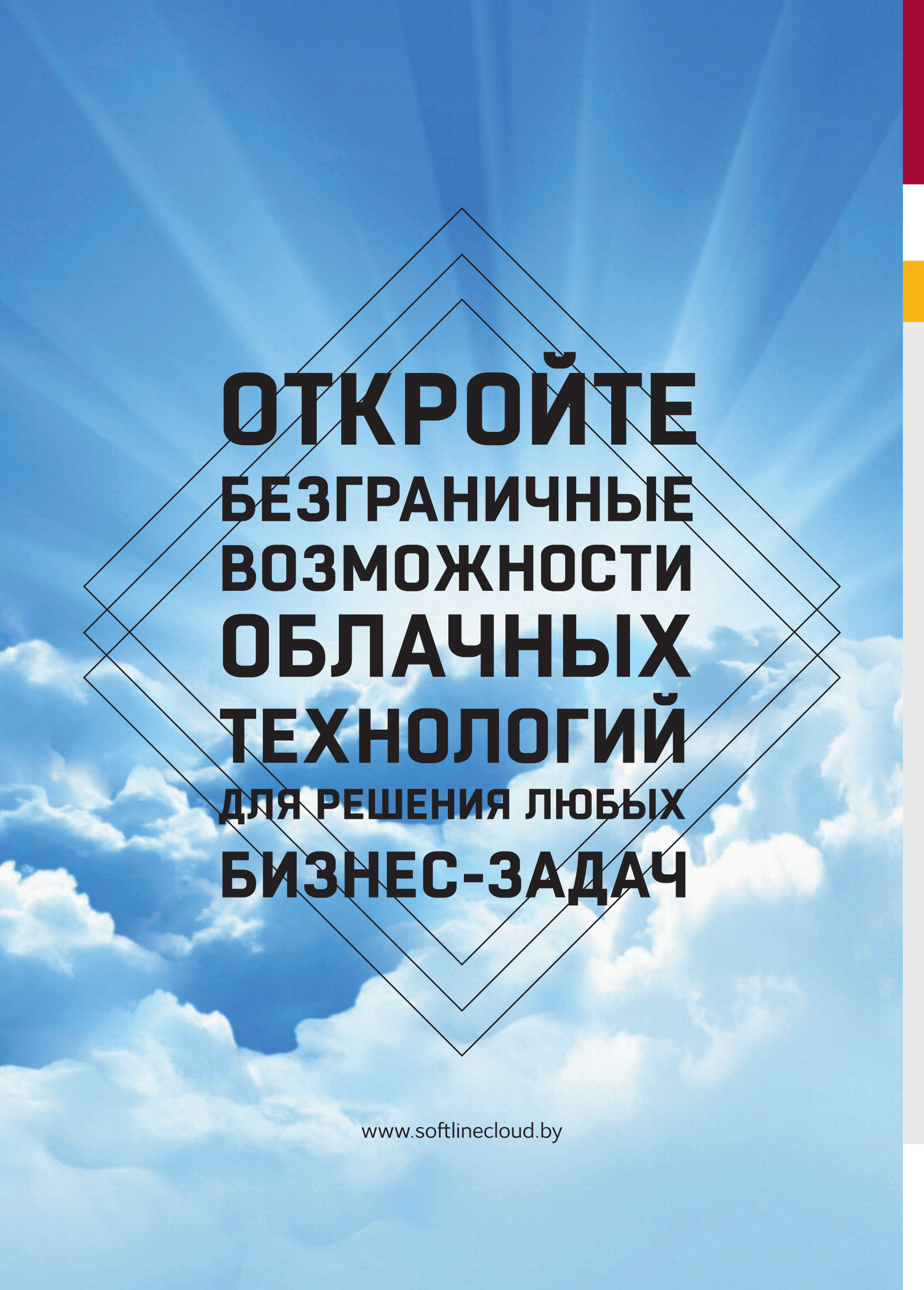
КАТАЛОГ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2 (33)
2018 BY

В будущее вместе с ИТ!

+375 (17) 336-55-95

www.softline.by


ОТКРОЙТЕ
БЕЗГРАНИЧНЫЕ
ВОЗМОЖНОСТИ
ОБЛАЧНЫХ
ТЕХНОЛОГИЙ
ДЛЯ РЕШЕНИЯ ЛЮБЫХ
БИЗНЕС-ЗАДАЧ
www.softlinecloud.by

Уважаемые коллеги, партнеры, друзья!

Мы рады представить вам новый выпуск каталога Softline-direct.

Благодаря цифровой трансформации мы выходим на качественно новый ритм жизни и работы. Среди наших заказчиков становится все больше компаний, которые понимают, как перевод бизнеса в «цифру» меняет их работу к лучшему – снижает издержки, повышает прибыльность и качество товаров и услуг, помогает устанавливать правильные отношения с клиентами. Своей главной миссией мы считаем помощь в выборе необходимых инструментов для решения этих задач.

Сегодня двигателем новой технологической революции является модель потребления ИТ в формате сервиса, без приобретения в собственность железа и софта, что позволяет существенно сократить расходы на инфраструктуру, электроэнергию и обслуживание.

Стратегия развития компании Softline на ближайшие годы опирается именно на предоставление ИТ в аренду. Наши основные партнеры в лице ведущих мировых разработчиков Microsoft, VMware, Cisco и многих других связывают свое настоящее и будущее с облаком, моделью аренды ИТ и аутсорсингом. Одна из тем этого выпуска будет посвящена облачным сервисам и преимуществам покупки ПО в аренду.

В Softline сформирована одна из самых мощных команд по информационной безопасности.

Мы внимательно следим за трендами как на белорусском, так и мировом рынках кибербезопасности, и стараемся внедрять технологии с учетом специфики бизнеса заказчиков. В одной из рубрик каталога мы рассмотрим актуальные сценарии реализации угроз ИБ, типовые схемы атак на банки, поговорим о современных средствах защиты – системе выявления инцидентов в реальном времени MaxPatrol SIEM, DLP-системах. Менеджер по продажам решений информационной безопасности Softline Юрий Богуш расскажет о преимуществах комплексных решений Check Point в области защиты структурных сегментов корпоративной сети.

Для стабильной работы любого бизнеса важно надежное хранение информации.

Непредвиденные атаки, технические неполадки, ошибки обновлений и другие обстоятельства могут привести к потере данных, а, значит, финансовым потерям организации. В одном из разделов каталога вы узнаете на что сегодня нужно обращать внимание при выборе средств резервного копирования и о правилах эффективного бэкапа.

Softline – команда профессионалов с глубокими знаниями и огромным опытом практического применения современных подходов и технологий.

Уверен, что вместе мы сможем поднять ваш бизнес на качественно новый уровень, получить возможность работать быстрее, лучше и эффективнее!

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

Каталог
ИТ-решений
и сервисов для
бизнеса

Softline
direct

НОЯБРЬ

2018-2(33)-BY

Учредитель:
ООО «СофтЛайн
Директ»

Главный редактор:
Людмила
Васильевна Пешкун

Выпускающий
редактор:
Яна Ламзина

Редактор:
Инна Савончик

Дизайн
и верстка:
Алексей Воропанов

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

Распространяется
бесплатно.

Тираж:
3000 экз.

Подписано в печать
31.10.2018
Отпечатано
в типографии
«ТриАпринт»,
Минская обл.,
Минский р-н,
а.г. Остромицкий
Городок,
ул.Ленина, 1.
Заказ № p2069

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

Контактная
информация:
marketing@softline.by

СОДЕРЖАНИЕ

Softline в соцсетях SoftlineBelarus @softline_belarus Softline Belarus

Представители Министерства промышленности Беларуси и белорусских промышленных предприятий посетили ПАО «КАМАЗ»

КАМАЗ является лидером среди предприятий СНГ по части автоматизации конструкторской и технологической подготовки изделий на базе программных решений разработки Siemens PLM Software. В ходе визита, организованного компаниями Siemens PLM Software и Softline, члены белорусской делегации совместно с экспертами Softline ознакомились с принципами построения и автоматизации конструкторской и технологической подготовки изделий, расчетными исследованиями и инженерным анализом конструкции автомобилей КАМАЗ.

Также для белорусской делегации провели экскурсию по сборочному конвейеру ПАО «КАМАЗ», познакомили со спортивной командой «КАМАЗ-Мастер», рассказали о производстве спортивных автомобилей и их компонентов.

Руководители белорусских предприятий отметили высокой уровень организации, культуры производства и автоматизации на предприятии.

По результатам визита на ПАО «КАМАЗ» представители Министерства промышленности Республики Беларусь и руководители белорусских компаний выразили заинтересованность во внедрении программных решений Siemens PLM Software с целью автоматизации и обеспечения конкурентоспособности белорусской промышленности.

Компания Softline, партнер компании Siemens PLM Software, помогает обеспечить внедрение средств автоматизации на промышленных предприятиях Республики Беларусь.

«Цифровая трансформация промышленных предприятий оказывает значительное влияние на процессы разработки изделий. Внедрение средств автоматизации конструкторско-технологической подготовки производства позволяет существенно сократить сроки разработки изделий, повысить качество процесса разработки и, как следствие, снизить себестоимость изделия, обеспечить быстрый переход к массовому производству и выход изделия на рынок.

Внедрение таких решений, как Siemens PLM Software, а также квалифицированная подготовка специалистов Softline позволили ПАО «КАМАЗ» обеспечить конкурентоспособность своей продукции, существенно расширить рынки ее сбыта, а также существенно улучшить качество», – отметил продакт-менеджер САПР по направлению «Машиностроение» в Softline Владимир Фонов.

Минский офис Softline переехал на новое место

В августе 2018 года офис компании Softline в Минске сменил адрес и в настоящее время расположен в бизнес-центре Riviera Plaza по адресу: пр-т Победителей, 108.

Обращаем ваше внимание на изменение реквизитов компании:

- Юридический адрес: пр-т Победителей, 108, 4 этаж, помещение 10, Минск, 220062.
- Новый контактный телефон: +375 (17) 336-55-95.

С радостью ждем вас в новом офисе!

Фото: realt.by

ПОРТРЕТ КОМПАНИИ

Наша миссия

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

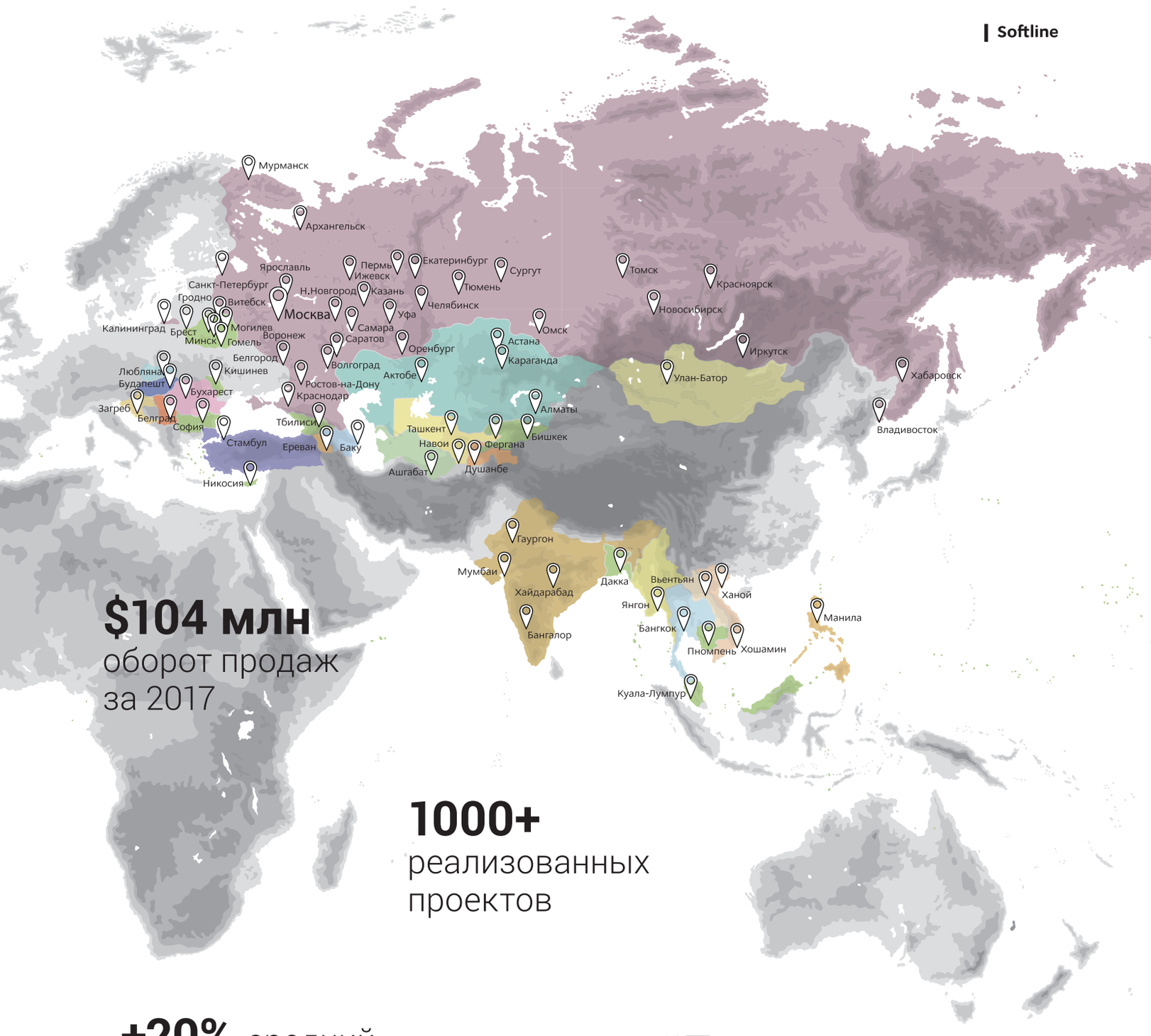
ПОЧЕМУ SOFTLINE?

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

Microsoft Partner — Gold Cloud Productivity, Gold Datacenter, Silver Cloud Productivity, Silver Collaboration and Content, Silver Messaging
HUAWEI Enterprise Partner Gold
KASPERSKY PLATINUM PARTNER
ORACLE Platinum Partner
TREND MICRO
SOLIDWORKS
intel
CITRIX PARTNER Silver Solution Advisor
vmware PARTNER
Google Cloud
Acronis | Platinum Partner
Synology Gold Partner
AXIS SOLUTION SILVER PARTNER
paloalto



$104 млн
оборот продаж
за 2017

1000+
реализованных
проектов

+20% средний
ежегодный рост продаж

17 лет на ИТ-рынке
Беларуси

Получен сертификат соответствия ОАЦ на платформу VMware NSX версии 6.4

Компания Softline получила сертификат соответствия на платформу виртуализации и обеспечения безопасности сети VMware NSX 6.4.

Сертификация продукта проводилась в Национальной системе подтверждения соответствия специальным органом по сертификации ОАЦ - Оперативно-аналитическим центром при Президенте Республики Беларусь.

Сертификат удостоверяет, что решение VMware NSX соответствует всем необходимым требованиям безопасности информационных технологий согласно государственным стандартам Республики Беларусь.

Сертифицированный NSX 6.4 теперь поставляется в составе пакетов, предназначенных для построения систем защиты информационных систем, обрабатывающих конфиденциальную информацию и персональные данные.

Встреча Softline с первым проректором БНТУ в рамках продвижения концепции Индустрии 4.0

В рамках продвижения Индустрии 4.0 в Беларуси и с целью подготовки кадров для промышленных предприятий состоялась важная встреча экспертов Softline с первым проректором БНТУ Георгием Вершиной и деканом машиностроительного факультета БНТУ Андреем Сафоновым.

Эксперты отдела САПР/ГИС Softline в лице Ольги Кончевской, Владимира Фонова и Сергея Глазкова совместно с профессором Карабюкского университета (Турция) Керимом Четинкая, а также исполнительным директором Академии новых технологий Али Джанмамедовым, обсудили вопросы внедрения в учебный процесс БНТУ новых технологий с целью повышения качества подготовки студентов. Также была проведена встреча с научно-преподавательским составом факультета.

По итогу были определены планы сотрудничества Softline и Белорусского национального технического университета.

Начало сотрудничества Softline с японской компанией RICOH

Компания Softline объявляет о начале сотрудничества с японской компанией RICOH, ведущим мировым производителем цифровых печатных машин. Компания специализируется на печатной технике, многофункциональных устройствах, широкоформатных системах, решениях для производственной печати, системах управления документооборотом.

Сотрудничество с RICOH позволяет Softline предложить белорусским предприятиям широкоформатные инженерные системы (устройства для печати, копирования и сканирования чертежей и графических изображений, монохромные МФУ) и услуги по управлению документооборотом. Современное цифровое оборудование поможет компаниям быстрее и удобнее обрабатывать техническую документацию, а также повысить производительность при выпуске технической документации, увеличить уровень защиты данных.

В Беларуси заработал «Центр компетенций цифровой трансформации строительной отрасли»

Компания Softline рада сообщить о начале работы «Центра компетенций цифровой трансформации строительной отрасли Республики Беларусь». Создание центра компетенций – это долгожданный проект как для Министерства архитектуры и строительства Республики Беларусь, так и для Softline. Работа над ним началась еще в 2016 году.

Сегодня главной стратегической целью развития информационных технологий в строительной сфере является повышение эффективности управления строительными организациями и улучшение степени взаимодействия участников процесса за счет внедрения и использования передовых информационных технологий.

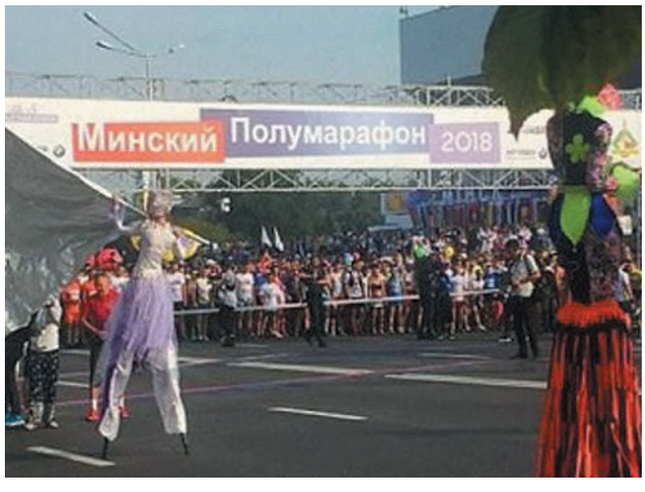
Еще один важный шаг в осуществлении цифровой трансформации строительной отрасли – внедрение BIM-технологий, которые позволяют автоматизировать сложные процессы, сокращать сроки проектирования и получать трехмерные информационные модели объекта. С их помощью можно исключить ошибки проектирования, сократить сроки на внесение изменений и получить высококачественную проектную документацию. Как показывает практика, далеко не все предприятия строительной отрасли в Беларуси готовы как организационно, так и технически к цифровой трансформации. Являясь ведущим системным интегратором рынка комплексных ИТ-проектов и обладая высокими компетенциями, международным опытом и экспертизой, компания Softline готова помочь в комплексном внедрении передовых информационных технологий. С этой целью и был создан Центр компетенций цифровой трансформации строительной отрасли при Министерстве архитектуры и строительства и Softline.

Деятельность центра будет направлена на разработку инновационных сервисов для построения интегрированных информационных систем.

В ближайших планах центра – создание единого информационно-технологического пространства «Госстройпортал». На первом этапе ресурс будет содержать новости о BIM-технологиях, раздел информационной поддержки процессов выполнения административно-регламентных процедур в строительной отрасли Беларуси. Также на портале будет представлен удобный каталог информационных 3D-моделей строительных материалов, изделий, конструкций с указанием необходимых параметров для проектирования и дальнейшего использования.

«И это только начало. В рамках работ по цифровизации строительной сферы ведется системная работа по созданию кросс-отраслевых процессов и цифровой экосистемы как основы для роста и развития строительной сферы Беларуси», – отметила руководитель Центра компетенций цифровой трансформации строительной отрасли Республики Беларусь Ольга Кончевская.

Команда Softline и Axoft приняла участие в Минском полумарафоне-2018



Марафон в 2018 году оказался невероятно масштабным мероприятием. В нем приняли участие 35 тысяч бегунов из 53 стран мира.

Этот спортивный фестиваль уже стал традицией: начиная с 2015 года в первые выходные сентября Минск отмечает не только День города, но и проводит праздник спорта, собирая на своих улицах профессионалов и любителей бега.

Стоять на старте, бежать под крики поддержки, преодолевать дистанцию с огромной толпой – наша команда получила невероятный заряд положительных эмоций. Участники из числа сотрудников Softline и Axoft успешно преодолели дистанции в 5,5; 10,55 и 21,1 км и показали отличные результаты.

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 статусов 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.

Microsoft 365

Специально для бизнеса компания Microsoft выпустила комплексное интеллектуальное решение Microsoft 365. В его состав входят такие продукты, как Office 365, Windows 10 и Enterprise Mobility + Security.

Комплексное решение Microsoft 365 призвано обеспечить сотрудников компаний современными, гибкими и эффективными рабочими местами, подключиться к которым можно независимо от вида используемого устройства. Пакет разворачивается равно успешно как на стационарном компьютере, так и на смартфоне. Решения, входящие в Microsoft 365, можно условно разделить на две группы:

- Windows 10 и Office 365 – операционная система и офисные программы, обеспечивающие комфортную работу сотрудников.
- Enterprise Mobility + Security – решение, позволяющее установить дополнительный контур безопасности и управлять всеми устройствами, подключенными к корпоративной сети.

Microsoft 365

Office 365

Windows 10

Enterprise Mobility + Security

Состав решения Microsoft 365

С помощью Microsoft 365 реализуются пять сценариев безопасности.

1. Управление доступом сотрудников к корпоративным сервисам и ресурсам. Многофакторная идентификация. Контроль доступа к корпоративным ресурсам с любых устройств.
2. Управление устройствами и приложениями. Для доступа к порталу на устройство устанавливается следящее приложение, чтобы обеспечить его безопасность, соблюдение всех политик, разграничить управление приложениями. Например, со смартфона пользователь может открыть документ, но не может его скопировать (вплоть до запрета скринов).
3. Защита от киберугроз. Защита от спама, вирусов, троянов, мониторинг действий зараженных устройств.
4. Защита информации. Маркирование документов разным уровнем доступа: только для сотрудников, только для топ-менеджеров. Шифрование документов, предоставление доступа людям за пределами организации по облачному ID. Возможность отзывать права на доступ.
5. Контроль облачных сервисов. Представляет собой единый пульт управления, позволяющий отследить, какие сервисы используют сотрудники, пытаются ли они получить доступ к запрещенным ресурсам, хранят ли документы в незащищенных облачных хранилищах.

Почему Microsoft 365?

Потому что именно это решение является комплексным продуктом, обеспечивающим и соблюдение всех пяти сценариев ИТ-безопасности и, одновременно, создающим рабочие места для пользователей. Да, все это можно сделать с помощью набора решений, производимых разными компаниями-разработчиками, но обеспечить их интеграцию окажется намного сложнее.

