softline direct

КАТАЛОГ ИТ-РЕШЕНИЙ И СЕРВИСОВ ДЛЯ БИЗНЕСА

СПЕЦ
09
2018
ВЫПУСК

Исследование:
потребление облачных услуг российскими компаниями

Hardware as a Service

Путеводитель по Google Cloud

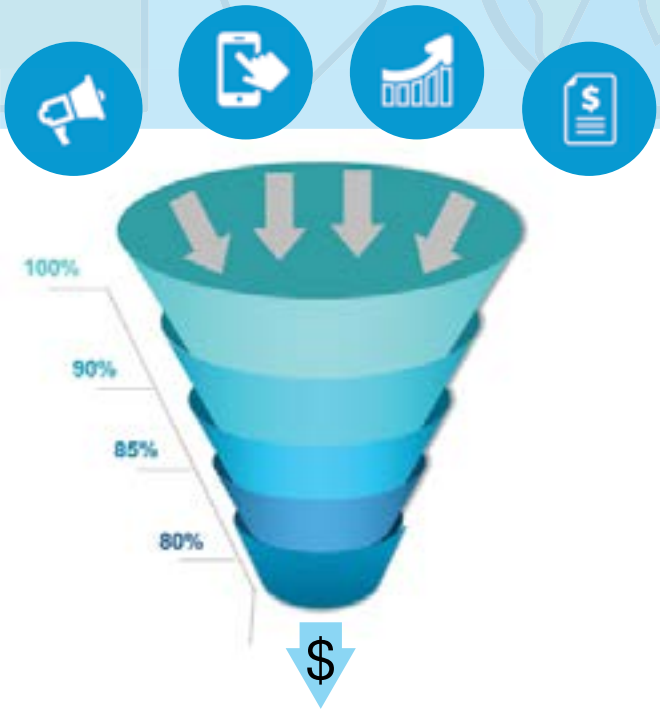
Безопасность в облачной среде

ИТ-ИНФРАСТРУКТУРА В АРЕНДУ от сервера до приложения

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

Allsoft Ecommerce

Увеличиваем ваши интернет-продажи с 2004 года



Обеспечим рост продаж минимум на **15%**

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

Нам доверяют:

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

и еще более 100 клиентов

Свяжитесь с нами: dev@allsoft.ru

Уважаемые коллеги, друзья!

Консерватизм в отношении технологий в наши дни – прямой путь к самоликвидации бизнеса. Новые подходы и решения взамен устаревших – это и есть цифровая трансформация, о которой так много говорят сегодня. Благодаря ей мы выходим на качественно новый ритм жизни и работы, а двигателем новой технологической революции является модель потребления ИТ в формате сервиса, без приобретения в собственность железа и софта.

Эта модель дает возможность эффективно решать задачи бизнеса: на сегодняшний день уровень развития сервисов позволяет заменить ими практически любую часть инфраструктуры, сэкономив при этом существенную часть ИТ-бюджета. **Наша задача – предоставлять заказчикам в аренду все компоненты ИТ, от сервера до приложения** и помочь им в полной мере реализовать все новые возможности и преимущества. Важнейшими среди них я считаю общедоступность решений уровня enterprise, прежде дорогих и доступных только крупнейшим богатым компаниям, экономическую эффективность (в облаке почти всегда дешевле) и широкую свободу творчества и развития, не ограниченную собственными ИТ-системами.

Стратегия Softline на ближайшие годы опирается именно на предоставление ИТ в аренду. Наши главные союзники в этом – ведущие разработчики технологий: Microsoft, Google, Amazon, VMware, Amazon, SAP, VMware, Cisco, Dell-EMC и многие другие. Они однозначно связывают свое настоящее и будущее с облаком, с моделью аренды ИТ, с аутсорсингом. А Softline – это команда профессионалов с глубокими знаниями и обширным опытом практического применения новых подходов и технологий. Наш экспертный уровень подтверждают многочисленные статусы вендоров и отзывы сотен заказчиков, уже оценивших преимущества ИТ в аренду.

Я приглашаю вас к сотрудничеству. Мы поможем вам пересмотреть ваш бизнес и разобраться, какие шаги можно предпринять, чтобы сделать вашу работу прибыльней, проще, прозрачней и стабильней, чтобы экономить время и деньги, снижать риски и освобождать драгоценное время и силы для развития и творчества. Сегодня экономика каждый день бросает вызовы бизнесу, и слоган «трансформируйся или умри» звучит уже не как отдаленная угроза, а как призыв к скорейшим действиям.

Каталог
ИТ-решений
и сервисов
для бизнеса

Softline
direct

#09-2018

2018-9(187)–RU

Учредитель:
АО «СофтЛайн Трейд»

Издатель:
Игорь Боровиков

Главный
редактор:
Максим Туйкин,

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

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

Над номером
работали:
Мария Михеева,
Мария Агаркова,
Светлана
Распутина,
Наталья
Пичужкина,
Ирина
Галактионова,
Екатерина Корбун,
Анатолий Герцен,
Александр
Сухарев,
Александр
Ефремов,
Елена Катасонова,
Наталья Решетова,
Екатерина
Паршикова,
Александр
Макаров, и др.

Тираж: 60 000 экз.

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

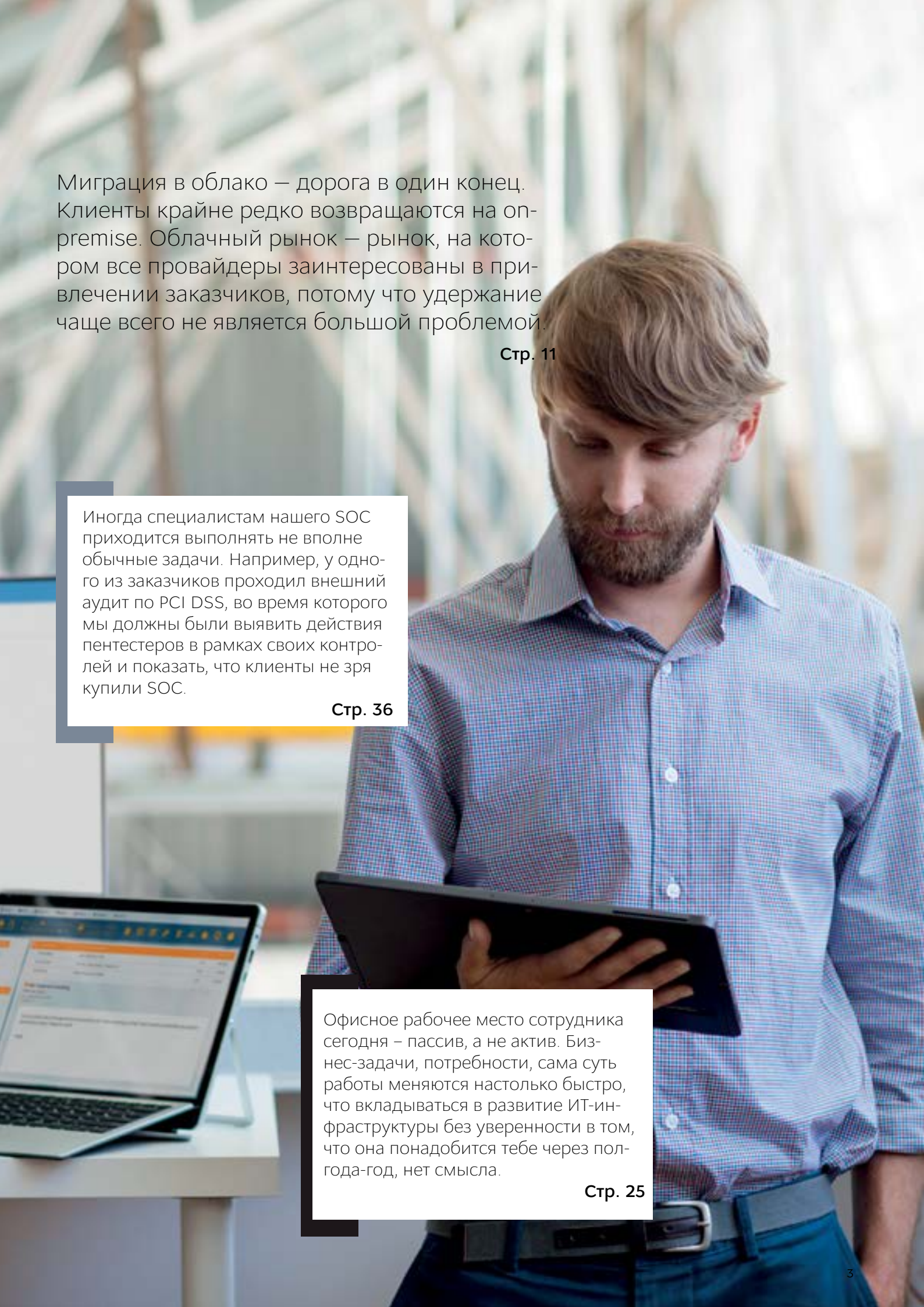
СОДЕРЖАНИЕ

DeviceLock DLP

СПЕЦИАЛЬНЫЙ ВЫПУСК: **ИТ-инфраструктура в аренду от сервера до приложения**

Softline в соцсетях

SoftlineCompany Softlinegroup SoftlineCompany softlinegroup



Миграция в облако — дорога в один конец. Клиенты крайне редко возвращаются на on-premise. Облачный рынок — рынок, на котором все провайдеры заинтересованы в привлечении заказчиков, потому что удержание чаще всего не является большой проблемой.

Стр. 11

Иногда специалистам нашего SOC приходится выполнять не вполне обычные задачи. Например, у одного из заказчиков проходил внешний аудит по PCI DSS, во время которого мы должны были выявить действия пентестеров в рамках своих контролей и показать, что клиенты не зря купили SOC.

Стр. 36

Офисное рабочее место сотрудника сегодня – пассив, а не актив. Бизнес-задачи, потребности, сама суть работы меняются настолько быстро, что вкладываться в развитие ИТ-инфраструктуры без уверенности в том, что она понадобится тебе через полгода-год, нет смысла.

Стр. 25

ПОРТРЕТ КОМПАНИИ

Наша миссия

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

ПОЧЕМУ SOFTLINE?

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

Digital Transformation and Cybersecurity Solution Service Provider

Статусы Softline

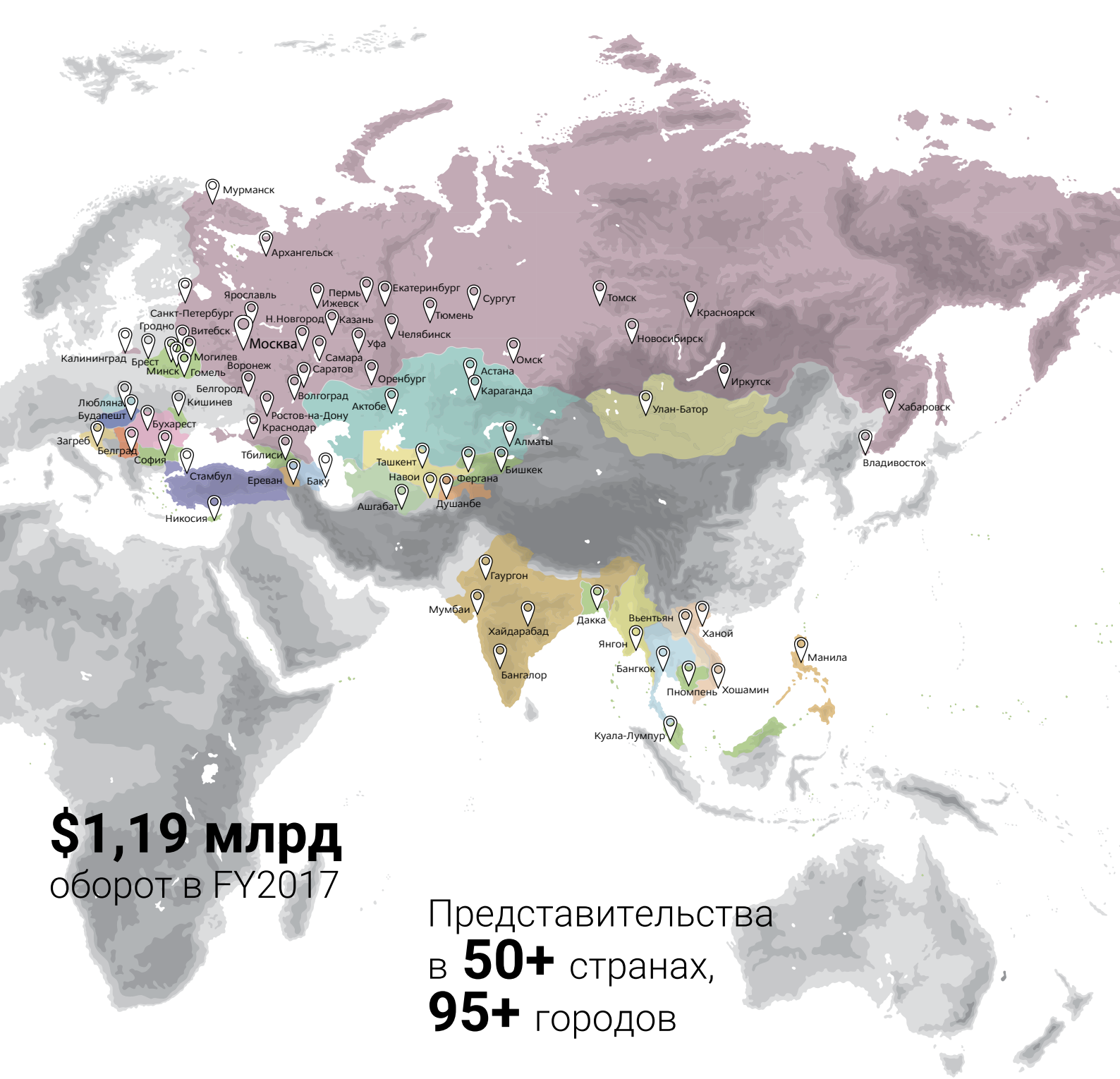
Microsoft Partner

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

Kaspersky ENTERPRISE PARTNER · Oracle Platinum Partner · VMware Partner · Gold Partner

Authorised Systems Integrator · IBM · Intel Software Elite Reseller · Citrix Partner Platinum Solution Advisor

Acronis Gold Partner · Veritas · APC · Corporate Premier Partner



$1,19 млрд
оборот в FY2017

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

+30% рост в FY2017
по группе компаний

25 лет
на ИТ-рынке

НАШИ ЗАКАЗЧИКИ

от стартапов до транснациональных корпораций

ПРОИЗВОДСТВО И ЭНЕРГЕТИКА

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

3000+ поставщиков программного и аппаратного обеспечения

РИТЕЙЛ, УСЛУГИ

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

БАНКИ, ФИНАНСОВЫЕ ОРГАНИЗАЦИИ

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

softline®

25 Years in IT

60 000 + корпоративных заказчиков

ТЕЛЕКОММУНИКАЦИИ, СМИ, РАЗВЛЕЧЕНИЯ

МТС | МегаФон | Telefonica | TELE2 | Ucell | Supercanal | Al Jazeera Turk | Ростелеком

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

ГОСЗАКАЗЧИКИ

РЖД | Рособоронэкспорт | POS Malaysia | Росатом | Роснано | ВЦИОМ

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

600+ технических специалистов

1100 аккаунт-менеджеров

НЕФТЕГАЗОВАЯ ОТРАСЛЬ

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

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

Исследование Softline

Потребление облачных услуг российскими компаниями

Цель настоящего исследования – сделать более открытым рынок облачных услуг, на котором ГК Softline занимается долю порядка 30% (по собственным оценкам). В периметр исследования вошли более 500 компаний – клиентов Softline.

Выводы, сделанные в рамках документа, получены в рамках эмпирического подхода: авторы изучили обезличенные данные более чем 1 тыс. проектов, в которых были применены облачные сервисы крупных вендоров, а также набор сервисов Softline Cloud.

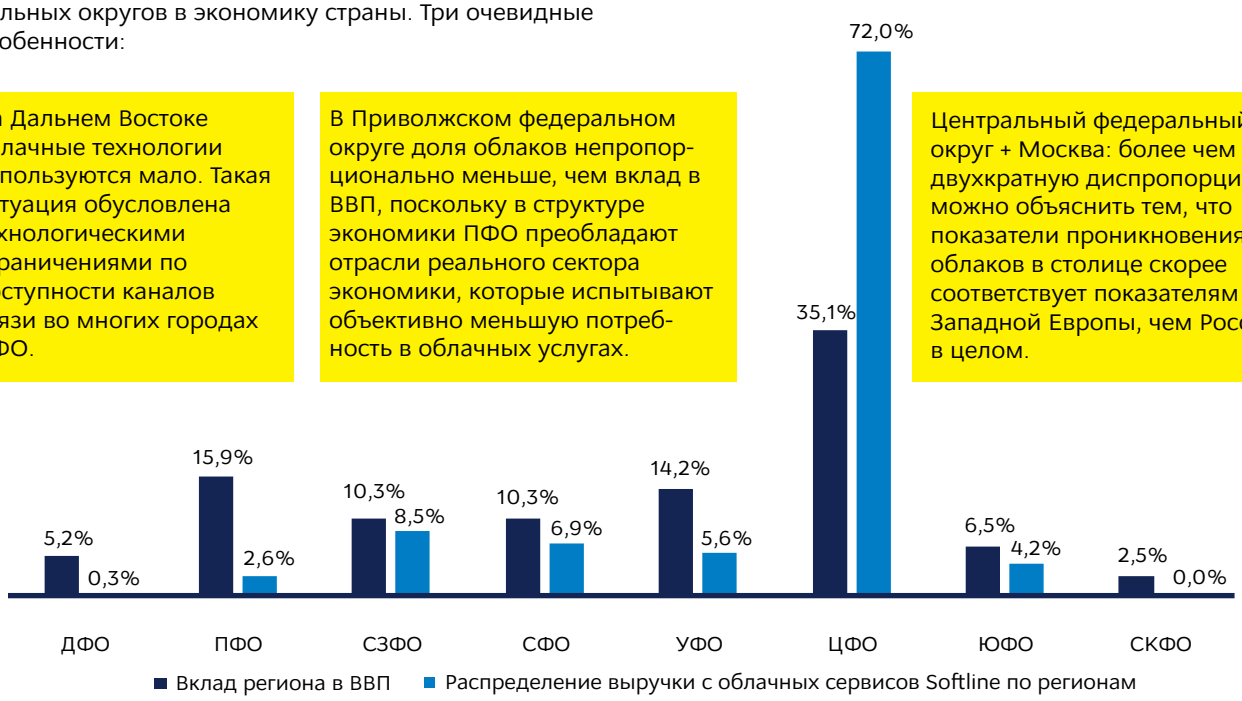
1. Региональное распределение заказчиков облаков

Структура распределения заказчиков по географическому признаку в целом соответствует вкладу федеральных округов в экономику страны. Три очевидные особенности:

