softline direct

КАТАЛОГ ИТ-РЕШЕНИЙ И СЕРВИСОВ ДЛЯ БИЗНЕСА

04
2018

- Защита критической информационной инфраструктуры
- Контроль пользователей
- DLP
- Целенаправленные атаки

СПЕЦВЫПУСК:

КИБЕР БЕЗОПАСНОСТЬ:

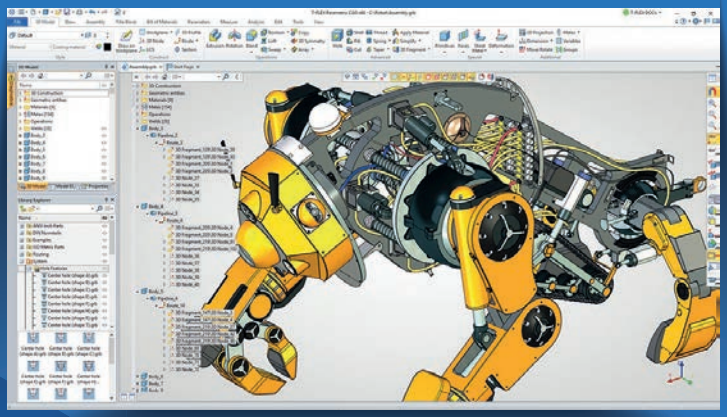
достигнуть и сохранить

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

ACTIVEDESK - ЕДИНОЕ РАБОЧЕЕ ПРОСТРАНСТВО ДЛЯ ИНЖЕНЕРНО-ПРОЕКТНЫХ КОМАНД

ActiveDesk - это привычный рабочий стол с мощной видеокартой для эффективной совместной работы с ресурсоемкими приложениями. Он доступен с любого устройства из любого места. Сервис создан на базе технологий виртуализации VMware и NVIDIA GRID и размещен в защищенном российском дата-центре мирового уровня.

ActiveDesk позволяет приобретать требуемое количество рабочих столов заданного быстродействия и оплачивать их использование на ежемесячной основе по факту реального потребления, что максимально удобно при проектном подходе.



ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ СЕРВИСА ACTIVEDESK

Удобство совместной работы

Возможность развернуть новый проект за несколько минут

Удаленный доступ с любого устройства из любого места

Беспрецедентная защита данных от копирования

Оплата услуг только по факту реального потребления

ПАРТНЕРЫ СЕРВИСА ACTIVEDESK

AUTODESK · GRAPHISOFT · NANOCAD УМНОЕ ПРОЕКТИРОВАНИЕ · esri CIS ArcGIS · T-FLEX · SolidWorks · MathWorks · Solution Partner PLM SIEMENS · АСКОН

СВЯЖИТЕСЬ С НАМИ, ЧТОБЫ УЗНАТЬ БОЛЬШЕ И ПОЛУЧИТЬ ВОЗМОЖНОСТЬ ПРОТЕСТИРОВАТЬ СЕРВИС!

Цена сервиса в день примерно равна

2 чашкам кофе

ActiveCLOUD

8-800-100-22-50
www.activedesk.ru
welcome@activedesk.ru

Уважаемые читатели!

Как часто, когда мы читаем о новых технологиях, у нас захватывает дух от скорости их появления и возможностей, которые они предоставляют. Современные гаджеты и мобильные устройства, не только красивые, но и функциональные, облачные технологии, стирающие любые ограничения по удобству, доступности и масштабируемости сервисов, невероятные объемы хранения, реализованные в том числе в мобильном исполнении, — все это доступно не за космические деньги, а практически каждому!

Просто безграничные возможности! Остается только не забывать, для кого они появляются.

Любое изменение в инфраструктуре и процессах работы компании – это новые возможности не только для вас, но и для злоумышленников. Когда изменения происходят постоянно, не всегда под контролем подразделений по кибербезопасности, а иногда даже без привлечения ИТ-тделов, — это самый желанный подарок для киберпреступников.

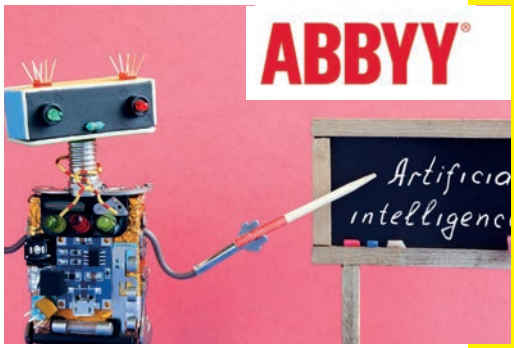
Для Softline крайне важно обеспечть качество реализации проектов по кибербезопасности. Для этого мы внимательно следим за трендами как на российском, так и мировом рынках кибербезопасности, а изучая новые веяния, всегда стараемся оценить применимость технологий с учетом территориальной специфики и отраслевой принадлежности заказчиков.

В этом выпуске мы хотим поделиться с вами информацией по технологиям, которые считаем наиболее актуальными в текущем году. Желаю интересного чтения!

Олег Шабуров,
руководитель департамента
информационной безопасности Softline

СОДЕРЖАНИЕ

Интервью номера



Производство

Решение об увеличении территории продаж SOLIDWORKS обосновано растущим спросом на продукты и сервисы, а также широким географическим разбросом клиентов Dassault Systèmes в России и СНГ. Таким образом, Dassault Systèmes начала выстраивать сеть партнеров и реселлеров, которая будет предлагать продукты бренда SOLIDWORKS, включая новейший релиз – SOLIDWORKS 2018.

Эффективность бизнеса

До GIFTD механизмы поведенческого маркетинга с эффективным конверсионным потенциалом были доступны только большим компаниям с внутренними ИТ-отделами, которые разрабатывали его годами. Благодаря GIFTD доступ к подобным инструментам имеют также малый и средний бизнесы.

Обучение

Облачные технологии

Каталог ИТ-решений и сервисов для бизнеса

Softline direct

#04-2018

2018-3(182)–RU

Учредитель: АО «СофтЛайн Трейд»

Издатель: Игорь Боровиков

Главный редактор: Лидия Добрачева

Редакторы: Яна Ламзина,

Максим Туйкин,

Вячеслав Гречушкин,

Антонина Субботина

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

Над номером работали:

Олег Шабуров, Виктория Гущина, Татьяна Гапоненко, Ирина Щербакова, Ольга Лебедева, Наталья Решетова, Наталья Иванова, Екатерина Паршикова, Александр Макаров, Ксения Сазонова, Ирина Галактионова, Александр Ефремов, Екатерина Корбун, Анатолий Герцен, и др.

Тираж: 60 000 экз.

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

Softline в соцсетях

SoftlineCompany Softlinegroup SoftlineCompany softlinegroup

СПЕЦИАЛЬНЫЙ ВЫПУСК: Кибербезопасность

За безопасность необходимо платить, а за ее отсутствие — расплачиваться.

Уинстон Черчилль

Конспект.

ПОРТРЕТ КОМПАНИИ

Наша миссия

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

ПОЧЕМУ SOFTLINE?

1. Мы — глобальная сервисная компания, которая помогает бизнесу и государству осуществить цифровую трансформацию
2. Надежность, профессионализм и компетентность Softline признаны клиентами, вендорами и независимыми источниками
3. Единая точка решения всех ИТ-задач, мультивендорная поддержка и сопровождение
4. Softline всегда рядом и говорит с заказчиками на родном языке более, чем в 30+ странах и 80+ городах
5. Softline доверяют ведущие игроки рынка, государственные организации, средние и малые компании