Возможности Windows 10 Enterprise

Windows 10

Доверенная платформа	Повышение продуктивности	Персонализация	Широкий спектр устройств
Enterprise Data Protection Защита от утечек данных за счет отделения корпоративной информации от личной	**Azure Active Directory Join** Включение устройства в облачную или гинфраструктуру организации	**User Experience Virtualization** (UX-V) Синхронизация пользовательских настроек между устройствами и виртуальными средами Windows	**Windows 10 for Industry Devices** Использование недорогих, массовых устройств в качестве терминалов, киосков и др.
Windows Hello for Business Доступ к системе на основе биометрии	**MDM enablement** Управление устройством средствами MDM-решений	**Granular UX Control** Управление интерфейсом через централизованные политики	
Credential Guard Защита учетных записей с помощью аппаратных средств изоляции	**Windows Store for Business, Private Catalog** Каталог приложений, предоставляемых сотрудникам организацией		
AppLocker Запуск нежелательных и подозрительных приложений в изолированной среде	**Application Virtualization** (App-V) Упрощение развертывания и управления приложениями		
Device Guard Запрет на запуск недоверенных приложений на устройстве			
Windows 10 Enterprise E3			
Advanced Threat Protection Анализ угроз за счет обнаружения подозрительного поведения, сопоставления с базой данных известных атак			
Windows 10 Enterprise E5			

Возможности Enterprise Mobility + Security E3/E5

Управление учетными записями и доступом	Безопасность учетных записей	Управление устройствами, в т.ч. мобильными	Защита информации
WS RMS CAL + WS CAL + Azure Active Directory Premium P1 Единая учетная запись для локальных и облачных приложений Многофакторная аутентификация, контроль доступа с разных устройств, отчетность и аналитика	**Microsoft Advanced Threat Analytics** Анализ трафика и событий безопасности в локальном AD заказчика, предупреждения и проактивные действия Локальный сервис (не облако)	**SC Config Manager + + Microsoft Intune** Управление мобильными устройствами и приложениями (политики пароля, пин-кода, шифрования для устройства, разделение приложений и учетных записей в них на личные и рабочие)	**SC Endpoint Protection + Azure Information Protection Premium P1** Защита файлов через шифрование с помощью RMS Отслеживание доступа к файлам (только через Azure RMS) Ручная классификация документов
EMS E3			
Azure Active Directory Premium P2 Расширенная аналитика и действия по событиям, связанным с учетными записями Дополнительная защита для привилегированных учетных записей	**Microsoft Cloud App Security** Обнаружение фактов использования облачных сервисов (через анализ сетевых журналов) Управление облачными сервисами (Microsoft и др.)		
EMS E5			

Для каждой компании важен свой набор сценариев. Инструменты Microsoft 365 обеспечивают их полное соблюдение.
Microsoft 365 представляет собой гибридный облачный сервис, в котором часть приложений устанавливается на устройство.
Являясь одним из ведущих экспертов в области ИТ-безопасности, компания Softline разворачивает комплексные проекты, в рамках которых осуществляется и внедрение Microsoft 365 в той конфигурации, какая требуется для решения поставленных задач. ▮

Возможности Office 365 E3/E5

Office 365

Приложения	Клиентский доступ и сервисы	Безопасность	Аналитика
Office 365 Pro Plus: Office на 5 ПК или Mac **Office для мобильных устройств:** Приложения для планшетов и смартфонов	**Exchange Std + Ent CAL + Exchange online + EOP:** Электронная почта и календарь бизнес-класса **One Drive for Business:** Облачное хранилище и обмен файлами **SharePoint Std + Ent CAL:** Внутренние порталы и сайты **SfB Std + Ent CAL + SfB online:** Встречи, IM, Видеоконференции **Yammer:** Частная социальная сеть **Teams:** Взаимодействие команд в чате **StaffHub:** Управление сменными рабочими	**Advanced Threat Protection:** Расширенная защита почты: от неизвестных угроз (угроз «нулевого дня») и фишинговых атак **Advanced Security Management:** Панель для сбора аналитики и контроля за действиями пользователей **Customer Lockbox:** Тотальный контроль и защита данных в облаке **Advanced eDiscovery:** Сервис для поиска данных, проведения электронного аудита и расследования действия пользователей	**Power BI Pro:** Корпоративная аналитика по всем источникам данных в реальном времени **MyAnalytics:** Трекер персональной продуктивности работы сотрудников (количество и качество встреч, аналитика общения с коллегами и руководителем и т.д.)
	Office 365 E3		Коммуникации в облаке
			Cloud PBX + SfB Plus CAL: Подключение облака O365 к корпоративной телефонии, выделение номеров пользователям **PSTN Conferencing:** Присоединение к онлайн-собраниям по звонку из любой точки мира, выделение номера для конференции
			Office 365 E5

Легальное ПО – это дорого?

Евгений Андрейчук, руководитель направления по продаже решений Microsoft в странах Восточной Европы и Центральной Азии

Многие представители бизнеса уверены, что, используя нелицензионное программное обеспечение, они экономят бюджет компании. Как ни странно, такое стереотипное мышление, до сих пор встречается на белорусском рынке.

С появлением первых компьютеров, понятия легальный софт, как такового, не существовало. Нужную программу можно было купить на диске в любом киоске, не задумываясь о правах на нее, а стоимость первых лицензионных приложений была настолько высокой, что оказалась просто недоступной для большинства компаний. С тех пор прошло очень много времени, но проблема, слегка снизив свою остроту, тем не менее, не потеряла своей актуальности.

Согласно июньскому отчету Business Software Alliance (международной ассоциации производителей программного обеспечения), риски использования нелицензионного ПО гораздо выше, чем «выгода» от его приобретения. Исследования показывают, что в процессе поиска, загрузки и установки подобного программного обеспечения пользователь подвергает свой компьютер риску в 92 случаях из 100.

Кроме того, установлено, что в компаниях с высоким уровнем использования нелицензионного ПО, критический сбой систем обходится в среднем в $40 тыс. В конечном итоге, размер ущерба от использования подобного ПО значительно превосходит затраты на покупку лицензионных программ от проверенных поставщиков.

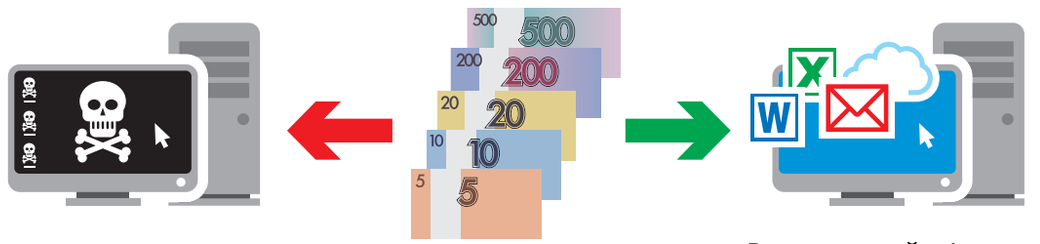
Практика лицензирования постоянно меняется и развивается, появляются новые и более доступные модели приобретения программного обеспечения. В настоящее время уже не нужно приобретать дорогостоящие «коробочные» лицензии, опустошая бюджет компании.

Компания Softline предлагает удобный, простой и, главное, недорогой способ приобретения легального программного обеспечения – покупку ПО в аренду. Вместо весьма затратного приобретения бессрочной или долговременной лицензии вы приобретаете право пользования программой, внося ежемесячные платежи.

Пять причин отказаться от использования нелегального ПО в пользу аренды лицензий

Пиратский софт может оказаться значительно дороже. Стоимость аренды одной лицензии начинается от 5 BYN в месяц, тогда как юридические и финансовые риски использования нелегальных программ могут в разы превышать эту сумму. К тому же многие приложения имеют упрощенное лицензирование: одна лицензия на пользователя дает право установки ПО сразу на несколько устройств. Кроме того, затраты на аренду софта относятся к операционным, что означает дополнительную экономию на налоге на прибыль.

735 BYN* (30 базовых величин) **– это:**



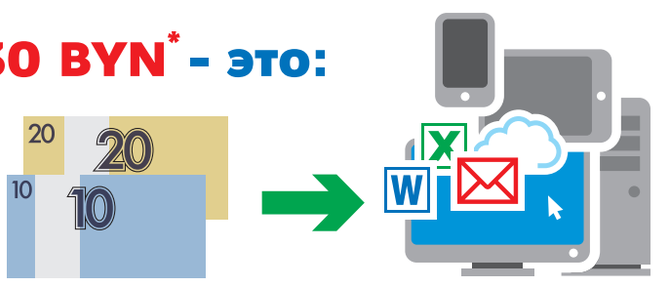
Минимальный штраф для юридических лиц за использование нелицензионного ПО

Виртуальный офис для **120** ПК/ **24** пользователя
(приложения MS Office, электронная почта, облачное хранилище, корпоративный портал и многое другое)

Аренда лицензий – быстрый доступ к необходимому ПО. Вам не нужно скачивать программы из неизвестных источников, искать к ним ключи и заниматься длительной установкой для каждого рабочего места. Аренда позволяет в любой момент изменять набор необходимого программного обеспечения, а также за считанные минуты добавлять и удалять новых пользователей.

Легальный софт повышает эффективность работы. Пиратские программы имеют измененный исходный код и ограниченный функционал, их нельзя обновить или обратиться в техподдержку для устранения неполадок. Аренда лицензий обеспечивает не только доступ к самым последним версиям приложений, но и их автоматическое бесплатное обновление, а значит постоянно появляющиеся новые возможности для вашего бизнеса.

30 BYN* **– это:**



Стоимость одной лицензии на пользователя
(5 ПК + 5 планшетов + 5 смартфонов)

Аренда лицензий делает бизнес мобильнее. Лицензионные программы можно использовать не только на установленном компьютере, но и из любой точки выхода в интернет.

Оплата только за используемые приложения и за необходимый период времени. Оплачиваются только реально используемые ресурсы, что сокращает расходы на инфраструктуру, электроэнергию и обслуживание.

Аренда лицензионного ПО гарантирует безопасность и сохранность данных, предоставляет возможность бесплатных обновлений без финансовых и репутационных рисков для компании. ▮

Если у вас остались вопросы, обращайтесь к **Евгению Андрейчуку**, руководителю направления по продаже решений Microsoft в странах Восточной Европы и Центральной Азии, по телефону +375(17)336-55-95, доб. 4474 или по e-mail: **Evgeniy.Andreychuk@softline.com.**

** - данная стоимость не является публичной офертой*

ПАРТНЕРУ ПО СЕКРЕТУ

Как готовые ISV-решения помогают бизнесу опережать проблемы

Топливо любого бизнеса — бесконечно успешное преодоление. И идея иметь под рукой каталог, который раскрыл на любой странице — и получил готовое, уже проверенное кем-то другим решение своей проблемы, настолько заманчивая, что удивительно, почему никто его еще не создал. Или создал? О том, что можно найти в каталоге ISV-решений Microsoft, рассказал Александр Затеса, руководитель направления развития бизнеса, Softline.

Александр Затеса, руководитель направления развития бизнеса, Softline

- Что такое ISV Partner-to-Partner?

- Мы, Softline, как глобальный, стратегический партнер Microsoft, движемся в соответствии с идеями, которые нам задает, в том числе, он. И Microsoft идет в облачные технологии, где каждый выбирает по подписке сервисы по своим потребностям. Одно из направлений развития этого решения — облачная платформа Azure, на которой уже сейчас десятки сервисов, они представляют различный спектр возможностей: начиная от управления виртуальными машинами, и заканчивая сервисами, которые умеют распознавать эмоции человека из видеоряда.

Большинство таких сервисов являются основой для создания конкретных бизнес-решений, исходя из потребностей заказчика или целой отрасли. ISV-партнеры (independent software vendor, независимый поставщик программного обеспечения — прим. SLD) — это компании, которые являются экспертами в какой-то конкретной предметной области, они разрабатывают подобные решения и размещают их в Azure. Несложно догадаться, что число таких решений еще больше, чем число сервисов Azure. Найти и выбрать нужное решение — не всегда простая задача, особенно если требуется решить нетиповую проблему.

Softline является таким Uber'ом в ИТ, который отбирает проверенные решения ISV-партнеров и внедряет их своим заказчикам, используя Azure в качестве платформы.

- Softline выступает в роли модератора или эксперта?

- Softline является признанным экспертом на ИТ рынке в России и за ее пределами. Заказчики нам доверяют решение бизнес-задач при помощи ИТ-инструментов, и мы постоянно растим собственную экспертизу в этом направлении.

Помимо собственных разработок и решений, внутри Softline начало работать направление ISV Partner-to-Partner, которое нацелено на расширение портфолио сервисов Softline.

Мне очень нравится модель «уберизации» в различных отраслях. И в данной истории Softline является таким Uber'ом в ИТ, который отбирает проверенные решения ISV-партнеров и внедряет их своим заказчикам, используя Azure в качестве платформы.

Нельзя быть экспертом во всех предметных областях, но в то же время надо оставаться доверенным экспертом для наших клиентов в стремительно меняющихся рыночных условиях. В этом нам и помогает partner-to-partner взаимодействие. При этом хотелось бы отметить, что в этой ситуации мы выступаем не как marketplace, который сводит покупателя с поставщиком, а являемся полноценным бизнес-партнером выполняя комплексный и законченный проект для заказчика.

- То есть ISV-направление — это портфель готовых решений?

- Да, который регулярно пополняется, потому что это направление на ИТ-рынке относительно новое, его только начинают развивать мировые вендоры. Регионы, где представлен Softline, — Латинская Америка, Россия, Азия стартовали в этом направлении примерно в одно и то же время, Россия, может быть, чуть попозже к этому пришла, но у каждого региона есть свой пул решений, учитывающий локальную специфику. И есть идея в дальнейшем не только расширять количество таких решений в каждом регионе, но и осуществлять обмен между регионами. Уже сейчас есть примеры, когда ISV-партнер, который был успешен в Индии, оказывается востребован на рынке в России. Таким образом мы помогаем нашим партнерам выйти на новые рынки. Аналогичный пример с решением по видеоаналитике из России: им заинтересовались наши коллеги из Латинской Америки и уже запланировали вывод этого решения на рынок. В этом и есть суть ISV Partner-to-Partner в Softline — помогать клиентам решать задачи и одновременно расширять горизонты своего бизнеса.

Все решения дорабатываются и идут от потребности заказчика. Понятно, что ISV-решения из западных стран достаточно дорогие для российского рынка, Латинской Америки и Индии. И большее предпочтение отдается местным разработчикам. У нас, например, очень хорошо отлажено взаимодействие со странами СНГ, как с местными партнерами, так и партнерами из России: передача и масштабирование решений на страны СНГ и обратно.

Более всего заинтересованы отрасли, которые испытывают явные предпосылки к цифровой трансформации и которым нужны новые решения, опять же, в рамках облачного подхода, когда не надо вливать огромное число денег, чтобы оцифровать проект, а достаточно просто пилотировать идею и в дальнейшем масштабировать наработки.

- В какой отрасли готовые решения уже зарекомендовали себя?

- Сложно сказать, официальной статистики пока нет. По опыту могу сказать, что более всего заинтересованы отрасли, которые испытывают явные предпосылки к цифровой трансформации и которым нужны новые решения, опять же, в рамках облачного подхода, когда не надо вливать огромное число денег, чтобы оцифровать проект, а достаточно просто пилотировать идею и в дальнейшем масштабировать наработки. Это ретейл, банки и госучреждения регионального, областного уровня, большой запрос есть с их стороны. При этом ретейл уже готов к различного рода решениям, банки накладывают свою специфику работы с коммерческой информацией, а федеральные и областные госучреждения заинтересованы в комплексных проектах.

- И если какое-то решение должно быть доработано для какого-то конкретного бизнеса, то это делается экспертами...

- ...Softline совместно с партнерами. На самом деле сложное конструирование касается больших и сложных проектов. Идея как раз в том, чтобы отбирать решения коробочные, универсальные и требующие минимальных доработок для того, чтобы сразу запустить их у заказчика и иметь возможность быстрого масштабирования и унифицированного подхода. Повторю: нельзя быть экспертом во всех областях. Понимать, как это решение развернуть и как его технически проинтегрировать с другими системами заказчиками, да, но для того, чтобы глубоко настроить уже само решение, требуется экспертиза партнера.

Мы видим постепенное изменение подходов наших заказчиков. Вначале это действительно было в духе «давайте что-то сделаем, непонятно для чего», но сейчас уже есть четкие стратегии у самих заказчиков, они понимают, зачем им это надо.

- Есть подозрение, что заказчику непросто разобраться и самому сформулировать, какой именно он хочет видеть результат и какое именно решение ему нужно. Как выбирается решение?

- Если говорить про Беларусь, то сама цифровизация и движение в сторону цифровой экономики, по факту, здесь только начинается и коснулось, в основном, крупных организаций. Поэтому, да, не все организации понимают, чего именно они хотят однако прогресс по сравнению с предыдущими годами очень заметный. Здесь, конечно, наш партнер Microsoft очень помогает, потому что они этот рынок развивают, и идея цифровой трансформации продвигается компанией уже несколько лет. Мы на правильной волне.

- Вы упоминали пример с видеоаналитикой, как и где может быть реализовано это решение?

- В России это одно из самых востребованных решений. Есть несколько основных сценариев. Первый — промышленная безопасность. Это решение, которое анализирует видео с камер наблюдения на предмет соблюдения техники безопасности: например, надета каска на рабочего или не надета, застегнута спецодежда или не застегнута, разрешено ли человеку ходить в опасную зону или нет, и т.д. В случае нарушений на пульт инженера приходит уведомление.

Второй сценарий — аналитика по работе торгового зала для ретейла: какие стенды и какие участки павильона являются самыми интересными, где люди больше всего останавливаются.

Дополнительно данный сценарий можно расширить для более глубокого анализа: подсчитывать число потенциальных покупателей, которые прошли мимо павильона, считать, сколько зашли в павильон и подошли к кассе. После интеграции с учетной системой в конечном итоге получается классическая воронка с цифрами конверсии: сколько прошли мимо магазина, сколько зашли и сколько купили.

Третий вариант — использование сервисов Azure для распознавания лиц. Таким образом возможно реализовать более сложные сценарии, например, сколько раз человек приходил в этот магазин перед покупкой. Либо это может быть применимо для точек обслуживания: когда распознается лицо посетителя и еще до подачи документов уже готовится к открытию карточка клиента с необходимой информацией.

Или возможен обратный сценарий (особенно актуален для финансовых организаций) — лицо посетителя распознается и проверяется в базе данных неблагонадежных заемщиков или мошенников.

- То есть в этом случае мы работаем с теми самыми большими данными, о которых все говорят?

- Не совсем, но очень похоже. Однако благодаря тому, что решения развернуты в облаке, обработка любых данных (в том числе и видео) происходит очень быстро и независимо от объема.

- Вопрос в другом, насколько сам бизнес готов анализировать эти большие данные. Собрать и передать их – полдела...

- Мы видим постепенное изменение подходов наших заказчиков. Вначале это действительно было в духе «давайте что-то сделаем, непонятно для чего», но сейчас уже есть четкие стратегии у самих заказчиков, они понимают зачем им это надо. Это наглядно происходит в ретейле. Они испытывают конкуренцию наиболее остро, поэтому увеличение маржи на полпроцента и создание базы более лояльных покупателей для ретейла — критически важная задача. И здесь как раз нужны решения эффективного использования этих огромных данных.

На недавней конференции как раз обсуждали пример, когда был запущен проект по сбору данных, их анализа. Однако за время самого проекта сменилось несколько руководителей, каждый из которых видел задачу по-своему, и проект заглох, потому что все данные собирались, но что с ними делать, до конца не решили.

- Как ведется работа по ISV-решению?

- Как правило, такие проекты проходят несколько классических стадий: идея – пилотирование – проверка идеи на стадии пилота – вывод в промышленную эксплуатацию и затем масштабирование либо на другие модули, либо на другие группы товаров, либо на всю Россию и за ее пределы — в зависимости от ситуации клиента.

- Сколько на это уходит в среднем времени, на внедрение одного проекта?

- Универсального времени нет, но в среднем от 3 до 12 месяцев.

- По результатам 3 месяцев уже можно сделать какой-то вывод?

- Можно сформировать ожидание: пойдет дальше проект или не пройдет. На самом деле это ничем не отличается от других сложных проектов. Просто идея в том, чтобы не создавать какие-то решения с нуля, так как это требует очень много временных и денежных инвестиций.

Это классический пример комплексного проекта. То есть, так как это связанно с цифровой трансформацией, это тянет за собой изменение бизнес-процессов внутри заказчика: изменение регламентов и процедур и, естественно, технической и технологической части, потому что, несмотря на то, что большая часть решений работает в облаке, их все равно необходимо свести с другими решениями, которые есть у клиента, провести интеграцию, дописать какие-то дополнительные модули... Это все требует проведения технических работ, изменений в инфраструктуре заказчика, обучения сотрудников и важный элемент — демонстрации, что система работает, и оценки ее результатов. Мы помогаем заказчику сделать оценку возврата инвестиций, чтобы клиент принял решение о возможности дальнейшего масштабирования проекта. Этот шаг зачастую упускается, но наша тесная работа с заказчиком позволяет уделять ему внимание.

- Все звучит как решения для крупного и очень крупного бизнеса. Есть ли что-то для стартапов и малого бизнеса?

- Есть решения, которые как раз предназначены для малого и среднего бизнеса, они исповедуют совершенно другую концепцию — они максимально «упакованы в коробки». Такие решения требуют минимальных доработок и заточены под какую-то очень специфичную функцию.

Например, роботизированный колл-центр в облаке или решение для автоматизации процессов продаж. Это все четко описанные задачи. Чем проще и понятнее решение, тем легче понять, для чего оно нужно, чем жестче рамки, тем меньше доработок потребуется. Это все делается потому что мы понимаем, что малому и среднему бизнесу нужно достаточно быстро внедрить недорогое решение.

Пока, в силу того, что направление не так давно стартовало в Softline, мы больше сфокусированы на средних и крупных проектах, но смотрим и отбираем более тщательно решения для малого бизнеса. С малым бизнесом нужно лучше ощущать рынок, и для нас это следующий шаг развития — создание портфолио для малого бизнеса, которое будет автоматизировано с нашей платформой по продаже облачных решений.

Мы помогаем заказчику сделать оценку возврата инвестиций, чтобы клиент принял решение о возможности дальнейшего масштабирования проекта. Этот шаг зачастую упускается, но наша тесная работа с заказчиком позволяет уделять ему внимание.

- Какие цели ставятся в этом направлении? Куда дальше оно будет развиваться?