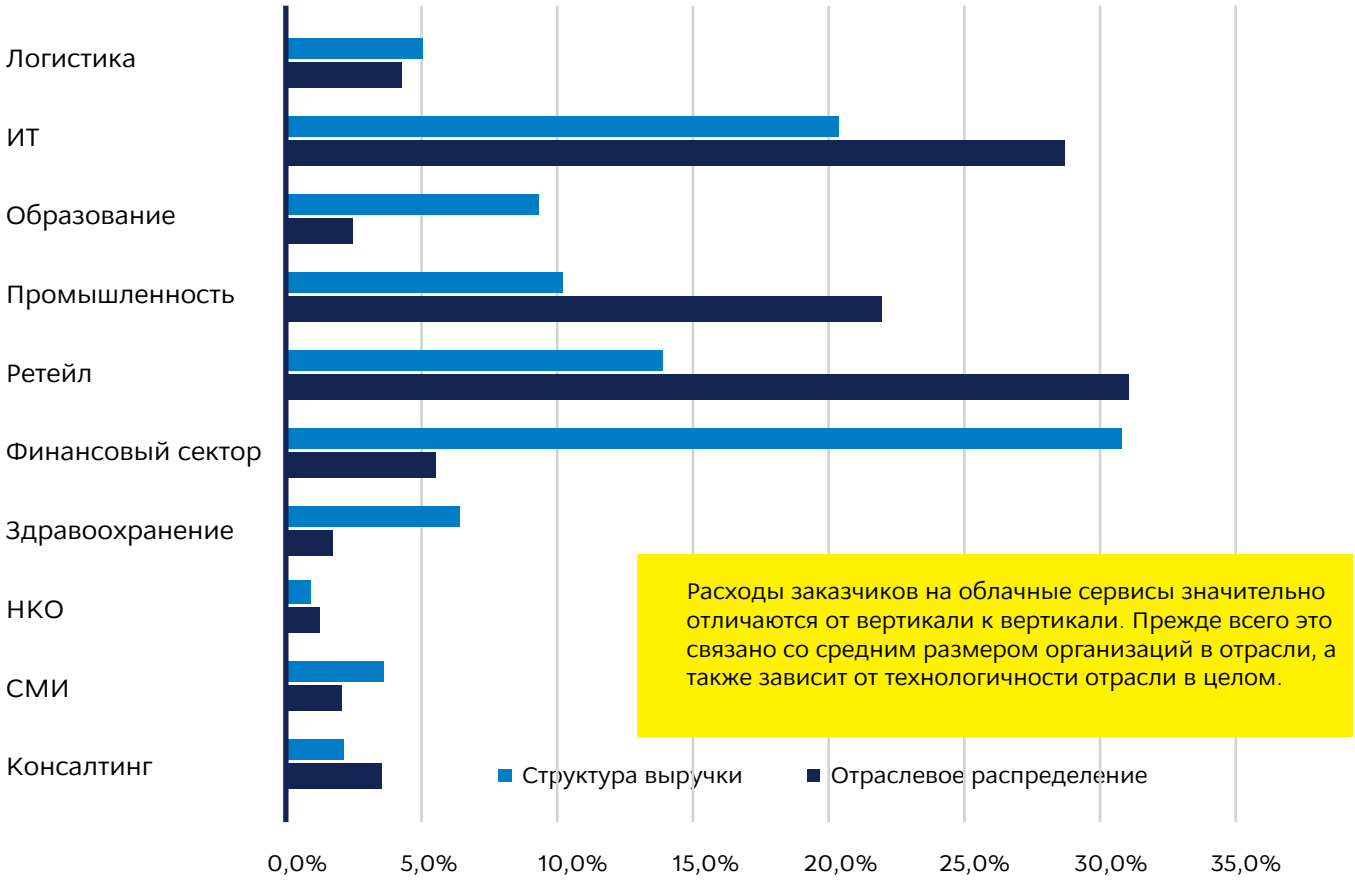
На Дальнем Востоке облачные технологии используются мало. Такая ситуация обусловлена технологическими ограничениями по доступности каналов связи во многих городах ДФО.

В Приволжском федеральном округе доля облаков непропорционально меньше, чем вклад в ВВП, поскольку в структуре экономики ПФО преобладают отрасли реального сектора экономики, которые испытывают объективно меньшую потребность в облачных услугах.

Центральный федеральный округ + Москва: более чем двухкратную диспропорцию можно объяснить тем, что показатели проникновения облаков в столице скорее соответствует показателям Западной Европы, чем России в целом.

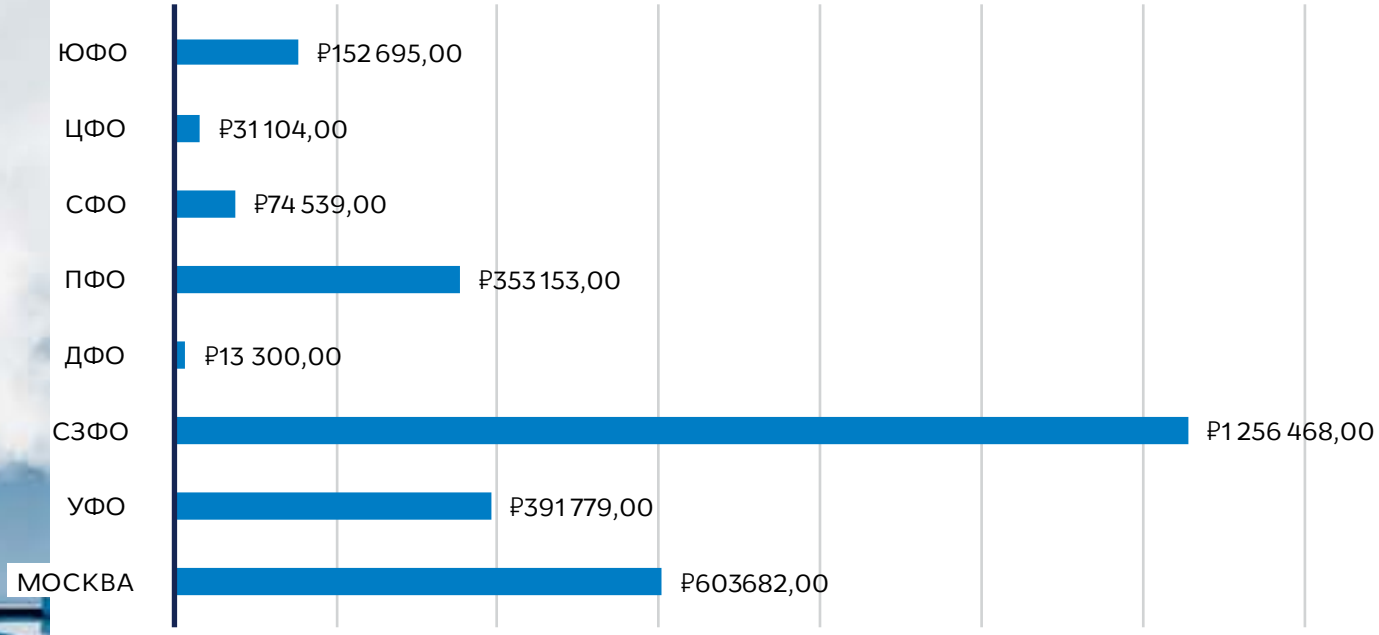


2. Отраслевое распределение заказчиков облаков в портфеле Softline и структура выручки



Расходы заказчиков на облачные сервисы значительно отличаются от вертикали к вертикали. Прежде всего это связано со средним размером организаций в отрасли, а также зависит от технологичности отрасли в целом.

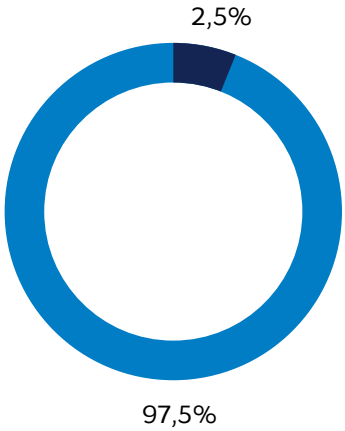
3. Средний чек по регионам, руб.



Самый значительный средний чек демонстрируют заказчики Softline в Северо-Западном федеральном округе. Этот вывод стал неожиданным даже для авторов исследования. Лидерство СЗФО в плане среднего чека можно объяснить близостью к Европе и более европейским бизнес-укладом, предусматривающим более широкое использование облачных технологий.

4. Мультиоблачность (по данным Softline Cloud)

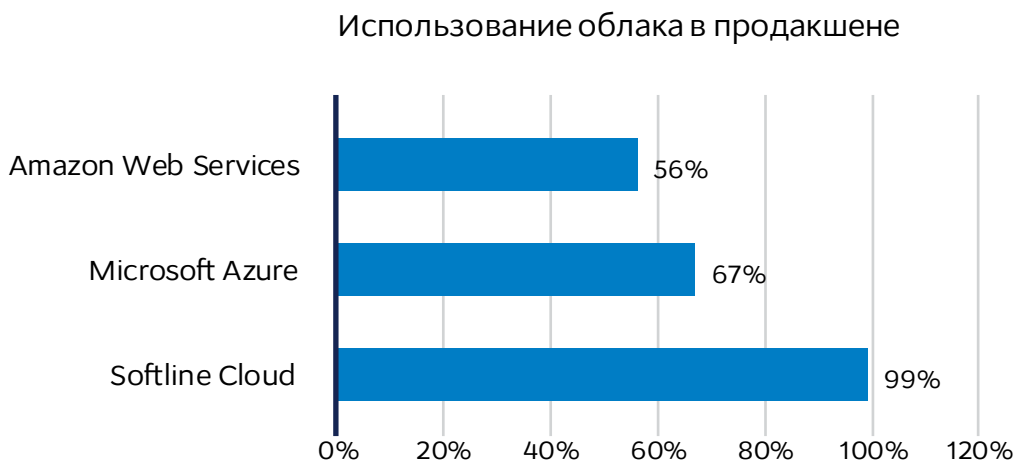
Под мультиоблачностью авторы исследования понимают использование одним заказчиком облаков разных вендоров. Клиенты Softline Cloud не демонстрируют повышенного интереса к мультиоблачности. Вероятно, таким образом реализуется сценарий, связанный с дублированием информационных систем либо их частей (например, баз данных или резервных копий production-систем) в российских облаках.



Использует ли заказчик мультиоблачность?

Да Нет

5. Тестирование или продакшен?

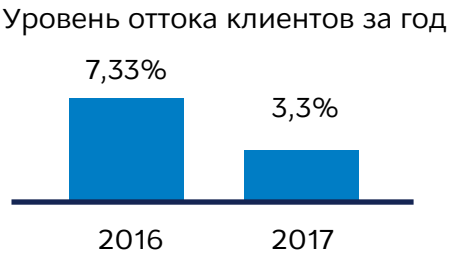


Еще одно неожиданное открытие, полученное в рамках исследования. Распространенный на рынке тезис «облака – только для тестирования», равно как и тезис о том, что компании переводят в облака только третьестепенные ИТ-системы, не подтверждаются. В основном в облаке размещают как раз продакшен-системы.

6. Бизнес-критичные системы в облаке

Согласно данным исследования, в облако компании переносят ERP, включая бизнес-критичные системы (27%), почту (7,5%) и специализированные отраслевые приложения (например, медицинские, страховые и др.). Популярность облаков для ERP-систем обусловлена потребностью этих систем в новых ресурсах, обеспечивать которую в рамках собственной инфраструктуры довольно дорого. Кроме ERP в облака переносят специализированные приложения, в которых есть большие базы данных, и которые предъявляют высокие требования к ресурсам.

7. Динамика оттока клиентов



Миграция в облако — дорога в один конец. Клиенты крайне редко возвращаются на on-premise. Облачный рынок — рынок, на котором все провайдеры заинтересованы в привлечении заказчиков, потому что удержание чаще всего не является большой проблемой.

Авторы исследования

Сергей Самоукин
заместитель руководителя департамента облачных технологий ГК Softline

Владимир Егорычев
руководитель группы регионального развития Департамента облачных технологий Softline

HP DaaS от Softline:

рабочие места и периферия под ключ

Компания HP разработала услугу Device-as-a-Service (DaaS), по которой Softline стала ее первым сертифицированным партнером. Этот сервис представляет собой не только аренду оборудования, а целый комплекс решений по выполнению бизнес-задач, позволяющих компании высвободить свои финансовые и кадровые ресурсы для основной деятельности. О ключевых преимуществах и особенностях сервиса рассказал Василий Ларионов, руководитель направления продаж услуг HP Inc.

С какими проблемами сегодня сталкиваются руководители ИТ-отделов, решившие значительно расширить парк корпоративных устройств?

Руководители ИТ-отделов сталкиваются с большим числом проблем, даже если парк устройств остается неизменным с точки зрения их количества.

Например, одна из распространенных проблем – гетерогенность парка устройств. Как правило, у организаций среднего и большого размера наблюдаются следующие типовые ситуации:

- Устройства разных производителей с различными уровнями сервиса и условиями обслуживания
- Разнообразные форм-факторы устройств: от настольных ПК до планшетов
- Различные операционные системы: от Windows до iOS/Android.

Как следствие, нагрузка на ИТ-отделы приходится колоссальная, так как централизованно управлять всем этим парком устройств крайне сложно: требуется много ресурсов, знаний и опыта.

Большинство организаций с этим не справляется. В качестве доказательства этого факта мы видим рост числа взломов и проникновений через устройства пользователей. Все прекрасно помнят, какое количество крупных и уважаемых компаний в России и за ее пределами стали жертвами ransomware под названием Petya. И это неудивительно.

Возвращаясь к вопросу про рост числа устройств, - ситуация выглядит здесь вдвойне критичной: согласно прогнозам аналитических агентств, к 2020 году на каждого сотрудника в среднем будет приходиться 4 устройства. И каждое устройство будет со своей ОС и своими особенностями в обслуживании. И это еще один серьезный вызов для компаний и их ИТ-специалистов.

Как сервис HP DaaS может обеспечить безопасность использования корпоративных устройств?

Приобретая устройства и услуги через сервис HP DaaS, организации получают в свое распоряжение виртуального помощника – это сервисные специалисты HP. В их функционал входит большое число задач по разгрузке ИТ-отделов клиента, а также по защите устройств.

Специалисты HP помогут выстроить политики безопасности и будут отслеживать их соблюдение. К примеру, внештатными ситуациями, когда HP может прийти на помощь, могут быть:

- Кража или потеря устройств: HP может удаленно заблокировать или полностью стереть все данные, чтобы избежать утечки информации.
- Управление обновлениями ОС и ПО для безопасности: устройства с необновленными ОС – излюбленная цель для злоумышленников.
- Соблюдение политик по шифрованию носителей информации.
- Удаленная настройка доступа в корпоративные точки Wi-Fi без раскрытия паролей доступа: кстати, очень распространенная проблема, из-за которой многие компании не переходят на беспроводные сети.

Какие вы бы выделили преимущества этой услуги, отличающие ее от других подобных сервисов?

DaaS — это больше, чем программа финансирования, такая как, например, «ПК как услуга», которую предоставляют другие производители. Услуга DaaS предоставляет комплексное решение, включающее в себя устройства и аксессуары, точно подобранные под каждую компанию. В рамках этой услуги мы предоставляем возможности поддержки, аналитики и централизованного управления конечными устройствами в течение всего их жизненного цикла. При этом модель оплаты является прозрачной и рассчитывается на основе единой цены за устройство. Гибкость услуги позволяет подобрать необходимые условия и цикл обновления устройств под конкретные нужды бизнеса.

Одной из уникальных и ценных составляющих тарифных планов DaaS является услуга аналитики и упреждающего централизованного управления конечными устройствами, предоставляемая высококвалифицированными специалистами HP. Она позволяет оптимизировать мониторинг парка устройств и управление ими, уменьшая время простоя конечных пользователей и повышая эффективность работы ИТ-отдела. Вы можете делегировать большую часть управления повседневными процессами специалистам HP, чтобы ваши сотрудники посвящали больше времени работе над проектами, которые способствуют развитию бизнеса. Технологии HP помогут оптимизировать использование ИТ-ресурсов компании.

В чем заключается услуга управления жизненным циклом устройств пользователей?

Мне очень нравится одна аналогия. Представьте себе огромный айсберг. Как известно, то что мы видим над водой – это всего лишь небольшая часть этого айсберга, а львиная доля находится вне нашего поля зрения. Так вот, большинство организаций фокусируется на видимой части айсберга – на закупках. Погруженная в воду и невидимая зрению часть – это стоимость владения устройством: затраты на различные этапы жизни устройств. Среди эти затрат, к примеру:

- Логистика, управление заказами и развертывание устройств.
- Гибкая настройка устройств под нужды пользователей (загрузка корпоративных образов системы, настройка BIOS или периферийных портов).
- Оптимизация производительности устройств.
- Поддержка работоспособности, реагирование на инциденты.
- И много других аспектов, включая вывод устройств из основных средств, удаление всей информации с носителей и дальнейшей утилизации.

Как правило, в организациях разными этапами жизни занимаются разные отделы, каждый со своим бюджетом и штатом. Чем больше организация, тем труднее посчитать реальную стоимость владения устройствами.

Я приведу в качестве примера короткий вывод из одного исследования: расходы на перечисленные выше этапы могут доходить до 1000 долларов США в год в пересчете на одно устройство. Компании тратят много сил на экономию при закупке, при этом мало кто считает стоимость владения и то, сколько денег неэффективно расходуется в течение всего цикла жизни оборудования. HP и Softline могут провести экспертный анализ текущих процессов на протяжении всего цикла жизни устройств в организации и предложить совместное решение с прозрачной ценой за весь период эксплуатации.

Таким образом, переходя на сервисную модель HP DaaS, организации переходят от закупок оборудования к потреблению устройств как услугу, точно зная во сколько им обойдется итоговая стоимость владения.

Каким образом тарифный план может быть адаптирован к потребностям конечных пользователей?

С HP каждая компания вне зависимости от размера и специфики работы сможет найти именно тот тарифный план, который будет соответствовать задачам бизнеса лучше всего. Наши планы просты и включают в себя предоставление самих устройств, а также поддержки, аналитики и управления.

План DaaS можно легко дополнить услугами управления жизненным циклом для помощи в установке, настройке, безопасном выводе из эксплуатации и переработке. Это позволяет создать набор услуг, которые полностью удовлетворяют потребности компании. словия финансирования также отличаются гибкостью, чтобы компании сами решали, когда обновлять парк устройств.

HP предлагает три плана: Standard (стандартный), Enhanced (расширенный) и Premium (премиальный).

План Standard включает в себя предоставление устройств, поддержку, отслеживание их состояния и средства отчетности, что помогает ИТ-отделу быть более эффективным и проактивным. Они позволяют нам выявлять и устранять проблемы до того, как они приведут к простою в работе. Наши средства машинного обучения становятся все более умными и эффективными, что позволяет сотрудникам ИТ-отдела экономить время и ресурсы на управлении устройствами и поддержке пользователей.

Аналитика, которую мы предоставляем, очень полезна и помогает принимать более взвешенные решения. К тому же ее спокойно можно использовать с другими системами управления устройствами (EEM/EMM), если вы уже вложили средства в их приобретение.

Выбирая план Enhanced, вы получаете преимущества расширенной поддержки оборудования. Более того, вы можете передать задачи ежедневного мониторинга устройств и управления ими специалистам HP по обслуживанию. Они возьмут на себя общее администрирование устройств, которое включает в себя настройку политик безопасности и контроль за их исполнением, удаленную поддержку пользователей, поиск и защиту украденных или утерянных устройств и автоматическую упреждающую замену запасных частей, таких как аккумуляторы и накопители, чтобы возможная в будущем поломка не помешала работе ваших сотрудников (только для устройств HP).

Premium план услуги DaaS включает в себя все, что содержится в плане Enhanced, а также более продвинутую поддержку наших специалистов по обслуживанию, включая управление исправлениями ОС, предоставление доступа к Wi-Fi без отправки сетевых паролей, составление «белых» (Whitelisting) и «черных» (Blacklisting) списков приложений и развертывание программ. Для повышения уровня безопасности данных используется платформа Windows Information Protection, которая автоматически выполняет шифрование конфиденциальных документов.