Digital Transformation & Cybersecurity Solutions Service Provider

Статусы Softline

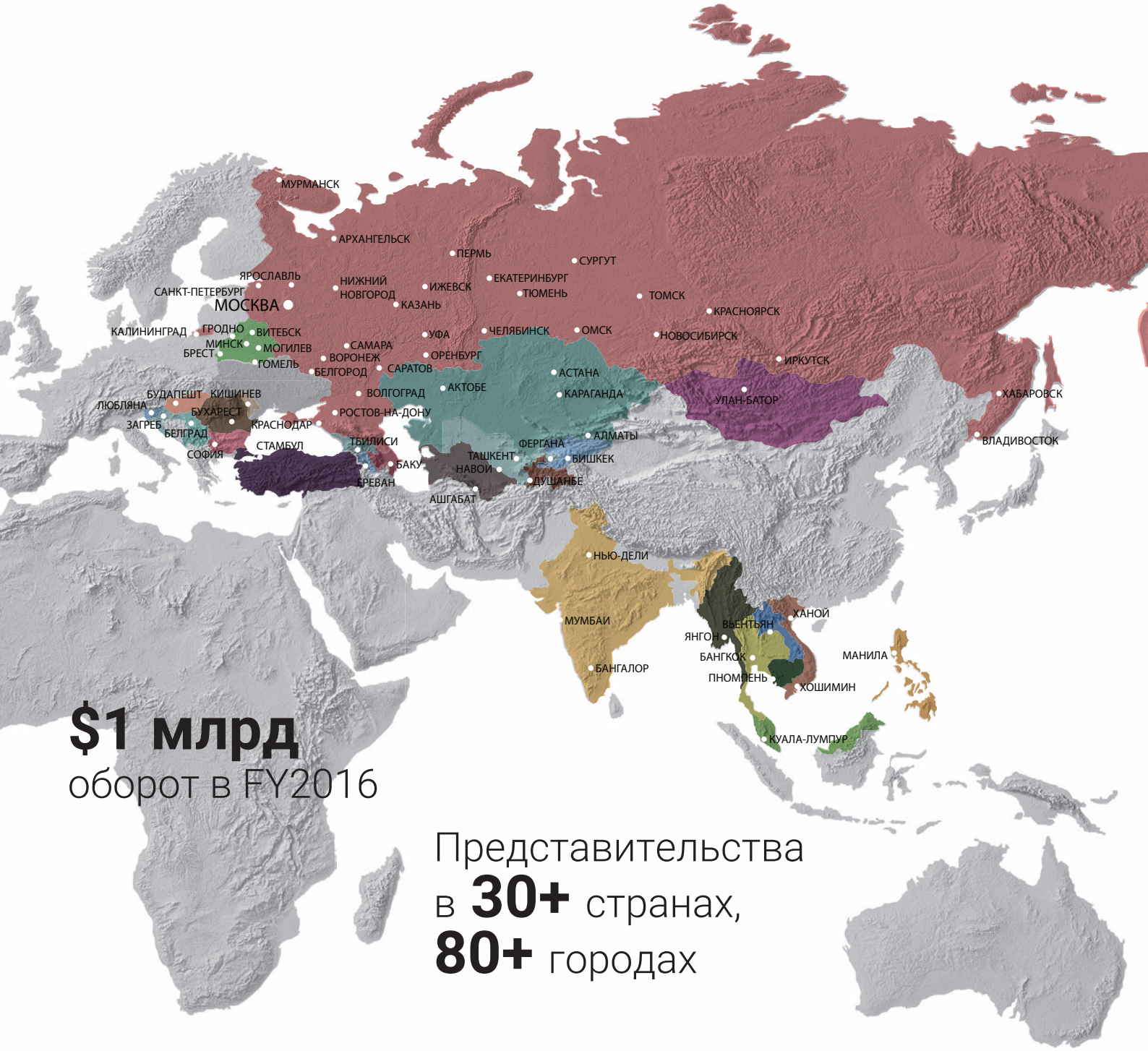
Microsoft Partner

- Gold 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 PREMIER SOLUTION PROVIDER · Hewlett Packard Enterprise Gold Partner

Dell PartnerDirect Preferred · IBM Gold Business Partner · Intel Software Elite Reseller · Citrix PARTNER Platinum Solution Advisor

Acronis Gold Partner · Veritas Partner Force Platinum Partner · APC by Schneider Electric PREMIER PARTNER · ESET Corporate Premier Partner



$1 млрд
оборот в FY2016

Представительства
в **30+** странах,
80+ городах

+39% среднегодовой рост
за последние 10 лет

25 лет
на ИТ-рынке

НАШИ ЗАКАЗЧИКИ

от стартапов до транснациональных корпораций

ПРОИЗВОДСТВО И ЭНЕРГЕТИКА

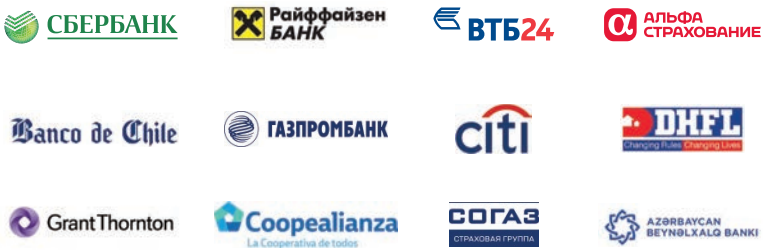
А также:
Объединенная компания РУСАЛ | Интер РАО ЕЭС | Акрихин | Трансмашхолдинг | Соллерс | Сибур | Chinfon Cement | Джи Эм-АВТОВАЗ | Toyota Tsusho | Caterpillar | Мосэнерго | Камчатскэнерго | ОГК-2 | Вимм-Билль-Данн | МРСК Северного Кавказа | STADA CIS | Hever Solar | Onninen | Металлимпресс | Damate | 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 | Telefónica | TELE2 | Ucell | Supercanal | Al Jazeera Türk | Ростелеком

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

ГОСЗАКАЗЧИКИ

ROSOBORONEXPORT | POS Malaysia | РЖД | Росатом | Kyrgyzpatent | Роснано | ФИРВ | Ministerio de Educación Presidencia de la Nación | Perú Ministerio del Interior | 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

ABBYY®

ВСЕ СЛОЖНОЕ — ВОЗМОЖНО

В компании ABBYY работают люди, которые мыслят на шаг вперед. Гость нашего номера Дмитрий Шушкин, генеральный директор ABBYY Россия, несомненно, ценит инновационность во всем, особенно в мышлении, и подчеркивает, что программистов, инженеров, лингвистов, менеджеров ABBYY мотивируют нестандартные, а часто и уникальные задачи. Вместе сотрудники создают технологии и решения в области интеллектуальной обработки данных для различных задач бизнеса.

— Дмитрий, как в последние годы меняются потребности ваших заказчиков и задачи, стоящие перед ними?

— В последние несколько лет заказчики все чаще выбирают решения, которые уже завоевали себе место на рынке и доказали эффективность: помогли компаниям увеличить выручку, уменьшить расходы, создать новые каналы получения дохода или повысить качество обслуживания. Кроме того, компании заинтересованы в быстром возврате инвестиций от внедрения ИТ. Более привлекательны решения, которые окупаются за год, а лучше – еще быстрее. Наконец, заказчики стремятся нарастить конкурентные преимущества, в том числе за счет машинного обучения и роботизированной автоматизации процессов (RPA).

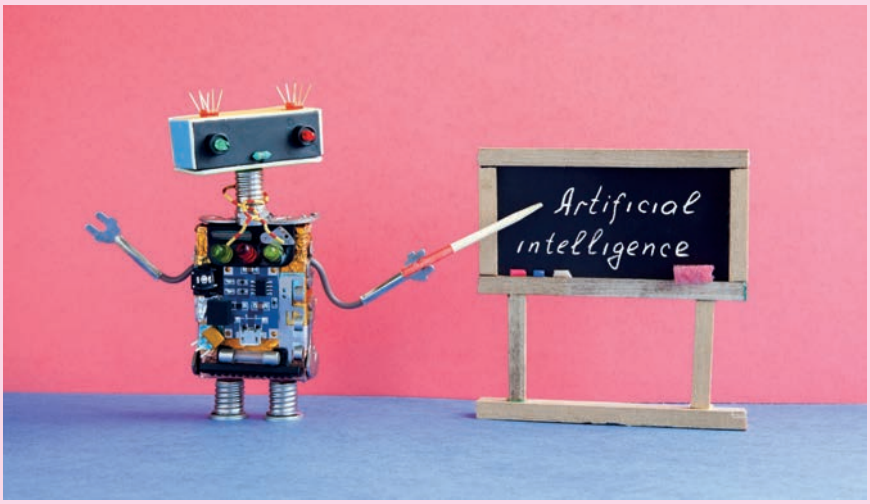
Мы видим, что все больше становятся востребованы решения, которые умеют искать и анализировать неструктурированные данные из разных источников: бумажных, электронных документов, внутренних баз компании, СМИ и социальных сетей. Например, чтобы регистрировать клиентов, принимать решения об открытии банковских счетов или выдаче кредитов, оценивать поставщиков товаров и услуг на тендерах, искать документы в корпоративных системах и т.д.

Наиболее «продвинутой» с точки зрения внедрения технологий искусственного интеллекта в России можно назвать банковскую отрасль. Здесь высока конкуренция, и финансовым организациям важно ускорять все процессы — быстрее открывать счета, одобрять кредиты, выводить на рынок новые банковские продукты. Также большим спросом интеллектуальные решения пользуются в энергетике, нефтегазовом секторе и ИТ.

— Какую технологию ABBYY вы считаете самой уникальной, непревзойденной?

— В структуре бизнеса ABBYY продукты и решения тесно связаны между собой и функционально дополняют друг друга. Наша универсальная платформа для интеллектуальной обработки данных ABBYY FlexiCapture извлекает данные из любых документов: электронных писем и вложений, бумажных документов, электронных документов в офисных форматах, фотографий с камер и мобильных устройств. А технологии искусственного интеллекта понимают смысл и извлекают только значимую информацию из всего потока. Вместе или по отдельности, эти решения трансформируют бизнес-процессы банков, энергетических компаний, розничных сетей, телеком-операторов и других компаний, которые обрабатывают большой объем документов.

ABBYY также активно развивает технологии для разработчиков (SDK). В прошлом году мы предложили рынку ABBYY Real-Time Recognition SDK — технологию, которая умеет мгновенно извлекать информацию не только из документов, но и с поверхностей различных предметов. Например, с этикеток, счетчиков, автомобильных номеров, экранов мониторов, паспортов, транспортных накладных, счетов на оплату. Технологию уже тестируют и внедряют банки, телеком-операторы, транспортные и другие компании.