- Направлений развития будет несколько. Первое — это продвижение ISV-решений с облачными решениями Microsoft и увеличение самого числа проектов для того, чтобы иметь портфолио для всех индустрий и закрыть их основные потребности. Это приведет к тому, что значительная часть тех, кто покупает себе облако Microsoft, будут получать себе ISV-решения в том или ином виде вместе с этим облаком. Второе направление — создание единого каталога из ISV-решений для всех географий присутствия Softline, чтобы наши заказчики имели доступ к лучшим решениям со всего мира, а наши партнеры могли выходить на новые рынки. ▮

Microsoft Teams
Командная работа на новом уровне

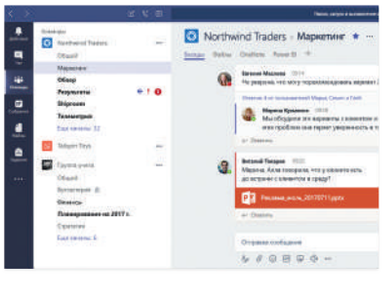
Microsoft Teams представляет собой сервис для упрощения командной работы в организации. С помощью этого инструмента можно создавать рабочие группы, общаться, проводить собрания и видеозвонки, обмениваться файлами и вести совместные проекты.

Евгений Андрейчук, руководитель направления по продаже решений Microsoft в странах Восточной Европы и Центральной Азии

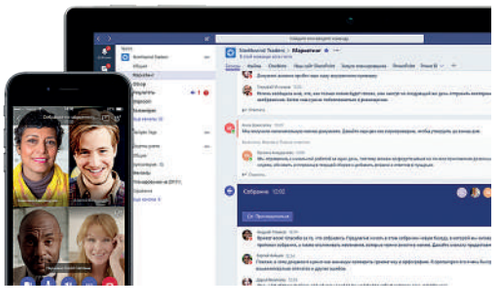
В есной исполнился год с момента появления общедоступной версии Microsoft Teams. За это время на платформу успели перейти свыше 300 тыс. компаний по всему миру. Клиентское приложение Microsoft Teams работает на Windows, Mac, iOS, Android и Windows Phone. В июле 2018 года компания сделала Teams бесплатным для всех пользователей. До этого сервис был доступен только подписчикам Business или Enterprise пакета приложений Office 365.

Огромным преимуществом решения является то, что оно изначально является частью пакета Office 365 и не требует отдельной интеграции. Пользоваться можно с любого устройства как через приложение, так и через веб-интерфейс. Весит приложение меньше, чем Skype для бизнеса, а позволяет значительно больше.

Что умеет Microsoft Teams?



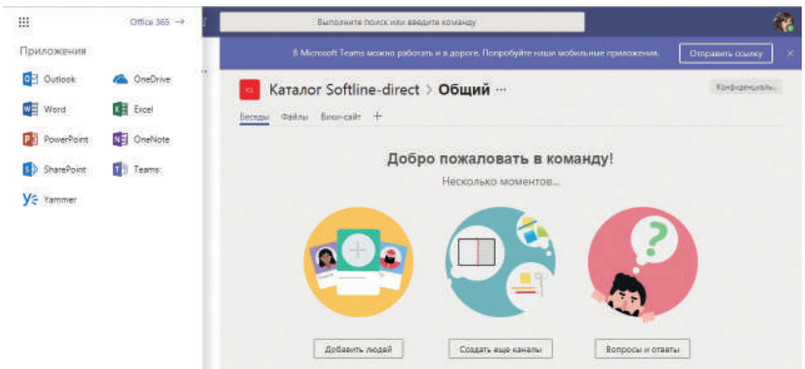
Групповой чат. Сохраняемый групповой или приватный чат с несколькими ветками бесед. Чат поддерживает обмен файлами и позволяет совместно редактировать контент.

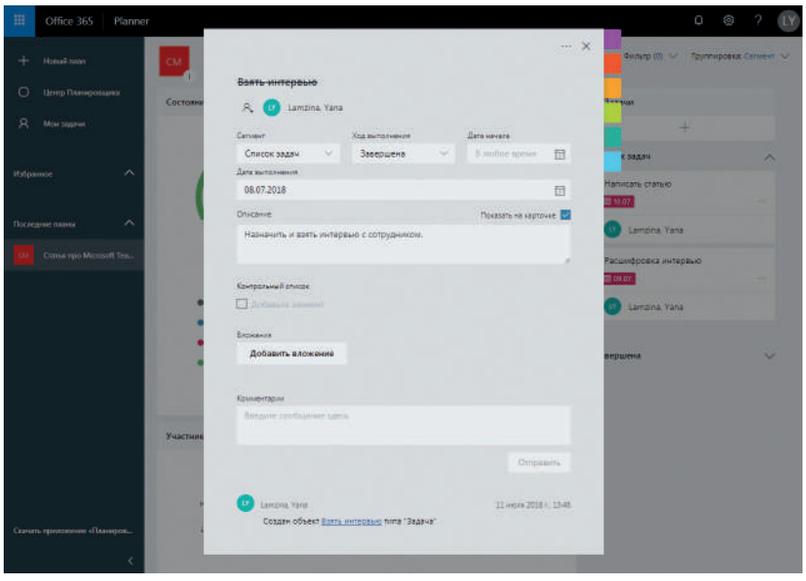


Собрания по сети. Microsoft Teams позволяет проводить собрания команды, осуществлять потоковые трансляции и подключаться к конференциям с помощью телефонного звонка. Для собраний Microsoft Teams можно использовать компьютер, мобильный телефон и даже систему Skype Room Systems с поддержкой HD-видео.

Встроенные приложения Office 365. Встроенные приложения Office 365 (Word, Excel, PowerPoint, OneNote, SharePoint и Power BI) позволяют открывать файлы непосредственно из интерфейса Teams для совместного редактирования файлов и работы с ними.

Подключение к проекту партнеров, клиентов и т.д. В случае, если к проекту нужно подключить кого-то вне организации, предусмотрено создание гостевого аккаунта.





Планировщик. Для того чтобы команда работала эффективней, в Teams есть специальный планировщик, позволяющий понять, на каком этапе находится та или иная задача. Здесь же можно посмотреть диаграммы выполнения проектов сразу по всей команде.

Облачное хранилище. При покупке Office 365 под команду Teams создается облачное пространство, в котором хранятся все необходимые файлы. Большим преимуществом является то, что информация остается в компании даже в случае увольнения сотрудника.

В сентябре 2018 года Microsoft представила несколько новых функций Teams, основанных на технологиях искусственного интеллекта:

- размытие фона во время видеозвонков;
- запись разговоров (пользователь в любое время может воспроизвести записанные аудио и видео);
- автоматические текстовые расшифровки записей.

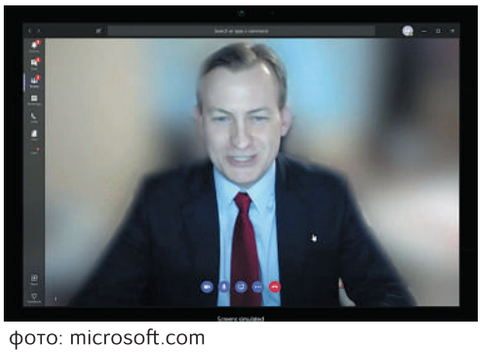


фото: microsoft.com

Кому будет полезен Microsoft Teams?

В первую очередь решение подходит всем заказчикам, которые работают в командах: разработчики, проектные организации.
Продукт также идеально подойдет для служб, оказывающих техническую поддержку. В случае возникновения инцидента, нужных специалистов можно подключить по фамилиям и быстро посмотреть, кого уже подключали к работе над подобными ситуациями.
В проекте использование Teams в качестве альтернативы офисной АТС.

Новая платформа **MaxPatrol SIEM** сертифицирована для использования в Республике Беларусь

MaxPatrol SIEM – первая в Беларуси SIEM-система, которая успешно прошла испытания на соответствие требованиям технического регламента Беларуси «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

С помощью этой платформы белорусские компании смогут:

- создавать системы защиты ограниченной к предоставлению информации;
- системы безопасности критически важных объектов информатизации;
- обеспечивать подлинность электронных документов в специализированных государственных информационных системах.

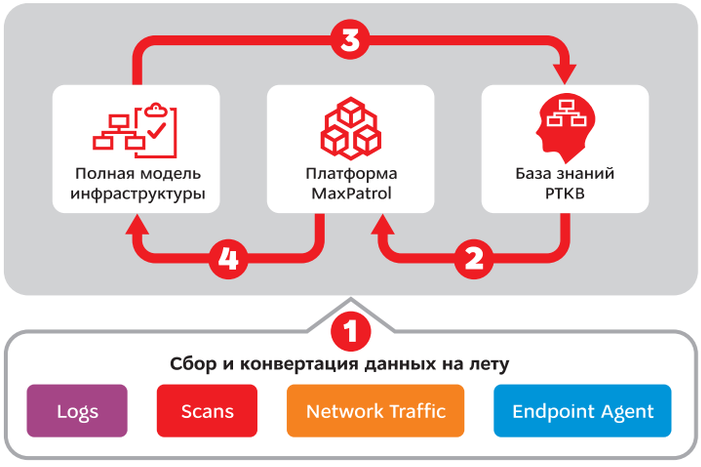
MaxPatrol SIEM поможет оперативно выявлять атаки и повысить уровень защищенности предприятий.

Преимущества и особенности системы MaxPatrol SIEM

Решение автоматически обновляется новыми событиями, результатами сканирований, данными сетевого трафика и агентов на конечных точках. Таким образом, правила корреляции могут оперировать не только отдельными IP-адресами или сетевыми именами, а также активами и их динамическими группами.

Преимущества MaxPatrol SIEM:

- Приоритезация активов, их динамических групп, уязвимостей с присвоением им метрик в рамках одной платформы.
- Открытый API для использования информации на любом этапе работы.
- Подключение актуальных источников в ходе реализации проектов без дополнительных затрат.
- Широкая функциональность сбора данных с поддержкой основных видов транспорта.
- Быстрая миграция.
- Гибкость модульной архитектуры, позволяющей построить любую конфигурацию системы.

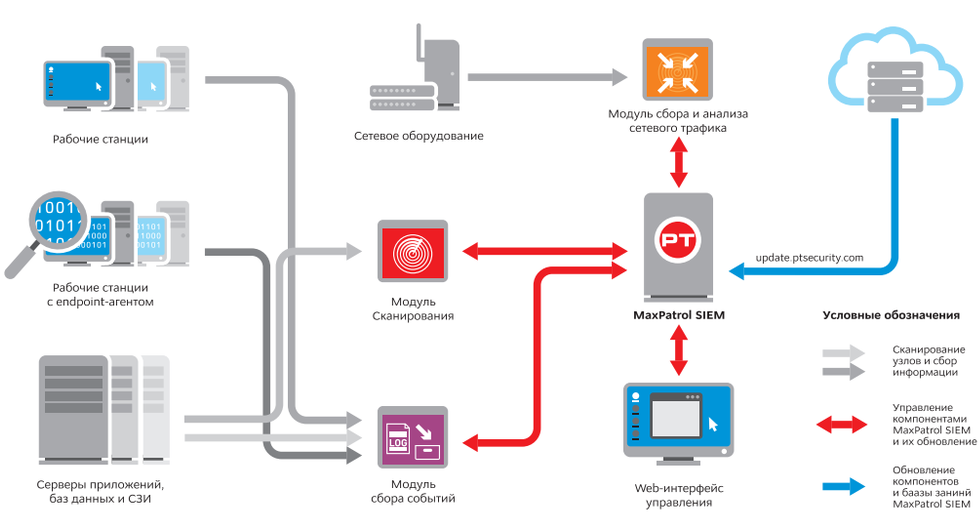


Этап 1. Информация поступает в систему и проходит нормализацию.

Этап 2. Проводится через ядро и модель инфраструктуры для привязки к существующим активам.

Этап 3. Сопоставляется с данными базы знаний Positive Technologies Knowledge Base (PT KB).

Этап 4. Проводится через коррелятор с учетом всех данных, полученных на предыдущих этапах.



MaxPatrol SIEM обрабатывает события ИБ, собирает данные об активах и автоматически выявляет угрозы, в том числе ранее неизвестные. Служба ИБ моментально получает уведомления об инцидентах, что помогает оперативно отреагировать на атаку, провести детальное расследование и предотвратить репутационный и финансовый ущерб. ▮

Кибербезопасность крупного бизнеса

KASPERSKY lab

Кибербезопасность облачных сред

Надежная защита гибридной облачной инфраструктуры

- Динамическая интеллектуальная защита для гибридного облака
- Минимальное влияние на производительность
- Многоуровневая безопасность частного облака
- Расширенная защита публичных облаков, включая Amazon Web Services и Microsoft Azure
- Удобное и гибкое управление из единой консоли

www.kaspersky.ru/enterprise

#ИстиннаяБезопасность

softline®

Ваш надёжный поставщик
ИТ-сервисов и решений

Получить консультацию по продуктам «Лаборатории Касперского» вы можете у эксперта Softline:

Виталий Шавель,
+375 17 336-55-95 доб. 4440
Vitaliy.Shavel@softline.com

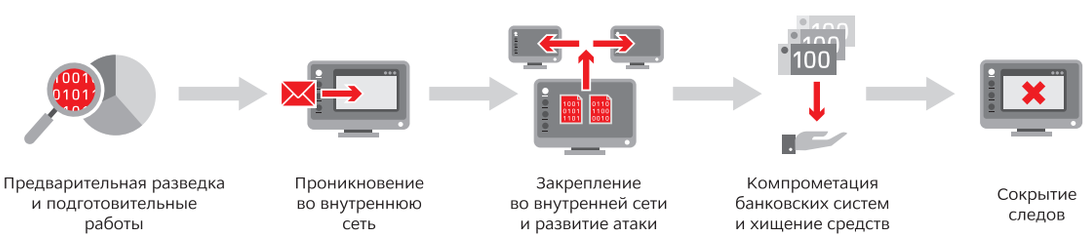
Как грабят банки сегодня?

В последние несколько лет в СМИ регулярно появляются заголовки о новых ограблениях банков. Как хакерам удается обойти существующие системы защиты, какие недостатки в механизмах безопасности позволяют им прочно закрепиться в инфраструктуре банка? Представляем вам отчет, основанный на результатах работ по анализу защищенности информационных систем отдельных банков за последние три года.

Типовая схема атаки

Выбор цели злоумышленника во многом обусловлен технической подготовкой, имеющимися инструментами и знаниями о внутренних процессах банка, которыми располагают преступники. Они действуют по довольно простым сценариям, состоящим из пяти основных этапов, которые представлены на схеме.

Основные этапы атаки



Этап 1. Разведка и подготовка

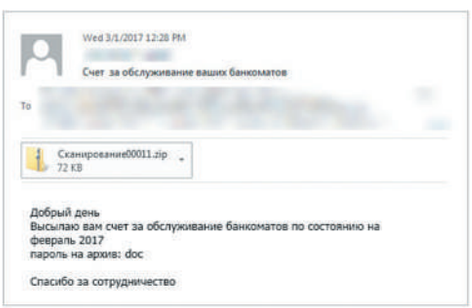
Первый этап достаточно длительный и трудоемкий. Перед злоумышленниками стоит задача собрать как можно больше информации о банке, которая поможет преодолеть системы защиты. Поскольку сканирование внешних ресурсов может быть выявлено системами защиты, то преступники прибегают к пассивным методам получения информации, например, для выявления доменных имен и адресов, принадлежащих банку. Для разведки также активно привлекаются недобросовестные сотрудники банков, готовые за вознаграждение поделиться информацией. Множество объявлений об этом легко найти на соответствующих форумах в интернете.

Этап 2. Проникновение во внутреннюю сеть

После всестороннего изучения жертвы и подготовки к атаке злоумышленники переходят в наступление.

Крупные и средние банки сегодня уделяют достаточно много внимания защите своего сетевого периметра, поэтому организовать атаку на серверы или веб-приложения не только сложно, но и рискованно, поскольку велика вероятность обнаружить себя.

Наиболее распространенным и эффективным методом проникновения в инфраструктуру банка является фишинговая рассылка электронных писем в адрес сотрудников банка.



Фишинговое письмо, отправленное группировкой Cobalt

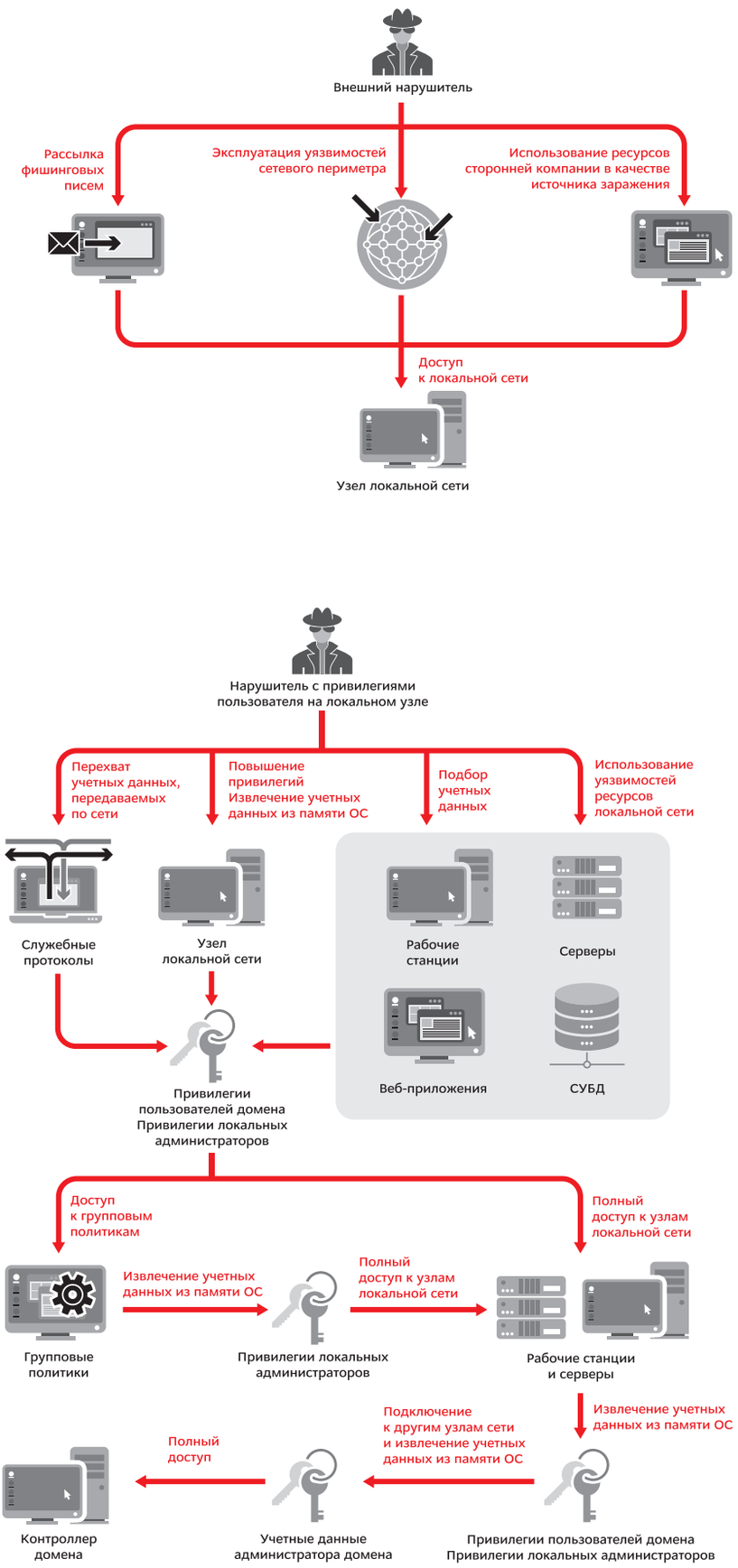
Другой вариант первичного распространения вредоносного ПО — взлом сторонних компаний, которые не столь серьезно относятся к защите своих ресурсов, и заражение сайтов, часто посещаемых сотрудниками целевого банка.

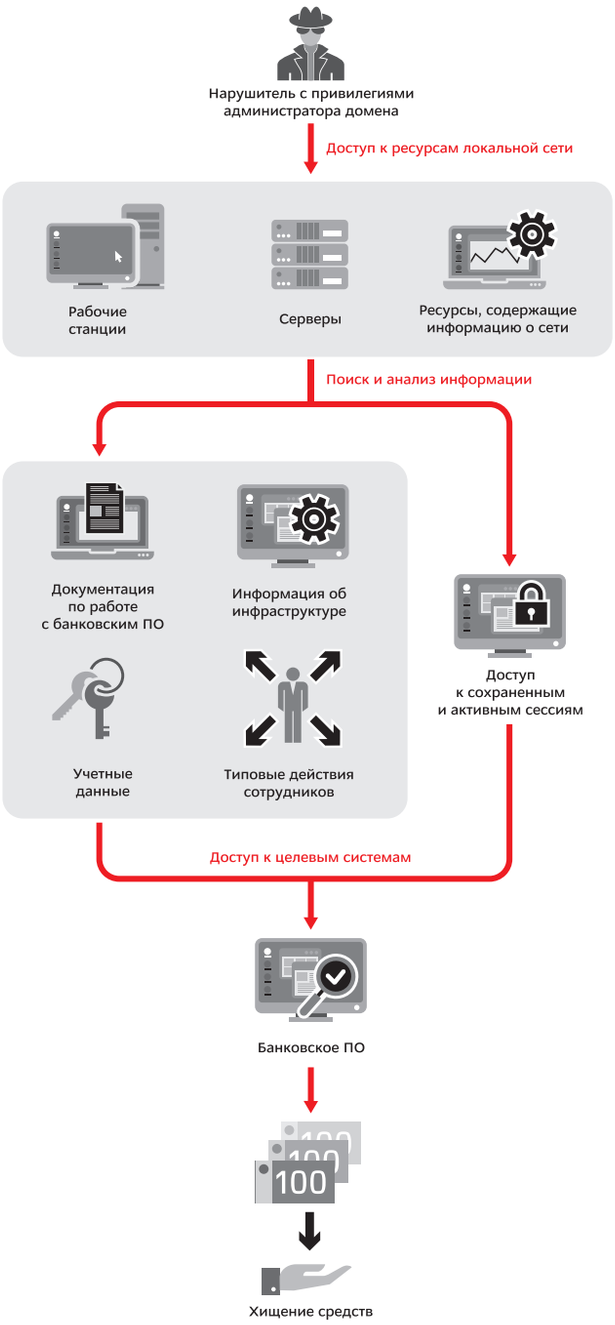
Этап 3. Развитие атаки и закрепление в сети

После того, как преступники получают доступ к локальной сети банка, им необходимо получить привилегии локального администратора на компьютерах сотрудников и серверах.

В этом им помогают следующие распространенные уязвимости:

- использование устаревших версий ПО и отсутствие актуальных обновлений безопасности для ОС;
- множественные ошибки конфигурации (в том числе избыточные привилегии пользователей и ПО, а также установка паролей локальных администраторов через групповые политики);
- использование словарных паролей привилегированными пользователями;
- отсутствие двухфакторной аутентификации для доступа к критически важным системам.





После получения максимальных привилегий в ОС на узле преступники получают из памяти ОС учетные данные всех пользователей, подключавшихся к ней (идентификаторы, пароли или хеш-суммы паролей). Эти данные используются для подключения к другим компьютерам в сети. Перемещение между узлами обычно осуществляется посредством легитимного ПО и встроенных функций ОС (например, PsExec или RAdmin), то есть с помощью тех средств, которыми ежедневно пользуются администраторы и которые не должны вызвать подозрений.