Важно отметить, что функции аналитики и упреждающего управления HP уже включены в услугу DaaS. Я также хочу подчеркнуть, что это не программное решение, а комбинация ПО и услуг, предоставляемых специалистами, что делает HP DaaS действительно уникальным предложением на рынке. ▮

HaaS аппаратные сервисы

Почему Softline

Мы поставляем в аренду любое оборудование ведущих мировых производителей, оказываем техническую поддержку и обслуживание. Арендованное серверное оборудование можно разместить на хостинге в дата-центрах уровня Tier III, защищенных в соответствии с российским законодательством и международными нормами. Техническая поддержка 24x7 гарантирует непрерывность бизнес-процессов.

Hardware as a Service

Hardware as a Service – альтернатива приобретению аппаратного оборудования. Оборудование для аренды выбирается под потребности каждого конкретного заказчика. Сервис рассчитан на компании, не имеющие возможность выводить деньги на покупку оборудования из оборота, стартапы или дочерние компании. Сервис HaaS помогает заказчику экономить на создании и поддержке ИТ-инфраструктуры!

Мы предлагаем в аренду любое ИТ-оборудование: серверы, СХД, сетевое оборудование, ПК, ноутбуки, принтеры, другую периферию. Любые производители из огромного числа партнеров Softline. От 1 года до 3 с правом последующего выкупа

Основные этапы проекта:

- выбор оборудования и подписание договора с Softline;
- поставка, установка, настройка оборудования;
- возможно размещение оборудования в дата-центрах Softline уровня Tier III;
- ежемесячные платежи за аренду оборудования.

Dedicated Dell EMC Hardware

Выделенные серверы нового поколения Dell EMC PowerEdge G14 с процессорами Intel Scalable можно взять в аренду на любой срок (от 1 месяца) без обязательств по выкупу. Техническая поддержка включена. Возможно подключение любых облачных сервисов. Также возможна аренда систем хранения данных и сетевого оборудования.

Приобретая услугу Dedicated в Softline, вы получаете гибко масштабируемую ИТ-инфраструктуру без капитальных затрат с подключаемыми ресурсами в публичном облаке (IaaS) и приложениями (SaaS).

Возможно размещение на территории заказчика.

Проект «Платежный стандарт» запущен на арендованном оборудовании

Для реализации проекта в составе группы компаний «Обувь России» была создана небанковская кредитная организация «Платежный стандарт». Компании требовалось создать ИТ-инфраструктуру, отвечающую всем требованиям по безопасности и отказоустойчивости.
Использование специализированного ПО не позволяло разместить систему в облаке, но выводить средства на покупку оборудования из оборота заказчик не планировал. В связи с этим специалисты Softline предложили воспользоваться услугой — оборудование в аренду и разместить его в отказоустойчивом ЦОДе.
Специально под задачи заказчика были закуплены серверы, которые отвечали всем его требованиям. В результате ГК «Обувь России» обеспечила техническое сопровождение нового сервиса, сократив капитальные затраты на закупку дополнительного серверного оборудования.

АРЕНДА ОБОРУДОВАНИЯ ПОМОГЛА ЗАКАЗЧИКУ ЗАПУСТИТЬ ПЛАТЕЖНЫЙ ПРОЕКТ С МИНИМАЛЬНЫМИ ЗАТРАТАМИ

Новый дата-центр для «Обуви России» в Москве

ГК «Обувь России» получила комплексное решение на базе платформы Hewlett-Packard Enterprise, которая использовалась и в предыдущих проектах, что даст возможность легкой интеграции с существующими мощностями. Оборудование размещено на площадке Softline. Выбор в пользу аренды стороннего ЦОДа помогает избежать больших капитальных затрат и снимает все ограничения на дальнейший рост ИТ-обвязки бизнеса «Обуви России».
Эксперты Softline, предложили систему хранения данных, наиболее подходящую требованиям заказчика, способную производить репликацию на три площадки заказчика (Москва, Новосибирск и Хабаровск) и масштабируемую. Оплата за оборудование идет равными долями в течение пяти месяцев. При развертывании ЦОДа в Москве заказчик принял решение воспользоваться арендой площадки Softline для размещения своего оборудования.

ВЫБОР В ПОЛЬЗУ АРЕНДЫ СТОРОННЕГО ЦОДА СНИМАЕТ ВСЕ ОГРАНИЧЕНИЯ НА ДАЛЬНЕЙШИЙ РОСТ БИЗНЕСА

Серверное оборудование для парфюмерно-косметической компании «Аромат»

ОАО «Аромат» – крупный игрок на рынке парфюмерно-косметической продукции.
В рамках модернизации ИТ-инфраструктуры заказчик запланировал приобретение нового сервера для установки в здании офиса.
Предпочтение заказчика было отдано оборудованию Dell, оптимально подходящему по цене и техническим характеристикам. Команда Softline разработала готовое решение, максимально соответствующее нуждам бизнеса, и предложила финансовую схему покупки оборудования, согласно которой плату за использование сервера можно вносить не единовременно, а ежемесячно. Контракт был заключен на 13 месяцев. По истечении этого срока оборудование можно выкупить по остаточной стоимости.

ОПТИМИЗИРОВАЛИ ЗАТРАТЫ НА ПРИОБРЕТЕНИЕ СОВРЕМЕННОГО ОТКАЗОУСТОЙЧИВОГО ОБОРУДОВАНИЯ

Статус EMC VSPEX accredited partner подтверждает компетентность компании в области поставки, внедрения и технической поддержки облачных инструментов вендора.

intel Technology Provider Platinum 2017

Наивысший партнерский статус Platinum в программе Intel Technology Provider присваивается компаниям с большой ресурсной базой и экспертизой.

NetApp GOLD PARTNER

NetApp Cloud Service Provider свидетельствует о компетенциях Softline в предоставлении облачных сервисов на основе технологий NetApp из собственного виртуального ЦОДа.

cisco Powered

Softline имеет возможность предоставлять облачные услуги, авторизованные Cisco, во всех странах, где есть представительства компании.

DELL EMC PARTNER TITANIUM

Наивысший партнерский статус Dell EMC на территории России – Titanium, который подтверждает заслуги компании в области продвижения продуктов и услуг вендора на отечественном рынке.

Типовые **облачные решения** Softline

ИТ-процессы любой компании можно условно поделить на индивидуальные, характерные лишь для нее или для предприятий того же профиля, и стандартные. Стандартные (базовые) ИТ-процессы в том или ином виде присутствуют во всех компаниях. К их числу относятся такие распространенные корпоративные сервисы, как антивирусы, почта, Skype, защита от DDoS-атак. Такие сервисы не ранжируются по отраслям и не зависят от размера компании. Они востребованы практически в любой организации.

К примеру, если сотрудникам компании нужно создать типовые рабочие места с настроенной электронной почтой и Skype для бизнеса, то создание персонального проекта не требуется. В таких случаях куда проще воспользоваться типовой услугой Softline, которая позволит очень быстро развернуть нужное количество рабочих мест и не потребует затраты таких средств и времени, какие понадобились бы на индивидуальный проект.

К преимуществам типовых сервисов можно отнести:

- минимальные трудозатраты на оказание услуг;
- высокую экспертизу по данному направлению;
- низкую цену за единицу сервиса;
- максимально возможный функционал, лицензии, емкости, мощности.

Антон Нагов, руководитель направления продаж облачных сервисов

Что такое типовой сервис?

1. Типовой сервис – массовый шаблонный сервис, который оказывается большому количеству заказчиков без серьезных изменений в типовом проекте.
2. Отсутствует классический проект внедрения. Сервис может быть предоставлен за несколько дней или часов после оплаты. Минимальный набор документации, по которой осуществляется проект, уже существует. При появлении заказчика все процедуры прогоняются по шаблону, за счет этого сервис подключается очень быстро.
3. Со стороны заказчика не требуется наличие специалистов в данной области. Все сервисы поддерживаются сотрудниками Softline. Заказчик выступает только как пользователь того или иного вида услуг.

4. На рынке присутствует достаточное количество игроков с аналогичными предложениями, поэтому заказчику просто определить адекватность цены, сравнить функционал разных решений и сделать выбор.
5. Заказчик может сделать персональный проект, но потеряет либо в качестве, либо в стоимости, так как на его площадке отсутствует эффект масштаба. Найм отдельного специалиста для работы с индивидуальным решением нерационален. В отношении качества ситуация еще проще: если в одного из клиентов Softline обнаруживается уязвимость, ошибка, сбой, для остальных предпринимаются превентивные меры, исключив возможность повторения ситуации. В случае с индивидуальным проектом придется учиться только на своих ошибках.

Виртуальный офис Softline

Включает электронную почту и Skype для бизнеса по подписке. Все корпоративные коммуникации размещаются в облаке.
Виртуальный офис Softline включает все, что нужно на типовом рабочем месте: электронную почту, уведомления, статус присутствия, возможности голосового общения и демонстрации экрана.
Сегодня игроков на рынке облачных услуг можно условно поделить на две основные части. Первая часть – те, кто собирает первых клиентов за счет цены. Стремление предложить сервис по минимальной стоимости почти всегда означает проседание по качеству. Большинство заказчиков начинают свою работу как раз с таких сервисов, выбирая их по цене.
В дальнейшем те, кого устраивает не всегда работающая почта или Skype для бизнеса, продолжают пользоваться этими сервисами, потому что стоимость входа в них действительно минимальна.
Однако более зрелые компании, для которых неприемлемы простои и потеря данных, в последующем, выбирая провайдера, смотрят уже не только на цены, но и на SLA, гарантии и технические решения.

Почему виртуальный офис Softline?

- Качественная архитектура.
- Дополнительные меры по защите и сохранности информации.
- Гарантия высокого и жесткого SLA как по доступности сервиса, так и по скорости ответа инженеров.

Облачный Veeam

Готовый сервис резервного копирования и репликации для заказчиков облака Softline, а также для собственных площадок клиентов, которые пользуются отдельными сервисами этого облака.
На базе семи дата-центров Softline (два из них находятся в Москве, пять – в регионах) развернуто полноценное корпоративное решение Veeam Backup & Replication 9.5, благодаря которому клиенты могут реализовывать внутри облака Softline сценарии резервного копирования Disaster Recovery. Заказчики, которые приобрели ПО Veeam для своей локальной площадки, могут воспользоваться облаком Softline для бэкапов или репликации.
Объектами резервного копирования могут выступать различные объекты со стороны заказчика:

- Виртуальные серверы на платформах виртуализации VMware и Hyper-V.
- Физические серверы с операционными системами Windows и Linux.
- Рабочие станции ключевых специалистов (главный бухгалтер, дирекция, ведущие специалисты).

Применение программных комплексов Disaster Recovery позволяет очень сильно сэкономить, по сравнению с классическим подходом, при котором для создания резервной площадки заказчик фактически выстраивал небольшой ЦОД с железным оборудованием. Это было достаточно дорого – от 30 до 60% стоимости основного дата-центра. Использование программных продуктов, например, Veeam и облачного провайдера позволяет в три раза сократить эти цифры (с 30-60% до 10-30%).
Все средства резервного копирования предоставляются клиентам в облаке по умолчанию. Протестированная готовая система работает без сбоев. Есть возможность выбрать один из нескольких сценариев резервного копирования и репликации.
Большим преимуществом сервиса является упрощенная тарификация. К примеру, в сценариях резервного копирования предусмотрено всего две переменных: количество объектов,

которые защищаются, и дисковое пространство, которое занимают резервные копии заказчика в системах хранения данных. И никаких дополнительных факторов. Не имеют значения ни передача трафика, ни количество точек резервного копирования и т.д.
В случае, если сервис приобретается заказчиком, имеющим свои локальные площадки, использование технологии Veeam Cloud Connect позволяет передавать данные по общим каналам интернета. Это означает, что не нужно покупать дорогостоящее оборудование для организации сетевой связности и т.д. Возможно использование дедупликации, когда с площадки заказчика на площадку Softline передаются только уникальные данные. Это позволяет значительно меньше загружать существующие каналы связи заказчика.

VDI – инфраструктура готовых рабочих столов в облаке

Инфраструктура готовых рабочих столов в облаке по назначению разделяется на два вида:

- Предназначенная для обычных офисных сотрудников.
- Профессиональная инфраструктура с использованием графических ускорителей, предназначенная для решения задач проектирования и расчетов.

Инфраструктура виртуальных рабочих столов подразумевает выделение под каждого пользователя отдельной виртуальной машины, на которую ставится Windows 10. Соответственно, не возникает никаких проблем ни с драйверами, ни с совместимостью. В отличие от классических терминальных ферм, не возникает конкуренция за ресурсы.

Отличие VDI от классических терминальных ферм

VDI	Терминальные фермы
Под каждого пользователя выделены отдельные ресурсы. При запуске ресурсоемких задач работа остальных пользователей идет в прежнем режиме.	Если один из пользователей фермы запустил ресурсоемкую задачу, она начнет оттягивать на себя ресурсы остальных пользователей.
Даже если одно из устройств клиента заражается вирусом, то вредоносное ПО остается только на одной единственной станции.	Если взламывают пользователя или в систему проникает вирус, то данные остальных пользователей тоже могут быть потеряны.
На виртуальных машинах работает Windows 10, благодаря чему нет проблем ни с драйверами, ни с совместимостью.	На терминальном сервере используется Windows Server, а это может приводить к проблемам с драйверами и совместимостью.

Инфраструктура виртуальных рабочих столов предоставляется по подписке в двух основных видах.
Классический VDI для офисных сотрудников. Это обычные рабочие места на Windows 10 с офисными приложениями, доступными из облака. Главное преимущество такого варианта заключается в том, что любые компании с временными проектами, удаленными площадками и т.д. могут обеспечить своим пользователям подключение к рабочим местам с любых устройств. При этом важно понимать, что обеспечивается абсолютная безопасность данных, поскольку фактически на рабочих местах пользователей находится только картинка. Все программы, данные, действия, контур безопасности остаются на серверах провайдера. Даже если устройство заказчика будет заражено вирусами, то вредоносное ПО останется в пределах одной рабочей станции.
VDI для профессиональных пользователей с использованием графических ускорителей. Компания Softline является официальным партнером nVidia. Мы используем в нашем облаке графические карты nVidea Tesla.
Любые компании, которые работают с графикой, проектированием, проектами, требующими визуализацию, испытывают потребность в специальных профессиональных рабочих столах, которые может предоставить компания Softline. В любой момент возможно увеличение или

уменьшение количества таких виртуальных рабочих мест, в зависимости от того, сколько их нужно. Особенно это актуально для организаций, которые нанимают специалистов на временные проекты. В таких случаях неразумно тратить большие средства на приобретение профессиональной техники и программного обеспечения, которые будут простаивать после завершения проекта. Вместо этого можно на временной основе получить доступ к виртуальным рабочим столам, на которых используется специфическое ПО для проектирования.

STaaS – хранилище как сервис

Сервис позволяет расширить возможности клиентов по хранению данных как в облаке Softline, так и на собственной площадке. В последнее время количество хранимой информации очень сильно увеличивается. Темпы этого увеличения исчисляются десятками процентов в год. Соответственно, большинство компаний начинает испытывать потребность в дисковых массивах для хранения данных.
Для хранения «горячих» данных, с которыми ежедневно ведется работа и «холодных», к числу которых относятся архивы документов, статьи журналов, видеоролики, компания Softline предоставляет хранилище как сервис. Фактически это часть наших СХД, которые мы отдаем по iSCSI для нужд заказчика. Никаких других пользователей и конкурентов за производительность на сданных емкостях не будет. STaaS гарантирует изначально заданную производительность и емкость системы хранения данных.

DDoS-защита от сетевых атак

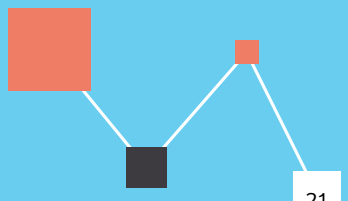
Этот сервис подразумевает две возможные схемы: размещение ресурса в канале с постоянной защитой или перемещение его туда только в момент атаки.

1. **Постоянная защита** – каналы связи изначально и на постоянную основу размещаются в защищаемом сегменте сети. Защита работает на постоянной основе.
2. **Защита на время атаки** – используются обычные каналы связи. В случае начала атаки ресурсы переводятся в защищаемый сегмент и гарантируется определенный уровень легитимного трафика. При продолжительных или частых атаках рекомендуется изначально размещаться в постоянно защищаемом сегменте. Процесс переноса в защищаемый сегмент происходит очень быстро, в течение нескольких минут. Чаще всего такие интервалы не наносят существенного ущерба клиентам заказчика или его потенциальным покупателям.

Антивирус как услуга

Предоставление продуктов ESET в облаке Softline по подписке.
Возможно приобретение виртуальной машины в облаке Softline с предустановленным антивирусом. Все работы по настройке, обновлению и сопровождению этого антивируса будут находиться на стороне специалистов Sotline.
У этого сервиса простая модель лицензирования, все оплачивается в одном счете. Нет необходимости искать какие-то решения именно для виртуализации, выбирать оптимальную модель лицензирования.
Заказчики, приобретающие антивирус как сервис, подвержены лишь 5-10 атакам из 100 возможных, поскольку даже платные базовые антивирусы существенно сокращают объем зловредов, которые могут проникнуть в подключенную к сети машину.

Как видим, спектр типовых решений Softline весьма велик и закрывает большую часть самых востребованных направлений. Если вы все еще сомневаетесь в том, какой вариант следует предпочесть, свяжитесь с нашими специалистами, они помогут вам принять взвешенное решение.



Облачные услуги в едином окне.

Multicloud от Softline

Мультиоблачность — стратегия развертывания ИТ-инфраструктуры на базе нескольких облачных провайдеров и платформ без привязки к одному поставщику услуг. Бизнес может быть заинтересован в мультиоблаке по нескольким причинам. Главные из них: возможность сохранить техническую и экономическую независимость от провайдера, повысить доступность ИТ-систем за счет увеличения отказоустойчивости и таргетированно подбирать облачные предложения под свои конкретные задачи. О том, какими собственными и партнерскими мультиоблачными услугами сегодня располагает и как реализует мультиоблачную стратегию Softline, рассказал Сергей Самоукин, Руководитель отдела облачных решений Softline Департамента облачных технологий.

— Почему в Softline в свое время было принято решение взять курс на развитие мультиоблачных сервисов?

— Так исторически сложилось, что Softline — мультивендорная компания. Мы продаем софт различных разработчиков, мы продаем железо различных вендоров. И у нас это отлично получается! Стратегии multicloud в Softline уже много лет. Фактически, как только компания стала заниматься облаками, уже изначально концепция развития облачных сервисов включала в себя понятие «мульти». Более 5 лет назад мы начали продавать облачные сервисы Amazon Web Services, Microsoft Office 365, Microsoft Azure, IBM.

— В чем заключается мультиоблачная стратегия Softline?

— Мы продаем собственные портфель решений и вендорские облака Azure, Amazon, IBM, Softlayer, Google. Здесь может возникнуть вопрос: зачем нам такой широкий пул вендоров? Все просто: удовлетворить любые потребности заказчика. Если, к примеру, ему не подходит сервис какого-либо вендора, то мы предлагаем сервис другого вендора или наше облако. Основное преимущество здесь – взаимозаменяемость. Можно провести аналогию с туристическим бизнесом: зачем турагентства работают со множеством разных операторов? Чтобы закрыть спрос и быть более гибкими на рынке.