— Компания проводит интересные мероприятия (конкурсы идей, хакатоны), организует конференцию «Диалог» и поддерживает работу двух кафедр в МФТИ. Вклад в науку и образование и просветительская деятельность – это миссия компании или маркетинговая стратегия?

— ABBYY разрабатывает интеллектуальные решения, которые основываются на результатах серьезных научных исследований в области искусственного интеллекта, распознавания образов и компьютерной лингвистики. Поэтому мы поддерживаем ряд образовательных и научных инициатив. Некоторые из них, такие как работа в МФТИ и других ведущих российских вузах, конкурсы, хакатоны, помогают нам находить идеи для развития бизнеса, придумывать и реализовывать новые проекты, искать молодых специалистов: талантливых разработчиков, data scientists, архитекторов нейросетей и других. Более четверти наших коллег из департамента R&D вовлечены в академические программы компании. Студенты, которые проходят обучение на кафедрах, еще во время учебы имеют возможность получить практические навыки создания инновационных проектов. Некоторые из них приходят работать к нам по окончании вуза.

Поддержка конференции «Диалог» — это некоммерческая инициатива компании. Это мероприятие проводится уже больше 35 лет, и последние несколько десятков лет ABBYY – его основной организатор. Основные идеи «Диалога» совпадают с теми позициями в сфере обработки естественного языка, которых всегда придерживалась наша компания: что будущее компьютерной лингвистики – в соединении современных инженерных и математических методов и полноценной лингвистики. «Диалог» призван привлечь внимание к тем направлениям, в которых сильна российская компьютерная лингвистика. Для этого мы приглашаем исследователей с мировым именем, и они рассказывают о своих проектах, делятся опытом работы.

— Расскажите немного о людях, которые работают в компании. Как вы можете охарактеризовать свою команду?

— ABBYY создает сложные технологии и решения в области искусственного интеллекта. Поэтому в нашей компании работают люди, которые мыслят инновационно, они способны и желают самостоятельно учиться. Мы по-настоящему глобальная команда: наши 16 представительств работают в 13 странах. Сотрудники ABBYY в России активно взаимодействуют с коллегами по всему миру, делятся идеями, обмениваются опытом.

— Если бы вы не были генеральным директором ABBYY – то чем бы занялись? Есть ли еще какая-то сфера деятельности, которая привлекает вас не меньше, чем руководство компанией?

— Мне всегда было интересно создавать нечто, что приносит пользу людям, и делать это добросовестно и с душой. Даже если бы я не руководил компанией, уверен, что есть множество профессий, где такие качества были бы востребованы.

— Как руководитель, чему вы еще хотели бы научиться, совершенствуясь в профессиональном плане? И какой свой навык/знание считаете самым ценным на сегодняшний день и почему?

— Я считаю, что само по себе умение непрерывно учиться, развиваться, изучать новое — необходимы, хотя и не являются единственным условием успеха в любом деле. Каждый день я узнаю что-то новое от коллег, клиентов, партнеров, родителей, семьи, друзей. Иногда – даже от своих детей. Самое ценное — это, конечно, опыт: его ни на что не променяешь.

Автоматизация работы call-центра энергосбытовой компании

«Тольяттинская энергосбытовая компания» получила обновленную систему IP-телефонии на базе решения Avaya, что позволило автоматизировать рутинную работу по обработке входящих и исходящих вызовов.

Ситуация

Клиентская база ОАО «ТЭК» насчитывает более 20 тыс. абонентов. Для эффективной работы call-центра требовалась модернизация системы телефонной связи, поскольку компании необходимо было обеспечить масштабируемость и подключить дополнительный функционал для приема показаний приборов учета электроэнергии и автообзвона должников. На конкурсной основе партнером была выбрана компания Softline, которая предложила самое оптимальное по стоимости и функциональным возможностям решение.

Решение

В рамках проекта была произведена поставка и установка телефонной станции Avaya IP Office R10 и новых телефонных аппаратов. Специалисты Softline осуществили плавную миграцию пользователей и настроили голосовое меню на едином многоканальном номере компании. Следующим этапом стала автоматизация работы call-центра посредством программного комплекса Personal IT от компании ProfIT. Для заказчика был развернут центр обработки вызовов с распознаванием голоса и эффективной маршрутизацией звонков. Клиенты «Тольяттинской энергосбытовой компании» для передачи показаний счетчиков могут воспользоваться сервисом автоматизированной обработки данных, который доступен из голосового меню, или позвонить по специальному выделенному номеру. Электронный оператор сверяет данные с клиентской базой, принимает и фиксирует показания приборов учета электроэнергии, а интеграция решения с другими системами повышает скорость обработки информации. Для оптимизации работы call-центра была реализована возможность автоматизированных исходящих кампаний. В учетной системе формируется список должников, который при синхронизации переносится в центр обработки вызовов, и электронный оператор совершает звонки с целью донесения персональной информации о задолженностях.

Результат

«Программный комплекс Personal IT позволил автоматизировать управление исходящими и входящими вызовами заказчика. Функциональные возможности и специализированный интерфейс повышают скорость и качество работы с клиентами, позволяя быстро находить и фиксировать в базе необходимые данные. В дальнейшем решение можно дорабатывать и увеличивать объем рабочей нагрузки, например, привлекая электронного оператора для информирования клиентов компании об изменении тарифов или ремонтных работах», — прокомментировал Сергей Сидоренко, менеджер по работе с крупными корпоративными клиентами Softline.

О компании

ОАО «Тольяттинская энергосбытовая компания» — региональный поставщик электроэнергии для населения и юридических лиц.

Модернизация системы телефонной связи прошла в короткие сроки и незаметно для пользователей. Развернутое решение позволило нам существенно повысить эффективность работы call-центра. Рутинная работа по обработке типовых звонков теперь осуществляется электронным оператором, а наши специалисты могут больше времени уделять решению сложных вопросов и нестандартных ситуаций. Отдельно стоит заметить, что своевременное автоматизированное информирование потребителей об имеющихся задолженностях положительно влияет на их лояльность к компании.

Денис Демидов,
начальник отдела информационных технологий ОАО «Тольяттинская энергосбытовая компания»

кибер **НЕ** безопасность

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

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

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

Конспект
Рубрику ведет
Ольга Батчикова

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

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

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

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

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

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

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

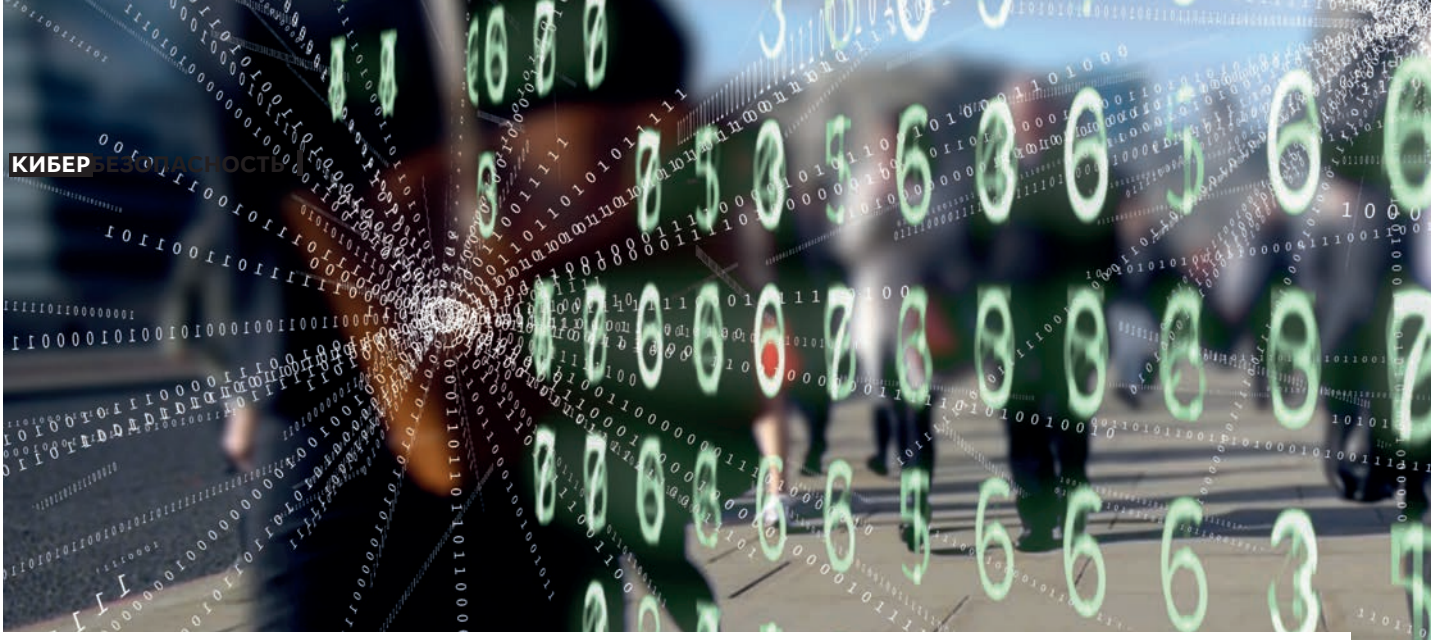
$7 млн были потеряны в результате подмены злоумышленниками адреса Ethereum-кошелька в атаке на Coindash.io

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

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

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

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



Карта решений:

подход Softline к проектированию ИБ-систем

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

Анализ и оценка информационной безопасности компании

Аудит информационной безопасности

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

Разработка концепции информационной безопасности

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

Внедрение и управление политикой безопасности и рисками

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

Защита от мошенничества

Antifraud

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

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

Сервис детектирования взлома хостов (определение зараженности ПК)

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

Системы проверки контрагентов

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

Внедрение системы обеспечения информационной безопасности

Защита онлайн-сервисов

- **Защита веб-приложений (WAF)**

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

- **Защита от DDoS-атак**

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

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

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

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

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

- **Анализ кода**

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

Защита веб и почты

- **Защита веб-трафика**

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

- **Защита почтового трафика**

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

Защита серверов, рабочих станций, виртуальной инфраструктуры, мобильных устройств

- **Защита серверов, конечных точек**

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

- **Защита виртуальной инфраструктуры**

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

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

- **Решения класса DBF (DataBaseFirewall) –** комплексный инструмент защиты корпоративных СУБД, предотвращающий основные угрозы для доступности, целостности и конфиденциальности данных.