Чтобы скрыть свое присутствие, злоумышленники часто используют бестелесный вредоносный код, который выполняется только в оперативной памяти, а для сохранения канала удаленного управления после перезагрузки компьютера добавляют ВПО в автозагрузку ОС.

Этап 4. Компрометация банковских систем и хищение денег

Закрепившись в сети, преступники должны понять, на каких узлах находятся искомые банковские системы и как будет удобнее получить к ним доступ. Преступники исследуют рабочие станции пользователей в поисках файлов, указывающих на то, что с данной рабочей станции осуществляется работа.

Этап 5. Сокрытие следов

С целью затруднить расследование инцидента преступники принимают меры для уничтожения следов своего пребывания в системе. Несмотря на то, что злоумышленники переключаются на использование скриптов, выполняющихся в оперативной памяти, в системе остаются признаки их присутствия: записи в журналах событий, изменения в реестре и другие зацепки. Поэтому неудивительно, что некоторые нарушители предпочитают обезопасить себя, насколько это возможно, и не просто удаляют отдельные следы, а полностью выводят из строя узлы сети, стирая загрузочные записи и таблицы разделов жестких дисков.

Уязвимости при проведении тестов на проникновение

В зависимости от исходного уровня привилегий нарушителя различают внешнее тестирование, в рамках которого проверяется возможность преодоления сетевого периметра, и внутреннее, целью которого является получение полного контроля над инфраструктурой или доступ к критически важным системам.

Для этого исследования мы выбрали двенадцать наиболее информативных проектов, выполненных нами в банках за последние три года, в ходе

Контактные данные
Александр Дубина, руководитель направления информационной безопасности
Тел.: +375(17)336-55-95, доб. 4496
E-mail: Alexander.Dubina@softline.com

которых накладывались минимальные ограничения на действия экспертов.

На сегодняшний день банки выстроили достаточно эффективные барьеры для защиты от внешних атак, однако основная проблема состоит в том, что они не готовы противостоять нарушителю во внутренней сети.

Зная это, злоумышленники легко обходят системы защиты сетевого периметра с помощью простого и эффективного метода — фишинга, который доставляет вредоносное ПО в корпоративную сеть. Преступники внимательно следят за публикацией новых уязвимостей и быстро модифицируют свои инструменты. Например, в 2017 году хакеры из группировки Cobalt использовали уязвимости в Microsoft Office CVE-2017-0199 и CVE-2017-11882 в расчете на то, что банки не успели установить соответствующие обновления безопасности.

Внутри сети злоумышленники свободно перемещаются незамеченными с помощью известных уязвимостей и легитимного ПО, которое не вызывает подозрений у администраторов. Пользуясь недостатками защиты корпоративной сети, злоумышленники за короткое время получают полный контроль над всей инфраструктурой банка.

Крайне важно своевременно получать уведомления систем защиты и незамедлительно реагировать на них. Для этого необходим постоянный мониторинг событий безопасности силами внутреннего или внешнего подразделения SOC, а также наличие SIEM-решений, которые могут существенно облегчить и повысить эффективность обработки событий информационной безопасности.

Если вы не уверены в максимально надежной защите ваших ресурсов, обратитесь к специалистам Softline и получите аудит безопасности вашей сети. ▮

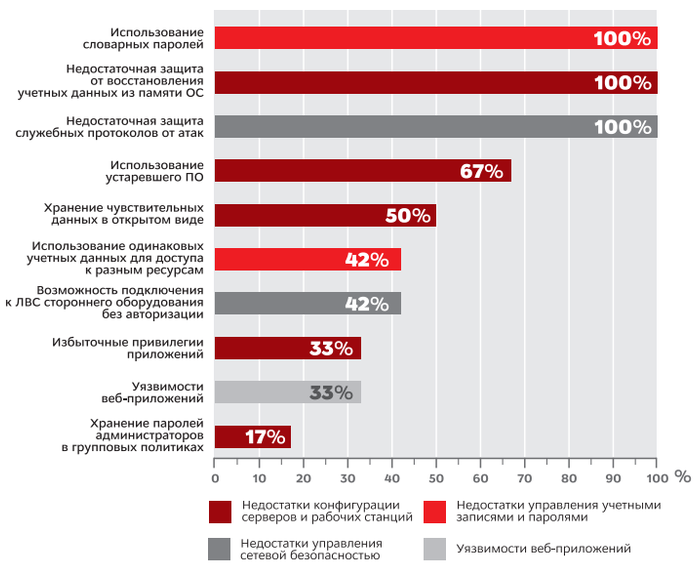
Источник данных: исследования Positive Technologies – одного из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений.

Уязвимости сетевого периметра

Десятка самых распространенных уязвимостей на сетевом периметре (доля банков)

Уязвимости внутренней сети

Наиболее распространенные уязвимости во внутренней сети (доля банков)



Уязвимости, использовавшиеся для доступа к банковскому ПО

Check Point.
Комплексная защита сетей и данных

Быстрый рост вредоносного ПО, растущее мастерство хакеров и появление новых неизвестных угроз «нулевого дня» требуют применения иного подхода к защите корпоративных сетей и данных. Комплексные решения Check Point являются сегодня одним из наиболее популярных направлений в области защиты структурных сегментов корпоративной сети. О ключевых компонентах и преимуществах этих решений рассказал менеджер по продажам решений информационной безопасности Softline **Юрий Богуш**.

— Расскажите, что такое комплекс решений Check Point, какие именно продукты он включает и для чего предназначен?

— Определяя безопасность организации как непрерывный бизнес-процесс, Check Point предоставляет решения для защиты всех структурных сегментов корпоративной сети.

Ключевыми компонентами, составляющими решение Check Point по защите информационной системы финансовой организации, являются:

- Защита корпоративной сети, включающая защиту периметра и региональных офисов, обеспечение устойчивости при атаках класса DDoS, сегментацию и защиту центров обработки данных (ЦОД), а также обеспечение соответствия требованиям PCI DSS.
- Защита рабочих станций и мобильных устройств, включая решения по обеспечению безопасности данных и документов.
- Система управления с единой консолью для всех компонентов системы ИБ.
- Обеспечение соответствия требованиям регуляторов.

— Почему именно Check Point? В чем заключаются его преимущества, и в чем шлюз безопасности Check Point превосходит своих конкурентов?

— Основным преимуществом продукта является система централизованного управления политикой ИТ-безопасности с единой консоли администратора. Вне зависимости от размера сети управление всеми шлюзами безопасности происходит из единой точки. При этом администратор прописывает политику безопасности без обязательной привязки к конкретным шлюзам.

Это достигается за счет того, что SmartCenter автоматически генерирует и рассылает политики на шлюзы безопасности, исходя из данных об интерфейсах и топологии сетей, находящихся за каждым из них. А топологию определяет администратор в свойствах шлюза безопасности. Наличие единой базы сетевых объектов предприятия и единой целостной политики безопасности повышает прозрачность ИТ-системы, уменьшает количество ошибок, вызванных человеческим фактором.

Наличие централизованного управления имеет еще одно преимущество – все события безопасности (логи) собираются и обрабатываются централизованно.

Юрий Богуш, менеджер по продажам решений информационной безопасности Softline.

— В каких случаях следует предпочесть Check Point?

— При необходимости создания в организации системы защиты любой ИТ-системы необходимо использовать комплекс средств защиты информации (СЗИ), состоящий из межсетево-

го экрана (firewall), системы предупреждения/предотвращения вторжений (IDS/IPS), средств криптографической защиты передаваемых данных, систем защищенного доступа к данным, средств строгой аутентификации. Продукты Check Point лучше всего подходят в качестве основы такого комплекса СЗИ. Эффективность системы информационной безопасности достигается за счет возможности гибко выбирать функционал продуктов Check Point благодаря использованию «программных блейдов».

На протяжении многих лет Check Point постоянно находится на лидирующих позициях среди межсетевых экранов корпоративного уровня. Этот факт подтверждается аналитической компанией Gartner и иллюстрируется знаменитым «магическим квадрантом». Также доказательством преимуществ Check Point перед конкурентами является факт использования продукции вендора всеми компаниями списка Fortune 100 и 98% компаний списка Fortune 500.

— Какие сложности могут возникнуть в процессе внедрения продукта или его эксплуатации?

— Систему информационной безопасности нужно постоянно проверять и улучшать. К сожалению, многие компании после внедрения такой системы уверены, что на этом проблема защиты от киберпреступников решена раз и навсегда. Но они не учитывают, что постоянно появляются новые опасные киберугрозы.

Персонал компании необходимо обучать основам информационной безопасности. Согласно исследованиям, большинство инцидентов, связанных с ИБ, вызваны человеческим фактором, причем к значительной части таких случаев привели действия рядовых пользователей.

Одна из важных проблем обеспечения корпоративной информационной безопасности — точечные решения. Например, сеть, рабочие станции, файловый сервер и почтовый сервер защищены по отдельности, причем зачастую продуктами разных производителей.

Существует также проблема развития угроз во времени. У многих компаний нет четкого плана действий в случае появления вредоносного ПО, а хаотичные реакции наподобие отключения почтовых серверов могут привести к намного более тяжелым последствиям, нежели влияние вируса. При этом ни начальник службы безопасности, ни производитель средств защиты не может заранее написать для администраторов никаких инструкций, так как заранее неизвестно, что за вирус появится в будущем. Регламентированы должны быть не действия, а каналы получения информации. В случае большой компании с распределенной сетью также должна существовать схема оповещения всех администраторов.

— Есть ли какие-то вариации продукта? Выпускается ли он в разных модификациях?

— Решения Check Point по сетевой безопасности строятся на основе архитектуры программных блейдов (Check Point Software Blades) и могут устанавливаться как на устройства Check Point, виртуальные платформы, так и на открытые совместимые серверы (IBM, HP, Dell и др.). Check Point Software Blade (программный блейд) – это модульный независимый функционал, и заказчик может выбирать именно те возможности, которые ему нужны. На каждом аппаратном или виртуальном устройстве может быть запущен любой из программных блейдов, определенный набор блейдов, или же все блейды вместе.

Варианты реализации:

- Виртуальные шлюзы безопасности.
- Программное обеспечение, установленное на серверы.
- Программно-аппаратные комплексы Check Point.

— Расскажите об особенностях лицензирования Check Point.

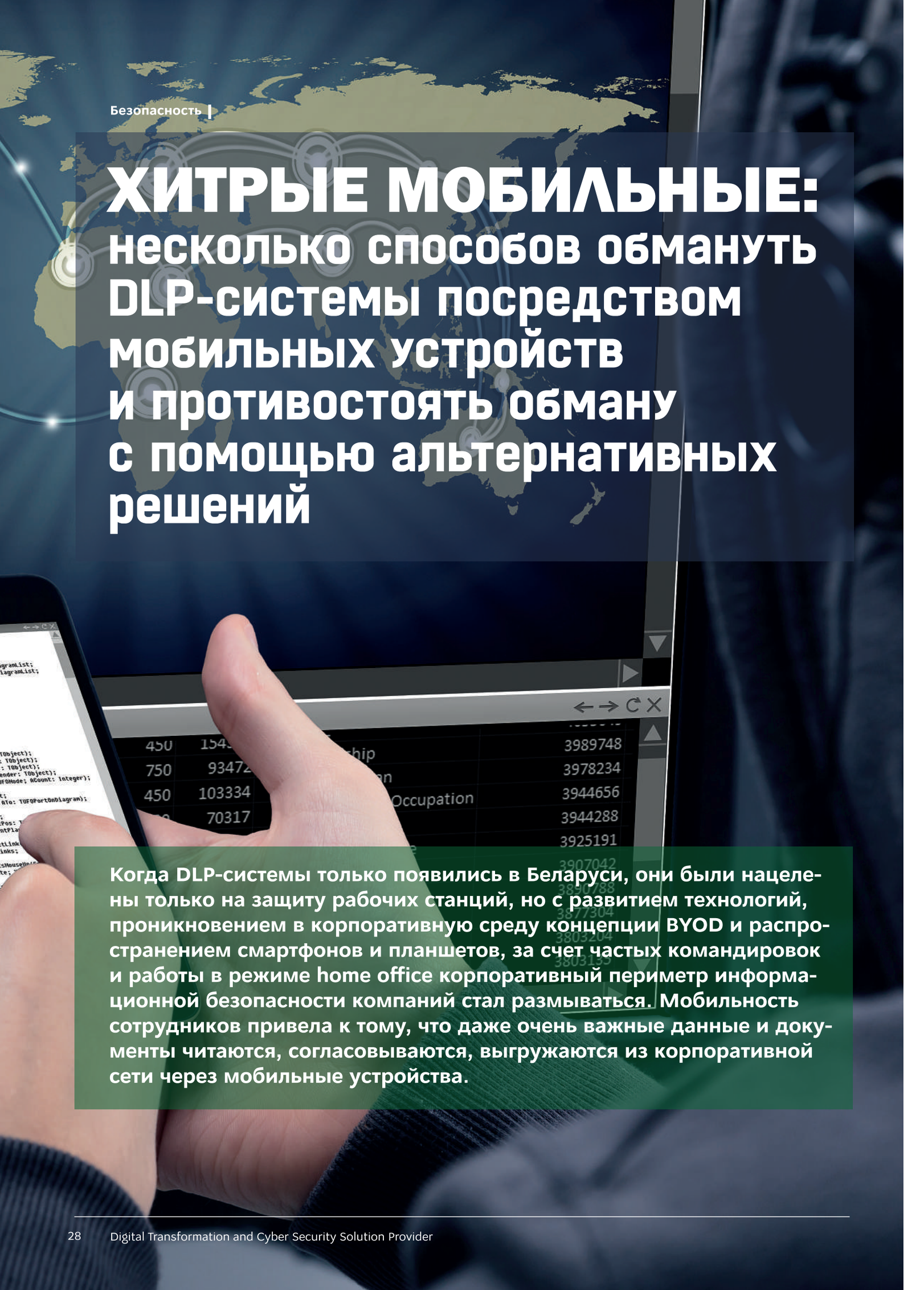
— Существует два варианта поставки шлюза безопасности:

Лицензия Next Generation Threat Prevention (NGTP). Базовый пакет, включающий все основные механизмы защиты: Firewall, IPS, Application Control, URL Filtering, Antivirus, Anti-Bot, Anti-Spam & Email Security.

Лицензия Next Generation Threat Prevention & SandBlast (NGTX). Расширенный пакет, необходимый для обеспечения защиты от неизвестных ранее угроз. В этом случае лицензия NGTP должна включать модули (blade) Threat Extraction и Threat Emulation, необходимые для интеграции с песочницей SandBlast. ▮

Остались вопросы? Обращайтесь к менеджеру по продажам решений информационной безопасности Softline **Юрию Богушу** по телефонам +375 (17) 336-55-95 доб. 4482 | +375 (29) 326-63-92 или e-mail **Yuriy.Bogush@softline.com**.

ХИТРЫЕ МОБИЛЬНЫЕ: несколько способов обмануть DLP-системы посредством мобильных устройств и противостоять обману с помощью альтернативных решений



Когда DLP-системы только появились в Беларуси, они были нацелены только на защиту рабочих станций, но с развитием технологий, проникновением в корпоративную среду концепции BYOD и распространением смартфонов и планшетов, за счет частых командировок и работы в режиме home office корпоративный периметр информационной безопасности компаний стал размываться. Мобильность сотрудников привела к тому, что даже очень важные данные и документы читаются, согласовываются, выгружаются из корпоративной сети через мобильные устройства.

Сценарии угроз

Утечка данных через веб-клиент корпоративной почты OWA (Outlook Web Access)

Пример ситуации. Несмотря на наличие почтовых клиентов для Microsoft Outlook практически для всех современных платформ, пользователи зачастую предпочитают обмениваться электронной почтой через OWA. Именно возможность работать с почтой через браузер становится «тонким местом» для DLP-систем. Выглядит это так: сотрудник создает черновик письма на рабочем ПК, прикладывает к нему какой-либо конфиденциальный документ, сохраняет черновик в почте, приезжает домой, подключается через OWA и выгружает конфиденциальный документ на свой ПК (ноутбук, мобильное устройство). Утечку служба безопасности не проконтролирует, поскольку личный ПК – это сугубо персональное устройство, на которое DLP-агент не установлен.

РЕШЕНИЕ: MDM + DLP + VPN (опционально)

Для этого как раз и применяются MDM-решения, закрывающие OWA. В периметре компании разворачивается MDM. Вся работа с корпоративными данными ведется через интерфейс MDM решения: электронная почта, работа с корпоративной сетью, календарем, документами и т.д. Благодаря этому закрывается канал потенциальной утечки OWA. Важно, что MDM выступает в роли своего рода песочницы, которая разграничивает личную и корпоративную среду. Контроль ведется только над корпоративной средой.

Пример ситуации: порой злоумышленник может иметь доступ к календарю жертвы. Сотрудник прикрепляет вложение, содержащее конфиденциальную информацию, ко встрече в календаре. Очень часто злоумышленники имеют доступ к календарям сотрудников и к вложенным в них документам.

РЕШЕНИЕ: MDM + DLP

В случае скачивания злоумышленником вложения DLP-система уведомит службу безопасности. С помощью интеграции MDM и DLP контролируется не только почта и скачивание документов, но также контролируются вложения в календаре. Если злоумышленник скачивает вложение из календаря, DLP-система должна это проконтролировать. Сотрудник, работая с MDM удаленно, может подключаться к корпоративной среде и выгружать какие-то конфиденциальные документы. Соответственно, то, что он выкачивает на локальную память своего устройства, также необходимо контролировать. Данная интеграция это позволяет.

Пример ситуации: утечка данных через скачивание информации с корпоративных ресурсов на мобильное устройство. Зачастую сотрудникам предоставляется доступ к корпоративным ресурсам с мобильных устройств – возможность пользоваться почтой, порталом и т.д. Сотрудник скачивает документ с файлового сервера, либо с SharePoint на мобильное устройство и дальше использует его в своих целях.

РЕШЕНИЕ: MDM + DLP + VPN

Теневая копия скаченного документа отправляется в DLP-систему на анализ конфиденциальной информации. Существует жесткая необходимость контролировать, что сотрудник скачивает. Конечно, можно настроить права доступа к папкам и файлам, но зачастую это не работает.

По передаче теневых копий с мобильного устройства на сервер DLP-системы очень часто применяют решения VPN, если необходимо шифрование открытого канала, в том числе по ГОСТУ.

Утечки визуализируются в консоли управления DLP. Мы видим канал утечки — MDM, контакты, объект утечки и т.п., что позволяет проводить расследования не только с рабочей станции. При этом есть возможность настраивать правила по времени контроля (к примеру, рабочее время 9-00 – 18-00)

СИНГАПУР

глобальный лидер кибербезопасности

На сегодняшний день Сингапур защищает свое киберпространство успешнее всех в мире. Узнаем, какие проблемы остаются нерешенными, и как организована борьба с киберпреступностью в прогрессивном городе-государстве.

Сингапур обладает самым высоким уровнем кибербезопасности в мире, он занимает первую строчку в рейтинге ООН (Global Cybersecurity Index 2017). Международные эксперты заключили, что система защиты от хакерских атак в этой стране практически совершенная. Эта заслуга принадлежит правительству Сингапура, которое с 2005 г. последовательно реализует план развития ИТ-инфраструктуры в рамках государственной инициативы «Умная нация». Проект буквально превратил страну в открытое поле для тестирования цифровых решений: каждый дом имеет доступ к высокоскоростному интернету, активно реализуются телемедицинские проекты, повсюду «умные автомобили», на каждых двух жителей государства приходится по три смартфона, а в любой точке острова действует бесплатный Wi-Fi (по материалам издательства Engadget).

В торжественной речи на открытии Международной недели кибербезопасности в Сингапуре в 2016 году премьер-министр Ли Сянь Лун заявил: «Сингапур претендует на звание «Умного государства», но, чтобы ему соответствовать, мы прежде всего должны обеспечить высокий уровень кибербезопасности». Такой подход весьма оправдан, ведь чем прочнее в нашу жизнь входят достижения информационных технологий, тем более зависимыми от них мы становимся, а это делает нас уязвимыми. Согласно данным «Лаборатории Касперского», в том же году, когда Сингапур поднялся на первое место в индексе сетевой готовности (NRI), он занял и седьмое место в мире по количеству нацеленных на него хакерских атак.

Для решения задач в данной сфере был разработан «Национальный генеральный план по обеспечению кибербезопасности 2018», к реализации которого приступили в 2013 г.

Цель первого пункта заключается в укреплении кибербезопасности критически важных секторов Сингапура: правительства, инфокоммуникаций, энергоснабжения, наземного и морского транспорта, гражданской авиации, водоснабжения, банковского и финансового секторов, а также сектора здравоохранения. К действиям по обеспечению кибербезопасности относится организация эффективных согласованных действий в ответ на кибератаки, а функция развития промышленности заключается в создании надежной экосистемы, укомплектованной надлежащими кадрами для реагирования на кибератаки, и их ослабление. И наконец, деятельность агентства в области информационно-просветительской деятельности, направлена на развитие отношений с местными и глобальными отраслями и лидерами общественного мнения через мероприятия по информированию общественности, повышающие осведомленность в сфере кибербезопасности.

Проблемы

Несмотря на то, что Сингапур является одной из стран Азиатско-Тихоокеанского региона, обладающей самой передовой ИКТ, он сталкивается со множеством тех же самых проблем в сфере кибербезопасности, что и другие страны. К ним относятся и объекты критически важной инфраструктуры: электросети, водоочистительные установки, заводы, которые проектировались еще во времена, когда о кибератаках ничего не слышали, и нежелание крупных корпораций внедрять единые стандарты, так как они уничтожают конкурентные преимущества. Например, правительство США так и не смогло убедить Apple изменить iOS таким образом, чтобы предоставить сотрудникам правоохранительных органов доступ к доказательствам по делу о теракте в Сан-Бернардино, которые, по их мнению, хранятся в смартфоне. Сказывается и отсутствие международного руководства, потому что какой бы ни была совершенной система защиты одного государства, борьба с киберпреступностью требует взаимосвязанных усилий всего мира.

Заместитель генерального директора CSA, Тео Чин Хок на конференции CyberTech Asia 2016 отметил, что особую опасность представляют атаки, подобные WannaCry, так как их тактики шифрования становятся все более изощренными, а также в 2018 году возможен рост банковских кибератак, спонсируемых государством.

По мере роста числа проблем в области кибербезопасности, правительство приняло решение о необходимости создания «Агентства по кибербезопасности» (CSA), оно находится при канцелярии премьер-министра и управляется Министерством связи и информации. В его основные обязанности входит:

- **разработка стратегии и политики,**
- **действия по обеспечению кибербезопасности,**
- **развитие промышленности,**
- **информационно-просветительская деятельность.**

Как их решают

Согласно отчету Cybersecurity Ventures, к 2021 году в Сингапуре будет создано **3,5 миллиона** незанятых рабочих мест в сфере кибербезопасности.