— Какими собственными мультиоблачными сервисами на сегодняшний день располагает компания?

— Мы продаем вендорские облака и свои собственные решения. Собственное облако на платформе VMware размещено в 7 ЦОДах 6 городов России: Москва (2 площадки), Санкт-Петербург, Самара, Ростов-на-Дону, Екатеринбург, Новосибирск. По сути, у нас 7 независимых друг от друга облаков. И их можно объединить под задачи конкретного заказчика. Также у нас в наличии собственное облако на платформе Hyper-V 2016 и готовые инструменты для сборки частных облаков (гибридные решения с публичным облаком).

— А какие имеются партнерские решения на основе облачных вычислений?

— Среди партнерских сервисов модели IaaS на данный момент мы располагаем: Open Stack на базе нашего партнера (Москва), Open Stack на базе нашего партнера в Европе, VMware на базе наших партнеров в Европе, частные облака в Европе, Microsoft Azure, AWS, IBM, Google. Все эти сервисы независимы друг от друга. Единственное, что их объединяет – их можно приобрести у компании Softline.

— Какие планы по реализации стратегии мультиоблачности? К чему в конечном итоге стремится Softline?

— Среди приоритетных задач: развитие текущих сервисов и создание новых. К примеру, строительство S3-совместимых хранилищ. Будем заниматься развитием собственных платформ, проактивным мониторингом, развитием отношений с облачными вендорами, улучшением экспертизы по этим направлениям. Компания стремится к созданию единой панели управления. С ее появлением возрастет скорость решений задач для наших заказчиков. Многие задачи заказчик сможет делать самостоятельно и, что самое главное, в «едином окне». ▮

Контакты

Сергей Самоукин
руководитель отдела облачных решений,
Департамент облачных технологий Softline
Звоните: +7 (495) 232 00 23 доб. 1065;
+7 (903) 5384584
Пишите: Sergey.Samoukin@softlinegroup.com

Бизнес – это работа с информацией. Сегодня побеждает тот, кто не просто владеет ею, но умеет быстро обработать данные и принять на их основании верные решения. Исходя из этого, в конкурентной гонке компании стремятся усилить позиции собственных ИТ-департаментов. Softline принципиально изменяет этот подход и доказывает, что эффективно управлять бизнес-информацией можно без капитальных затрат.

ИТ без CAPEX

Аренда «железа» с облачными решениями Microsoft

Облачные решения Microsoft, предустановленные на арендуемое в Softline «железо», помогают заказчику полностью закрыть текущие информационные бизнес-потребности любой организации от стартапа до крупной компании.

Юрий Новиков, руководитель направления развития бизнеса, отдел решений Microsoft

Принцип работы

Офисное рабочее место сотрудника сегодня – пассив, а не актив. Бизнес-задачи, потребности, сама суть работы меняются настолько быстро, что вкладываться в развитие ИТ-инфраструктуры без уверенности в том, что она понадобится тебе через полгода-год, нет смысла.

Чтобы играючи оперировать важными для бизнеса данными и получать из этого выгоду, собственная ИТ-инфраструктура не нужна: если ваш бизнес прибылен в модели покупки ИТ-оборудования, то он будет еще более прибылен в модели его аренды. Удобство аренды «железа» с предустановленным, уникально подобранным под потребности каждого конкретного бизнеса пакетом Microsoft состоит в том, что такая инфраструктура создается только при необходимости и не требует финансовой или технической поддержки за рамками проекта.

Если бизнес любой компании прибылен в модели покупки оборудования, то он будет более прибылен в модели аренды этой ИТ-инфраструктуры.

All inclusive

Конечное решение выглядит для пользователя как ноутбук, на котором предустановлено решение Microsoft 365 (Windows, Office 365 и Enterprise Mobility + Security) с гарнитурой в комплекте. За видимой частью в решение включена работа серверов сервиса Office 365: SharePoint Online, Exchange Online, Skype for Business Online, OneDrive, Teams и множество других сервисов, в зависимости от приобретаемой подписки. Пользователь получает готовое почтовое решение, чаты, конференц-связь, хранение данных, порталы, аналитику, обеспечение безопасности и т.д.
Условия могут быть гибкими — с помесячной оплатой.
Решение идеально подходит для:
- бизнесов с яркой сезонностью;
- временных проектов;
- проектных команд;
- стартапов;
- георасределенных организаций.

Клиентская инфраструктура:
ноутбуки, планшеты, телефоны, гарнитуры, которые можно взять в аренду.

\+

Microsoft 365
и все его компоненты, Azure.

Проектная работа для крупного бизнеса

Решение ИТ без CAPEX оптимально для любых временных проектов. Так, ретейлеры при открытии магазинов в регионах традиционно привлекают локальных специалистов для решения текущих задач по запуску. При этом смысла в закупке для них оборудования нет, поскольку это автоматически требует дорогих логистических решений: «железо» нужно где-то складировать, обслуживать, перевозить и т.д.
Приобретение техники на месте также не решает проблему – такое оборудование потребует вмешательства ИТ-департамента компании для предустановки нужного ПО и настройки инфраструктуры. Также останется актуальным вопрос удаленного контроля за данными.
ИТ без CAPEX позволяет создать ИТ-инфраструктуру под конкретные цели любой проектной или временно созданной организации. При этом решение позволяет как сделать проектную систему закрытой, так и интегрировать ее в существующую инфраструктуру заказчика.

Решения для стартапов и малого бизнеса

Услуга закрывает все потребности в ИТ для организаций «с нуля»: любых стартапов, быстрорастущих организаций, особенно георасределенных, например, когда перед владельцами бизнеса встает задача обеспечить ИТ-инфраструктуру для разбросанного по точкам штата от 50 человек.
Собственники могут построить ИТ-инфраструктуру самостоятельно, набрав штат людей, которые будут закупать оборудование, обслуживать, до-

Сценарии применения

«Киоски» или использование для firstline workers

Задача:
информирование продавцов в крупных сетевых магазинах, людей, которые не являются офисными сотрудниками и не имеют стационарного рабочего места, но нуждаются в доступе к расписанию, тренингам, базовым документам и т.д.
Решение:
установка одного устройства с предустановленным ПО и интеграция его в инфраструктуру компании; это позволяет сразу многим пользователям иметь доступ к информации для ознакомления. Стоимость одного подключенного человека минимальна, так как одно решение делается для всех.

Полнофункциональный пакет для офисного сотрудника

Задача:
базовый пакет и сервисы общения.
Решение:
в максимальной комплектации в него может быть добавлен сервис Cloud PBX (виртуальная телефония), который позволяет при помощи Skype for Business или Teams звонить на городские и мобильные номера, а не на устройство. Такое решение требует установки у себя специального устройства, которое условно будет связывать облачную инфраструктуру, например, с городской телефонной сетью. Softline предоставляет эту услугу как сервис под ключ.

Базовый пакет для менеджера

Задача:
обработка входных данных, составление отчетов на основе поступающей информации, выполнение поставленной задачи, например, работа бухгалтера или проектного управляющего.
Решение:
установка на персональное устройство пакета, включающего почтовый сервис, Excel, Word.

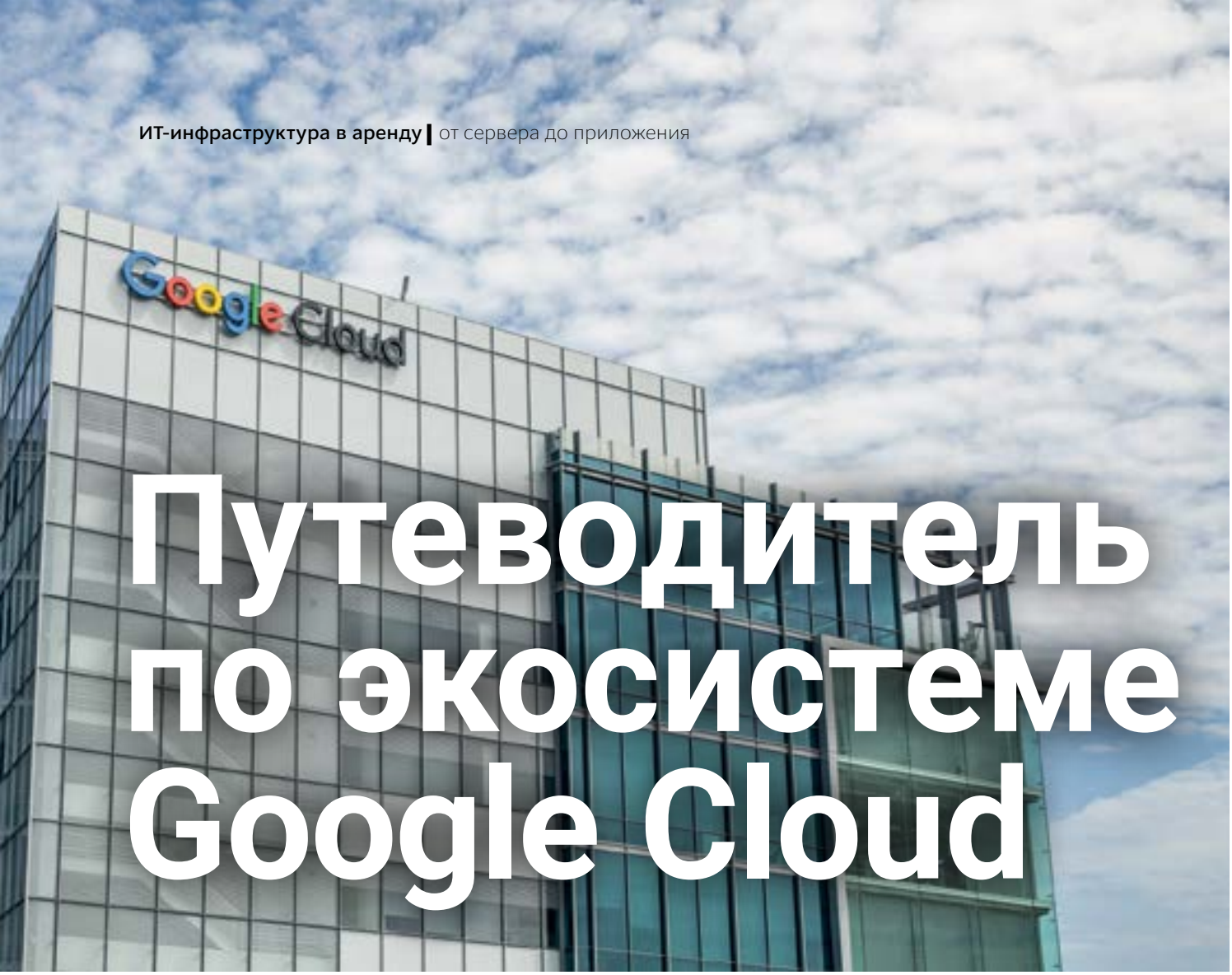
ставлять и т.д. В случае передачи этих функций на аутсорс решение будет выглядеть как строчка на затраты, не требуя от собственника ничего более ни с точки зрения технического обеспечения, ни с точки зрения управления, логистического или финансового.

Управление безопасностью

В услуге ИТ без CAPEX предусмотрены несколько способов обеспечения безопасности данных. Прежде всего, BitLocker – стандартный функционал Windows 10, шифрующий данные на самом жестком диске. Если устройство будет украденного, потеряно или с ним физически случится что-то еще, без пароля или двухфакторной идентификации, когда чтобы зайти в компьютер, нужно сначала ввести пароль, а потом – код из смс, доступа к информации не будет.
Другую гарантию дает функция управления устройствами, в рамках которой владельцу компании или управляющему проектом предоставляются права на пакет Microsoft. Это значит, что он может иметь доступ к управлению всеми девайсами, мобильными телефонами, ноутбуками – всему, что может содержать какую-то коммерческую информацию, и самостоятельно удалять на них что-то, блокировать, стирать, накатывать обновления, требовать соблюдения политик. В полнофункиональном решении включена защита от небезопасных вложений, подозрительных ссылок и прочих киберугроз.
Backup (резервное копирование). Позволяет безопасно хранить всю информацию, созданную на арендованных устройствах внутри рабочей группы. Это полезно в том числе для ограниченных во времени проектов, так как дает возможность при необходимости вернуться к каким-то данным в будущем.

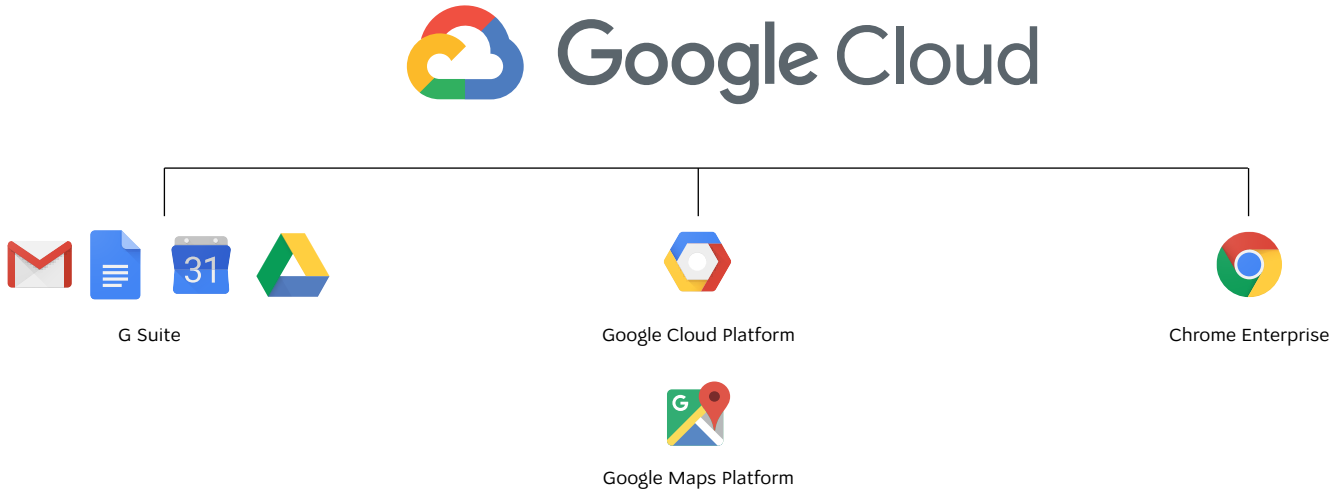
Где доступно

В городах присутствия Softline. ▮



Путеводитель по экосистеме Google Cloud

В семейство Google Cloud входят приложения для совместной работы команды, множество сервисов для создания цифровых продуктов, аренды виртуальных мощностей или построения гибридной инфраструктуры. Кроме того, сторонними разработчиками созданы готовые решения, дополняющие это семейство. Запутаться легко. В этой статье вы сможете узнать, из каких именно частей состоит экосистема Google Cloud.



G Suite

Пакет облачных сервисов, который включает все, что может потребоваться рядовому сотруднику. Это полностью готовое рабочее место, доступное удаленно с любого устройства.

Состав решения G Suite

Инструменты для общения
- Корпоративная почта на базе Gmail.
- Голосовой и видеочат.
- Безопасный сервис для общения в командах.
- Общие календари.

Функционал для совместной работы
- Документы, таблицы и презентации.
- Упрощенная среда разработки приложений.

Решения для хранения информации и ее поиска
- Неограниченное пространство для хранения.
- Поиск контента в сервисах G Suite с помощью Cloud Search.

Инструменты управления
- Круглосуточная поддержка по телефону и электронной почте.
- Инструменты обеспечения безопасности и управления доменом.
- Предоставление электронных документов: хранение электронной почты, чатов и файлов.

Почему G Suite?

- Переход от капитальных к операционным расходам.
- Прозрачное бюджетирование.
- Простая миграция, развертывание и поддержка.
- Возможность интеграции с другими системами.
- Эластичность и масштабируемость.
- Отказоустойчивость лежит на вендоре, SLA 99.98%; техническая поддержка 24/7.
- Мобильный доступ с любого устройства.
- Сервис работает на всех платформах.
- Встроенные средства для контроля и безопасности, в том числе MDM и DLP.
- Лучшее решение для совместной работы.

Google Cloud Platform (GCP)

Google Cloud Platform предлагает множество сервисов для цифровой трансформации и создания новых продуктов. Вы можете выбрать управляемую прикладную платформу, включить в проект геосервисы, использовать технологии контейнеров для получения большей гибкости или создать собственную максимально контролируемую облачную инфраструктуру. С этим решением, с одной стороны, появляются широкие возможности самостоятельного управления ресурсами, а с другой, если это не требуется, Google может взять все управление инфраструктурой на себя.

GCP по модели IaaS. Виртуальная инфраструктура Google Cloud предлагает широкий выбор опций вычислительных мощностей для решения широкого спектра задач — от простых виртуальных машин до глобальных, балансированных высоконагруженных сервисов.

GCP по модели PaaS содержит преднастроенные сервисы для создания цифровых продуктов и разработки. Идеально подходит для прототипирования новых проектов. Большой набор инструментов по работе с большими данными и машинным обучением позволяет быстро реализовывать работоспособные модели и не тратить время на разработку.

Google Maps Platform позволяет расширить функционал карт и на их основе разрабатывать собственные продукты. В 2018 году окончательно вошла в состав Google Cloud Platform, за счет чего состоялась ее интеграция с аналитикой и Big Data. Появилась возможность создавать даже игры в реальном мире.

Почему Google Cloud Platform

- Гибкая ценовая политика Google.
- Модель оплаты подстраивается под клиента.
- Скидки за длительное использование.
- Изменение конфигурации услуг в зависимости от потребностей клиента.
- Проверенная инфраструктура.
- Поддержка Open Source решений.

Партнерские приложения

Приложения и системы, созданные сторонними разработчиками с учетом особенностей экосистемы Google Cloud и дополняющие ее функционал. Таких приложений бесконечно много. В качестве примера можно привести CRM-систему Salesforce и сервис для создания корпоративных порталов LumApps.

Salesforce – одна из наиболее популярных CRM-систем во всем мире. Google и Salesforce заключили стратегическое партнерство, что означает полную совместимость сервисов. Например, в интерфейс Gmail автоматически подтягивается информация о соответствующих записях и данных в Salesforce CRM, таких как контакты, организации, возможные сделки и другие записи. Файлы в Salesforce связаны бесшовной интеграцией с Google Drive. Возможно быстрое редактирование потенциальных сделок в Google Sheets с моментальным отображением изменений в Salesforce.

Порталы LumApps – облачные корпоративные порталы, которые объединяют сотрудников компаний. LumApps рекомендованы Google как решение, идеально дополняющее G Suite.

Кастомизированный портал отображает только актуальную информацию, необходимую для работы, представляет собой главный центр коммуникации в компании. На портале размещаются корпоративные новости, личная информация, социальные сообщества и командные проекты.

LumApps позволяет создавать и редактировать портал, используя графический редактор без необходимости программирования.

Инфраструктура Google Cloud является базой для таких высокоскоростных глобальных сервисов, как Gmail, Карты, YouTube, Поиск и др. — с ежедневной аудиторией более 1 млрд активных пользователей каждый.

Корпоративная экосистема Chrome

- Chrome Enterprise — система управления парком устройств Chrome.
- Chrome OS — легкая защищенная операционная система. Преимущества: безопасность и цена. Вся работа идет только в браузере. Антивирус не нужен. Вирусов быть не может.
- Chrome Devices — устройства, работающие на Chrome OS. ∎

Некоторые интересные сервисы Google Cloud Platform

Google Compute Engine предлагает полностью кастомизируемые параметры для виртуальных машин с лучшими сервисами по системе оплаты pay-for-what-you-use.