Управление доступом

- **IDM, SSO, PKI**

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

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

- **PAM**

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

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

- **Аудит доступа к файловым ресурсам**

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

Защита информации

DLP

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

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

IRM

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

Защищенный обмен данными

Для надежного и безопасного обмена данными мы предлагаем следующие решения:

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

Классификация информации

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

Шифрование

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

Защита сети, ATP

Межсетевые экраны нового поколения

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

Защита от целевых атак и атак «нулевого дня»

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

Firewall management

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

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

Безопасность КИИ и АСУ ТП

Защита АСУ ТП

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

Решения по однонаправленной передаче данных

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

Центры реагирования ИБ (SOC)

SIEM

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

SECaaS

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

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

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

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

Поддержка

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

Система мониторинга и отчетности использования информационных ресурсов

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

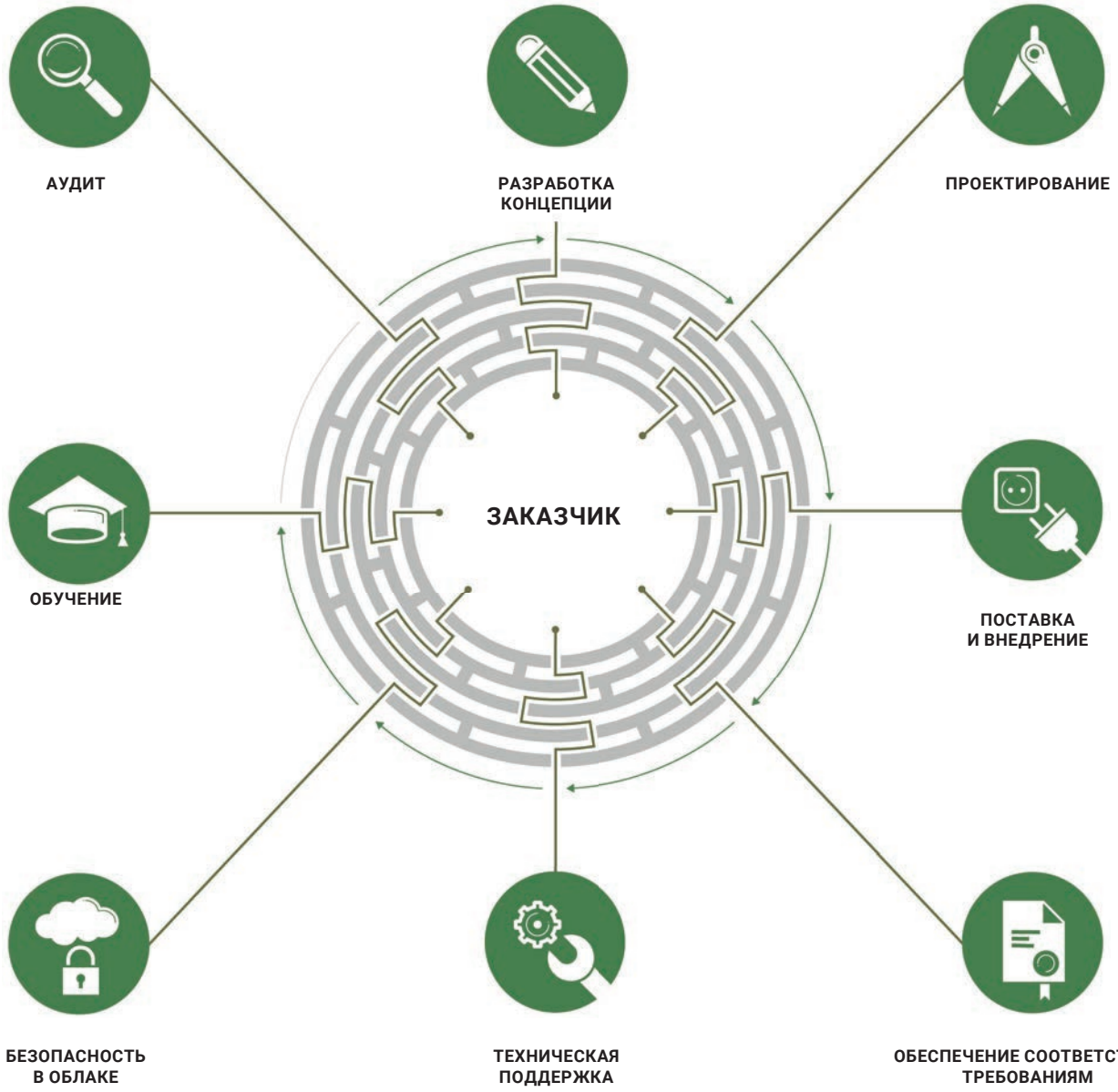
Техническая поддержка и сопровождение систем ИБ

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

Обучение специалистов заказчика

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

Комплекс услуг по проектам



Безопасность облака в соответствии с требованиями законодательства

Предоставляя мощности нашего центра обработки данных клиентам, мы должны быть уверены в безопасности сервисов. Риски могут оцениваться в миллионах рублей, поэтому мы доверяем проектирование и внедрение системы защиты профессионалам. Сегодня наше облако надежно защищено благодаря решениям партнеров.

Олег Морозов,
директор направления связи группы компаний «Искра»

Оценка уровня обеспечения ИБ АСУ ТП в соответствии с требованиями законодательства

Выступив в проекте как внешний аудитор, Softline провела обследование систем автоматики и разработала для нас необходимые документы по информационной безопасности АСУ ТП для исполнения требований приказа ФСТЭК №31. Все работы были выполнены качественно и в установленные сроки.

Владимир Демидов,
начальник службы информационной безопасности ООО «Транснефть – Порт Приморск»

Надежный партнер по обеспечению безопасности

В Softline сформирована одна из самых компетентных в России команд по кибербезопасности. Выполняя сотни проектов в год, мы учитываем отраслевую специфику наших заказчиков и гарантируем сочетание высокого качества, приемлемой стоимости внедрения и сопровождения систем безопасности.
Наш портфель включает широкий спектр решений: от DLP и защиты ПДн до проектов по защите от направленных атак и обеспечения безопасности критических инфраструктур. Для максимальной отдачи от внедрения сложных систем мы проводим обучение сотрудников организаций и предлагаем техническое сопровождение систем.
Неизменно высоким спросом у наших государственных заказчиков пользуются проекты по проведению аудитов безопасности и аттестации объектов автоматизации. Мы обладаем всеми необходимыми лицензиями для осуществления работ по информационной безопасности и будем рады поделиться опытом с вами.

Более
50 консультантов

Более
20 руководителей проектов

Более
50 инженеров

Орган по аттестации и лаборатория
специальных исследований

Учебный
центр

Поддержка
24x7x365

Присутствие
в 15 городах России

Создание защиты ИТ-инфраструктуры Правительства Камчатского края

Удобная отчетность, гибкие политики информационной безопасности и успешно пройденная проверка характеристик для получения сертификата ФСТЭК России доказывают эффективность работы созданного программно-аппаратного комплекса и подтверждают правильный выбор решения.

Инга Леонтьева,
руководитель Агентства по информатизации и связи Камчатского края.

Создание криптозащищенной сети передачи данных Сибирского регионального центра МЧС России

В ходе проекта специалисты Softline разработали архитектуру независимой сети, обеспечили поставку необходимого оборудования, внедрили и настроили решение. В настоящее время администрирование сети полностью перешло под контроль Сибирского регионального Центра МЧС в Красноярске.

Валерий Вамбольдт,
заместитель начальника отдела связи и АСУ СРЦ МЧС России.