Надежная отказоустойчивая инфраструктура

С момента своего создания CSA тесно сотрудничает с регулирующими органами критической информационной инфраструктуры, чтобы понять проблемы, с которыми они сталкиваются, и принимать меры для управления этими рисками. Агентство также проводит учения Cyber Star Exercise, в ходе которых устраиваются симуляции киберпреступной активности, для того чтобы проверить готовность компаний к экстренному реагированию на внезапные атаки.

Для повышения общей эффективности мониторинга безопасности государственного сектора был создан Центр кибернаблюдения, использующий самые современные аналитические инструменты для обработки больших объемов данных и предоставления государственным учреждениям подробного анализа киберугроз и рекомендаций о том, как принимать своевременные превентивные меры.

Квалифицированные кадры

Серьезной проблемой Сингапура является нехватка квалифицированных кадров. Согласно отчету Cybersecurity Ventures, к 2021 году в стране будет создано 3,5 миллиона незанятых рабочих мест в сфере кибербезопасности.

Чтобы повышать компетентность граждан, CSA учредила Академию для обучения специалистов по кибербезопасности. Она сотрудничает с ведущими поставщиками услуг в области профессиональной подготовки, ее первым партнером стала американская компания FireEye, которая известна подготовкой аналитиков вредоносных программ для некоторых самых престижных правительственных учреждений и компаний по всему миру.

Компания Singtel основала Институт кибербезопасности для создания новых продуктов и услуг в сфере защиты данных с помощью ультрасовременного комплекса, который имитирует реальные среды ИКТ. Также агентство CSA сотрудничало с Министерством информации, связи и искусства Сингапура с целью увеличения стипендий на специальностях, связанных с кибербезопасностью, в рамках национальной стипендиальной программы, для того чтобы побудить лучших студентов получить диплом в сфере кибербезопасности.

Кроме того, Правительство Сингапура четко осознает, что стартапы — это один из ключевых источников инновационных решений, поэтому CSA стремится расширять конвейер новых бизнес-проектов по кибербезопасности.

Государственно-частное партнерство

В соответствии с Национальным генеральным планом по обеспечению кибербезопасности 2018 г. правительство Сингапура запустило информационно-просветительскую кампанию, направленную на повышение информированности бизнеса и общественности в вопросах кибербезопасности. Проводятся национальные соревнования для молодых специалистов, тренировочные мероприятия для банковского и финансового сектора, CSA также сотрудничает с Комиссией по защите персональных данных для подготовки руководителей малых и средних предприятий к защите данных своей компании, а также с полицией Сингапура, телекоммуникационными компаниями и провайдерами интернет-услуг.

Для того чтобы развивать функции кибербезопасности, необходимо перенимать положительный опыт. Для этого были подписаны протоко-

лы о взаимопонимании (Memorandum of Understanding) с компаниями Singtel, Check Point Software Technologies и FireEye для расширения сотрудничества и обмена передовыми практиками.

Международное сотрудничество

Заместитель генерального директора CSA, г-н Teo справедливо заметил: «CSA не может делать все самостоятельно». Киберугрозы — это общие враги, для борьбы с которыми необходимо международное доверие и сотрудничество, а также общие нормы и правила. Киберпростарнство должно быть безопасным для всех, и начало этому положено – правительство Сингапура подписало протоколы о взаимопонимании с Францией, Великобританией, Индией и Нидерландами. Они предусматривают сотрудничество как в сфере научных исследований, так и цифровых разработок, мероприятий по обмену опытом в сфере кибербезопасности.

Нестандартные методы

Помимо всего выше упомянутого сингапурские государственные органы, ответственные за кибербезопасность, иногда идут на смелые решения и эксперименты. К примеру, для того чтобы обеспечить сохранность важной государственной информации в компьютерах чиновников, им просто не предоставляют доступ к интернету на рабочем месте. Конечно, служащие могут обмениваться информацией в пределах локальной сети, а для отдельных лиц выделяются специальные интернет-терминалы, но в таких условиях вероятность утечки данных стремится к нулю. Несмотря на то, что Сингапур одна из самых технологически продвинутых стран мира, даже такие методы имеют место быть.

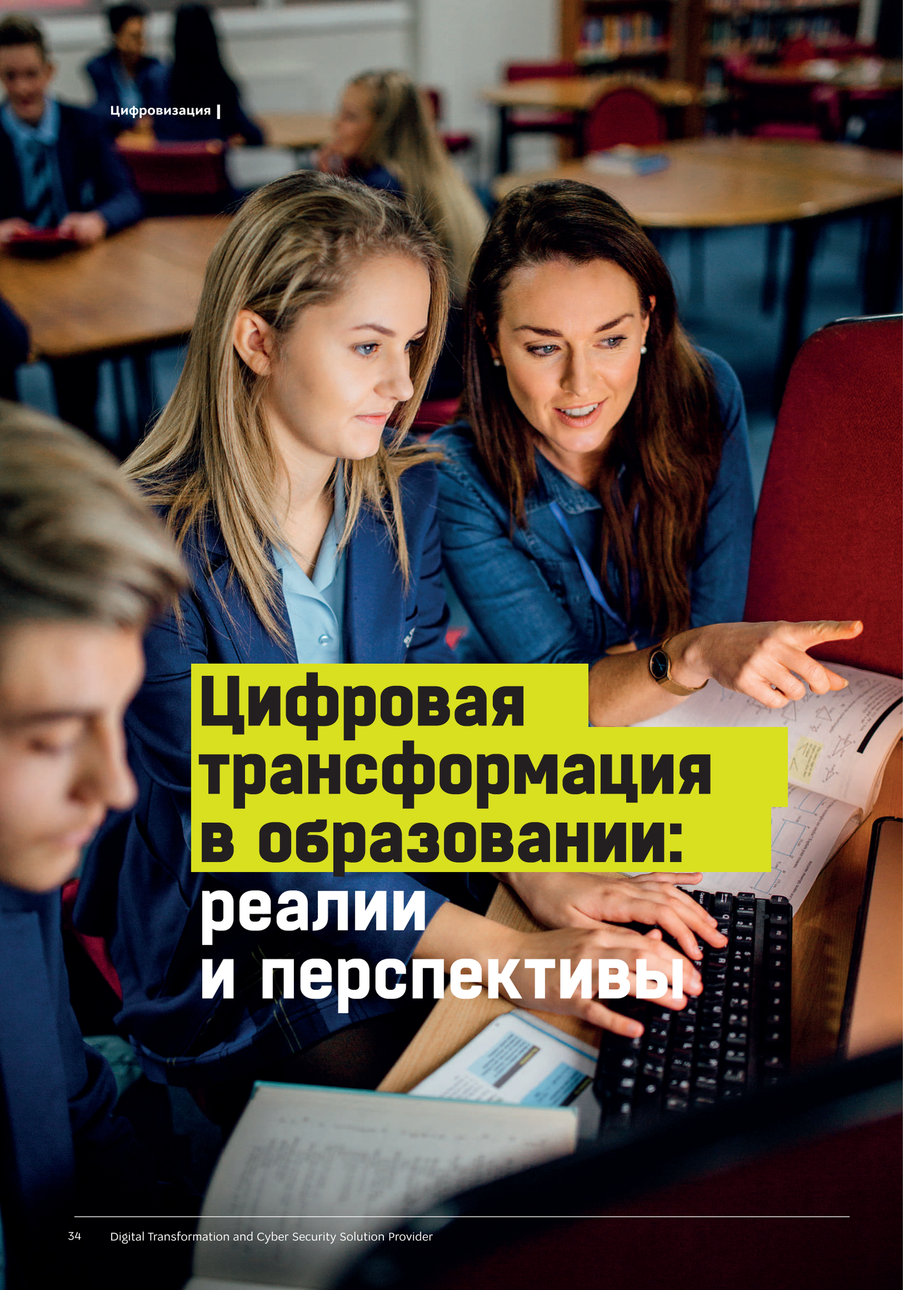
В начале 2018 года Министерство обороны Сингапура пригласило 300 хакеров для выявления уязвимых мест в их системах кибербезопасности. Для этого им предоставлялась возможность взломать минобороны, а за каждую найденную в компьютерных системах ошибку предназначалось вознаграждение в размере от 150 до 20 тысяч сингапурских долларов, в зависимости от серьезности бага. Для сравнения, команда специализированных сотрудников обошлась бы в несколько миллионов долларов.

«Заместитель генерального директора CSA, г-н Teo справедливо заметил: «CSA не может делать все самостоятельно». Киберугрозы — это общие враги, для борьбы с которыми необходимо международное доверие и сотрудничество, а также общие нормы и правила.»

Общий язык безопасности

В своей активной борьбе с киберпреступностью Сингапур активно ищет новых партнеров, готов обсуждать общие требования и создавать возможности для сотрудничества. Эрик Коул, один из ведущих экспертов в области кибербезопасности на мировом рынке и научный сотрудник в Институте системных администраторов и стандартов безопасности утверждает, что нужно найти один общий технически-тактический язык безопасности и на его основе создать стратегию исполнения с едиными стандартами». Это относится ко всем заинтересованным государственным и международным партнерам, научным кругам и частному сектору. Сингапур может стать глобальным лидером в борьбе с киберпреступностью. Значительным шагом на пути к эффективному международному сотрудничеству сотрудничеству стало вступившее в силу в этом году постановление Европейского союза — Общий регламент о защите данных — который означает, что все организации, которые принимают, обрабатывают и хранят персональные данные любого гражданина ЕС, должны соответствовать утвержденным правилам. Компании, нарушившие данный регламент, будут оштрафованы на сумму в размере 4% от общего оборота. Таким образом, соответствие международным стандартам и защита данных станут основными направлениями деятельности в сфере кибербезопасности на ближайшие годы. ▮

Чтобы обеспечить сохранность важной государственной информации в компьютерах чиновников, им просто не предоставляют доступ к интернету на рабочем месте.



Цифровая трансформация в образовании: реалии и перспективы

Современные средства коммуникации и взаимодействия меняют наше представление о способах получения знаний. В этой статье мы расскажем о виртуальном педагоге по имени Джилл Уотсон, поразмышляем над тем, как изменится подход к обучению, и какие новые профессии могут появиться в образовательной сфере в ближайшем будущем.

Виртуальный помощник IBM Watson

Ашок Гоэль, профессор информатики из Технологического института Джорджии, нанял в качестве помощника для проведения занятий Джилл Уотсон – программу-робота с искусственным интеллектом. В течение семестра она помогала отвечать на вопросы студентов в онлайн-режиме, тем самым взяв на себя часть работы преподавательского состава.

В начале семестра профессор предоставил своим студентам список из 9 учебных ассистентов, включая Джилл, диалоговый сервис, разработанный с помощью студентов и компании IBM. Гоэль и его учебные ассистенты получили более 10 000 вопросов за семестр от студентов с онлайн-форума. Зачастую обучающиеся задавали одни и те же вопросы. И тогда Гоэль впервые задумался над тем, как можно было бы автоматизировать рутинный процесс ответов на повторяющиеся вопросы.

Чтобы обучить систему IMB Watson, профессор «накормил» ее постами с форума из предыдущего семестра. Это позволило Джилл получить обширную базу знаний по вопросам и ответам на них.

Ашок тестировал систему несколько месяцев в конфиденциальном режиме: учебные ассистенты проверяли, правильно ли Джилл отвечает на вопросы.

Системе было позволено отвечать, только если вероятность правильного ответа равнялась 97% или больше. Гоэль выяснил, что это значение гарантировало точность ответов. Робот смог ответить на 40% вопросов, включая наиболее трудные. С остальными Джилл не справилась – на них отвечали учебные ассистенты-люди.

Большинство студентов до последнего момента не подозревали, что уведомления на почту и ответы на вопросы они получают от системы искусственного интеллекта. «Было весело, когда студенты узнали о Джилл, они так оживились и воодушевились идеей. Никогда прежде такого не видел», – сказал Гоэль.

В опросе приняли участие более 1800 специалистов в сфере образования, возраст более 80% из которых превышал 30 лет. Большинство откликов было получено из Северной Америки, Соединенного Королевства, Австралии, Новой Зеландии и Индии. Участниками были управленцы и руководители (26%), педагоги (47%) и работники сферы образования с административными функциями (27%).

Каким станет образование к 2025 году?

Согласно опросу 2025 Education Innovation Survey Report*, проводившемуся среди специалистов разных профессий в сфере образования, ключевыми методами взаимодействия с материалом и контентом станут совместная работа посредством видеоконференции и мобильные устройства. Помимо самих результатов исследования, обнаружились и другие интересные факты. Каковы же основные тренды развития современного образования?

Возможность обучаться откуда угодно и в любое время

Доступность обучения для тех, кому это действительно нужно, – один из самых важных факторов успеха в образовании. Школьные специалисты со всего мира (25%) поставили доступность обучения на первое место среди других факторов. Под доступностью здесь имелся в виду географический аспект: какое расстояние необходимо преодолеть, чтобы предоставить обучение там, где нужно.

Видеоконференция с учителями в реальном времени

67% школьных специалистов считают, что центральный элемент получения знаний – сами учителя и преподаватели. Однако ожидается значительный рост использования дистанционных форм обучения: 53% специалистов верят, что к 2025 году совместная работа посредством видеоконференции и мобильных устройств будет для студентов основным способом изучения материала. Несмотря на это, многие специалисты полагают, что учителя и преподаватели продолжат играть важную роль наставников.

Улучшение качества подготовки учителей; индивидуальное и контекстуальное обучение станут основой

Большинство специалистов сферы образования убеждены, что основной целью, помимо отмены госконтроля и изменения стандартов соответствия, должно стать качество подготовки учителей. 18% респондентов из Северной Америки и 21% из Индии считают, что также необходимо обратить внимание на создание более индивидуального и контекстуального обучения.

Больше онлайн-доступа к образовательным материалам

Согласно мнению 47% опрощенных (большинство из Северной Америки и Соединенного Королевства) ответили, что онлайн-доступ к обучающим материалам и лекциям это то, что студенты и их родители хотят от образовательных учреждений больше всего.

Коллективное использование онлайн-ресурсов и самообразование для учителей

В 2025 году коллективное использование ресурсов через онлайн-каналы будет еще больше способствовать профессиональному росту учителей. Опрошенные полагают, что в будущем учителя будут пользоваться онлайн-ресурсами для обмена информацией и станут более независимыми в определении своих собственных целей обучения.

Профессии будущего (образование)

Учитывая динамичное проникновение ИТ-технологий в образование, можно смело предположить, что профессии в области обучения в будущем станут еще актуальнее, а специалисты этой области еще нужнее. Ниже подборка профессий образовательной сферы, которые по версии atlas100.ru появятся в ближайшие годы.

Игровой преподаватель

Профессия появится после 2020 года.
Специалист в разработке образовательных программ, основанных на игровых технологиях. Действует от лица игрового персонажа. Этот специалист заменит традиционных учителей в школе.

Экопастор

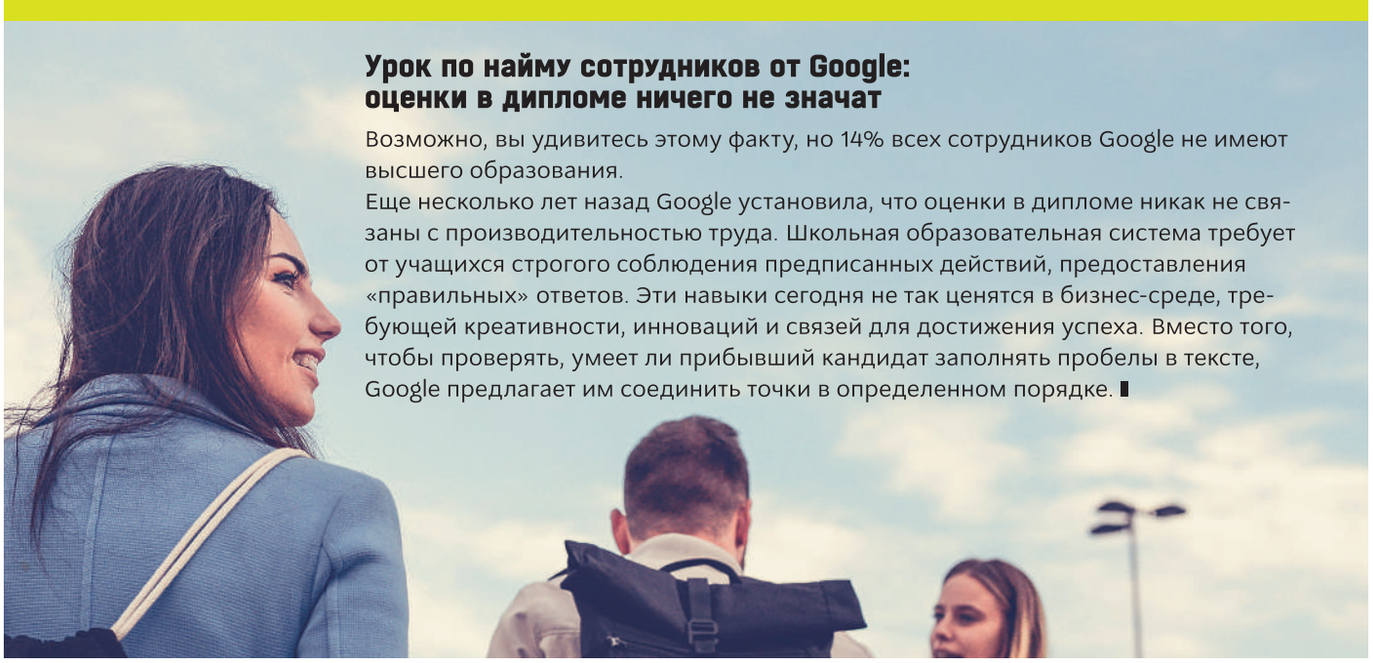
Профессия появится до 2020 года.
Специалист занимается разработкой и внедрением образовательных и методических программ для детей и взрослых, обучая их правильному взаимодействию с окружающей средой (перерасход, раздельный сбор мусора, безвредный для окружающей среды образ жизни), а также программ для промышленных предприятий по более экологически безопасным практикам.

Стартап-наставник

Профессия появится до 2020 года.
Специалист имеет опыт запуска собственных стартапов. Руководит новыми стартап-командами, обучая их бизнес-навыкам по кейсам исходя из своего опыта создания проектов. На Западе ментор – устоявшаяся профессия, а в Беларуси она только набирает обороты из-за плохо развитого малого бизнеса. Однако в центрах освоения бизнеса и бизнес-акселераторах (к примеру, бизнес-инкубатор ВШЭ, Стартап Академия «Сколково» и Венчурная академия LaunchGurus) уже разрабатывают менторские программы. Востребованы также услуги независимых специалистов.

Организатор обучения по проектам

Профессия появится до 2020 года.
Специалист в разработке и организации программ обучения, направленных на подготовку и внедрение проектов в реальном секторе экономики с обязательным изучением теоретического материала.



Урок по найму сотрудников от Google: оценки в дипломе ничего не значат

Возможно, вы удивитесь этому факту, но 14% всех сотрудников Google не имеют высшего образования.
Еще несколько лет назад Google установила, что оценки в дипломе никак не связаны с производительностью труда. Школьная образовательная система требует от учащихся строгого соблюдения предписанных действий, предоставления «правильных» ответов. Эти навыки сегодня не так ценятся в бизнес-среде, требующей креативности, инноваций и связей для достижения успеха. Вместо того, чтобы проверять, умеет ли прибывший кандидат заполнять пробелы в тексте, Google предлагает им соединить точки в определенном порядке.

Основные тренды цифровизации и их реальные перспективы

В качестве основных строительных блоков цифровизации обычно называют следующие технологические тренды: интернет вещей, искусственный интеллект, облачные технологии, 3D-печать, Big Data. Что скрывается за этими словами и в каком состоянии на настоящий момент «киты», держащие на спине всю цифровизацию?

Начнем с основ: любые «жизнеспособные» технологии проходят определенные этапы своего становления или «принятия» обществом. Появление теоретических основ и опытных образцов, как правило, очень сильно отстоит по времени от создания и распространения коммерчески интересных и популярных решений.

Этапы принятия обществом новых решений и технологий
Рис. 1.

Когда на рынке появляются первые экземпляры инновационных продуктов, первыми их подхватывают так называемые «новаторы» и «ранние последователи». По сути это увлеченные люди, которым интересны новинки, которые раньше других могут заметить их высокий практический интерес и готовы заплатить за первые образцы значительные суммы. Далеко не всегда подобные прогнозы сбываются, но... с них начинается переход абстрактной технологии на коммерческие рельсы.

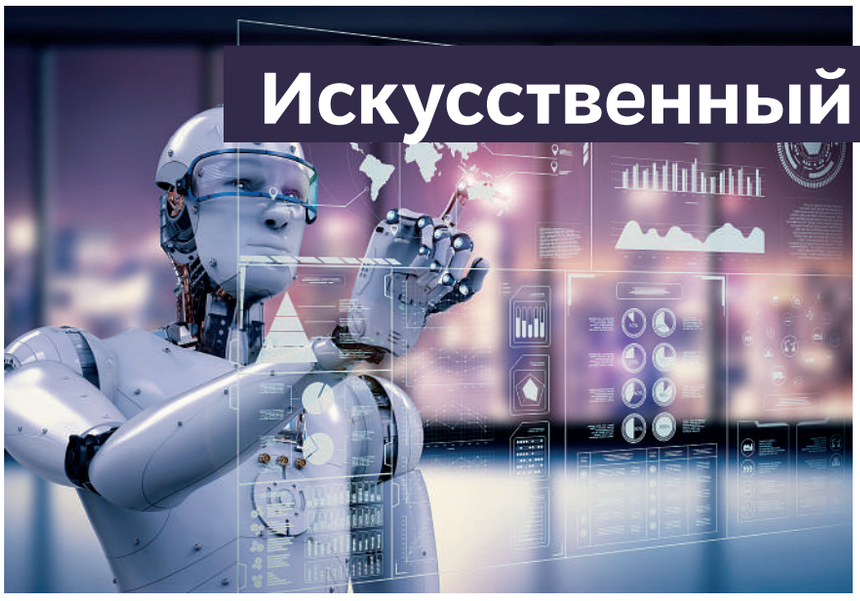
Увы. После того, как «новаторы» и «ранние последователи» оценят удобство новых решений и технологий, наступает так называемый «провал» - время, когда видимых подвижек не происходит. Решение тестируется, выявляются недостатки, которые устраняются в новых версиях. Накапливается «критическая масса» ранних последователей и лишь после того, как продукт проходит испытание временем, к нему потихоньку начинают приглядываться представители «раннего большинства». Если ранее они считали, что решение может оказаться просто дорогой игрушкой для гиков и выжидали, то теперь они видят, что «испытание временем» пройдено, популярность растет и необходимо присмотреться. После этого момента интерес к продукту повышается очень быстро. В дело вступает «позднее большинство», а со временем, когда решение становится неотъемлемым атрибутом жизни, к ним волей или неволей присоединяются и «скептики». Что же происходит с трендовыми технологиями на текущий момент? Рассмотрим более детально.

Интернет вещей

Начнем с определения. Интернет Вещей (IoT) – это взаимодействие физических устройств, оснащенных электронными сенсорами и исполнительными устройствами, через коммуникационные сети.