Google Kubernetes Engine — оркестратор, который позволяет использовать полностью управляемые кластеры Kubernetes для развертывания, управления контейнерами.

Auto ML Vision. API-сервис, который позволяет создавать модели для распознавания изображений, не требующий от пользователей знаний специфических алгоритмов машинного обучения. В основе техноло-

Логистическая компания Deliver использует сервисы Google по максимуму

Deliver – это прогрессивный сервис, расширяющий возможности традиционной логистической системы, исключая посредников из процесса организации перевозок. У компании собственная технологическая платформа, автоматизирующая процесс заказа перевозок, их отслеживание и документооборот.

Компании было необходимо выстроить с нуля сервис, который позволит нарастить мощности и обеспечит высокую производительность. Работа на собственном серверном оборудовании оказалась достаточно дорогостоящей и не обеспечила бы в дальнейшем гибкого масштабирования.

Выбор был сделан в пользу Google Cloud, предоставляющего глобальный охват необходимых сервисов и прозрачную модель масштабирования. Облачное решение дает возможность увеличивать вычислительные ресурсы практически до бесконечности в режиме реального времени, а встроенные в Google Cloud Platform функции балансировки позволяют уравновешивать рабочую нагрузку, что особенно актуально в период пиковых загрузок.

Облачное решение Google Cloud Platform идеально интегрируется с Google Maps и позволяет с легкостью подключать другие сервисы, обеспечивая удобную в управлении ИТ-инфраструктуру. Единый продукт обеспечивает создание серверов, размещение многочисленных баз, хранение пользовательских данных и внутренней документации.

Сейчас Deliver активно использует практически все сервисы Google Cloud: Compute Engine, Cloud SQL, Cloud Storage, Cloud DNS, G Suite и Firebase.

Возможность удаленного доступа к рабочим документам и корпоративной почте была объективной необходимостью для сотрудников компании в связи с географической распределенностью команды. Решение G Suite позволило вести дела из любой точки мира, поскольку каждый сотрудник автоматически получает полный спектр необходимых для работы инструментов с любого устройства.

гии – предобученные нейронные сети. На основе имеющихся данных происходит автоматическое определение и классификация новых признаков.

Google Speech API. Сервис распознавания голоса, который позволяет преобразовать речь в текст. Этот сервис используется как прикладной для функции голосового ввода в Google Docs и G Suite. Популярный Google Assistant на смартфонах также основан на этой технологии. Инструмент считается лучшим в своей области.

Cloud Video Intelligence. Сервис для поиска и обнаружения медиаконтента. Позволяет распознавать большие объемы видео, точно определять, кто, что и на какой минуте появилось в кадре. Осуществляет поиск по видеокаталогу, анализирует видеоархив и расставляет тэги по запросу.

Google Dataprep. Служба, позволяющая обрабатывать и структурировать большое количество данных для их анализа. В графическом интерфейсе отображается искомая информация по заданным критериям.

Cloud Spanner. Управляемая реляционная база данных как сервис – полностью консистентная и горизонтально масштабируемая. Если раньше поиск по базе данных осуществлялся легко, только если она была локальной, то в данном сервисе можно получать актуальные данные в любое время, в любых частях света.

Apigee. Сервис для управления API. Сервис берет на себя роль посредника между разработчиком и пользователями, позволяет управлять созданными API.

Главные анонсы Google Cloud Next’18

В конце июля в Сан-Франциско состоялась конференция Google Cloud Next’18, где было сделано более 100 анонсов. Мероприятие было посвящено машинному обучению/искусственному интеллекту и контейнерам.

G Suite

На конференции было анонсировано много полезных изменений в сервисах G Suite. Например, Gmail получил новый интерфейс, новые функции, в том числе касающиеся безопасности: Confidential Mode, письма с ограничением по времени и возможность отзывать отправленные письма.

В G Suite появилось также много дополнений, связанных с использованием искусственного интеллекта: проверка грамматики с учетом местных наречий и сленга, предсказание текста еще до того, как фраза дописана.

В G Suite Enterprise теперь будут доступны звонки на телефоны — корпоративная версия Google Voice to G Suite.

Cloud Search получит интеграцию со сторонними приложениями. Появится долгожданное продолжение устаревшего Google Search Appliance в гибридном исполнении. Файлы будут храниться локально, а поиск — проводиться в облаке.

На конференции был представлен новый тарифный план G Suite Standalone offering of Drive Enterprise — набор функций по работе с Google Drive из расширенного пакета Enterprise с гибкой системой оплаты: $8 за каждого активного пользователя в месяц + $0.04/ГБ.

Salesforce Add-on для Google Таблиц позволяет делать экспорт отчетов в таблицы, применять изменения и мгновенно загружать обновленные данные обратно в Salesforce.

Google Cloud Platform

В дополнение к ранее выпущенному Cloud AutoML Vision появились новые сервисы AutoML Natural Language и AutoML Translation. С их помощью даже неспециалисты получили возможность работать с машинным обучением. Знания в области программирования не требуются.

Распознавание голоса Cloud Speech-to-Text теперь позволяет автоматически определить язык, добавляет метку вероятности перевода по каждому слову, распознает нескольких участников диалога.

В Dialogflow Enterprise Edition можно добавить телефонный номер для бота. Благодаря этому клиенты компании получат возможность голосового общения с виртуальным ассистентом. Этот полностью управляемый сервис включает распознавание голоса, Natural Language Processing, позволяет использовать коннекторы к неструктурированным документам типа FAQ, производить коррекцию грамматики и анализировать настроение (позитивное, негативное или нейтральное).

Contact Center AI — искусственный интеллект, предназначенный в помощь колл-центрам. На конференции был продемонстрирован пример eBay, где процесс возврата товара полностью выполняется роботом. При звонке покупателя робот делает верное предположение, о каком заказе идет речь, а после предлагает замену. Подбор аналога осуществляет оператор с помощью Agent Assist in Contact Center AI, используя базу аналитики с записями предыдущих разговоров с клиентом Conversational Topic Modeler in Contact Center AI.

На конференции также была показана новая группа сервисов Cloud Services Platform, предназначенная для более удобного управления инфраструктурой (не только GCP, но и on-prem). В частности, Managed Istio, Apigee API Management for Istio, Stackdriver Service Monitoring и, наконец, гвоздь программы — Kubernetes GKE On-Prem с мультикластерным управлением (coming soon to alpha), который позволяет реализовать настоящую гибридную архитектуру. Например, при пиковых нагрузках Kubernetes из дата-центра прозрачно масштабируется в Google Cloud.

Сервис BigQuery получил возможность обрабатывать задачи по машинному обучению с помощью SQL-команд BigQuery ML, а BigQuery GIS теперь позволяет делать SQL-аналитику по геоданным.

Благодаря тому, что Google Maps Platform окончательно вошла в состав Google Cloud Platform, состоялась ее интеграция с аналитикой и Big Data. Она теперь даже позволяет создавать игры в реальном мире!

Компания Google первой запустила коммерческие контейнерные приложения сторонних разработчиков в своем GCP Marketplace, в котором можно легко найти нужное партнерское решение и развернуть его в консоли буквально в два клика. Биллинг находится на стороне Google, поэтому клиенты будут получать единый счет как за сервисы GCP, так и за сторонние решения.

Новая модель биллинга Resource-based pricing model в Compute Engine позволит еще точнее рассчитывать реальное потребление ресурсов и таким образом снизить ежемесячный счет.

Google начала выпускать чипы Edge TPU для запуска TensorFlow Lite ML, предназначенного для ускорения машинного обучения в облаке и быстрой обработки данных прямо на конечной точке. Размер чипа так мал, что на монете в один цент умещается четыре таких чипа.

Компания Softline, как Premier партнер, приняла участие в дополнительных партнерских сессиях с высшим руководством Google Cloud.

Автор фото Роман Веселов

В этом году конференция Google Cloud Next получилась еще более масштабной и насыщенной. Ее посетили 25 тыс. участников. Под мероприятие был занят целый квартал: 3 выставочные площадки в 5 зданиях, в которых проводилось до 40 параллельных сессий.

ВМЕСТО ТЫСЯЧ ЧЕЛОВЕКО-ЧАСОВ...

Когда недостаточно... спецов

Михаил Апостолов, руководитель продуктового направления отдела SOC Softline

Уже полгода клиенты нашей группы компаний могут воспользоваться сервисом **SOC** (от англ. Security Operation Center – центр мониторинга и реагирования на инциденты информационной безопасности) «Инфосекьюрити» (ГК Softline). На текущий момент в проработке по этому направлению находится около 40 проектов.

Что ищут клиенты? Почему они обращаются к нам?

С одной стороны, у нас есть уже готовые и построенные процессы, изначально рассчитанные на очень крупную организацию (около 70 тыс. источников событий), а также используемые технологии, прежде всего, open-source и свои разработки. В SOC Softline работают около 50 специалистов: аналитики и группа мониторинга, которые реагируют на типовые инциденты; собственные разработчики, которые постоянно совершенствуют сервис ISOC.

С другой стороны, услуги по информационной безопасности из облака сейчас недооценены. Причины всем известны: боязнь нового, опасение утечек данных на сторону и желание самостоятельно управлять своими процессами. Такой клиент, услышав на рынке о ISOC Softline, приходит к нам и просит построить «такое же, но с перламутровыми пуговицами» внутри его инфраструктуры.

У нас сейчас уже есть проекты так называемого SOC под ключ, но, несмотря на крупные суммы контрактов, мы отговариваем заказчиков от такого варианта.
Наверняка вы помните повальное увлечение своими ЦОДами на рынке. Так вот, рынок SOC сейчас проходит ту же стадию развития. Интересно, насколько загружены сейчас те ЦОДы? Если, конечно, они не прогорели в жесткой конкуренции.
Многие клиенты, как правило, упускают из внимания, что свой SOC – это очень дорого и долго, а ожидания, увы, могут не совпадать с результатами.

По каким причинам мы отговариваем от SOCа под ключ?

В ходе первых проектов стали очевидными следующие факты:

- Наш SOC (ISOC) существует уже несколько лет, его качество прошло проверку временем. Эти несколько лет развития ISOC никак не уложить в сроки менее одного года. Вы понимаете, не могут девять беременных женщин выносить одного ребенка за один месяц!
- Теперь вспомним про деньги. В ИТ вашей компании уже вложены огромные средства и руководство наверняка считает, что этого вполне достаточно, чтобы отбиться от хакеров. ФОТ раздут, новых сотрудников нанимать в ИТ не дают, их и так много, и вообще руководству не очень понятно, что они все там делают. А еще говорят, что кризис. Средств на инвестиционные затраты нет и в ближайшие пять лет не будет. По самой грубой оценке, стоимость таких проектов начинается от 250 млн рублей за два года.
- В процессе самостоятельного построения своего SOC у потенциального клиента возникает дикое желание сделать так, чтобы в его системе смешалось все, что можно и нельзя: процессы, технологии, кони, люди. После этого на выходе он, скорее всего, получит тяжелое разочарование оттого, что цель была совсем другая, а пришел он не туда, куда хотел.

Если и вам приходилось сталкиваться с упомянутыми выше вопросами, то, скорее всего, вы уже задумывались о возможности использования модели «SOC как услуга».
Кадровый голод на рынке оставляет еще меньше шансов тем компаниям, кто хочет строить собственный SOC. Посмотрите на HH.ru, сколько стоят специалисты по кибербезопасности. Заработная плата такого специалиста в Москве составляет примерно 100 тыс. руб./мес. и выше.
Например, ФОТ для работодателя за три линии поддержки (около 14 человек) ориентировочно составляет 28 млн руб. в год со всеми социальными и пенсионными платежами. А сами такие специалисты напоминают тех самых сусликов, которых не видно, а они есть. Их навыки и квалификация редкие, исключительные, а клонировать таких сотрудников пока, к сожалению, не научились.
Не стоит также забывать, что при этом рынок постоянно «пылесосят» вендоры и другие компании, страждущие построить что-то свое. Поверьте, таких немало. То есть вы будете вкладывать средства в свой SOC, развивать сотрудников, которых потом будут переманивать, не только парализуя этим работу SOC, но и обесценивая уже сделанные инвестиции в людей. И все будет идти по кругу.
Пофантазируем далее. Вы набрали ВСЕХ(!) специалистов, и тут проявляется человеческий фактор. Ваши «штучные» редкие специалисты оказываются халатными, любят поболеть, а если им начальник не нравится, то будут работать спустя рукава. В итоге у вас в самом лучшем случае получатся 1,5 линии поддержки с графиком 8/5.
Вы уже поняли, к чему я вас агитирую: облачная модель ISOC!

Почему именно облачная модель ISOC?

Потому что этот сервис обеспечивает быстрое подключение, большое разнообразие настроек и моделей обслуживания, к тому же по затратам он даже близко не сопоставим с созданием собственного SOC. Схема позволяет произвести быстрый облачный старт, обкатать разные пропорции услуг и моделей работы. Если вы рассматриваете облачную модель ISOC в качестве промежуточного шага на пути к построению своего собственного SOC, то с нашей помощью вы сможете спокойно обосновать бюджеты на следующие годы, произвести спокойный самостоятельный найм персонала, подготовить инфраструктуру и осуществить ПЛАНОВЫЙ переход к своему SOC.
На текущий момент команда нашего ISOC, как уже говорилось, насчитывает 50 человек. Наш сервис обслуживают более сотни серверов. Ежемесячно это более 10 тыс. заявок и несколько десятков типов инцидентов, список которых постоянно увеличивается. Количество логов событий, которое нам присылают, более 2TB за сутки. И SLA, разумеется, везде выполняется на самом высоком уровне.

△

Интерфейс «Открытые инциденты» Центра мониторинга и реагирования по информационной безопасности ISOC

Иногда специалистам нашего SOC приходится выполнять не вполне обычные задачи. Например, у одного из заказчиков проходил внешний аудит по PCI DSS, во время которого мы должны были выявить действия пентестеров в рамках своих контролей и показать, что клиенты не зря купили SOC. Наши аналитики справились с этой непростой задачей и выявили всех пентестеров.

А бывают и такие клиенты, у которых есть свои внутренние команды пентестеров. Когда эти команды замечают, что SOC справляется и снижается поток событий, они начинают нас атаковать всевозможными средствами, а потом нашим специалистам прилетают кейсы со словами: «За 2-3 дня найдите нашего пентестера». И мы их находим – куда деваться, хотя обнаружить пентестера за два дня – это серьезная задача. Например, они ломают хост внутри сети, где 20 тыс. ПК. При этом задача обнаружить тест на проникновение может ставиться уже тогда, когда проникновение началось и специалистам нужно увидеть, где именно оно произошло.

По статистике обнаружение целенаправленной атаки (APT) нарушителя и его действий может занимать до 293 дней, а мы делаем это всего за два дня.

Другое выигрышное преимущество нашего ISOC – реагирование на инциденты. На рынке мало компаний гарантируют реагирование на инциденты под ключ. Зачастую они останавливаются просто на выявлении событий, и это вносит некоторый диссонанс в общий процесс мониторинга безопасности. Практически все умеют подключать события в SIEM, настраивать корреляции и другие механизмы выявления угроз. Делают неплохое оповещение по почте, но, к сожалению, у заказчиков не хватает компетенций для того, чтобы самостоятельно выстроить процесс дальнейших действий после выявления угрозы. В случае необходимости мы готовы взять на себя функцию по сбору доказательной базы и предоставить ее для дальнейшего юридического разбирательства.

SOC как услуга – это интересно, а можно ли посмотреть на него в действии?

Надеюсь, вы уже захотели посмотреть на облачный SOC в действии. Сделать это несложно: вам нужно предоставить нам площадку с тестовой инфраструктурой, либо возможность подключить свой сервер. Далее мы настроим комплекс и средства защиты, произведем забор логов. После этого покажем вам те результаты и те инциденты, которые нашли. Если клиент не будет против, мы можем параллельно, в режиме 24/7 осуществлять реагирование на тот объем событий и инцидентов, который оговорен. Это позволит понять, как работает наша служба реагирования, какие отчеты в боевом режиме вы будете получать.

Пилотный проект не только возможен, но еще и бесплатен.

△

Интерфейс «Обработка инцидентов» Центра мониторинга и реагирования по информационной безопасности ISOC

Однако если я вас не отговорил, и вы все равно хотите свой SOC под ключ, то мы сможем выполнить и такую задачу, хотя это будет дорого и долго. Ориентировочную стоимость и сроки я уже указывал ранее.

Каковы планы и перспективы?

Совершенству нет предела. Сейчас мы работаем над улучшением отчетности, которая будет доступна клиенту; повышением качества предоставляемых материалов, автоматизации, внутренней работы по инфраструктуре; совершенствованием правил для инцидентов, которые обрабатываем; повышением качества процессов, а также тех тестов, которые мы проводим для улучшения предоставляемых нами сервисов.

Есть мысли в будущем реализовать и дополнить наш ISOC услугой «Live Forensic as a Service». В рамках данной услуги планируется извлечение образа машины, которая подверглась атаке, проведение расследования и формирование полной оценки произошедшего. Такой своеобразный офлайн-менеджмент и компьютерная криминалистика. Мы провели несколько пробных кейсов, отработали их по тем инцидентам, которые приходили от заказчиков. Результат обнадеживающий.

Благодаря интеграции в ISOC данной услуги мы сможем оперативно получать информацию о компрометации станции по определенным метрикам. ISOC выдает уведомление, а дальше наши специалисты проводят расследование и получают результат. Эта услуга важна и будет востребована в крупных организациях с территориально распределенной сетью. Когда, например, что-то происходит на географически удаленном хосте и проще не ехать туда, а снять образ диска и передать его в ISOC.

Улучшения коснутся и нашей SIEM-системы (система обеспечивает анализ в реальном времени событий безопасности, исходящих от сетевых устройств и приложений). В планах стоит разработка отдельного модуля формирования оповещений. Многим клиентам, как оказалось, необходима не работа SOC по инцидентам, а получение оповещений для своих нужд. Поэтому в будущем мы создадим отдельный модуль, формирующий отчеты по выявляемым системой уведомлениям, которые могут отправляться непосредственно заказчику.

Вопросы создания SOC и выбора оптимальной стратегии обширны и непросты. Я постарался рассказать о том, как мы можем помочь вам сберечь человеко-часы сотрудников и снизить расход средств с помощью сервиса SOC «Инфосекьюрити». Приступить к живому знакомству с ISOC вы можете в любое время. ▮

Кибербезопасность в облачной среде. CASB и другие технологии

Федор Азаров, менеджер по развитию бизнеса Департамента информационной безопасности, Softline

Бизнес переживает фундаментальные перемены в связи с вступлением в эпоху цифровой трансформации. Прежние модели и бизнес-процессы становятся неэффективными, старые методы коммуникации не работают. У каждого сотрудника появляется все больше персональных гаджетов, которые активно используются в работе, в том числе и за пределами организации. Для поддержания продуктивной работы сотрудников, вне зависимости от типа используемых устройств и геолокации, применяются облачные приложения, такие как Office 365, Google Apps, Salesforce, Github, Microsoft Azure, Amazon Web Services и др. Вследствие этих изменений происходит «размытие» или «распад» периметра сети.