КИБЕРБЕЗОПАСНОСТЬ В SOFTLINE

Представительства

30+ стран **80+** городов

ОРГАН ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

- Более 180 аттестованных объектов с 2015
- Наличие собственной измерительной площадки
- Консалтинг по оформлению лицензий ФСБ, ФСТЭК

СЕРВИСНЫЙ ЦЕНТР

- Круглосуточная линия технической поддержки 24x7
- Более 200 поддерживаемых производителей
- Более 100 сертифицированных инженеров и администраторов

РАЗРАБОТКА СРЕДСТВ ЗАЩИТЫ

«Стахановец» и Phishman – производители средств защиты в группе компаний Softline

SOC (SECURITY OPERATION CENTER)

- Цент управления кибербезопасностью
- Управляемые услуги по безопасности

УЧЕБНЫЙ ЦЕНТР

- №1 на рынке корпоративного обучения
- Более 100 курсов по информационной безопасности
- Центры тестирования в 11 городах России и 12 городах СНГ
- Очное и дистанционное обучение в любом городе

СИСТЕМНАЯ ИНТЕГРАЦИЯ

- Лицензия на ТЗКИ с 2005
- Более 1500 реализованных проектов по ИБ с 2010

ПОСТАВКА ПО

- Высшие партнерские статусы по большинству ключевых производителей средств защиты на рынке
- Возможность поставки решений как от лидеров рынка, так и экзотических решений

150+ специалистов

по направлению ИБ

Расчетный центр ЖКХ в Волгограде усовершенствовал систему безопасности

С помощью Softline компания внедрила систему контроля и управления доступом, систему управления рабочим временем и систему видеонаблюдения.

Ситуация

В течение нескольких лет в приоритете АО «ИВЦ ЖКХ и ТЭК» Волгограда были вопросы информационной безопасности. Обучение персонала, применение эффективного программного обеспечения и поддержание его в актуальном состоянии позволили выстроить надежную систему противодействия хакерским атакам. Оставалось усовершенствовать защиту физического периметра центрального офиса расчетного центра и его удаленных объектов.

Решение

Для обеспечения наблюдения за территорией в главном офисе заказчика были использованы камеры компании RVI, в удаленных филиалах с той же целью используется оборудование Dahua. Управление доступом организовано с помощью решений фирмы Tantos: все комплектующие интегрируются между собой. Система управления рабочим временем организована с помощью контроллера российского производителя – компании «Эра». Отечественный продукт показал себя надежным, функциональным и соответствующим задачам заказчика.
подзаголовок

Результаты

«Проект с таким крупным заказчиком – хорошая возможность для Softline продемонстрировать экспертизу в области инфраструктуры зданий и сооружений на юге России. Четко поставленная заказчиком задача – объединить несколько систем в одно функциональное решение – была блестяще реализована нашими инженерами. Теперь физический периметр находится под постоянным контролем автоматизированной системы», — говорит Игорь Доброшенко, менеджер по продаже решений группы компаний Softline. ▮

Обеспечение безопасности – это комплексный вопрос, который должен решаться как на уровне ИБ, так и на уровне контроля за физическим периметром. Очевидно, что автоматизация доступа в помещения существенно снижает риски, связанные в том числе и с кибербезопасностью. Мы благодарны коллегам из Softline, которые оперативно справились со всеми поставленными задачами.

Дмитрий Завьялов,
Заместитель генерального директора по безопасности ИВЦ ЖКХ и ТЭК г. Волгограда

КОНТРОЛЬ привилегий

Рассказывает Иван Молотилов, руководитель направления управления доступом компании Softline.

Процесс предоставления доступа и фиксации действий привилегированных пользователей требует повышенного внимания, особенно, если доступ необходим к информационным системам с критически важными для бизнеса данными или процессами. Чем больше прав – тем больше рисков злоупотребить предоставленным доступом или совершить и скрыть ошибку, которая может стоит бизнесу очень дорого.

Все современные системы инфраструктуры или безопасности строятся по принципу разграничения прав, но всегда остаются так называемые немногочисленные привилегированные пользователи с абсолютными правами. Контролировать их затруднительно, так как для этого необходимо быть не менее опытным специалистом в области администрирования. Наблюдателей за сотрудниками, работающими удаленно, тем более не приставишь.

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

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

Во внедрении PAM заинтересованы не только специалисты безопасности компании, а в равной степени и руководители ИТ-подразделения, так как именно они отвечают перед бизнесом за непрерывность ИТ-процессов, выбор субподрядчиков и интеграторов для делегирования задач внедрения и обслуживания информационных систем. Определенная степень интереса есть и у внутренних заказчиков от бизнеса, если задачи их подчиненных связаны с определенными финансовыми или технологическими рисками (например, риском мошенничества). Хотя эти пользователи и не являются администраторами, они также являются привилегированными, и необходима возможность фиксации их действий с последующим использованием в качестве доказательной базы при расследовании инцидентов.

Ключевые возможности PAM

- Управление паролями общих и привилегированных учетных записей.
- Анализ и фильтрация вводимых команд и действий.
- Аудит действий привилегированных пользователей.
- Управление доступом привилегированных УЗ, по запросу, с ограничением времени доступа.
- Изоляция целевых серверов и ресурсов.

Какие вопросы в этой связи стоят перед руководителями ИТ и ИБ?

- **Кто имеет доступ к критически важным ресурсам и как контролировать работу этих людей?**

  Зачастую контроль над учетными записями ведется слабо или не ведется вообще. Потенциально среди них могут оказаться backdoor-аккаунты, эксплуатируемые злоумышленниками или вредоносными программами. Забытая и недеактивированная учетная запись может позволить эксплуатировать эксплоиты систем и поднять привилегии. Это причинит большой вред всей инфраструктуре компании. PAM-решение поможет минимизировать количество технологических УЗ, вести их учет, а также тщательно журналировать факты их использования и деанонимизировать пользователей, так как технологические УЗ имеют очень «размытых» ответственных, максимум — зафиксированных на бумаге.

- **Как защитить системы и данные от ошибок пользователей, а также от злонамеренного умысла?**

  Никто не деален, все совершают ошибки. Для минимизации человеческого фактора в процессе обслуживания систем PAM дает возможность фильтрации команд и действий пользователей по черным и белым спискам, которые можно тонко настроить на группы систем и пользователей как политики. Есть и обратный эффект, если сбой или инцидент произошел не по вине человека, а из-за багов ПО системы, то PAM поможет доказать, что сбой произошел не по вине администраторов или пользователей.

- **Как расследовать инциденты, где брать доказательства?**

  «На лету» всех за руку поймать невозможно: нужна доказательная база, журнал событий, видеоархив сессий, логи, которые пользователь не сможет почистить за собой. Все это обеспечит детальную картину и последовательность действий приведших к инциденту. Такой разбор позволит предпринять меры, чтобы в будущем ситуация не повторилась.

- **Кому известны пароли от привилегированных учетных записей, и как контролировать распространение паролей?**

  Смена и стойкость паролей — это извечный вопрос на стыке безопасности и удобства. Вместе с тем, пароли меняются с недостаточной периодичностью и надежностью, поскольку те легко забываются. Аутентификацию нужно проходить не в одной, не в двух, а более чем в десятках систем, и в результате часто сотрудники используют 3-5 «золотых» паролей «для всего». Отдельно стоит выделить работу с базами данных или иными системами, которые необходимо бэкапировать. Если пароли меняются, то вспомнить, какой пароль действовал для конкретного бэкапа в прошлом – почти невозможно, проще их вообще не менять годами, иначе бэкап может оказать бесполезным. PAM может защищенно хранить пароли и историю их изменений на любую дату в прошлом. Помимо этого, гранулированно предоставлять их пользователям или аутентифицировать пользователя по принципу SSO без раскрытия пароля от конечной защищаемой системы. Пользователю достаточно знать только свою учетную запись для входа в PAM, которая может быть и учетной записью AD, опционально усиленной дополнительным фактором аутентификации, например, значением OTP.

Эти вопросы могут быть контрольными для оценки необходимости внедрения PAM системы, если у вас нет уверенного ответа хотя бы на один из них, то стоит более пристально присмотреться к решениям и, возможно, организовать пилотный проект.

Аудиторы и субподрядчики

Работа с субподрядчиками – большой тренд сегодняшнего дня: многие компании передают обслуживание ИТ-инфраструктуры на аутсорсинг, внедрение новых систем проводится силами компетентных интеграторов. Благодаря функционалу PAM ваша организация может контролировать SLA и быть уверенной, что они не делают ничего сверх или, наоборот, менее того, что, согласно договору, должны делать.

К привилегированным пользователям можно отнести и внешних аудиторов — независимых или из проверяющих госорганов, чтобы не предоставлять им абсолютные права, а только те, которые необходимы для проведения аудита или проверки. Такой подход позволит быть уверенным, что аудиторы не унесли с собой коммерческую тайну, не являющуюся целью аудита, и не оставили программных закладок.

Пароли и ключи

Решения для контроля над привилегированными пользователями появились порядка 20 лет назад.

Изначально функциональность первых PAM-систем была ограничена менеджерами паролей корпоративного уровня — централизованным хранением паролей и безопасной выдачей их пользователям. От безопасности логинов и паролей администраторов (или root для *nix систем) зависела и всегда будет зависеть эффективность работы всей компании. Согласно статистике, большинство угроз информационной безопасности реализуется через хищение учетных записей — как пользовательских, так и администраторских.