В каком он сейчас состоянии? Как тренд — да, есть такое. У «новаторов» и «ранних последователей» уже есть «умные дома», а в некоторых странах даже почти «умные города». Слово «почти» стоило бы выделить.

Человеческое общество довольно косно, как ни больно это признавать, поэтому большинству проще потерять время и сделать все привычным образом, чем попытаться усвоить новый метод действий, пусть даже и значительно более простой и быстрый — это одна из причин, почему интернет вещей, оставаясь перспективной технологией, до сих пор не так уж и глубоко проник в нашу повседневную жизнь.



Искусственный интеллект

С искусственным интеллектом дела обстоят тоже непросто. Начнем с того, что в настоящее время по-прежнему нет четкого определения, что же такое этот самый искусственный интеллект. Если считать им частичное выполнение машинами определенных функций человеческого мозга, то да, он используется. Скажем, те же человекоподобные роботы, которыми в настоящее время известны японские разработчики. Или, с определенной натяжкой, к искусственному интеллекту можно отнести известных и используемых многими электронных помощников: Siri, Cortana, «Алиса» и другие. Однако при всей своей интеллектуальности, они пока не очень-то и интеллектуальны. Дело будущего.

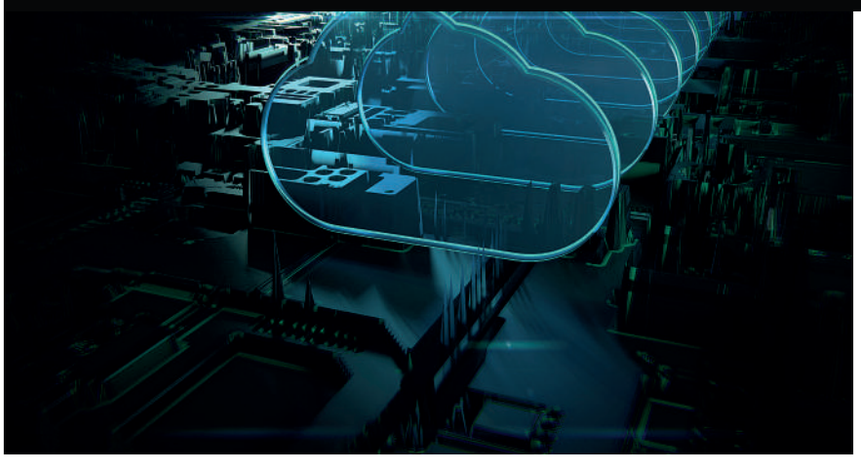
Отдельный интерес представляют собой сложные системы аналитики, к примеру, построенные по принципу нейронных сетей. Подобные математические системы уже сейчас способны создавать и обсчитывать модели, прогнозирующие развитие ситуаций, ход экспериментов, поведение людей и т.д. Пожалуй, это наиболее очевидное в настоящее время достижение интеллектуальных компьютерных систем.

Также нельзя забыть про автомобили, способные передвигаться без водителя. Подобные грузовые автомобили уже нашли свое применение на дорогах США. Потихоньку разрабатываются и даже производятся легковые автомобили, но время, когда они минуют «провал» и выйдут хотя бы на уровень «раннего большинства» еще не пришло. Причина: отсутствие юридических и нормативных баз, а также сравнительно недавнее начало использование подобных автомобилей.

Big Data

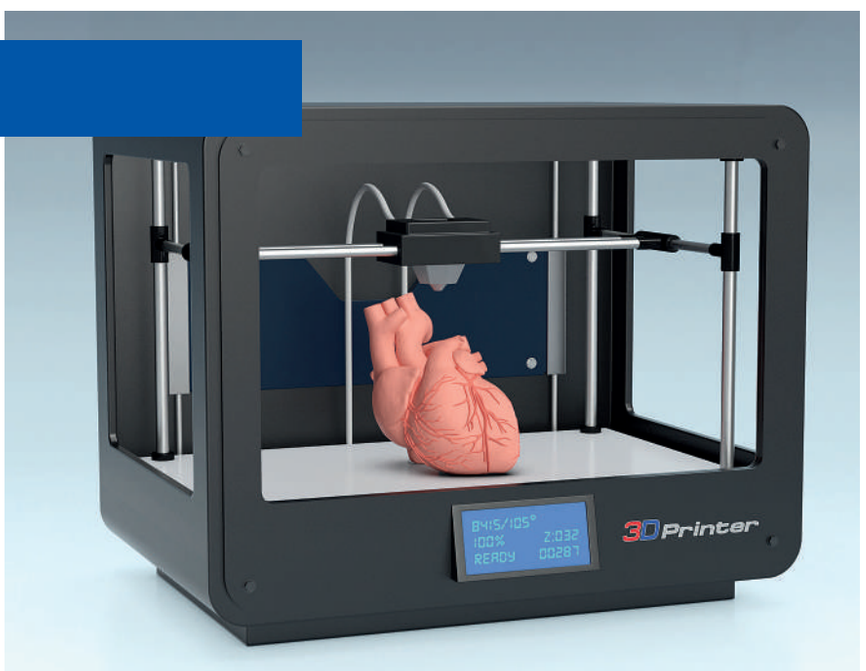
Про «раннее большинство» в контексте этой технологии уже можно говорить. Системы, использующие принципы Big Data, успешно применяются в медицине, промышленности, маркетинге. Большая часть преград для распространения технологии связана со сложностью получения больших объемов релевантных данных. Иногда это связано и с геополитическими сложностями — отсутствие возможности получать данные за пределами той или иной страны. Отчасти проблема на стороне недостаточного охвата технологиями учреждений, владеющих потенциально интересной информацией. Порой сложности появляются на стороне законодательства. И тем не менее успехи уже есть, использование технологии набирает обороты.

Облачные технологии



Облачные технологии уже давно выбрались из провала. «Раннее большинство» тоже успело оценить по достоинству их удобство. В настоящее время продажи облачных решений растут, значительно опережая темпы остального ИКТ-рынка. Можно смело говорить о начале формирования «зрелого» рынка. А это значит, что облачные технологии уже надежно встали на ноги и становятся неотъемлемой частью жизни общества.

3D-печать



Пожалуй, из провала технология уже выбралась или близка к этому как никогда. Ее успехи в медицинской сфере просто потрясают. В сфере производства препятствием изначально была скорость работы 3D-принтеров, но в настоящее время в промышленности появляются скоростные модели. Их пока немного, но уже можно говорить о начале распространения. Известны отдельные случаи использования 3D-принтеров для серийного производства. Например, компания Adidas запустила 3D-печать подошв для кроссовок. В прошлом году первые партии такой обуви поступили в магазины. Также появились 3D-принтеры, печатающие из металла, причем не хрупкого (этим отличались первые пробные варианты), а вполне прочного и пластичного. Потенциально это способно в корне изменить многие отрасли промышленности, так как такая печать стоит намного дешевле и осуществляется быстрее. Мы полагаем, что в ближайшие годы следует ожидать еще большего ее распространения.

Что мы видим в итоге? — Если облачные технологии уже стали полноправным участником рынка, то остальные направления, с которыми связывается успех цифровизации, сейчас находится либо все еще на уровне «испытания временем», либо только распространилась на «раннее большинство». В ближайшее десятилетие следует ожидать их развития и выхода в «свободное плавание». Однако вполне возможно, что развитие IoT и искусственного интеллекта пойдет не совсем так, как сейчас принято предполагать. Вполне вероятно, что внедрение IoT в частную жизнь — это дело не одного десятка лет, так же как и создание «умных городов» еще потребует многих усилий. Системы искусственного интеллекта — своего рода «темная лошадка». Потенциально они способны одним рывком перекроить привычную нам картину мира, но могут и остаться уделом высокотехнологичных компаний. ▮

Новые возможности vSAN 6.7 и vSphere 6.7

Весной 2018 года вышли большие обновления решений VMware: программного хранилища данных vSAN 6.7 и платформы виртуализации VMware vSphere 6.7.

VMware vSAN

Упрощенное хранилище данных на основе стандартных серверов x86. Решение позволяет грамотно выделять объем памяти на жестких дисках серверов и не закупать дорогостоящие СХД, что способствует снижению совокупной стоимости владения до 50% по сравнению с традиционными хранилищами.

Что нового в vSAN 6.7?

Новый пользовательский интерфейс на базе HTML5. Теперь vSAN можно управлять через HTML5-клиент vSphere Client, который построен на базе фреймворка Clarity. В новом интерфейсе оптимизированы рабочие процессы, сокращено число действий для выполнения задач. Использование рабочих процессов для кластеров хранилищ стало еще более простым и понятным.

Поддержка vRealize Operations. Традиционно пользователи vSAN использовали две консоли - консоль vCenter и консоль vRealize Operations. В новом vSphere 6.7 появилась функция vRealize Operations within vCenter, которая обеспечивает полную визуализацию сред HCI. Функция позволит просматривать информацию о кластере vSAN, его параметрах и проблемах через vSphere Client в разделе vRealize Operations.

Функция Adaptive Resync. Абсолютно новый инструмент Adaptive Resync позволяет адаптивно регулировать ширину канала для операций ввода-вывода VM I/O и Resync I/O, в зависимости от загрузки производственной системы. Функция гарантирует, что из-за выедания канала каким-то видом трафика, использующего его, остальные типы трафика не блокируются.

Оптимизированный механизм de-staging. В vSAN 6.7 оптимизирован дестейджинг данных из кэша на запись (Write Cache) в сторону дисков. Благодаря этому все работает намного быстрее, ускоряется работа виртуальных машин и каналов ресинхронизации.

Улучшенные проверки состояний (хэлсчеки). Новый уровень самодиагностики позволяет собирать данные о конфигурации кластера с помощью vSAN Support Insight и визуализировать их в vSphere Client.

vSAN ReadyCare. Используя прогнозное моделирование в vSAN Support Insight, службы проверки анализируют данные заказчиков и отправляют рекомендации по устранению проблем в режиме реального времени. Благодаря этому обеспечивается комплексная поддержка с привлечением ведущих экспертов и использованием новейших средств анализа и технологий.

VMware vSphere

Позволяет запускать на одном сервере несколько логических единиц – виртуальных машин, которые полностью воспроизводят работу независимых физических серверов. Это дает возможность компаниям не закупать отдельные серверы под каждое приложение, а размещать на одной единице оборудования несколько десятков независимых операционных систем и корпоративных решений, эффективнее используя ИТ-инфраструктуру.

Основные обновления vSphere 6.7

Улучшение Enhanced vCenter Server Appliance (vCSA) и масштабируемости инфраструктуры

- Появление новых API в vCSA, которые выводят управление платформой на новый уровень.
- Поставка vCSA с интегрированными службами Embedded Platform Services Controller (обеспечивающими работу служб Single Sign-On). Службы работают в режиме Enhanced Linked Mode.
- Увеличение числа операций vCenter в 2 раза.
- Уменьшение потребления памяти в 3 раза.
- Увеличение числа операций DRS в 3 раза (например, включение виртуальной машины и ее первичное размещение в кластере).

Улучшения механизма загрузки/перезагрузки хоста ESXi

- При появлении обновлений (Single Reboot) теперь достаточно один раз перегрузить платформу.
- С помощью нового механизма vSphere Quick Boot можно перезагрузить гипервизор без рестарта всего хоста.

Улучшение HTML5 vSphere Client

- Добавление функции управления vSAN и Update Manager.

Улучшения безопасности

- Появление виртуального модуля Virtual TPM 2.0 для защиты от атак с подменой хостов и виртуальных машин.
- Использование Encrypted vMotion при процессе миграции виртуальных машин между различными экземплярами vCenter для расширения сферы применения данной технологии до гибридных облачных инфраструктур (защищенная горячая миграция в дата-центр сервис-провайдера) или инфраструктур с географически разнесенными дата-центрами.
- Поддержка vSphere 6.7 технологии Virtualization Based Security для гостевых ОС Microsoft Windows.

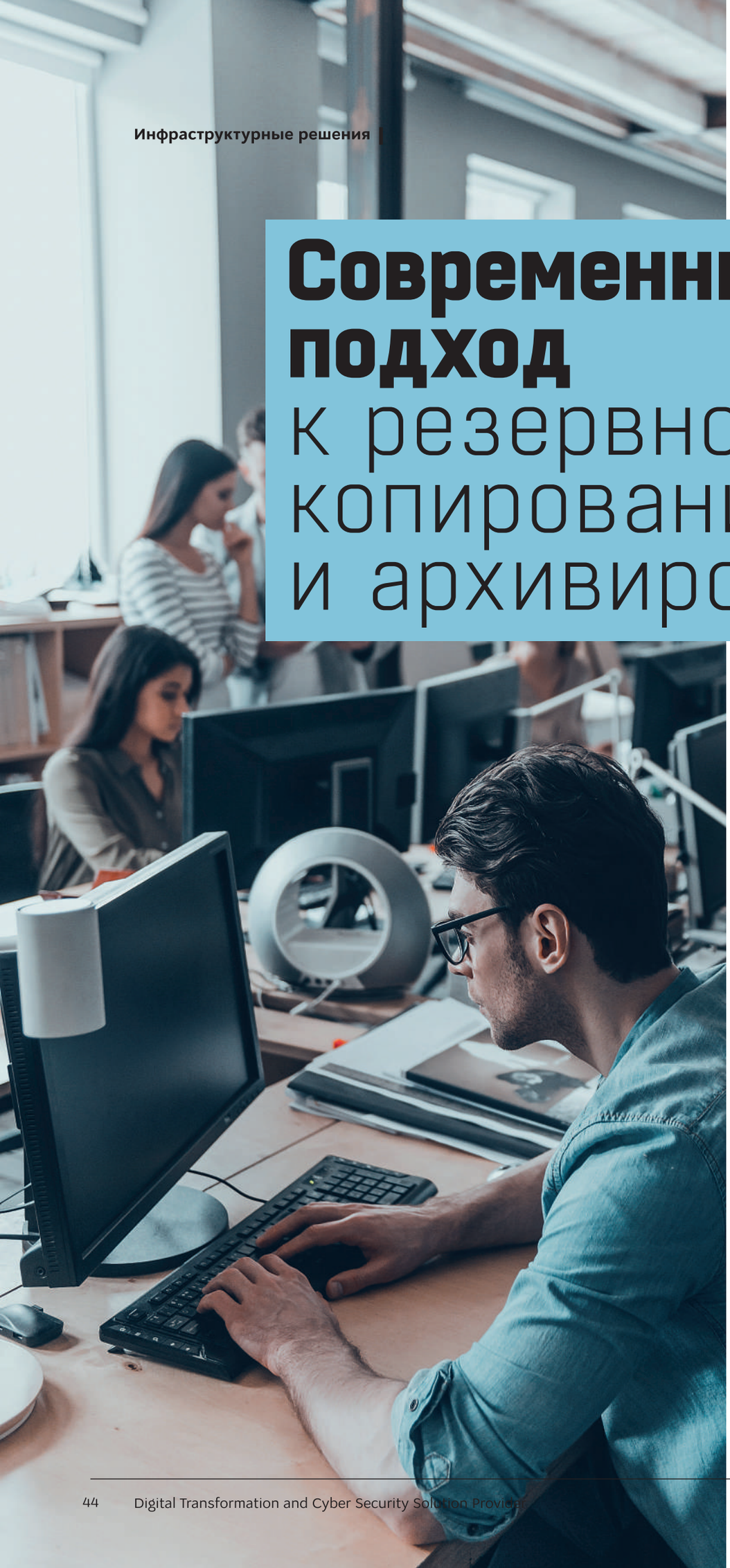
Улучшения поддержки высокопроизводительных приложений

- Использование аппаратных модулей от Dell-EMC и HPE для ускорения работы высокопроизводительных приложений с большим числом IOPS.

Бесшовная интеграция с гибридной средой

- Появление режима работы vCenter Server Hybrid Linked Mode для соединения двух инфраструктур – онпремизной с одной версией vSphere и облачной. ∎

По вопросам, связанным с продуктами VMware, обращайтесь к **Игорю Волокитину**, специалисту отдела аппаратных решений и виртуализации Softline по телефону **+375(17)336-55-95, доб. 4485** или e-mail **Igor.Volokitin@softline.com.**



Современный подход к резервному копированию и архивированию

Игорь Волокитин, специалист по решениям резервного копирования Softline, рассказал о правилах эффективного бэкапа.
Узнаем, какие опасности поджидают при внедрении и эксплуатации систем резервного копирования, зачем нужна архивация и как позаботится о бесперебойной работе, доверив свои сервисы Softline.

Игорь Волокитин,
Igor.Volokitin@softline.com

— Как сегодня выбрать оптимальное решение для резервного копирования?

— В первую очередь мы определяем, что нужно бэкапить, так как для серверов, рабочих станций, гетерогенных вариантов свой пул решений. Исходя из этого, подбираем программные компоненты различных вендоров, каждый из которых обладает своими преимуществами. Есть решения, поддерживающие бэкап на дисках, ленточных накопителях, в облаках, обладающие, к примеру, функцией репликации, которая позволяет обеспечить максимальную скорость восстановления, или дедупликации, организующую наиболее эффективное хранение данных, а также есть возможности создания образов системы, полной автоматизации резервного копирования, централизованного управления. Главная задача – обеспечить непрерывность бизнес-процессов, и специалисты Softline занимаются поиском индивидуального подхода к каждому клиенту, учитывая особенности инфраструктуры, стоимость решений, их функциональные характеристики, а также особенности внедрения и эксплуатации.

—Какие особенности стоит учесть при внедрении средств резервного копирования?

— При внедрении могут возникать такие технические проблемы, как несовместимость оборудования, недоработки ПО, а при эксплуатации – это в основном отказы, ошибки оборудования, человеческий фактор – администратор не проследил за процессом, пользователь случайно удалил важные файлы, а обнаружил это уже на момент истечения срока хранения резервных копий и т.п.

Чтобы учесть все важные тонкости и быть уверенными в защите данных своей организации необходимо довериться квалифицированному персоналу. Сотрудники ИТ должны работать быстро и качественно, обеспечивая непрерывность бизнеса, так как сбои и простои стоят заказчику больших денег и репутационных потерь.

— Как избежать технических проблем при внедрении или эксплуатации СРК?

— Конечно, на сегодняшний день практически все понимают важность резервного копирования и так или иначе его обеспечивают, однако у 75 % компаний нет планов аварийного восстановления. То есть они не тестируют свои системы на предмет ошибок, и в ситуациях определенных катастроф или выхода из строя «железа» они рискуют так и не восстановить данные. Мало установить систему, нужно быть в ней уверенными, а для этого необходимо периодически проверять ее и иметь четко прописанный план действий в случае экстренных ситуаций.

Отсутствие руководства администратора, содержащего информацию о том, как управлять системой резервного копирования, и пояснительной записки с характеристиками текущей системы может стать источником проблем. Например, в случае смены администратора, новый сотрудник должен понять, как система работает, как ее настраивать, обслуживать, как правильно восстановится, в случае, если какой-то сервис недоступен, и т.д. и не тратить на это драгоценное время.

$80 000

в среднем стоит час простоя

$90 000

в среднем стоят потери данных за один час

Среди других сложностей – вредоносное ПО – оно крайне опасно и может нанести удар в любое время, а правильно сделанный бэкап – это спасение. Но часто заказчики забывают о том, что, если, к примеру, шифровальщики проникнут на основной продуктив, то в случае синхронизации с репликой, то же самое вредоносное ПО попадет и на нее, поэтому копии должны храниться еще и за пределами основного ЦОДа.

— Расскажите о системах архивного хранения данных. Чем архив отличается от резервной копии?

— Отличаются они в первую очередь своим целевым назначением. Резервная копия создается для восстановления систем после повреждения данных или их полной утраты, время хранения определяется внутренними требованиями и функциональными возможностями.

Архив – это организация долговременного хранения данных, когда оригиналы перемещаются из основного хранилища в другое, возможно, не такое мощное, но откуда файлы можно извлечь. Это позволяет разгрузить основной продуктив, в результате чего он работает гораздо быстрее, а заказчик экономит на устройствах хранения.

Многие знакомы с ситуацией, когда найти нужную информацию в загруженной почте практически невозможно, поиск среди множества писем длится долго и порой безрезультатно. Архив позволяет разгрузить приложение, чтобы ему не приходилось оперировать огромными массивами данных, которые не требуются нам ежедневно, но обеспечивать хранение которых, необходимо. Контент, который находится в архиве, индексируется, в рамках приложения архивации есть инструменты для различных расследований, поиск работает по всему архиву и содержимому вложений. В целом, архивация позволяет снижать операционные затраты на хранение, тем самым экономить деньги.

— Позволяют ли системы интегрировать резервное копирование и архивирование в одном решении?

— Да, и это происходит всё чаще. Системы РК и архивного хранения совмещаются в решениях одного производителя, использующих принцип иерархического хранения данных. Система сама распределяет данные между уровнями хранения. Некоторые системы позволяют при совмещении использовать одну и туже базу дедупликации. Либо вариант, когда система резервного копирования позволяет помещать архивы на ленточные накопители или в виртуальные СХД, что позволяет уменьшить стоимость их хранения и обеспечить отказоустойчивость.

Простои и потери данных обходятся крупным компаниям до

$21 800 000 в год

— Как использование облаков упрощает управление бэкапами?

— В Беларуси сейчас появляется всё больше сервис-провайдеров облачных решений, которые оказывают услуги по предоставлению резервного копирования в облако. Если что-то происходит с сервером резервного копирования клиента, всегда можно восстановить информацию из облачного хранилища локального сервис-провайдера. Для заказчиков это означает снижение затрат на серверы, СХД и на управление ими.

Если клиенты переходят на полный облачный бэкап, им не нужно арендовать помещения, платить за покупку оборудования и заботиться об актуальности его состояния. За работу сервисов отвечает облачный провайдер, который обеспечивает необходимый клиенту SLA.

Если клиенту нужно увеличить серверные мощности, расширить место хранения или количество резервных копий, то возможности современного сервиса позволяют делать это с очень высокой скоростью, а затраты на покупку железа перевести в затраты на его аренду. Если сегодня вам нужно бэкапить 100 ГБ, а завтра больше, вы докупаете необходимое количество определенными порциями ровно столько, сколько вам нужно.

Способность быстро реагировать на изменения бизнеса крайне важна. Случалось, что компании, построив собственные дорогостоящие ЦОДы, становились банкротами, а бывшее в употреблении оборудование уже оценивается в десятки раз меньше. Компании же, которые развернули свои сервисы в облаках, например, в случае оттока клиентов просто отказывались от определенного количества мощностей и соответственно уменьшали свои расходы, что позволяло им поддерживать эффективность и рентабельность бизнеса.

— Какие услуги предлагает Softline в области резервного копирования?

— Первый этап – это, как правило, аудит. Обследование инфраструктуры компании-клиента позволяет собрать сведения обо всех серверах и сервисах компании, выявить их особенности и ограничения и выработать оптимальное решение.