Цифровая трансформация и миграция данных в облачные сервисы

По данным ведущих аналитических агентств Gartner и Forrester Wave, облачные сервисы в 2018 году будут составлять более 45% ИТ-бюджетов корпораций. К 2020 году затраты на ПО по модели SaaS вырастут на 75 миллиардов долларов. Пути назад уже нет. Вопрос в том, как организации смогут защитить свои данные в новом цифровом мире.

Зачем далеко ходить? К примеру, вы можете ответить на несколько простых вопросов? Уверен, что если ранее вы не задавали себе подобные вопросы, то ответы на них подтолкнут к интересным размышлениям.

- Какие облачные приложения используются сотрудниками вашей компании?
- Каким образом контролируется использование подобных приложений?
- Оценивается ли риск от использования этих приложений?

Ответ на подобные вопросы привел к возникновению нового класса средств защиты без которого, возможно, в скором будущем будет трудно представить функционирование современных компаний.

Новые подходы к кибербезопасности. Решения класса Cloud Access Security Broker (CASB)

Традиционные средства защиты информации, такие как средства защиты от утечек конфиденциальных данных (DLP), файрволы нового поколения (NGFW, UTM), средства защиты от вторжений (IPS) и др., изначально создавались для защиты периметра сети предприятия и абсолютно беззащитны в условиях «размытого» периметра, когда сотрудники обмениваются документами через облачные сервисы с мобильных телефонов и ноутбуков, находясь в любой точке мира. Для закрытия данной потребности существует специализированная технология, известная как CASB (Cloud Access Security Broker, или брокер безопасного доступа в облако).

Большинство компаний верит, что их сотрудники используют около десяти облачных приложений, а по факту их число в среднем превышает сотню. Наиболее известные компании, например, Amazon, Microsoft, Google, Adobe, Salesforce VMware и др., серьезно подходят к вопросу безопасности. Но есть и другие сервисы, которые являются очень удобными с точки зрения бизнеса, при этом уровень их безопасности страдает. Многие молодые компании развиваются по принципу grow fast or die slow, их основной задачей является предоставить пользователям удобный функциональный сервис, и все силы они бросают на добавление новых фич или оптимизацию пользовательского интерфейса. При этом времени на поддержание должного уровня безопасности своих продуктов не остается. К наиболее распространенным рискам можно отнести:

- Небезопасное хранение пользовательских данных и данных учетных записей на стороне производителя.
- Ненадежное управление учетными записями, ролями и доступом.
- Непостоянная доступность сервиса, уязвимость перед DDoS-атаками.
- Уязвимости в инфраструктуре производителя облачных сервисов, отсутствие современных средств защиты информации.
- Применение уязвимых технологий при разработке приложения.

Одной из ключевых функций CASB является обнаружение всех облачных сервисов, используемых в компании, оценка риска использования каждого из них и помощь в принятии решения о блокировки наиболее уязвимых. Но это не все, на что способны решения класса CASB. О других ключевых возможностях поговорим в следующем разделе.

Shadow IT (теневые ИТ) – ИТ-решения, которые не контролируются департаментом ИТ. Практически все облачные приложения можно отнести к Shadow IT, т.к. сотрудники компаний используют различные сервисы без привлечения ИТ-специалистов. Ресурсы, относящиеся к Shadow IT, не обязательно являются зловредными, т.к. зачастую департаменты используют облачные сервисы в легитимных целях, в том числе для повышения производительности команды. Для защиты пользователей и данных организации ключевое значение имеет получение видимости используемых облачных приложений в компании.

Четыре столпа CASB

Функционал решений класса CASB можно условно разделить не четыре основных блока:

- Аудит использования облачных сервисов.
- Безопасность данных.
- Защита от угроз.
- Соответствие регуляторам и корпоративным стандартам.

Аудит использования облачных сервисов

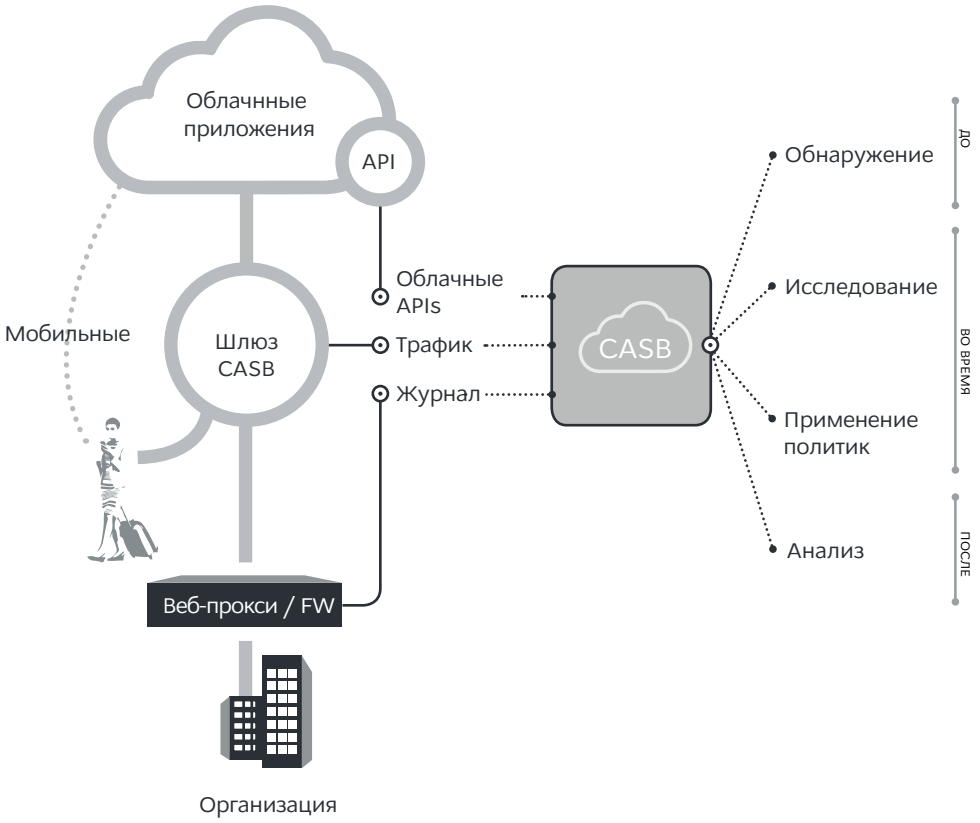
Стратегически важной задачей для бизнеса является прозрачность взаимодействия с облачными сервисами. Традиционные средства сетевой безопасности, такие как прокси, брандмауэры и журналы DNS, могут предоставить лишь некоторые базовые сведения. Однако лишь специализированное решение класса CASB способно обеспечить полную видимость и провести подробный анализ боле 10000 приложений, используемых в современном мире.

Для чего необходима прозрачность и анализ использования облачных приложений?

- Обнаружение Shadow IT. Дает понимание ИТ-специалистам об используемых облачных приложениях и пользователях, которые их применяют.
- Идентификация потенциально опасных облачных приложений. Для офицеров безопасности появляется возможность обнаружения уязвимых и мошеннических облачных приложений и внесение их в список нежелательных к использованию сотрудниками компании.
- Запрет и разрешение доступа к облачным сервисам. Получив картину, ИТ-подразделения могут применить политики доступа, разрешив использование полезных облачных сервисов и запретить опасные приложения.
- Соблюдение нормативных требований. Офицеры безопасности могут отслеживать используемые облачные сервисы и приводить их использование в соответствие нормативным требованиям.

Архитектура и принцип работы CASB

Решения CASB чаще всего разворачиваются в облачной среде и контролируют взаимодействие пользователей и приложений через API и/или прокси-сервера. Также имеется возможность использовать локальный и гибридный режимы. Выбор архитектуры развертывания CASB зависит от инфраструктуры и потребностей конкретной организации. Нет однозначного ответа, какой вариант лучше. Однако, ведущие аналитические агентства выделяют гибридный подход как наиболее полный по функциональным возможностям.



Безопасность данных

Решения класса CASB обладают функционалом, обеспечивающим защиту данных в облачных сервисах. Имеются инструменты управления правами доступа к определенным сервисам, с определенных устройств, а также разграничения прав доступа к критичным данным. Многие зрелые CASB-решения имеют встроенный механизм поведенческого анализа действий пользователей (UEBA), которые позволяют заблаговременно обнаруживать подозрительную активность.

Кроме того, CASB обладает функционалом категоризации информации, позволяющим обнаруживать и анализировать хранение и передачу конфиденциальных данных, что по сути является решением по защите от утечек данных (DLP) в облаке. Для получения продвинутого функционала защиты от утечек, имеется возможность интеграции сторонних DLP-систем с CASB.

И наконец, CASB позволяет обезличивать и шифровать чувствительные данные, передаваемые в облако. Есть возможность применять полное или выборочное шифрование и использовать различные алгоритмы.

Защита от угроз

Облачные приложения корпоративного уровня хорошо защищены. И основным вектором атак, применяемым злоумышленниками, является компрометация учетных данных пользователей и получение таким образом доступа к данным. Кроме того, у злоумышленников появляется возможность распространять вредоносное ПО и проводить целевые атаки на инфраструктуру организации.

Для защиты от угроз CASB имеет в своем арсенале различные методы предотвращения, такие как поведенческая аналитика, антивирусное сканирование, применение машинного обучения для установления шаблонов поведения, использование аналитики угроз в реальном времени от поставщиков облачных сервисов.

Соответствие требованиям регуляторов и корпоративным стандартам

Даже при частичном переходе организации в облако остается важным соответствовать внутренним и внешним стандартам, обеспечивающим безопасность личных и корпоративных данных. Благодаря наглядности и контролю всех используемых облачных приложений в компании, появляется возможность оценить текущее состояние облачной безопасности, а также использовать политики доступа для приведения ее в соответствие необходимым нормам.

Выбор решений CASB

Практически каждый крупный вендор имеет в своем портфеле решение данного класса. Среди лидеров ведущие аналитические агентства выделяют McAfee (Skyhigh Networks), Netskope и Symantec. Также CASB есть у Cisco, Forcepoint, Microsoft, Oracle, Palo Alto.
При выборе решения, наиболее подходящего для конкретной организации, рекомендуется учитывать следующие вопросы:

- **Обнаружение облачных приложений**
  - Сколько атрибутов риска используется для расчета рейтинга безопасности приложения? Имеется ли возможность ручного назначения весов для атрибутов риска?
  - Предоставляет ли решение автоматические отчеты по оценке рисков?
  - Есть ли возможность заблокировать нежелательные облачные приложения за счет интеграции с веб-прокси или брандмауэрами?

- **Наличие необходимых политик**
  - Имеется ли возможность настраивать политики безопасности как для запрещенных, так и для разрешенных приложений?
  - Поддерживает ли решение безопасное использование облачных сервисов с мобильных устройств и ноутбуков, находящихся за периметром организации?
  - Имеется ли возможность применять детальные политики к действиям пользователя на основе контекста и контента, например, имени пользователя, группы, устройства, местоположения, браузера или пользовательского агента?
  - Имеется ли возможность применять единые политики в нескольких облачных приложениях?

- **Развертывание**
  - Совместимо ли решение с существующими решениями веб-прокси для максимального повторного использования инвестиций в систему безопасности?
  - Организована ли модель ролевого доступа к системе?

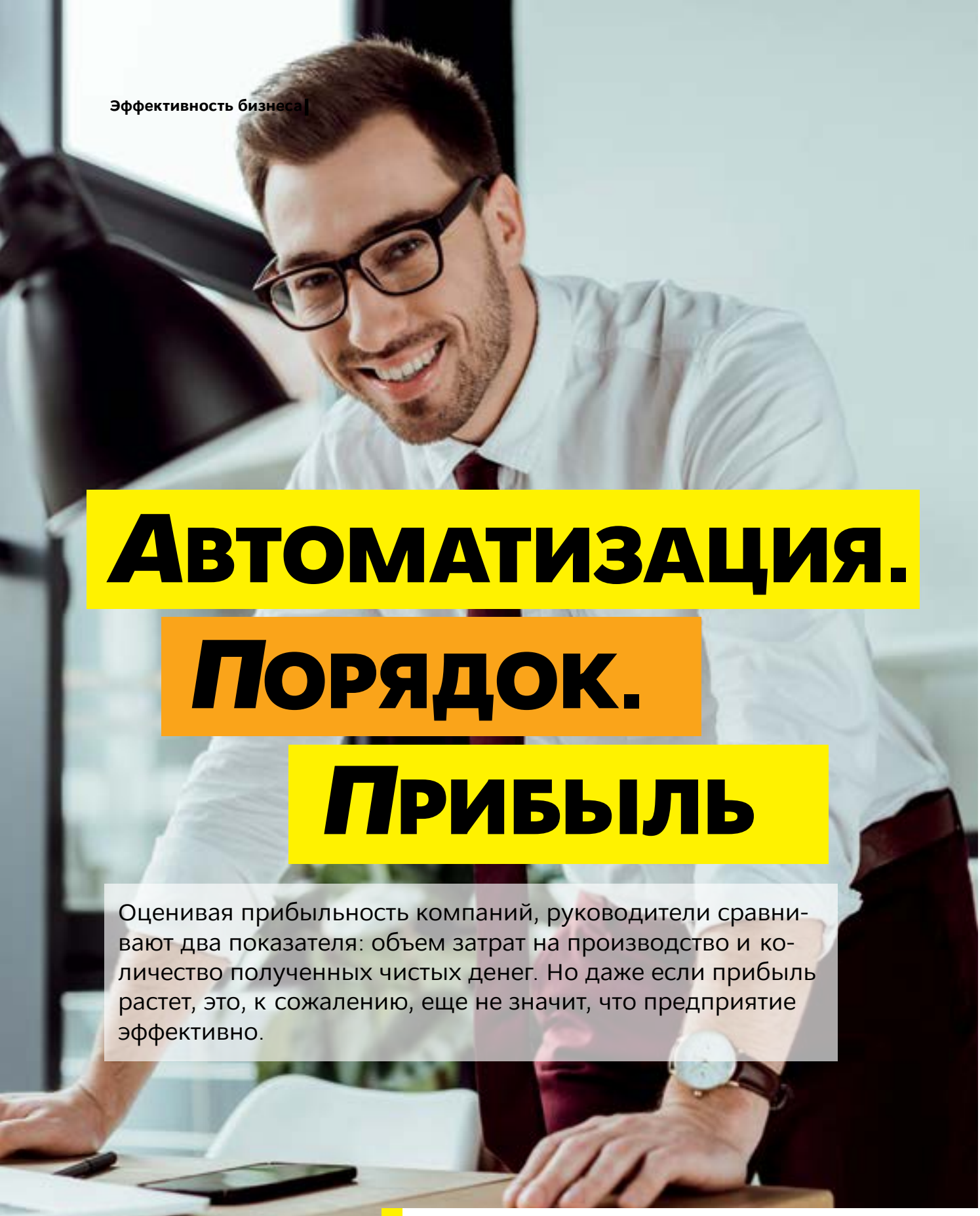
- **Управление данными**
  - Обладает ли система функционалом по защите от утечек данных (DLP)?
  - Имеется ли возможность интеграции со сторонними DLP-решениями?
  - Поддерживаются ли такие методы классификации данных, как регулярные выражения и контекстный анализ?
  - Поддерживает ли решение токенизацию и возможность шифрования данных на лету во время их передачи, использования и хранения в облаке?

- **Обнаружение угроз**
  - Обладает ли решение функционалом поведенческого анализа пользователей (UEBA) для обнаружения подозрительной активности?
  - Предоставляет ли решение расширенную визуализацию для наглядного изучения вредоносной активности?
  - Обладает ли решение встроенным функционалом обнаружения вредоносных программ?
  - Поддерживает ли решение интеграцию со сторонними решениями для защиты от целевых атак (ATP)?

- **Удобство использования и интерфейс**
  - Насколько сложным является решение для настройки и управления?
  - Насколько интуитивно понятен пользовательский интерфейс?
  - Возникают ли какие-либо задержки или неудобства при использовании для конечных пользователей?
  - Могут ли пользователи получить доступ к облачным приложениям при выходе из строя решения CASB?
  - Возможности масштабирования: какое количество пользователей и транзакций поддерживает решение?

Заключение

Решения класса CASB нацелены на защиту данных в облачных приложениях. Они способны обнаруживать Shadow IT, контролировать доступ, трафик и действия над данными и предоставляют наглядную аналитику использования разрешенных и запрещенных облачных сервисов. Решения CASB позволяют бороться с утечками данных, имеют инструменты по поведенческому анализу пользователей, способны обезличивать и шифровать передаваемую информацию. Также присутствует функционал защиты от вредоносного ПО и несанкционированного доступа.
Мировой рынок решений CASB до конца еще не сформирован, но на нем уже есть явные лидеры, предоставляющие в своих продуктах наиболее полный функционал. Отечественных решений данного класса пока нет, но уже есть информация о предстоящих релизах в 2019 году. Сложно не заметить взрывной рост развития и использования различных облачных сервисов в нашей повседневной жизни, и можно с уверенностью сказать, что интерес к CASB на российском рынке будет очень высок.



Автоматизация. Порядок. Прибыль

Оценивая прибыльность компаний, руководители сравнивают два показателя: объем затрат на производство и количество полученных чистых денег. Но даже если прибыль растет, это, к сожалению, еще не значит, что предприятие эффективно.

В центре внимания

Повышение прибыльности — бессрочная задача, и разрабатывая план действий по ее решению, вы наверняка включите в список увеличение рынка продаж, улучшение качества товара или большее разнообразие услуг, а также рост производительности труда, который во многом зависит от рационального использования мощностей компании, рабочего времени и силы сотрудников.

Что еще?

Также не менее важно заострить внимание и на том, чтобы сократить или полностью убрать затраты, напрямую к бизнесу не имеющие отношения. Так, удачным решением может стать аутсорсинг: например, запуск интернет-кампаний и ведение блога через маркетинговое агентство обойдется дешевле, нежели содержание собственной группы продвижения в штате.

ИТ-помощник

Стремление к максимальной производительности труда - фактор, имеющий значительное влияние на уменьшение затрат компании. Стоит сделать все для того, чтобы ваши подчиненные и вы сами старались работать быстрее, слаженнее и без проволочек.
Управлять затратами и их эффективностью, сравнивать постоянные и переменные расходы, осуществлять разносторонний менеджмент и следить за трудовой производительностью — все это помогает делать система управления процессами. Например — WorkFlowSoft, созданная не только для руководителей, но и для всей команды.
подзаголовок

Как поможет WorkFlowSoft?

С WorkFlowSoft все бизнес-процессы размещаются в одной системе: их схемы пользователи создают самостоятельно. Руководители сами решают, кого из организационной структуры компании назначать ответственным за тот или иной этап исполнения или согласования. Каждый процесс имеет понятную иерархию, и последовательность согласований автоматизирована. Не нужно помнить тысячу и одну особенность реализации того или иного процесса.

Все в одном

Электронные письма, заметки, диалоги, «почеркушки» на стикерах — раньше сотрудники получали уведомления о работе в устной форме или по почте, поэтому они часто забывали о своих задачах и работа тормозилась. Автоматизация рабочих процессов предоставляет возможность сосредоточиться на каждом конкретном этапе работы, упрощая всю процедуру в целом. WorkFlowSoft предоставляет наглядную информационную панель, на которой можно увидеть все ваши заявки, отчеты, статистику. Общение больше не зависит от сообщений электронной почты!