PAM-решение выдает пользователю пароль для работы с системой, затем автоматически его меняет по расписанию или событию. Автоматизация изменения паролей важна, чтобы человек не мог использовать полученный пароль повторно и вне регламента, если он смог его изменить или узнать в ходе сессии, а поскольку сотрудник обладает правами администратора — такая ситуация вполне возможна. Функционал управления паролями также включает автоматическое сканирование сети и сбор новых паролей и, при необходимости, перенос в защищенное хранилище. Эта мера позволяет исключить появление тех самых backdoor-аккаунтов.

«На лету» всех за руку поймать невозможно: нужна доказательная база.

При управлении паролями важно обеспечение отказоустойчивости и резервирования системы PAM для доступности парольной информации и возможности доступа к контролируемым системам. Радует тот факт, что большинство производителей уже в базовый функционал включают функции резервирования и аварийного восстановления.

Контроль сессий

Кроме обеспечения безопасности паролей стоит также позаботиться о контроле происходящего внутри сессий, будь то графический сеанс работы или текстовый лог команд. Первые подобные решения появились около 10-15 лет назад, но пик популярности в России они пережили относительно недавно.

Функционал некоторых PAM-систем подразумевает как управление доступом, так и паролями.

За рубежом большинство компаний выбирают решения по управлению учетными записями, а вот в России чаще склоняются к контролю за привилегированным доступом. Скорее всего, это результат того, что первыми на российский рынок вышли компании, предлагающие решения по управлению только сессиями.

За рубежом большинство компаний выбирают решения по управлению учетными записями, а вот в России чаще склоняются к контролю за привилегированным доступом. Скорее всего, это результат того, что первыми на российский рынок вышли компании, предлагающие решения по управлению только сессиями.

Архитектура

Самая распространенная архитектура решений контроля сессий — прокси-сервер: система «слушает» или перенаправляет трафик сессий и выполняет так называемую роль «man in the middle», не внося изменений в саму сессию, но фиксируя видеопоток для графических сессий или текст для SSH-сессий. Для разбора происходящего внутри графических сессий применяется технология распознавания текста OCR. Есть нюанс: OCR всегда работает постфактум и, к тому же, если на экранах много текста, — будет выдавать ошибочное срабатывание. Технология очень чувствительна к шрифтам, их прозрачности и контрастности фона. Потому такие решения скорее являются средствами фиксации и расследования событий, и в меньшей степени применимы для предотвращения инцидентов в реальном времени.

Решения, которые работают по принципу terminal-сервера или jump-сервера, для разбора происходящего внутри сессий используют информацию из самого протокола: видят заголовки окон, запущенные фоновые процессы и клавиатурный ввод пользователя. Это позволяет в режиме реального времени анализировать все происходящее в системе и применять соответствующие политики.

Решения

Мировым лидером PAM-отрасли является CyberArk — производитель наиболее функциональных решений. Один из самых узнаваемых и распространенных в СНГ среди прокси-решений для контроля сессий — BalaBit SCB.

Для хранения паролей компаниям enterprise-сегмента (1000+ пользователей) можно рекомендовать Lieberman Software — пионера в отрасли управления учетными записями. С ним отлично интегрируется решение ObserveIT, которое обеспечивает контроль сессий по агентской схеме, когда нет выделенного прокси-сервера, и на каждую контролируемую систему устанавливается агент.

Компаниям СМБ-сектора для хранения паролей подойдет Thycotic — молодое решение, которое активно догоняет CyberArk по функциональности, а для контроля сессий – FUDO, архитектурно схожее с BalaBit SCB.

Стоит отметить, что отдельные продукты по контролю доступа и управлению паролями разных производителей имеют штатные возможности интеграции между собой, что позволяет достичь единого более гибкого решения, с преимуществами каждой из интегрируемых систем.

Среди отечественных решений можно отметить SafeInspect – единственное решение в реестре отечественного ПО, потому интересное в первую очередь государственным компаниям и организациям.

Опыт Softline

Softline имеет опыт реализации проектов PAM в лидирующих компаниях из отраслей энергетики, финансов, нефтегазовой промышленности и ретейла. Архитекторы и консультанты компании по вопросам информационной безопасности готовы помочь в организации пилотных проектов и выборе оптимального решения для уникальных нужд каждого клиента. ▮

Остались вопросы?
Пишите: Identity@softline.com
Звоните: +7 (495) 2320023 доб. 1836

Softline SAM Cybersecurity

Анализ инфраструктуры клиента с точки зрения кибербезопасности от Softline основан на международной методологии SANS и опирается на лучшие мировые практики.

SAM позволяет оптимизировать программные активы с учетом потребностей бизнеса и современных технологий.

АНАЛИЗ
Эти данные используются для определения областей, которые нуждаются в улучшениях.

ОЦЕНКА
Необходимость оценки угроз ИБ для деятельности компаний становится критически важной для современного бизнеса.

РЕКОМЕНДАЦИИ
касательно того, на что директорам по ИТ и сотрудникам службы безопасности следует обратить внимание.

Вам нужен этот проект, если:

- в компании гибридная структура решений (локальных и облачных);
- есть большое разнообразие и количество используемых устройств и ПО;
- бизнес растет, требуется обеспечение соответствия ИТ-ресурсов новым бизнес-целям;
- возможны кибератаки для захвата бизнес-критичной информации;
- повысились требования к кибербезопасности;
- есть риски несоблюдения нормативных требований.

Результаты вас впечатлят

1. Оценка текущего уровня зрелости защиты ИТ-инфраструктуры от киберугроз.
2. Дорожная карта по улучшению состояния кибербезопасности.
3. Повышение управляемости процессов развертывания, приобретения и мониторинга ПО.
4. Основа для гибкой, адаптивной ИТ-инфраструктуры, готовой к изменениям ландшафта угроз.
5. Определение оптимального ПО и лицензий, соответствующих бизнес-целям.
6. Рекомендации по усилению кибербезопасности с использованием решений Microsoft и не только.

На этапе формирования итогового отчета с учетом особенностей конкретного заказчика подключаются смежные подразделения Softline: облачный департамент, департамент ИБ, департамент инфраструктуры и другие. При необходимости помимо базовых рекомендаций, может быть проведен полноценный проект по ИБ.

А что потом?

Softline предлагает решение обнаруженных проблем. Например, разработку стратегии кибербезопасности; аудит по ISO/IEC 27001; оценку готовности персонала; внедрение и поддержку решений для защиты от угроз; тесты на проникновение (Penetration Testing). ∎

Управление программыми активами и кибербезопасность тесно связаны. Чтобы понять, что и от чего защищать, нужно сначала разобраться в том, что имеется. Неопознанные и неподконтрольные ИТ-активы (аппаратные и программные) в корпоративной сети представляют существенную угрозу. Анализируя данные об установленном ПО, можно оценить текущую ситуацию и определить направления для усиления кибербезопасности.
SAM Cybersecurity дает свежий взгляд на нематериальные активы и указывает пути к решению важных вопросов информационной безопасности.

Илья Панкратов,
заместитель директора
департамента
бизнес-консалтинга Softline

General Data Protection Regulation

С 25 мая 2018 года в Европейском Союзе начнет применяться новый Регламент (ЕС) 2016/679 по защите персональных данных (General Data Protection Regulation, GDPR). Новый Регламент приходит на смену старому документу по защите персональных данных — Директиве 95/46/ЕС, действие которой прекращается.

Ринат Катчиев

В отличие от Директивы, Регламент является документом прямого действия, т.е. находится «выше» национальных законодательств и является обязательным для выполнения для всех стран Евросоюза.

Новый Регламент нацелен на защиту прав Субъектов персональных данных и дает им больше возможностей, например:

- **Право на доступ к данным.** Субъект может требовать информацию о характере обработки своих данных, цели и месте обработки, право доступа к своим данным и право на исправление неправильных данных;
- **Право не давать свое согласие** на обработку ПДн в целях, непосредственно не связанных с целями обработки ПДн (например, для целей прямого маркетинга), или ограничивать обработку своих данных определенным образом;
- **Право на удаление (право на забвение).** Субъект теперь имеет право требовать удаления своих данных не только из поисковых систем, но и от любого Оператора данных в условиях отзыва согласия и отсутствия других законных оснований для обработки ПДн;
- **Право на перенос данных.** Регламент предоставляет субъектам данных право потребовать у Оператора бесплатно предоставить ему копию всех обрабатываемых данные в структурированном и удобочитаемом виде или беспрепятственно передать данные другому Оператору в электронном виде.

Новый регламент расширяет перечень персональных данных, подлежащих защите. К персональным данным теперь относят не только идентификационные данные субъектов (ФИО, контактная информация, биометрические данные и т.д.), но и интернет-идентификаторы, такие как IP-адрес, cookie-файлы, RFID-идентификаторы и т.п., а также генетическую информацию (ДНК, РНК).

Принципы обработки персональных данных

Законность, справедливость и прозрачность. Данные должны обрабатываться на законных основаниях, справедливым и открытым образом в отношении субъекта данных.

Ограничение цели. Данные должны собираться и использоваться для конкретных, ясных и законных целей, заявленным Оператором и не должны в дальнейшем обрабатываться способом, несовместимым с этими целями.