Далее устанавливается и настраивается резервное копирование на территории заказчика, в облаке или комбинируется в зависимости от поставленных задач. Настраивается ротация резервных копий, дедупликация, проводится обучение технических специалистов заказчика, разрабатывается соответствующая документация, например, руководство администратора, пояснительная записка, планы аварийного восстановления. Если необходимо, то документация подготавливается согласно внутренним требованиями компании.

Также мы можем оптимизировать и модернизировать имеющуюся систему РК. Определить, насколько она хорошо работает, правильно ли настроена, вовремя ли обновляется, удовлетворяет ли RTO (время восстановления) и RPO (точка возврата), проверяем актуальность оборудования, тестируем аварийное восстановление. Если клиента не устраивает функционал определённого вендора, помогаем подобрать другого, который соотвествует требованиям в большей степени.

При необходимости мы проводим обучение заказчика работе с СРК на базе нашего учебного центра Softline, где официальные курсы читают квалифицированные инженеры, обладающие опытом внедрения данных решений.

— Каковы тенденции развития технологий резервного копирования и восстановления?

— Основное направление развития – это активная миграция в облака, а также интеграция с мобильными сервисами и объединение систем резервного копирования, архивации и репликации. Существует тенденция получать сервисы как услугу, при этом они должны быть мобильными и всегда доступными – нужно соответствовать актуальным требованиям и подстраиваться под потребности заказчиков. Клиенты должны быть уверены, что их данные будут в сохранности, бизнес не остановится и будет приносить прибыль. Технологии совершенствуются и усложняются, а процесс предоставления услуг упрощается. ▮

3%

жестких дисков ломается в первый же год при активном использовании из-за производственного брака. Далее с каждым годом вероятность поломки увеличивается на **6-8%.**

Veeam: защита от вымогателей

Общий объем издержек из-за киберпреступности неизбежно растет, и это не может не вызывать тревогу. Cybersecurity Ventures прогнозирует, что к 2019 году компании по всему миру будут страдать от атак вымогателей каждые 14 секунд. Veeam может предоставить решение для резервного копирования, которое обеспечит эффективное восстановление после атак при использовании рекомендуемых передовых методов.

Программы-вымогатели. Цена и последствия

Программы-вымогатели – это вредоносное программное обеспечение, которое блокирует доступ к компьютеру или конкретным файлам до тех пор, пока не будет выплачена требуемая сумма выкупа. Зашифровываются именно те данные, которые предположительно настолько важны для пользователей, что они будут готовы заплатить необходимую сумму.

Такие вирусы появились еще в 1989 году, а распространение получили в 2012. С тех пор способы заражения стали гораздо изощреннее, а пути доставки вредоносных программ проще. Министерство юстиции США определяет вымогателей как новую бизнес-модель киберпреступности. По данным отчета Cybersecurity Ventures, к 2019 году общий ущерб от действий программ-вымогателей превысит $11,5 млрд в год. Большая часть этих затрат относится не к выплаченной сумме выкупа, а к широкому спектру последствий. Основной ущерб от работы этих вредоносных программ заключается в повреждении или потере критически важных данных, что становится причиной вынужденного простоя на производстве и потери производительности. Нарушение нормального хода хозяйственной деятельности приводит к утрате доверия со стороны сотрудников, репутационным потерям и необходимости восстановления захваченных вымогателями систем.

Примером может послужить атака на Медицинский центр округа Эри в Нью-Йорке в апреле 2017 г. Больница не заплатила запрошенный вымогателями выкуп в размере 30 000 долларов, и последствия инцидента обошлись почти в $10 млн. Примерно половина этой суммы была выделена на компьютерное оборудование, программное обеспечение и поддержку, необходимые после нападения. Другая часть сложилась из возросших расходов, таких как оплата сверхурочной работы персонала и снижение доходов в результате упущенной выгоды во время простоя системы. Если бы руководство приняло решение заплатить требуемую сумму, расходов и потерь было бы еще больше. По данным исследовательской фирмы CyberEdge Group, половина компаний, которые платят выкуп, никогда не получают свои данные обратно, а другая половина сообщает о полной потере данных.

Программы-вымогатели становятся на сегодняшний день основной киберугрозой. Veeam дает компаниям и конечным пользователям уверенность в том, что их цифровая жизнь будет Always-On, то есть не встретит на своем пути препятствий благодаря правильной защите против вымогателей и программам восстановления.

Обеспечивать безопасность компании необходимо за счет использования передовых и эффективных методов. Veeam предлагает двойной подход: готовность к тому, что может произойти неизбежная атака и готовность к восстановлению, в том числе из облачной копии.

По данным отчета Cybersecurity Ventures, к 2019 году общий ущерб от действий программ-вымогателей превысит $11,5 млрд в год. Большая часть этих затрат относится не к выплаченной сумме выкупа, а к широкому спектру последствий.

Как защититься?

Известны наиболее частотные методы и правила защиты от вирусных атак. Интеграция Veeam Backup & Replication и Veeam ONE в стратегию защиты данных повысит сопротивляемость к таким нападениям.

Установка патчей

Все элементы ИТ-ифраструктуры – операционные системы, антивирусы, браузеры, плагины – требуют постоянных обновлений. Программы-вымогатели в своих атаках, направленных на заражение, чаще всего ориентируются на уязвимости конечных устройств, которые можно легко устранить с помощью патчей.

Обеспечивать безопасность компании необходимо за счет использования передовых и эффективных методов. Veeam предлагает двойной подход: готовность к тому, что может произойти неизбежная атака и готовность к восстановлению, в том числе из облачной копии.

Правило 3-2-1

«Делать минимум три резервные копии на двух типах носителей, при этом одна копия должна быть передана на внеофисное хранение». Это правило помогает устранить любой аварийный сценарий без использования специальных технологий. Услуга Veeam Cloud Connect предусматривает хранение резервных копий за пределами своего предприятия в облаке локального сервис-провайдера. Используется дедупликация на источнике и шифрование данных для обеспечения быстрой и безопасной репликации и резервного копирования.

Автономное хранилище в облаке локального сервис-провайдера

Следуя вышеупомянутому правилу, необходимо убедиться в том, что одна из копий хранится изолированно, т. е. в независимом хранилище. Veeam предлагает множество вариантов автономного (и полуавтономного) хранения. К ним относятся: лента, мгновенное копирование основного хранилища, жесткие диски, но наиболее актуальным способом стало хранение в облаке.

Использование различных учетных данных для хранения резервных копий

Это стандартная и хорошо известная практика защиты от программ-вымогателей, следовать которой чрезвычайно важно. Контекст имени пользователя, который используется для доступа к хранилищу резервных копий, требует основательной защиты и применения исключительно для этой цели. Другие контексты безопасности не должны предполагать доступа к хранилищу резервных копий, кроме учетных записей, необходимых для фактических операций резервного копирования.

Использование различных файловых систем для хранения резервных копий

Для того чтобы задействовать данный способ подготовки к атакам, необходимо, чтобы пользователи добавляли резервные копии в хранилище, требующее различной аутентификации. Хорошим примером служит система Linux, функционирующая в качестве хранилища данных. Риск прохождения программ-вымогателей вполне можно уменьшить, используя другую файловую систему и варианты резервного копирования Veeam с аутентификацией и восстановления через Linux. Однако следует отметить, что есть пути обхода этой стратегии и она не является полностью отказоустойчивой.

Регулярная оценка рисков

Для выявления потенциальных рисков и подготовки к восстановлению в случае атаки обязательно нужно проверять восстанавливаемость данных. Решение Veeam ONE – это мощный инструмент мониторинга, отчетности и планирования производительности для инфраструктуры резервного копирования Veeam. Оно предусматривает готовую отчетность по оценке уровня защиты, а также систему предупреждения о возможных активностях программ-вымогателей.

Задание резервного копирования

Это отличный инструмент для создания различных точек восстановления в другом хранилище с другими правилами хранения. Тем не менее задание резервного копирования также может быть инфицировано программой-вымогателем, если копия не находится в облаке.

Обучение сотрудников

Вредоносная деятельность вирусных программ и вымогателей имеет успех тогда, когда сотрудники в компаниях недостаточно информированы о том, как работают злоумышленники и какой ущерб могут причинить. Действенный механизм обучения, коммуникации и поддержки сможет обеспечить готовность к противодействию.

Как восстанавливаться?

Платформа Veeam Availability Platform предлагает надежные решения для быстрого и эффективного восстановления рабочих операций и критически важных данных после кибератаки программы-вымогателя.

Защита центра обработки данных

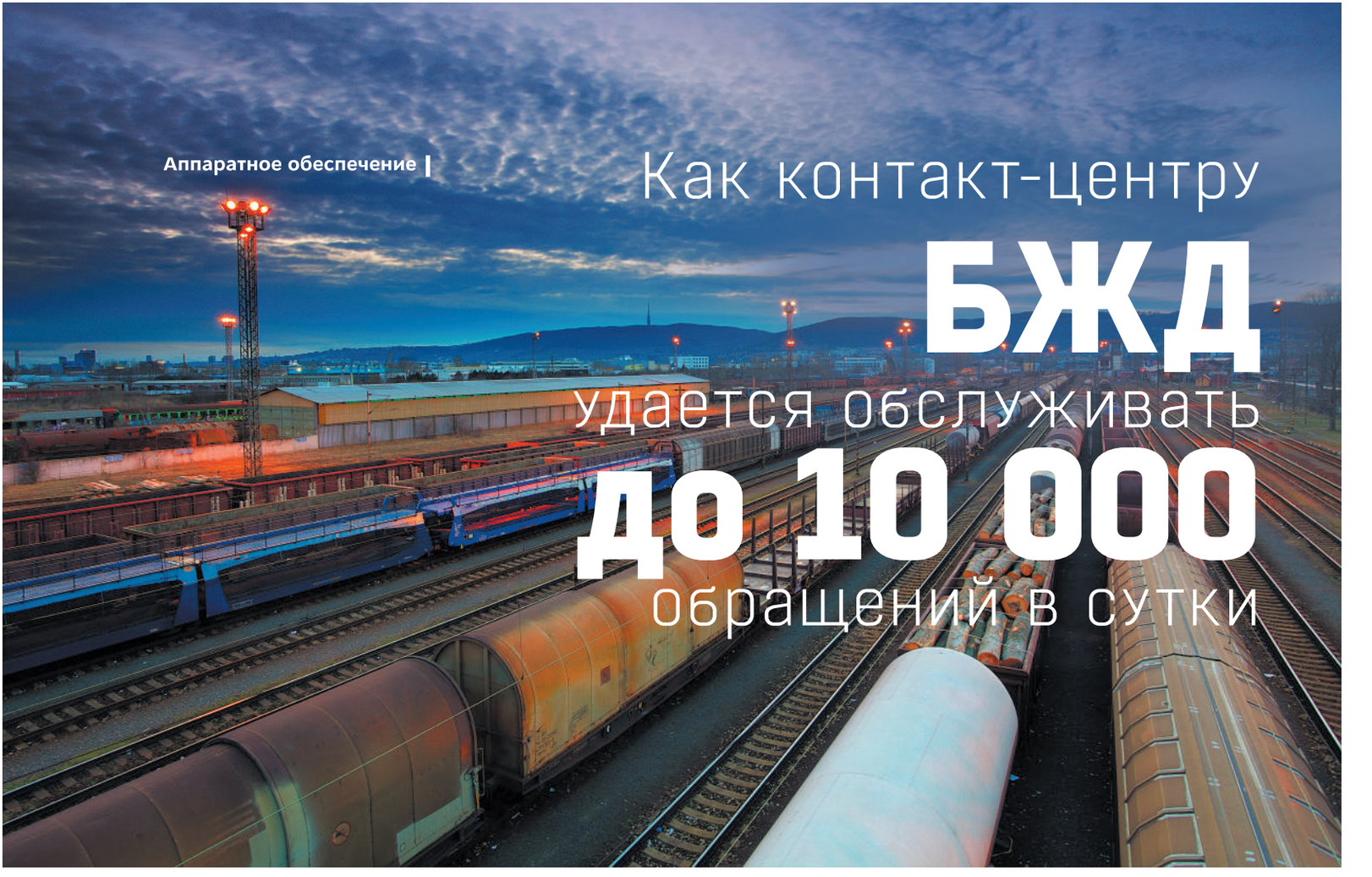
Veeam Availability Suite, неотъемлемая часть платформы Veeam Availability Platform, предоставляет решение для восстановления после подобных атак. Также разработано решение корпоративного уровня для обеспечения доступности данных в повседневной работе – это быстрое восстановление после атак программ-вымогателей через быструю виртуальную машину и гранульное восстановление. Оно предназначено для замены зашифрованных программами-вымогателями баз данных, приложений, файлов и операционных систем. Это легко сделать с помощью Veeam Explore для мгновенного копирования хранилища и сценария восстановления файлов в один клик.
За счет тесной интеграции с ведущими поставщиками систем хранения, такими как Hewlett Packard Enterprise (HPE), Dell EMC, NetApp, IBM, Lenovo, достигается быстрое восстановление и бесперебойная работа приложений. А для того, чтобы быстро и легко обнаружить последнюю правильную точку восстановления с помощью Veeam on-Demand Sandbox, проводится тестирование и определение точек восстановления.

Защита конечных точек

Эффективный план восстановления всегда предусматривает защиту конечных устройств: ноутбуков и ПК. Veeam Agent для Linux и Veeam Agent для Windows предлагают возможность размещения резервных копий в разных файловых системах благодаря интеграции с Veeam Availability Suite и облаком сервис-провайдера.

Забота о будущем с Veeam

Cybersecurity Ventures прогнозирует, что к 2022 году число пользователей интернета достигнет шести миллиардов. Зависимость от сети стремительно растет, а киберпреступники постоянно находятся в поиске уязвимостей. Распространение стратегии BYOD и внедрение Интернета вещей еще больше усложняют обеспечение безопасности ИТ-среды. Многие компании убедились на собственном опыте, что игнорирование программ-вымогателей обходится очень дорого и защищать свои данные нужно любой ценой. Используя Veeam и рекомендованные методы защиты, можно обеспечить полную готовность к восстановлению данных в случае их заражения программами-вымогателями. Платформа Veeam Availability Platform в совокупности с облаком Softline – это надежное решение для поддержки компаний и конечных пользователей на пути к созданию эффективной системы защиты, восстановлению и обеспечению доступности по всем направлениям работы. ▮



Как контакт-центру БЖД удается обслуживать до 10 000 обращений в сутки

Заказчик: БЖД
Отрасль: транспорт
Задача: внедрение телекоммуникационной платформы для контактного центра
Решение: внедрение ПО на базе Glare Unified Communication Platform (CallWay)
Результаты: высокая отказоустойчивость ИТ-системы, создание гибкой и масштабируемой виртуализированной инфраструктуры.

О компании

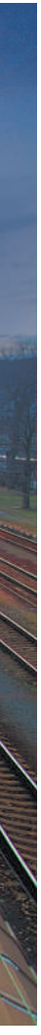
Белорусская железная дорога (БЖД) обеспечивает в Беларуси около 63% грузооборота всех видов транспорта общего пользования и около 38% пассажирооборота. Предприятие реализует комплекс мероприятий по развитию электронных продаж, совершенствованию системы оформления проездных документов, поддержки пользователей, развитию информационно-справочного обслуживания.

Ситуация

Управление распределенной структурой подразумевает организацию эффективных и удобных коммуникаций как внутри предприятия, так и вовне. Одна из важнейших задач железной дороги – эффективная работа с пассажирами, оперативное предоставление им справочной информации и оказание помощи в разрешении различных ситуаций.

До 2017 года предоставление справочной информации на Белорусской железной дороге, а также бронирование проездных билетов происходило по городским телефонным линиям силами справочных вокзалов. Это влекло за собой ряд неудобств для пассажиров и управления справочной службой: неконтролируемые наплывы звонков, частый сигнал «занято» при попытке дозвониться, невозможность масштабирования справочной службы, неудобства обслуживания разрозненных телефонных номеров. О таких вещах, как статистика звонков и запись разговоров, не было и речи. Поддержка и развитие справочной, работающей на устаревших технологиях, требовали больших финансовых и ресурсных затрат.

Так появилась необходимость глубокой модернизации службы с целью повышения качества обслуживания пассажиров. Вскоре было принято решение о создании контакт-центра Белорусской железной дороги на базе контакт-центра РУП «Могилевское отделение Белорусской железной дороги». К этому времени Могилевский контакт-центр обслуживал еще и Витебское отделение с поэтапной передачей функций по предоставлению справочной информации из других отделений.



Решение о внедрении телекоммуникационной платформы для контактного центра БЖД было принято для повышения качества обслуживания пассажиров и сокращения расходов на содержание устаревших телефонных систем. Подобные проекты закрепляют репутацию железной дороги как современной, технологичной и клиентоориентированной компании.

Благодаря нашим партнерам из Glare Global Communications, команде профессионалов с десятилетней отраслевой экспертизой, опытом проектирования и построения индивидуальных телекоммуникационных решений, мы смогли реализовать видеосвязь с пассажирами через стационарные терминалы, установленные на вокзалах.

Мы надеемся на дальнейшее сотрудничество и уверены в том, что с помощью команд Softline и Glare Global Communications сможем обеспечить пассажирам современный и качественный сервис при обращении в контактный центр железной дороги.

Первый заместитель начальника РУП «Могилевского отделения Белорусской железной дороги» С.В. Приставко

Задачи

После аудита телефонной и ИТ-инфраструктуры БЖД, пересмотра текущих процессов обслуживания пассажиров по телефону были сформированы задачи, которые предстояло решить в ходе реализации проекта по созданию единого контакт-центра:

1. Создание системы обслуживания пассажиров по единому номеру телефона 105.
2. Повышение производительности телефонной системы и проработка возможности обслуживания клиентов БЖД на территории страны.
3. Обеспечение отказоустойчивости систем контакт-центра.
4. Интеграция с системами фиксации обращений и бронирования билетов.
5. Внедрение удобных инструментов онлайн-мониторинга для супервизоров.
6. Настройка инструментов контроля работы контакт-центра для его руководителя.
7. Внедрение инновационного модуля видеотелефонии, позволяющего реализовать видеосвязь с пассажирами.

На конкурсной основе партнером по проекту была выбрана компания Softline, которая предложила лучшие условия по созданию контакт-центра на базе решения Glare Unified Communication Platform (CallWay) с оптимальным соотношением цены и качества.

Решение

«В процессе работы над проектом был проведен аудит и последующий реинжиниринг процессов обслуживания обращений, внедрен стандарт скорости обработки звонков, стандарт качества обслуживания. Для контроля стандартов обслуживания установлена и адаптирована под особенности проекта система отчетов: доступны отчеты как за прошедший период, так и в режиме реального времени. Выбранная телекоммуникационная платформа позволяет достаточно гибко настраивать индивидуальные графики и отчеты, работать с рейтингами операторов, а также выводить оперативную информацию о работе контакт-центра на информационную видео-стену».

Начальник контактного центра Белорусской железной дороги В.В. Гаврилова

Подробный анализ задач с поправкой на действующие процессы и существующую инфраструктуру позволил выполнить внедрение в максимально сжатые сроки. В марте 2018 года контакт-центр Белорусской железной дороги был запущен в предтестовую эксплуатацию, одновременно с передачей ему функции обслуживания Гомельского отделения. На подготовку

каналов связи, настройку серверной части телеком-платформы, составление планов распределения звонков и включение ушло около месяца, при этом большинство работ было выполнено удаленно. Уже в мае 2018 года персонал созданного контактного центра начал работать с полнофункциональным комплексом.
07 июля 2018 года все запланированные задачи проекта были решены и контакт центр был переведен в промышленную эксплуатацию. После его открытия специалистами Softline и Glare Global Communications проведен технический аудит с целью получения дорожной карты последующего развития проекта.

«Особое внимание при внедрении уделили функциям мониторинга и контроля. Так, была произведена установка информационной панели, на экран которой в режиме реального времени выводятся сведения о поступивших звонках, времени их приема и обработки, проценте пропущенных звонков, рейтинге операторов. Супервизорам настроен доступ к онлайн-мониторингу и статистике звонков с их рабочих мест».

Руководитель проекта Е.А. Куцев

Сложности в процессе реализации проекта

Ранее возникшая проблема не позволяла реализовать видеотелефонию для обеспечения звонков из интерфейса установленных на вокзалах терминалов в интерфейс оператора контакт-центра. В ходе работы над проектом удалось найти способ обойти аппаратные ограничения терминальных устройств и реализовать видеосвязь с пассажирами к дате официального запуска контакт-центра.

Результат

Специалистами Softline и Glare Global Communications было внедрено новейшее программное обеспечение для контакт-центра на базе решения Glare Unified Communication Platform (CallWay), обеспечена высокая отказоустойчивость ИТ-системы, создана гибкая и масштабируемая виртуализированная инфраструктура.
Программная платформа для контакт-центра позволила:

- создать единый стандарт решения вопросов организации пассажирских перевозок;
- оперативно консультировать клиентов по телефону и оказывать помощь в разрешении необходимых вопросов;
- повысить доступность услуг БЖД для лиц с ограниченными физическими возможностями;
- повысить качество обслуживания и лояльность пассажиров.

На текущий момент контакт-центр Белорусской железной дороги успешно запущен и ежедневно обслуживает около 5 тыс. обращений.
Специалисты Softline и Glare Global Communications предоставляют поддержку операторам, руководителям и техническим специалистам контактного центра в режиме 24/7/365.

«Мы довольны проделанной работой. Всегда приятно запускать такие значимые проекты в срок и видеть удовлетворенных клиентов. Сразу после открытия контакт-центра мы приступили к планированию второго этапа работ с целью развития и улучшения достигнутого результата. В будущем планируем предложить БЖД развивать интеллектуальные сервисы для автоматизации процессов обслуживания пассажиров.
Благодарим наших партнеров – компанию Softline – за возможность реализовать такой интересный и масштабный проект. Благодарим специалистов Могилевского отделения Белорусской железной дороги за сложные задачи и активное содействие в ходе работы над его внедрением. Еще многое предстоит сделать, и мы уверенно смотрим вперед!» ■

Директор по продажам
в государственном секторе
Glare Global Communications
Р.А. Бондаренко

softline® 25 Years in IT

Microsoft

ОПТИМИЗИРУЙТЕ ИТ-ИНФРАСТРУКТУРУ НА БАЗЕ МУЛЬТИПЛАТФОРМЫ AZURE

Microsoft Azure — это постоянно расширяющийся набор облачных служб, который помогает вашей организации решать бизнес-задачи. Это свобода создания, развертывания приложений и управления ими в обширной глобальной сети с использованием ваших любимых инструментов и платформ.

Продуктивность

Сократите время выхода ваших продуктов и услуг на рынок с помощью более чем 150 готовых сервисов.

Интеллект

Создавайте интеллектуальные приложения, используя мощные службы обработки данных и искусственного интеллекта.

Гибридная среда

Разрабатывайте и развертывайте в удобном для вас месте с помощью единственного согласованного гибридного облака на рынке.

Надежность

Присоединяйтесь к стартапам, правительственным организациям и 90 % компаний из списка Fortune 500, которые уже используют Microsoft Cloud.