Время — деньги

Применение в вашем бизнесе средств автоматизации позволит понять, на какие задачи уходит больше всего времени, или на каком этапе работа «зависает» чаще всего. Отслеживайте статус каждой конкретной задачи и имейте четкое представление обо всей рабочей ситуации в целом: сколько запросов пришло, сколько согласовано или отклонено, сколько времени потрачено на каждую задачу. Колоссальный объем пищи для размышлений! То, что нужно руководителю.
В несколько кликов скачивайте отчеты, сформированные автоматически, чтобы следить за статусом каждой конкретной задачи и этапами ее согласования. Получив бесценную информацию, посвятите больше времени отладке рабочего процесса и обсуждению новых стратегий.
Грамотно автоматизированная работа в конечном итоге обеспечивает удовлетворение потребителей, а значит — основную цель предпринимательства. WorkFlowSoft делает бизнес прибыльнее.

ИГРА ВСЕГДА СТОИТ СВЕЧ

Грамотно понижая себестоимость и одновременно наращивая объемы продаж, вы делаете компанию более конкурентоспособной и гибкой. В нужный момент у вас появляется возможность снизить цены без ущерба бизнесу — а скорее всего, даже во благо. Хотите контролировать рост прибыли — внимательно управляйте и тщательно следите за бизнесом: в процессах для вас, как для руководителя, не должно быть «белых пятен».

WORK FLOW SOFT

Рецепт успешного корпоративного УЦ.

Добавьте немного автоматизации

«Забудь все, чему тебя учили, и смотри, как на самом деле» – частая фраза наставников, когда они встречают новых сотрудников с обучающих курсов. О том, как не стоит организовывать работу корпоративных УЦ и каких правил нужно придерживаться, чтобы наладить эффективную систему обучения, узнаем из интервью с Русланом Фазиловым, руководителем учебного центра Softline.

— Почему у компаний возникает необходимость создания собственных УЦ и каким образом Softline сотрудничает с ними?

— Действительно, сегодня многие крупные компании отказываются от аутсорсинга образовательных услуг в пользу создания собственных корпоративных УЦ. Во многом это удобнее и выгоднее, например, если в организации высокая текучка кадров. К примеру, вакансии сотрудника call-центра или менеджера по продажам отличаются особой подвижностью, поэтому необходимость обучать новых работников присутствует всегда. В этом случае гораздо проще и дешевле наладить свой конвейер подготовки специалистов, ориентируясь на студентов или выпускников вузов, которых за 2-3 недели можно обучить делать базовую работу. Если сотрудник уволился, перегорел или пошел на повышение, система готова в любой момент выпустить новую боевую единицу, способную работать, приносить доход и пользу даже не столько качественными, сколько количественными показателями.

Организация корпоративного обучения неизбежна в случаях, когда в связи со спецификой производства предприятия обладают уникальным оборудованием, возможно самостоятельно разработанным, возможно секретным. Приходится подготавливать множество мастеров, наладчиков, специалистов по сборке определенных деталей, так как от этого напрямую зависит качество выпускаемой продукции.

Следующий момент связан с большим объемом работ в сфере обучения сотрудников. Во многих организациях необходимо систематически проходить многочисленные проверки знаний, так как от того, подтвердит ли работник свои навыки, зависит, получит он допуск на продолжение своей деятельности или нет. Такое отслеживание качества и уровня компетенций позволяет обеспечить уверенность в своих специалистах. Для этого и появляются УЦ, которые массово организуют все эти процессы для корпоративных сотрудников.

Наша роль в сотрудничестве с корпоративными учебными центрами — это предложение услуг по тем направлениям, которые у них не представлены. Мы разрабатываем специализированные авторские курсы. Создавая авторский курс, мы собираем информацию о клиенте, определяем, что конкретно ему нужно, в каком виде и, оперируя его терминологией, подстраиваясь под специфику заказчика, преподаем требуемый материал.

— **С какими проблемами в основном сталкиваются корпоративные УЦ?**

— Одна из сложностей в том, что мы уже описали выше – они не могут обучить всему и потому в частных случаях все равно приходится пользоваться услугами аутсорсинга.

Второй момент – зачастую в корпоративных учебных центрах обучение проводят сотрудники, активно вовлеченные и в другие виды деятельности. Например, аналитиков и руководителей проектов часто «выдергивают» из рабочего процесса для того, чтобы они провели тот или иной тренинг. В связи с высокой загруженностью трудно обеспечить стабильное и качественное обучение, да и хороший специалист не всегда может оказаться хорошим учителем.

Следующая достаточно распространенная проблема заключается в устаревших методических разработках и неактуальных материалах обучения. Многие преподаватели, уже много лет работающие в одном и том же учебном центре, зачастую не меняют программу обучения годами, не обновляют пособия и учебные материалы. В то время как даже крупные корпорации, заводы, государственные учреждения ежегодно преображаются, меняется законодательство, нормы, подходы к работе, все это имеет огромное влияние на адаптацию персонала. Когда после такого обучения сотрудник приходит на работу, ему говорят: «Забудь все, чему тебя учили, и смотри, как на самом деле». Приходится снова тратить время на самостоятельное изучение и это тогда, когда человек уже должен активно работать.

> …можно вырыть траншею лопатой, а можно экскаватором, результат будет тот же, но скорость и трудозатраты разные. Для этого мы и начали оказывать услугу автоматизации рабочих процессов, которая позволяет в том числе оценить качество учебных программ и сделать прозрачным процесс обучения как для руководителя, так и для сотрудника.

Еще одним важным фактором в работе УЦ служит хорошо налаженная система обратной связи и оценки качества образования. В процессе автоматизации работы корпоративных учебных центров Softline настраивает инструменты, позволяющие получать статистику о результатах обучения и определять, какие темы были усвоены хорошо, а какие не очень. Обязательно анализируется и корректность методики преподавания, ведь если, к примеру, большинство обучаемых допустили ошибки в одних и тех же заданиях, значит, нужно пересмотреть материал, изменить формат изложения, акцентировать внимание на сложных моментах.

УЦ Softline помогает справляться корпоративным учебным центрам с вышеперечисленными трудностями и тем самым повышать эффективность обучения своих сотрудников.

— Вы упомянули автоматизацию работы корпоративных УЦ. Расскажите поподробнее, в чем она заключается?

— В работе учебных центров очень много сложных, рутинных процессов: проверка тестовых заданий, заполнение документов в Excel, отправка их в бухгалтерию и многое другое. Как говорится, можно вырыть траншею лопатой, а можно экскаватором, результат будет тот же, но скорость и трудозатраты разные. Для этого мы и начали оказывать услугу автоматизации рабочих процессов, которая позволяет в том числе оценить качество учебных программ и сделать прозрачным процесс обучения как для руководителя, так и для сотрудника.

Что УЦ Softline предлагает для автоматизации работы? Мы оформляем общие знания компании и опыт сотрудников в определенные курсы, а также создаем учебные материалы, пособия. Это могут быть видеоматериалы, 3D-модели для сборки деталей, видеосхемы, инфографика или конкретные инструкции в виде интерактивных презентаций. Также мы организуем виртуальный корпоративный университет на базе систем дистанционного обучения, где база необходимых знаний хранится в удобном виде по блокам для соискателей, для сотрудников на испытательном сроке, для руководителей. Они могут в любое удобное время изучать материалы, скачивать их, проходить тестирование.

Наша главная задача – создать виртуальную площадку, которая объединяет все процессы обучения. Часто компании используют отдельные программы для тестирования, вебинары проводят через Skype, материал собирают в Excel и т.д. Мы предлагаем создать единую систему, в которой видно, сколько человек зарегистрировалось, сколько посетили вебинар, прошли тестирование, с какими результатами. Встроенные инструменты аналитики позволяют делать выводы о качестве учебных материалов, узнать, открывал ли конкретный сотрудник ту или иную тему, сколько минут или часов он ее просматривал и на сколько процентов усвоил. С помо-

> … развитие и обучение своих сотрудников в 2,7 раза эффективнее найма стороннего персонала даже высококвалифицированного.

Что УЦ Softline предлагает для автоматизации работы? Мы оформляем общие знания компании и опыт сотрудников в определенные курсы, а также создаем учебные материалы, пособия

щью таких инструментов руководитель может понять, кто из сотрудников вовлечен в процесс обучения, а кто относится безответственно, а также отследить, как это отражается на их результатах работы. В итоге заказчики получают систему обучения, которая позволяет эффективно подготавливать квалифицированный персонал, обеспечивать его качественную адаптацию и организовывать работу без авралов и простоев.

— Каких правил работы нужно придерживаться корпоративным УЦ для эффективной и успешной деятельности?

— Самое главное – нужно понять, что в корпоративном обучении не действует школьный подход: почитайте учебник, сделайте домашнюю работу, а потом приходите на контрольную. Это приведет к плохим результатам и оправданиям в стиле: «Мы учили, но не выучили». Учебный центр должен тщательно отслеживать, что преподается сотрудникам, как они запоминают материал и применяют знания на практике.

Один из наших клиентов, руководитель отдела продаж, однажды спросил у меня: «А как вы гарантируете, что повысите эффективность нашего сотрудника?». В первую очередь для этого нужно четко понимать составляющие хорошего менеджера по продажам: отличное знание продукции и конкурентных преимуществ, развитый навык переговоров, активность при обзвоне потенциальных клиентов, поставленная речь и т.д. Гарантировать успех мы можем, если проведем обучение сотрудника по каждому из этих факторов. В этом случае его способность совершать успешные продажи объективно увеличится, и останутся лишь незначительные обстоятельства, независящие от профессиональной подготовки.

Чаще всего сотрудники, которые уже давно работают в компании, обладают необходимыми компетенциями для успешной работы и для того, чтобы улучшить их результаты, нужно знать, какой именно из перечисленных навыков развит недостаточно. Для этого автоматизировать оценку усердий сотрудника, отслеживать его активность в CRM-системе, которая показывает, сколько он делает звонков, как долго ведет разговоры и т.д. Благодаря таким инструментам можно оцифровать всю работу менеджера, разложить по пунктам, проанализировать и выявить проблемные зоны. Возможно, он хорошо знает продукт, но плохо ведет переговоры или умеет общаться с клиентами, но не ориентируется в конкурентных преимуществах и т.д.

В зависимости от ситуации нужно проводить обучение по брендам, преимуществам продукции, по навыкам переговоров и др. Обязательно нужно снабжать руководителей чек-листами, с помощью которых они смогут контролировать, как сотрудник работает во время испытательного срока, его поведение, уровень развития профессиональных навыков, применение полученных знаний на практике и мн. др. Комплексный подход в обучении позволяет сделать работу с персоналом удобной и эффективной.

В прошлом году на ИТ-саммите Softline совместно с Headhunter представляли исследования о том, что развитие и обучение своих сотрудников в 2,7 раза эффективнее найма стороннего персонала даже высококвалифицированного. Нужно направлять много усилий и средств на обучение, так как это гораздо продуктивнее и выгоднее, чем ждать пока придут безмерно талантливые, универсальные люди, которые будут превосходить все ожидания. Корпоративным учебным центрам в своей работе нужно делать основной упор на повышение качества и доступности предоставления материала, а также необходимо автоматизировать системы аналитики и отчетности, которые позволят отслеживать, получил ли сотрудник нужные знания в той мере, в которой от него ожидают. ▮

... в корпоративном обучении не действует школьный подход: почитайте учебник, сделайте домашнюю работу, а потом приходите на контрольную. Это приведет к плохим результатам и оправданиям в стиле: «Мы учили, но не выучили». Учебный центр должен тщательно отслеживать, что преподается сотрудникам, как они запоминают материал и применяют знания на практике.

Office 365: дополнительные сервисы, о которых вы не знали

Про пакет Office 365 мы писали много и подробно. Этот набор веб-сервисов, распространяемый по подписке «программное обеспечение + услуги», в последнее время стал очень популярным. Однако есть ряд услуг, дополняющих это решение, о которых пока еще мало кто знает.

IP-телефония для Office 365

Компания Softline в настоящее время выходит на рынок с системой IP-телефонии, базирующейся на пакете Office 365. Согласно законам России, Microsoft, как иностранная компания, не может работать провайдером связи в стране. Компания Softline готовится выступить партнером Microsoft, который будет оказывать эту услугу от своего имени.

Облачная IP-телефония Softline – это услуга предоставления доступа к бесперебойной облачной IP-АТС для всех пользователей Office 365. С ее помощью можно подключать телефонные номера любых российских и международных операторов к подписке Office 365, используя Skype for Business не только как корпоративную IP-АТС, но и как ядро коммуникаций посредством аудио- и видеоконференцсвязи без ограничений по количеству участников виртуальных собраний.

Эти решения подходят как для крупных заказчиков, так и для SMB-сегмента.

IP-телефония для Office 365 в настоящее время базируется на Skype для бизнеса, но в перспективе уже сейчас идет разработка этой же услуги для Microsoft Teams.

Платформа для обучения

Продукт представляет собой платформу, которой может воспользоваться любой сотрудник компании, чтобы получить доступ к набору курсов, текстам, частично – к автоматизированной технической поддержке. В рамках размещенных на платформе материалов заказчик получает знания об особенностях работы с разными продуктами Office 365.

По умолчанию эта услуга не входит в пакет Office 365, но компания Softline до конца 2018 года будет бесплатно подключать ее для своих клиентов.

Типы курсов: «Обучение», «Эксперт», «Увлечение», «Примеры», «Зарисовки».

Для продвинутых пользователей также предусмотрен чат-бот, который отвечает на вопросы по работе с Office 365.

Back Up почты из Office 365

Бэкапирование почты из Office 365 предотвращает риски потери данных, ведь сообщения хранятся не бесконечно и, случается, когда они пропадают из-за программных или иных сбоев. Компания Softline предоставляет услугу по созданию резервных копий содержимого электронной почты. Осуществляется это с помощью сервиса Veeam, который сохраняет переписку на площадку заказчика, в облако Softline или в Azure. Благодаря этому процессу клиент всегда может найти нужные бэкапы.

Услугу Back Up почты из Office 365 нужно подключать отдельно.

Случаи, при которых необходимы резервные копии Ofiice 365

- Случайное удаление
- Неточности/ пробелы политик хранения
- Злоумышленники внутри компании/покидающие компанию
- Внешние угрозы (взломы/ вредоносные приложения)
- Сбои питания

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 Softline. Используется дедупликация на источнике и шифрование данных для обеспечения быстрой и безопасной репликации и резервного копирования.

Автономное хранилище в облаке Softline

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 и INFINIDAT, 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 облаке Softline.

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. ▮

Кибернация Израиля

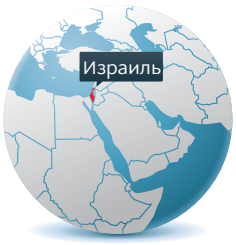
Страна с самыми крупными в мире инвестициями в кибербезопасность, рекордным количеством стартап-компаний, передовой кибермией и прогрессивной системой образования, которая стала международным центром инноваций и заняла лидирующие позиции в области защиты киберсреды государства.

Израиль – это страна, все усилия которой направлены на созидание. Не располагая никакими сырьевыми ресурсами и находясь в состоянии постоянной военной угрозы, государству удалось стать мировым центром науки и высоких технологий. Израильские разработки спасают мир от голода и жажды, возможности медицины считаются самыми передовыми в мире, а в ИТ-секторе страна сумела за короткий срок стать инновационным лидером. Люди живут здесь в террористической обстановке уже почти 70 лет, поэтому ценят настоящее и заботятся о будущем, делая все для того, чтобы страна крепла и развивалась.

Развитие сферы кибербезопасности находится в приоритете государства, так как Израиль – одна из самых компьютеризированных стран на Ближнем Востоке. Допустить уязвимость в работе информационной инфраструктуры для них равносильно нанесению тяжелого ущерба обороне государства и национальной безопасности.

Ответственность за защиту информации лежит на израильском агентстве безопасности «Шин бет» (или «Шабак»). Оно традиционно отвечает за обеспечение безопасности государственных органов и основной инфраструктуры – объектов электроснабжения, водообеспечения и финансовых учреждений. Также в 2010 году было создано Израильское национальное кибернетическое бюро (INCB), призванное продвигать киберполитику Израиля в трех основных направлениях:

1) совершенствование защиты и укрепление национального потенциала в киберпространстве,
2) превращение Израиля в центр информационных технологий,
3) поощрение сотрудничества между учеными, промышленниками, частным сектором, государственными служащими и общественностью по вопросам безопасности. (По материалам исследования Inter-American Development Bank, 2016).



Игаль Унна, генеральный директор INCB, заявил: «Мы работаем, чтобы гарантировать, что Израиль лидирует на мировой кибер-арене в технологических, организационных аспектах и аспектах безопасности. Это означает как развитие человеческого ресурса Израиля, так и развитие научно-технической экосистемы, которая была создана здесь в последние годы и которая заложена в основе относительного преимущества Израиля в мире».

За время работы данных органов критическим инфраструктурам Израиля не было нанесено никакого ущерба, несмотря на ежедневные кибератаки, активность которых с каждым годом

возрастает на 25%. Рассмотрим, за счет чего Израилю удалось добиться таких высот в хайтек-индустрии в целом и секторе кибербезопасности в частности.

ИТ-география

Рубрику ведет Антонина Субботина

Продвинутая образовательная система

По словам Саги Бар, директора центра киберобразования, в израильских школах дети с первого класса учатся читать, писать и кодировать. В стране даже есть детские сады, где учат работе на компьютере и с робототехникой. С четвертого класса ученики уже активно изучают программирование, а одаренные старшеклассники – технологии шифрования и методы борьбы с черным хакерством. О том, насколько глубоки знания израильских школьников можно судить по их развлечениям. Дети играют в игры, по условиям которых, к примеру, взломана воображаемая компьютерная сеть, и у ребят есть 45 минут, чтобы узнать неизвестный компьютерный код, восстановить контроль за сетью и взломать систему злоумышленника, чтобы установить его личность.

Израиль целенаправленно использует армию как кадровый резерв, для того чтобы обеспечивать сферу кибербезопасности квалифицированными трудовыми ресурсами. Так как в стране воинская повинность всеобщая, это позволяет военной разведке отбирать самых талантливых юношей и девушек. Часто применяется такая система, когда студенты запрашивают отсрочку от призыва на военную службу для получения технической степени, на что требуется от трех до четырех лет, в зависимости от специализации. После окончания студенты поступают на обязательную военную службу и служат по своей специальности в течение пяти лет (три года обязательной службы и дополнительные два года, если армия посчитает необходимым). Таким образом после завершения обязательной военной службы студенты уже обладают восьми или девятилетним опытом по выбранной ими специальности.

Такая система дает возможность сделать карьеру в хайтеке, даже не обучаясь в университете. Эран Лассер, бывший командующий подразделения кибервразведки армии обороны Израиля, в интервью для одного интернет-издания подтвердил: «У половины наших айтишников нет университетских дипломов, и работодателям не придет в голову их требовать».

Стратегическое международное сотрудничество

Поскольку инфраструктура кибербезопасности Израиля становится явным лидером в мировой индустрии, международные компании стремятся к сотрудничеству с еврейским государством. В конце 2016 года Биньямин Нетаниягу, премьер-министр Израиля, на Генасамблее ООН заявил: «Население Израиля составляет одну десятую процента населения земного шара, и все же в прошлом году мы привлекли около 20% мировых частных инвестиций в кибербезопасность. Я хочу, чтобы вы переварили это число. Вклад Израиля в кибербезопасность в 200 раз превышает его вес. Таким образом, Израиль также является глобальной кибер-силой. Если хакеры ориентируются на ваши банки, ваши самолеты, ваши электросети и практически все остальное, Израиль может предложить вам необходимую помощь».