Минимизация данных. Нельзя собирать больше данных, чем это необходимо для выполнения целей обработки. Необходимо стремиться к минимизации этого объема.

Точность. Обрабатываемые данные должны быть точны. Недостоверные данные должны быть уточнены или удалены.

Ограничение хранения. Личные данные должны храниться в форме, позволяющей идентифицировать Субъектов только в течение срока, необходимого для достижения целей обработки, не дольше.

Целостность и конфиденциальность. При обработке данных должна быть обеспечена защита от несанкционированной или незаконной обработки, уничтожения и повреждения.

Регламент обязует Операторов уведомлять регулирующие органы (в ряде случаев и субъектов данных) о любых нарушениях, связанных с персональными данными в течение 72 часов после обнаружения факта такого нарушения.

Кто попадает под новые требования?

Во-первых, организации, учрежденные в ЕС (включая представительства, дочерние подразделения зарубежных компаний). И во-вторых, любые иные организации, занимающиеся:

- предложением товаров или услуг субъектам из ЕС на платной или бесплатной основе (интернет-магазины, интернет-сервисы, операторы связи, туроператоры, банки и т.д. Определяющим признаком являются использование языка или валюты стран ЕС с возможностью заказывать товары или услуги на этом языке, либо упоминание потребителей/пользователей, находящихся в ЕС);
- Осуществляющие анализ действий в Интернете субъектов, находящихся в Евросоюзе (составление профиля пользователя, в том числе в целях принятия решений для анализа/прогнозирования их личных предпочтений, поведения, отношения к чему-либо или личностных характеристик. Сюда попадают интернет-магазины, поисковые системы, банки, сайты знакомств, социальные сети и иные подобные организации).

Основной нюанс в том, что действие нового Регламента экстерриториально и распространяется не только на организации стран ЕС, но и на иностранные организации, попадающие под условия, перечисленные выше. При этом надо понимать, что с появлением GDPR с трудностями столкнутся не только российские компании, а любые компании со всего света, которые хотят действовать в Европе и предлагать свои товары и сервисы европейцам.

Ответственность за невыполнение

В соответствии с Регламентом налагаемые штрафы должны быть эффективными, соразмерными и оказывать сдерживающее воздействие. Штрафы, которые могут накладываться надзорными органами за нарушения, именно такие. Если нарушение незначительно, то штраф может составлять €10 млн или 2% годового оборота. Если же регулятор сочтет, что нарушение значительно – штраф может составить €20 млн, либо до 4% годового оборота компании (в зависимости от того, что больше). Важно понять, попадает ли ваша организация под требования нового Регламента. Если у вас есть дочерние подразделения в ЕС или вы обрабатываете ПДн жителей ЕС или предлагаете им товары или услуги, рекомендуем предпринять следующие шаги:

- провести инвентаризацию информационных активов и определить, какие категории ПДн вы обрабатываете;
- описать потоки ПДн, циркулирующие в вашей компании, а также поступающие к вам и передаваемые вами;
- выявить все компании, с которыми вы обмениваетесь ПДн, которым поручаете обработку или которые поручают обработку вам;
- проанализировать законные условия, на которых вы используете персональные данные. Имеется ли у вас согласие пользователя? Можете ли вы показать, что данные обрабатываются с соблюдением баланса интересов?
- проверить пользовательские соглашения. Регламент требует, чтобы информация в них была изложена четким и доступным языком;
- подготовить политику и процедуры реагирования на утечку данных;
- создать механизмы отчетности. Компания должна иметь четкие внутренние стандарты по мониторингу, оценке и минимизации процессов обработки и хранения данных;
- определить, требуется ли назначение Инспектора по защите данных (Data Protection Officer) и представителя в ЕС;
- привести документальное обеспечение в соответствии с требованиями;
- привести в соответствие технические средства обработки ПД (шифрование, обезличивание, портативность данных и т.д.).

Мы готовы помочь!

Для реализации требований нового Регламента Softline предлагает юридический и технический аудит процессов обработки и обеспечения безопасности ПДн; оценку рисков нарушения конфиденциальности ПДн; разработку плана мероприятий и «дорожной карты» по приведению в соответствие требованиям; определение необходимых организационных и технических мер, процессов и контролей по защите ПДн; разработку необходимых организационно-распорядительных документов в части обработки и защиты ПДн; проведение оценки соответствия требованиям GDPR. ∎

Автор: Ринат Катчиев , руководитель направления аудита и консалтинга департамента информационной безопасности Rinat.Katchiev@softline.com

Новые возможности DLP-систем

InfoWatch, Solar Dozor и Forcepoint

В последнее время на российском ИТ-рынке фокус все больше смещается в сторону отечественных решений. Зарубежные аналоги также не стоят на месте. За последние два года функционал DLP-решений расширился и претерпел значительные изменения.

Из наиболее важных новшеств и тенденций следует отметить: интенсивное развитие проекта UEBA (поведенческий анализ); разработку модуля Discovery, позволяющего осуществлять поиск текстовых данных по рабочим станциям и файловым серверам; появление возможностей выстраивать графы связей, контролировать мобильные устройства и используемые облачные технологии.

Если раньше DLP-системы работали исключительно в режиме мониторинга, помогая лишь расследовать инциденты, то сейчас акцент сместился на их предотвращение. Созданы инструменты, блокирующие утечки на уровне сети и на уровне агента.

В рамках поддержки нестандартных информационных систем у InfoWatch и Solar Dozor реализована поддержка *nix-подобных систем, у Forcepoint – MacOS.

Наиболее активными потребителями DLP-систем являются крупный ритейл, банковский сегмент, нефтяная и оборонная промышленности. В последнее время к DLP-решениям проявляют значительный интерес компании, относящиеся к сегменту СМБ.

Solar Dozor

- Режимы работы – мониторинг и «в разрыв».
- Контроль каналов.
- Свой прокси.
- Модуль Discovery.
- Графы связей, встроенные в продукт.
- Анализ аномалий коммуникации.
- Единая консоль управления (веб).
- Наличие сертификатов ФСТЭК и ФСБ.
- Входит в реестр отечественного ПО Минкомсвязи.

Solar Dozor по функционалу не уступает зарубежным решениям. Интенсивно развивается аналитический центр People-Centric по работе с инцидентами. Отдельное внимание уделяется возможностям отслеживания аномалий коммуникаций и поведения сотрудников.

Из сильных сторон DLP-системы Solar Dozor следует отдельно отметить мощный автоматизированный функционал для проведения расследований и выявления мошеннических схем, аномалий поведения сотрудников. Он не является типовым функционалом данного класса решений. Единая консоль управления, где можно настраивать политики, видеть результаты, плюс встроенные инструменты для построения графов связей.

InfoWatch

Традиционный лидер российского DLP-рынка. Из нововведений последних пары лет в первую очередь следует отметить модуль InfoWatch Vision, который позволяет строить карту внешних коммуникации (визуальные схемы), что позволяет выявлять нехарактерные связи (к примеру, по каналу электронной почты с внешними контрагентами), отслеживать перемещение документов внутри организации.

Кроме того, компания InfoWatch сделала упор на мобильную тематику, обеспечивая различные подходы к обеспечению безопасности информации на устройствах.

1. Агентский подход к защите корпоративных устройств. На устройство устанавливается агент, который контролирует почту, веб, смс, мессенджеры, фото и приложения.
2. В случае, если сотрудники компании работают на собственных устройствах, больше подойдет концепция BYOD для обеспечения которой создается так называемый контейнер, через который сотрудник получает доступ к корпоративным ресурсам (почте, файловому серверу etc.). Любое скачивание документа с файлового сервера отправляется на анализ в DLP-систему. В том числе проверяются данные, отправляемые и получаемые через электронную почту. Важно отметить, что контролируется только информация, получаемая или отправляемая через контейнер. Личная информация сотрудника не проверяется.
3. Реализован модуль InfoWatch Person Monitor, который позволяет отслеживать посещаемые веб-ресурсы, либо запускаемые программы и время их активного использования. Все это сводится в единую статистику для специалистов по ИБ или HR-службы.
4. Нельзя не упомянуть также InfoWatch SDK (API) – программный интерфейс, позволяющий, интегрировать DLP-систему со сторонними сервисами (CRM-системами, базами данных и т.д.). С применением этой возможности связаны такие интересные кейсы, как создание DLP-системы, способной контролировать информацию, передающуюся в аудиоформате (например, контроль IP-телефонии), для чего в систему был внедрен модуль преобразования голоса в текст, а сам текст затем отправляется в DLP на анализ.

- Режимы работы – мониторинг и «в разрыв».
- Контроль веб и e-mail-трафика, IM, съемных носителей, хранилищ документов (SharePoint).
- Модуль Discovery.
- Мобильный агент для Android и iOS.
- Графы связей.
- Предусмотрен набор средств интеграции со сторонними сервисами, либо готовые наработки.
- Наличие сертификатов ФСТЭК и ФСБ.
- Входит в реестр отечественного ПО Минкомсвязи.