70+ соответствий требованиям и законодательным нормам – наибольшее количество в отрасли

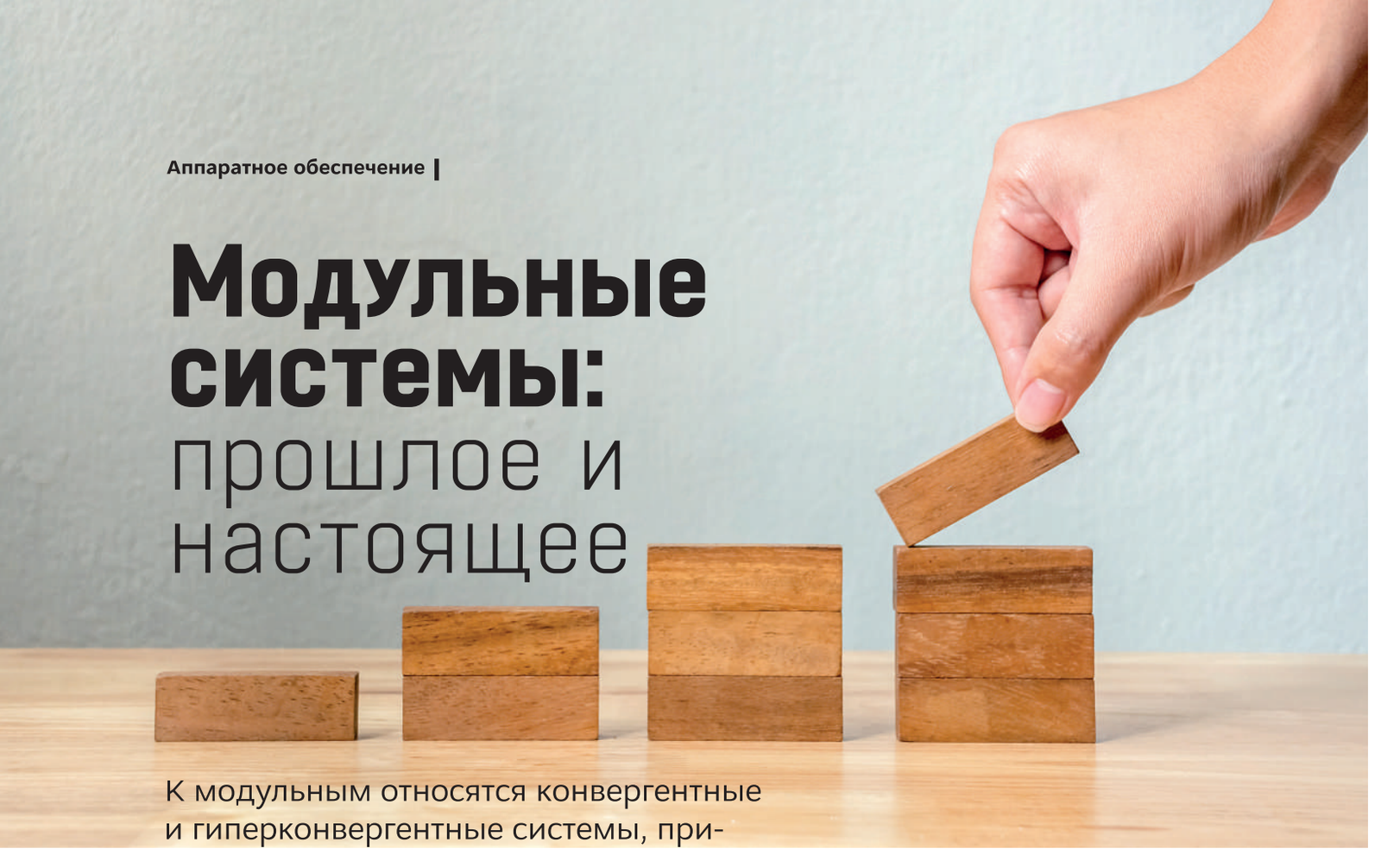
50 регионов Azure по всему миру — больше, чем у любого другого поставщика облачных решений

90% компаний из списка Fortune 500 доверяют свой бизнес Microsoft Cloud

+375 17 336-55-95 MS.belarus@softlinegroup.com azure.softlinecloud.by

Azure

Модульные системы: прошлое и настоящее



К модульным относятся конвергентные и гиперконвергентные системы, призванные упростить жизнь техническим специалистам, поддерживающим ИТ-инфраструктуру, и сократить стоимость владения ИТ для бизнеса.

При создании ИТ-инфраструктуры необходимо тщательно проектировать все составляющие: системы компьютерных вычислений, хранения и передачи данных, всю сетевую обвязку. При этом нужно многое просчитывать, увязывая разные факторы. Когда речь идет о небольших компаниях, это не является очень сложной задачей, хотя тоже может вызвать определенные затруднения. Но когда дело касается средних и крупных компаний, то все сильно усложняется.

Дело в том, что вендоры, как правило, специализируются на одном или нескольких определенных направлениях. У кого-то сильная сторона — СХД, у кого-то — серверное оборудование, а кто-то специализируется в основном на сетевых решениях. В результате ИТ-решения создаются из компонентов разных производителей. Это приводит к определенным сложностям, связанным, например, с администрированием и технической поддержкой ИТ-инфраструктуры. Отчасти решением проблемы стали конвергентные системы. За создание таких систем отвечает единственная компания, берущая на себя задачи расчета дисковых и серверных мощностей, подбора необходимых аппаратных компонентов, проектирование сетевой инфраструктуры, предустановку дополнительного ПО для автоматизации.

Первый этап развития: конвергентные системы

Конвергентные системы приобретаются как комплекс оборудования, необходимого для создания ИТ-инфраструктуры, вместе с программным обеспечением и технической поддержкой. У них очень короткий цикл пуско-наладки, и простая поддержка жизненного цикла. В случае, если с системой возникают какие-либо проблемы, решить их можно обратившись в общую (единую) техподдержку.

Наиболее известные решения — VCE vBlock и Cisco FlexPod.

Конвергентные решения масштабируются с помощью одинаковых модулей (коробок), включающих весь набор необходимых аппаратных и программных средств. Это обстоятельство является как их достоинством, так и недостатком. Для крупных компаний такая схема подходит, но для небольших и средних она неудобна. Модули стоят в 1,5-2 раза дороже самостоятельной сборки и каждый модуль означает значительное расширение системы, далеко не всегда оправданное. В Беларуси конвергентные системы не снискали популярность. Секрет их успеха в США и Европе заключается в высокой оплате труда ИТ-инженеров и серьезном влиянии профсоюзов. Компаниям проще переплатить производителям аппаратно-программных комплексов за дополнительные возможности автоматизации вместо того, чтобы расширять штат ИТ-специалистов. Для Беларуси эти проблемы не актуальны.

Второй этап развития: гиперконвергентные системы

Вместе с появлением технологий программно-определяемых СХД (Software-Defined Storage) появилось и новое понятие – гиперконвергенция. Характерная особенность гиперконвергентных решений — «кирпичиками» для строительства ИТ-инфраструктуры стали не блоки с набором СХД, серверов и сетевых устройств, а просто серверы с установленными на них гипервизорами. После того как появилась возможность создания высокопроизводительных отказоустойчивых подсистем хранения данных на локальных серверных накопителях, возможности по масштабированию компонентов ИТ-инфраструктуры перешли на качественно новый уровень.

Фактически достаточно отслеживать наличие свободных портов в коммутаторах доступа и просто приобретать, а потом добавлять новые серверы с локальными накопителями, получая «на лету» масштабирование кластера как по процессорам и оперативной памяти, так и по объему и производительности подсистемы хранения данных. Никаких пересчетов на дисках, перезагрузок, простоев в работе ИТ-сервисов – этим можно заниматься прямо в рабочее время. Учитывая низкий минимальный порог стоимости гиперконвергентных конфигураций, такие системы стали интересны даже малому бизнесу. Наиболее известные производители гиперконвергентных систем «под ключ» — HPE (SimpliVity) и Dell-EMC (VxRail), но в линейке продуктов компании VMware есть программное решение vSAN, которое практически не ограничивает заказчиков в выборе аппаратной платформы. Кстати, Dell-EMC VxRail используют в основе виртуализации СХД как раз VMware vSAN, так как VMware входит в группу компаний Dell-EMC.

Преимущества гиперконвергентных систем

- Просто внедряются и администрируются.
- Надежные и высокопроизводительные (All-Flash конфигурации выдают производительность, сравнимую с Mid-End СХД и даже выше!).
- Не просто легко, а беспрецедентно легко масштабируются.
- Программные продукты, в отличие от аппаратных, не подвержены амортизации. Серверы со временем меняются на новые, а ПО виртуализации всегда самой актуальной версии, со всеми самыми современными возможностями. Приобретаются только один раз, потом только продлевается подписка.

В 2017 году, который многие аналитики назвали «годом криптовалют», на рынке наблюдались серьезные проблемы с высокопроизводительными графическими картами. Не так давно мы выполнили проект, позволивший заказчику ощутимо сэкономить на покупке графических станций. Мы развернули гиперконвергентный кластер под VDI на 200+ пользователей, часть из которых являются проектировщиками, работающими с 3D-графикой. Серверные графические карты NVIDIA Tesla не так интересны для майнеров, и с их поставкой проблем не наблюдалось. В дополнение к экономии на графике и СХД заказчик получил все те возможности VDI, которые высоко ценятся ИТ-департаментами.

Дмитрий Галкин,
руководитель направления виртуализации

Для чего?

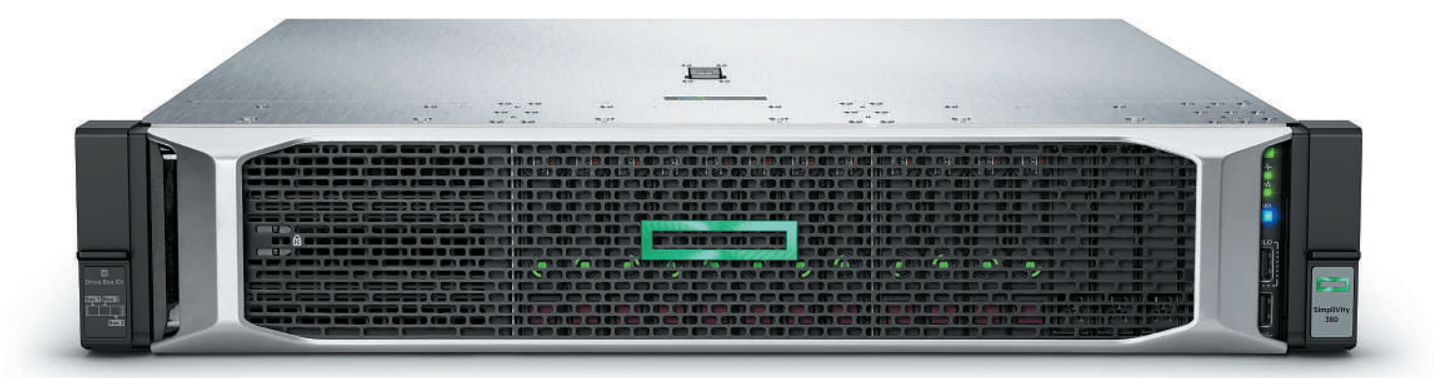
- Самый распространенный и выгодный сценарий использования — в инфраструктуре с виртуальными рабочими столами пользователей (VDI). Большое количество одинаковых виртуальных машин — легко посчитать требования к объему и производительности. Приходят новые сотрудники — создание для них рабочего места занимает минуты. Не хватает мощностей – добавляется еще один сервер и можно подключить дополнительно 100-150 пользователей.
- Гиперконвергентные системы - идеальный инструмент для создания катастрофоустойчивых конфигураций. Между двумя или несколькими площадками достаточно просто организовать растянутый кластер и получить единый виртуальный ЦОД без необходимости приобретения дорогостоящих СХД.
- Гиперконвергентные решения не подразумевают ограничений в использовании классических СХД. Например, для целей резервного копирования высокая производительность не так важна, как большие и недорогие объемы под хранение резервных копий и архивов. Обычные СХД вполне могут подключаться к тем же серверам и работать параллельно с виртуализированной СХД.

Гиперконвергентные системы Softline

Мы можем помочь подобрать аппаратную конфигурацию, программное обеспечение, соответствующее поставленным задачам. Готовы спроектировать, поставить и интегрировать систему «под ключ». Как правило, это уже на этапе внедрения стоит дешевле классических инфраструктурных решений, но если даже и сопоставимо, то стоимость владения правильно спроектированной гиперконвергентной ИТ-инфраструктурой позволит получить существенную экономию уже в перспективе ближайших 2-3 лет.

HPE SimpliVity
Гиперконвергентное решение

В отличие от традиционных решений из отдельных компонентов (серверов, хранилищ, резервного копирования), гиперконвергентная инфраструктура HPE SimpliVity сочетает все необходимые возможности в одном продукте. Поэтому такое решение проще, надежнее и обходится дешевле в эксплуатации.



Территориально распределенные узлы выполняют резервное копирование друг на друга или в центр. Благодаря глобальной дедупликации в SimpliVity, передача данных работает быстро даже на очень медленных каналах связи.

- **Простая стандартизованная платформа.** С решением SimpliVity не нужно проектировать решение, выбирать компоненты, и интегрировать их между собой. Вы покупаете один готовый к работе продукт. Поэтому инфраструктуру легко поддерживать.
- **Непрерывная работа приложений и надежная защита данных.** SimpliVity не имеет единой точки отказа, выполняет резервное копирование раз в 10 минут локально и между площадками и мгновенно восстанавливает виртуальные машины из бэкапа. Поэтому исключены простои систем при отказах оборудования.
- **Защита от выхода из строя площадки целиком.** Предлагаемая архитектура включает резервное копирование на удаленную площадку и возможность переключения на нее. При использовании традиционной, а не гиперконвергентной инфраструктуры для этого обычно требуется целый набор сложных и дорогих решений.
- **Экономия на эксплуатации.** По сравнению с классическим решением, SimpliVity занимает меньше места в ЦОД и не требует множества дорогих контрактов на поддержку целого стека продуктов. Поэтому обходится дешевле в использовании. ▮

По всем вопросам вас проконсультирует Александр Мигаль, специалист по продажам отдела консалтинга Softline.

+375 (17) 336-55-95 доб. 4421 | Alexander.Migal@softline.com

Специальное предложение:
скидка 20% на программный комплекс

VMware HCI Kit

Программный комплекс HCI Kit – самый экономичный способ внедрения гиперконвергированной инфраструктуры VMware.

VMware HCI Kit включает в себя платформу виртуализации серверов vSphere и хранилище данных vSAN. С его помощью можно запустить платформу с подключением стандартных серверов x86, обычных ресурсов сети. После завершения настроек и подключения создается централизованное хранилище данных, которое раскрывает все потенциальные возможности виртуализации без необходимости разработки отдельных систем хранения данных.

При покупке ПО необходимо приобретение услуги Subscription and Support (SnS).

Предложение действительно до 25 января 2019 г.

Сокращайте расходы и снижайте риски вместе с VMware HCI Kit!

По всем вопросам обращайтесь к Игорю Волокитину, специалисту по виртуализации Softline

Пишите: Igor.Volokitin@softline.com

Звоните: +375 (17) 336-55-95 доб. 4485

Планировать обучение заранее не только предусмотрительно, но и выгодно!

В этом году учебный центр Softline предлагает лучшие условия на целый ряд курсов Microsoft, Cisco, Oracle и Kaspersky Lab, чем когда-либо.
У вас есть возможность сэкономить до 30% стоимости по акции раннего бронирования обучения на курсах.

Список курсов, участвующих в акции, можно найти в расписании на сайте **http://edu.softline.by.**
Все участвующие в предложении курсы отмечены словом «АКЦИЯ!» в названии. Информация об условиях продублирована на страницах всех соответствующих курсов.
Общие условия акции:

- при оплате курса не позднее чем за 2 месяца до планируемой даты начала предоставляется 30% скидка на обучение;
- при оплате курса не позднее чем за 1 месяц до планируемой даты начала предоставляется 20% скидка на обучение;
- при оплате курса не позднее чем за 2 недели до планируемой даты начала предоставляется 10% скидка на обучение.

Внимание! Условия по данной акции не суммируются с иными возможными скидками на обучение, а также не распространяются на корпоративные закрытые группы.

Новые курсы по информационной безопасности

Компания Softline представляет два новых курса: «Безопасность облачных вычислений (Cloud Security)» и «Защита коммерческой тайны и организация конфиденциального делопроизводства». Занятия будет вести Вячеслав Аксенов, инструктор по информационной безопасности Softline.

Курс «Безопасность облачных вычислений (Cloud Security)»
Использование технологий облачных вычислений становится тенденцией во всем мире. В Республике Беларусь постановление создать республиканскую платформу, действующую на основе технологий облачных вычислений, содержится в Указе Президента Республики Беларусь от 23 января 2014 года № 46. Согласно Указу, государственные органы и организации должны осуществить до 31 декабря 2018 года поэтапный переход на использование ресурсов республиканской платформы в соответствии с планом перехода, утверждаемым ОАЦ при Президенте РБ.

Однако вместе с очевидными преимуществами, использование технологий облачных вычислений для организаций приводит к необходимости решения следующих задач:

- Проектирование и создание систем защиты информационных систем, размещенных в облаке.
- Обеспечение информационной безопасности при использовании облачных услуг.
- Распределение ответственности между участниками информационных отношений, возникающих при использовании/предоставлении облачных услуг.
- Подтверждение соответствия системы защиты информации информационных систем, размещенных в облачной инфраструктуре, требованиям законодательства об информации, информатизации и защите информации.

В программу нового курса «Безопасность облачных вычислений (Cloud Security)» входит изучение способов решения вышеперечисленных задач и практических аспектов обеспечения безопасности облачных вычислений с учетом требований действующего законодательства Республики Беларусь об информации, информатизации и защите информации.

Курс «Защита коммерческой тайны и организация конфиденциального делопроизводства»

В рамках нового курса основное внимание уделяется практическим аспектам реализации механизмов защиты коммерческой тайны, определенных Законом Республики Беларусь от 5 января 2013 г. № 16-З «О коммерческой тайне» и другими нормативными правовыми актами.

На занятиях слушатели рассмотрят:

- Требования законодательства Республики Беларусь в области защиты коммерческой тайны и организации конфиденциального делопроизводства.
- Порядок установления, изменения и отмены режима коммерческой тайны организации.
- Практические вопросы разработки внутренних регламентов и документов, обеспечивающие реализацию режима коммерческой тайны.
- Подход к организации конфиденциального делопроизводства.
- Практические аспекты технической и криптографической защиты коммерческой тайны.

Новые версии [v6.7] популярных курсов VMware

После объявления о выходе новой версии платформы

vSphere 6.7 компания VMware обновила и линейку курсов. Учебный центр Softline уже начал проводить занятия на авторизованных курсах вендора по работе с vSphere 6.7:

- «VSICM 6.7 VMware vSphere: установка, настройка, управление [v6.7]»
- «VSOS 6.7 VMware vSphere: оптимизация и масштабирование [v6.7]»

Для специалистов, ранее прошедших обучение по предыдущим версиям VMware vSphere, доступен курс, освещающий новые возможности платформы:

- «VSWN 6.7 VMware vSphere: что нового [с версии v5.5 к v6.7]»

Учебный центр Softline является авторизованным партнером VMware по обучению (VMware Authorized Training Center), что означает следующее:

- Курсы проводятся сертифицированным специалистом, обладающим широкими знаниями и практическими навыками по данной тематике.
- Программа обучения создана специалистами VMware, и слушатели получают авторизованные обучающие пособия. Таким образом компания VMware осуществляет тщательный контроль качества всего обучения и предоставляет слушателям самую актуальную информацию.
- После прохождения курсов слушатели получают сертификат VMware, признаваемый во всех странах мира, и могут попытаться сдать экзамены на статус сертифицированного профессионала в центре тестирования Pearson VUE.

Связаться со специалистами учебного центра Softline, а также с администратором центра тестирования Pearson VUE вы можете по телефону **+375(17)216-18-66** или отправив заявку по электронной почте **edu.by@softline.com.**

Новое направление обучения – процессное управление

Учебный центр Softline предлагает новое направление курсов по разработке и внедрению систем менеджмента управления качеством, ИТ-услугами и информационной безопасностью на основе стандартов ISO. На данный момент в нашем каталоге уже есть три новых курса:

- «Системы менеджмента качества. Переход на новую версию ISO 9001:2015» (3 дня/24 ак. часа).
- «Разработка и внедрение системы менеджмента ИТ-услугами на основе требований ISO/IEC 20000-1» (3 дня/24 ак. часа).
- «ISO/IEC 27001:2013. Разработка и внедрение системы менеджмента информационной безопасности» (3 дня/24 ак. часа).

Обучение ITIL – не только теория, но и практика

Учебный центр Softline предлагает новый курс по основам ITIL, который включает:

- Теоретическую часть, формирующую понимание ITSM (IT Service Management) как подхода к управлению ИТ, и дающую общее знакомство с библиотекой ITIL.
- Бизнес-игру и практикум, которые позволят участникам наглядно смоделировать ситуации, возникающие в организации ИТ-деятельности компании и предложить варианты их решения.

Чтобы подробнее узнать о курсе смотрите программу «Основы ITIL. Практика внедрения» на сайте **http://edu.softline.by.**

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
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
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
10748	Планирование и развертывание System Center 2012 Configuration Manager	3 /24
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

Код	Название курса	Дни/часы
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	4 /32
BI-Excel-Adv	Бизнес-аналитика средствами Microsoft Excel, Power BI и Power BI Desktop	4 /32
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	Реализация мультипротокольной коммутации с использованием меток в сетях Cisco	5 /40
BGP	Настройка BGP на маршрутизаторах Cisco	5 /40
IP6FD	Основы протокола IPv6, дизайн и построение сетей на его основе	5 /40
Oracle		
12cDBA	Администрирование Oracle Database 12c	5 /40
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
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 веб-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

Код	Название курса	Дни/часы
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 6.7	VMware vSphere: установка, настройка, управление [V6.7]	5 /40
VSWN 6.7	VMware vSphere: что нового [с версии V5.5 к V6.7]	3 /24
VSOS 6.7	VMware vSphere: оптимизация и масштабирование [V6.7]	5 /40
VHICM 7.3	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
ITIL-Practice	Основы ITIL. Практика внедрения	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
КТ	Защита коммерческой тайны и организация конфиденциального делопроизводства	2 /16
CS	Безопасность облачных вычислений (Cloud Security)	3 /24

Полный каталог курсов и подробные программы обучения вы можете найти на нашем сайте **http://edu.softline.by**
Получить дополнительную информацию по курсам можно по телефону **+375 (17) 216-18-66** или e-mail **edu.by@softline.com**

Учебный центр Softline – то, что нужно для развития!

Учебный центр Softline – это:

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

85% клиентов обращаются к нам повторно

Лучший выбор авторизованных курсов

Мы обучили более 5 000 слушателей

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

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

Расписание курсов смотрите на сайте edu.softline.by

softline®

Курсы

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

Сертификация

KASPERSKY 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) 336-55-95 | www.softline.by