Для выстраивания партнерских отношений международные корпорации организуют и спонсируют форумы разработчиков программного обеспечения, тренинги, соревнования и встречи. Международные партнеры из различных отраслей активно участвуют в крупных конференциях по кибербезопасности, которые проводятся в Тель-Авиве в течение года. Стратегическое партнерство предполагает сотрудничество с местными участниками рынка, включая инвесторов, крупные компании и научные круги. Основная цель этого взаимодействия – получить знания и повысить осведомленность об инновациях в области кибербезопасности, что в конеч-

«Вклад Израиля в кибербезопасность в 200 раз превышает его вес».

Биньямин Нетаниягу, премьер-министр Израиля

Согласно данным организации Start-Up Nation Central, в 2017 году общий объем экспорта Израиля в индустрии кибербезопасности достиг $3,8 млрд, а компании данной отрасли получили инвестиции на сумму $815 млн в виде венчурного и частного капитала.

ном итоге приводит к инвестициям и взносам, коммерческим соглашениям, созданию совместных предприятий и т. д.

Крупнейшие транснациональные корпорации, в том числе Microsoft, Google, Apple, Cisco, IBM, Intel, HP, Siemens, General Electric, Philips Medical, PayPal создали в Израиле свои центры исследований и кибернетических разработок.

Инвестиции

Согласно данным организации Start-Up Nation Central, в 2017 году общий объем экспорта Израиля в индустрии кибербезопасности достиг $3,8 млрд, а компании данной отрасли получили инвестиции на сумму $815 млн в виде венчурного и частного капитала.

Финансирование израильских предприятий бьет все рекорды. Во многом это является фактором, благоприятно влияющим на развитие экономики страны. Добиться таких результатов Израилю удалось благодаря упорному многолетнему труду и учету собственных ошибок. Теперь вкладывать свои деньги в израильские стартапы мечтают инвесторы со всего мира и именно с международными инвесторами заключается большинство сделок. Это служит доказательством растущего признания Израиля как мирового лидера в области кибербезопасности.

Согласно данным исследовательского центра Cyber Security Ventures, девять израильских компаний входят в топ-100 самых успешных и прибыльных мировых компаний в сфере кибербезопасности. К примеру, Check Point Software занимает в этом рейтинге четвертое место с рыночной стоимостью $15 млрд.

Такие финансовые показатели служат подтверждением сравнительного преимущества израильской промышленности, которая характеризуется высоким уровнем внедрения инноваций и широким развитием передовых технологий.

Нация стартапов

За Израилем давно закрепился бренд «Startup Nation», также страну называют второй Силиконовой долиной. Все потому, что там процветает стартап-индустрия. В стране зарегистрировано 6 тысяч молодых высокотехнологичных компаний (по материалам газеты The Economic Times). Подразделение военной разведки 8200 получило звание «секретной стартап машины», так как многие израильтяне, служившие в нем, в последствии создали стартапы, оценивающиеся в миллионы долларов.

Многие, наверняка, помнят «аську» – бесплатный мессенджер ICQ, который разработали четверо молодых программистов из Тель-Авива. Позже они продали права на него за $407 млн компании America Online. Это было только начало бурной работы израильского стартап-инкубатора. Среди самых крупных сделок покупка Google за $1,1 млрд компании Waze, выпускающей приложения, которые соединяют в себе GPS-навигацию и социальные сети, позволяя пользователям собственными сообщениями улучшать построение маршрутов или карту пробок. Это позволяет сервису быстро реагировать на меняющуюся ситуацию на дорогах, в том числе на аварии или на появление радаров для контроля скорости. В 2017 году произошла самая крупная в мире сделка по купле-продаже компании хай-тек. Intel поглотил израильскую Mobileye за $15,3 млрд. Организация занимается разработкой и производством устройства, которое помогает водителям избежать аварий на дорогах.

И, конечно, в Израиле множество успешных стартапов по кибербезопасности, которые также привлекают внимание известных инвесторов. Венчурный фонд Flint Capital инвестировал $3 млн в Израильский стартап CyberX, который производит программное обеспечение в сфере кибербезопасности для промышленного Интернета вещей. Стартап Checkmarx, который предоставляет сервис для анализа исходного кода программного

обеспечения и обнаружения киберугроз на ранних стадиях, привлек $84 млн инвестиций.

В Израиле ежегодно появляется множество успешных проектов. Разработчики и предприниматели продолжают поражать воображение даже тогда, когда, казалось бы, что удивлять уже нечем. Многолетней работой Израиль заслужил себе надежную репутацию. Управляющий партнер израильской инвестиционной компании JSCapital Роман Гольд, говорит о том, что Израиль заслужил настолько надежную репутацию и прочное положение, что в этой стране стартапы выбирают инвесторов, а не наоборот.

За Израилем давно закрепился бренд «Startup Nation», также страну называют второй Силиконовой долиной.

Кибервойны

Хотя кибервойны и подразумевают борьбу в виртуальном пространстве, их последствия как нельзя более реальны. Вражеские злоумышленники могут вывести из строя системы электро- и водоснабжения, системы управления транспортом, больницами – полностью парализовать жизнь страны. В связи с тем, что зависимость Израиля от киберпространства в политической, военной и экономической сфере высока, а количество врагов, желающих посягнуть на компьютерные системы Израиля крайне велико, государство прикладывает много усилий для обеспечения адекватной системы кибернетической безопасности. Правительственные учреждения и ключевая инфраструктура страны ежедневно испытывают на себе кибератаки враждебных групп, но, как уже упоминалось ранее, безуспешно.

Эта заслуга во многом принадлежит израильским кибервойскам, которые отличаются беспрецедентной готовностью к виртуальным войнам. Они признаются ведущим родом войск в стране наряду с сухопутными, военно-воздушными силами и военно-морским флотом.

В Израиле существуют тайные учреждения, занимающиеся кибератаками. Наиболее известно подразделение военной разведки – 8200. Это аналог Агентства национальной безопасности США, в его задачи входит перехват разведданных, дешифровка, прослушивание вражеских целей и организация кибератак.

В Армии обороны Израиля (ЦАХАЛ) проводят специальный курс кибервойны, где обучают вести бои в виртуальном пространстве, распутывать сложнейшие головоломки, проникать в компьютерные системы врага и наносить по ним сокрушительные удары. Начальник курса майор Нимрод Фосцениану говорит следующее: «Наши курсанты приобретают ценнейший опыт в отражении разнообразных угроз, с которыми они не сталкивались в гражданской жизни. Нашей задачей является также привить им менталитет воина, готового вступить в смертельную схватку с реальным врагом. Солдат кибервойны должен быть в постоянной готовности различить в потоке информации следы, оставленные врагом, точно также как солдат-пехотинец различает среди шума деревьев шаги приближающегося врага».

В Армии обороны Израиля (ЦАХАЛ) проводят специальный курс кибервойны, где обучают вести бои в виртуальном пространстве, распутывать сложнейшие головоломки, проникать в компьютерные системы врага и наносить по ним сокрушительные удары.

В чем секрет?

Большой штат высококвалифицированных специалистов с многолетним опытом работы в сочетании с новаторским подходом и духом предпринимательства – прочная основа израильской кибербезопасности. Израиль стал инновационной супердержавой и превратился в мировой центр высоких технологий благодаря национальному желанию жить в мире и быть защищенными от вражеских воздействий. Постоянное стремление к выживанию активизирует главный и, пожалуй, единственный природный ресурс израильтян – их интеллект. Этим же обусловлен и их знаменитый дух предпринимательства: они не боятся провалиться, не боятся спрашивать и экспериментировать, они просто сразу начинают действовать, не тратя время на обдумывание и сомнения. ▮

Надежная DLP-защита данных от утечек

Наиболее эффективным методом предотвращения утечки информации (не ограниченного, но взаимосвязанного с возможностями пассивного наблюдения за потоками данных) является инспекция потоков данных и принятие решения о блокировке или разрешении передачи данных в сочетании с регистрацией событий непосредственно на используемых сотрудниками оконечных устройствах в любых сценариях их применения — как внутри, так и за пределами офиса, и вне подключения к корпоративной сети.

Такой всеобъемлющий контроль принципиально недостижим для сетевых устройств и сетецентричных DLP-систем, включая, кстати, и шлюзовые DLP-устройства — потому что они не могут контролировать по меньшей мере утечки через сервисы с проприетарным шифрованием, и фактически выключаются из процесса контроля, если компьютер (например, ноутбук) работает без подключения к корпоративной сети.

Когда утечка недопустима

Функция предотвращения утечки данных по максимально широкому спектру каналов передачи, от подключаемых устройств и принтеров до современных интернет-сервисов, на основании анализа содержимого передаваемых данных при попытке передачи, в реальном времени — а не когда утечка уже состоялась и остается только ее «расследовать», является наиболее сложной как в разработке DLP-системы, так и в ходе внедрения. Однако такой контроль незаменим, если утечка корпоративной информации и персональных данных недопустима.

Среди представленных на мировом рынке одним из лучших и единственным российским решением класса Endpoint DLP, обладающим полным набором функций контроля потенциальных каналов утечки данных, является программный комплекс российской разработки DeviceLock DLP Suite.

Почему DeviceLock DLP Suite

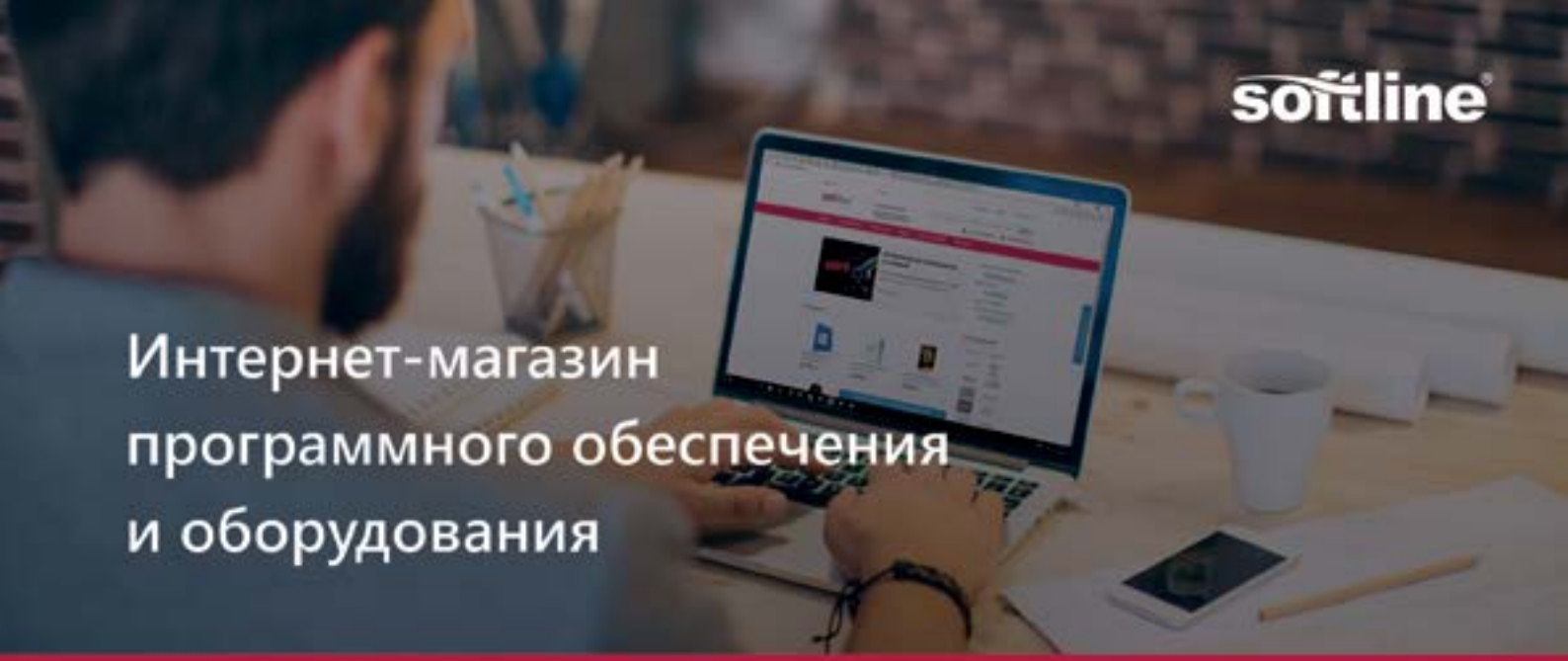
DeviceLock DLP позволяет предотвращать утечки данных ограниченного доступа и регистрировать факты и попытки передачи данных через локальные порты и устройства, сетевые сервисы и протоколы. Перехват и инспекция содержимого передаваемых данных в каналах утечки с автоматическим принятием решения о возможности передачи данных или протоколировании этого события выполняется непосредственно на контролируемом компьютере, а не на уровне сервера или шлюза, что позволяет также обеспечить эффективный контроль мобильных сотрудников, не использующих корпоративную сеть офиса.

Технология цифровых отпечатков, реализованная в новейшей версии DeviceLock DLP 8.3, позволяет выявить уникальный словесный шаблон в отправляемом по каналам сетевых коммуникаций, сохраняемом на внешний накопитель или отправленном на печать документе, сравнивая документ с имеющимся шаблоном (с цифровым отпечатком базового документа). Метод цифровых отпечатков является позволяет обеспечить наименьшее число ложных срабатываний для типовых документов и форм, заполняемых или дополняемых на основе базового документа или образца, поскольку контролируемый образец всегда входит в исходящий документ, и как следствие идентифицируется соответствие отпечатку.

DeviceLock DLP позволяет снимать цифровые отпечатки с образцов конфиденциальных документов и типовых форм для сбора персональных данных, сохраняя их в собственной базе данных отпечатков, а затем сравнивать их с отпечатками защищаемых при передаче документов. Если процент соответствия отпечатков превышает требуемый порог в соответствии с заданной DLP-политикой, проверяемые документы считаются конфиденциальными, и к ним в режиме реального времени применяются заданные в DLP-политике действия. Такими действиями могут быть блокировка передачи документа, создание теневой копии, отправка тревожного оповещения в службу ИБ. Точность детектирования персональных данных в DeviceLock DLP может быть значительно повышена благодаря возможности создания правил контентной фильтрации с условиями детектирования в сколь угодно сложных комбинациях с использованием логических функций и сочетанием метода цифровых отпечатков с анализом по ключевым словам и шаблонам регулярных выражений. ▮

DeviceLock® DLP

DeviceLock DLP открыт для свободного независимого тестирования. Полнофункциональный дистрибутив продукта опубликован на веб-сайте разработчика и уже содержит триальную лицензию.



softline

Интернет-магазин программного обеспечения и оборудования

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

Преимущества:

- Служба поддержки
- Более 25 000 позиций оборудования и программного обеспечения
- Отслеживание статуса оплаты заказа
- Мгновенное получение счета и шаблона договора
- Доставка по России
- Автоматическая отправка бухгалтерских документов на e-mail
- Постоянный доступ к данным заказа и документам
- 5 звезд на Яндекс-Маркет

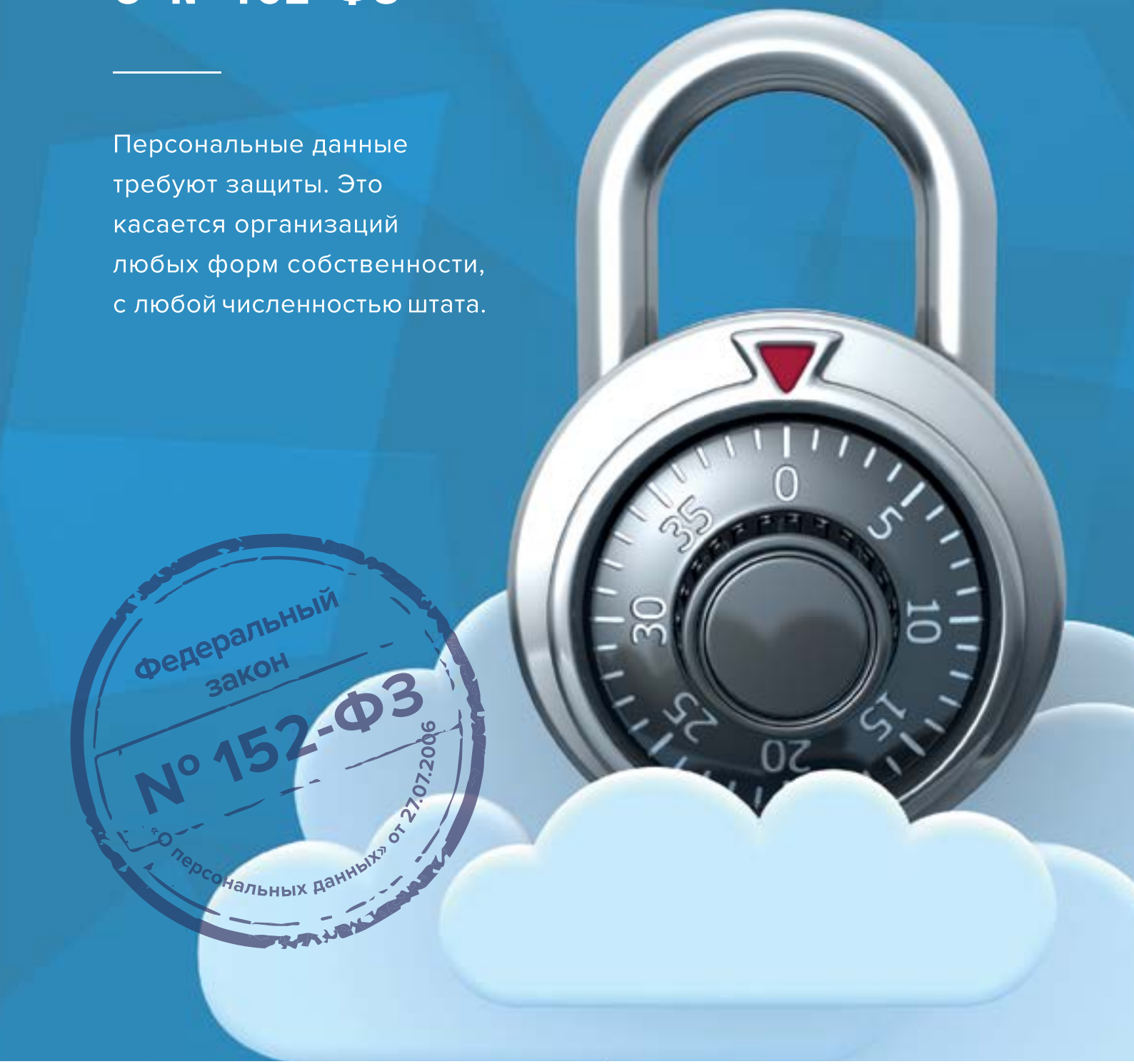
Microsoft · Adobe · embarcadero · Hewlett Packard Enterprise · ASUS · KASPERSKY · Authorised Systems Integrator · AUTODESK Gold Partner · DELL · ABBYY · Acronis · ATLASSIAN · Altium · DevExpress · COREL · eset · TeamViewer · VEEAM

Ещё более 1000 производителей доступно на сайте

store.softline.ru

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБЛАКЕ В СООТВЕТСТВИИ С № 152-ФЗ

Персональные данные требуют защиты. Это касается организаций любых форм собственности, с любой численностью штата.



Больше информации на **cloud.softline.ru**

Консультация специалиста:

8-800-232-00-23 **cloud@softline.com**

softline® 25 Years In IT