Forcepoint

Из сильных сторон Forcepoint следует отметить: AP-WEB; поддержку WEB 2.0; контроль социальных сетей; поддержку кириллического сегмента, зоны .рф; хорошую категоризацию рунета; Web DLP на борту и гибридную фильтрацию, движки анализа Flash, Java, XML, AP-DATA, блокировку отправки конфиденциальной информации на шлюзе и агенте; стабильную работу с Mac OS; контроль ActiveSync; выгрузки из СУБД; Email DLP на борту и предфильтрацию почтового трафика в облаке.

- Режимы работы – мониторинг и «в разрыв».
- Модуль Discovery.
- Поддержка MacOS.
- Работа с облаками.
- Свой прокси (в рамках подписки доступны прокси и антиспам).

За дополнительной информацией вы можете обращаться:

Борис Микулин,
руководитель направления по DLP-системам Softline
Boris.Mikulin@softline.com

Алексей Титков,
Менеджер по продаже решений группы технологического развития ИБ Softline
Alexey.Titkov@softline.com

ДЕРЖИМ ОБОРОНУ

Из года в год растет количество киберпреступников, цель которых не организация массовой атаки с поражением целого ряда случайных слабозащищенных жертв, а нанесение серьезного урона одной определенной, государственной или частной, компании. Рассказываем, какие меры стоит предпринять, чтобы минимизировать угрозу.

Громкой историей, которой дали название APT 1, стала атака на газету New York Times. Статья об этом вышла в вышеуказанном издании в 2013 г. Ответственность за организацию атаки приписывают вооруженным силам Китая. Вскоре рапорт об аналогичном кибервторжении предоставил и Wall Street Journal.

Целенаправленные атаки APT (Advanced Persistent Threat, «сложная постоянная угроза») — это всегда «долгоиграющие» мероприятия, имеющие четкий план и стратегию. Они рассчитаны не на внезапный удар по ИТ-системам, а на продолжительный захват: вы можете не знать о том, что в инфраструктуре уже действуют злоумышленники в течение долгого времени, иногда нескольких лет. Но и готовятся подобные атаки не один месяц. Им предшествует большая подготовительная работа и предварительная разведка. Кроме того, хакеры продумывают и то, каким образом впоследствии тщательно заметут следы.

Это очень опытные люди, которые умеют незаметно получfть ключи к корпоративным данным вашей компании и изучать или уничтожать их совершенно незаметно ни для кого — годами! По данным «Лаборатории Касперского», каждые семь дней появляется информация как минимум об одном случае громкой целевой атаки. На самом же деле их происходит более ста.

Какие механизмы взлома используются при организации целевых атак? С одной стороны, ничего необычного — фишинг и спам, уязвимости нулевого дня, заражение интернет-ресурсов. С другой, вирусы создаются под конкретные решения, использующиеся в компании, особенно под ПО собственной разработки и даже смежные информационные системы компаний-партнеров и поставщиков. Расчет в том, чтобы штатные средства защиты не среагировали на специально написанное хакерами вредоносное ПО.

Отличительные черты таргетированной атаки:

- долгосрочный проект с тщательной подготовкой с целью кражи денег/шпионажа;
- применяется к хорошо защищенным системам;
- атака на конкретную организацию/конкретную внутреннюю систему:
  - головной офис,
  - ПК руководителей (высший менеджмент всех департаментов по отдельности),
  - Производство,
  - ЦОД,
  - Базы данных (CRM/продажи/маркетинг/склад).

Борьба с целевыми атаками

Отметим, что полностью снять с себя все риски не удалось еще ни одному бизнесу: если вы успешны, ведете конкурентную борьбу, и у вас есть нечто конфиденциальное и очень ценное, обязательно найдется кто-то, кто будет готов заплатить немалые деньги за право обладания вашей ценностью – или же за то, чтобы вы ее лишились. Установка бэкдора (алгоритмического дефекта, предоставляющего несанкционированный доступ к данным или удаленному управлению ПК в целом) или загрузка кейлоггера на ПК руководителя — инструмента, который записывает все нажатия клавиш — ставит бизнес под серьезную угрозу.

Успешная борьба с APT должна включать работу по трем направлениям. Первое – внедрение инструментов кибербезопасности на уровнях сетевой активности и локальных ПК для быстрого обнаружения атаки. Второе – найм квалифицированных сотрудников, которые смогут правильно настроить эти инструменты. Третье – четко прописанные внутренние регламенты бизнес-процессов.

Арсенал APT

Kaspersky Anti Targeted Attack Platform (KATA)

KATA противостоит нападениям на всех этапах и способно обнаружить уже начавшуюся атаку и минимизировать ущерб от нее, а также защитить предприятие от потенциальных угроз, благодаря сочетанию сетевых, веб- и почтовых сенсоров, а также сенсоров рабочих мест.

В продукте сочетаются динамический анализ на основе «песочницы» и передовые технологии машинного обучения, что обеспечивает защиту от широкого спектра угроз. Решение имеет сертификат ФСБ РФ и входит в реестр отечественного ПО.

Check Point SandBlast

В основе устройства лежат две технологии. Первая, движок Threat Emulation, перехватывает вредоносное ПО уже на стадии эксплойта, до попытки применения техник, препятствующих обнаружению в «песочнице». Файлы инспектируются в виртуальной «песочнице» для обнаружения опасного внедренного кода и помещаются в карантин, предотвращая их распространение в сети. Технология совмещает инспекцию в песочнице на уровне операционных систем и на уровне центрального процессора (CPU-level inspection), обнаруживая и останавливая самые опасные эксплойты, таргетированные атаки и атаки нулевого дня.

Вторй важнейшй компонент решения, SandBlast Threat Extraction, создает для пользователей безопасную версию потенциально опасного содержимого.

TDS Group-IB

Система раннего предупреждения киберугроз, состоящая из трех компонентов. TDS Sensor ищет аномалии в сети, необычное поведение устройств, связь зараженных устройств с командными центрами. Потенциально опасные объекты извлекаются из сети компании для анализа в системе TDS Polygon, которая позволяет предотвратить заражения из рассылок, а также с использованием ранее неизвестного вредоносного ПО или за счет атак на браузер.

Заключение о степени опасности объекта делается на основании классификатора, формируемого системой машинного анализа. Компонент SOC Group-IB в режиме 24/7 анализирует и классифицирует инциденты руками опытных аналитиков, собирает данные о событиях ИБ для демонстрации в удобном web-интерфейсе и отвечает на вопросы с помощью тикет-системы.

На все вопросы ответит

Сергей Самойлов, руководитель группы технологического развития информационной безопасности Softline
Звоните: +7(495) 232-00-23 доб. 0275
Пишите: S.Samoylov@softline.com

187-ФЗ /КИИ /ГосСОПКА

Резкое увеличение инцидентов информационной безопасности в России и мире послужили предпосылками для разработки законодательной основы защиты критической информационной инфраструктуры (КИИ). Для эффективной борьбы с киберугрозами и обеспечения штатной работы объектов КИИ создается ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Нормативная база

- Указ Президента Российской Федерации «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» от 15 января 2013 г. N31c
- «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утвержденная Президентом РФ 12.12.2014 № К 1274
- 187-ФЗ «О безопасности критической информационной инфраструктуры РФ»

Регулирующие органы

- ФСТЭК России: Методологическая функция, формальный надзор выполнения требований
- ФСБ России: Техническая функция, надзор за реализацией технических мер, ГосСОПКА
- Минкомсвязь России: Отраслевое согласование требований к защите информации
- Центральный банк Российской Федерации: Отраслевое согласование требований к защите информации

Объекты и субъекты КИИ

Объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. К объектам КИИ относятся ИС, ИТС, АСУ в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, атомной энергетике, оборонной промышленности, ракетно-космической, горнодобывающей, металлургической промышленности, химической промышленности.

Субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей. К субъектам КИИ относятся государственные органы, государственные учреждения, юридические лица и индивидуальные предприниматели.

Softline предлагает

- Провести аудит всех информационных систем субъекта КИИ с целью выявления значимых информационных систем, с формированием подробного отчета и дорожной карты;
- Разработать модели угроз информационных систем;
- Провести категорирование значимых информационных систем в соответствии с актуальным законодательством;
- Подготовить уведомление ФОИВ (Федеральных органов исполнительной власти) о наличии информационных систем, при этом в отчете должны присутствовать и незначимые информационные системы, использующие одну инфраструктуру со значимыми;
- Разработать проект по обеспечению информационной безопасности;
- Внедрить комплексную систему защиты информации.

Что получаем на выходе?

Обследование инфраструктуры, категорирование объектов КИИ, выполнение мер защиты для объектов, подключение к ГосСОПКА и, как итог, — улучшение, развитие, модернизацию объектов КИИ. ▮

Защита АСУ ТП и КИИ

Актуальные вопросы в сфере защиты информационной инфраструктуры промышленных предприятий мы обсудили с Дмитрием Ковалевым, руководителем группы технологического продвижения Softline, и Максимом Прохоровым, менеджером по продаже решений.

Дмитрий Ковалев

Максим Прохоров

— Какие угрозы сегодня актуальны для промышленных инфраструктур?

— В 2017 г. рост киберпреступности потряс ИБ-индустрию. Атаки шифровальщиков-вымогателей WannaCry и ExPetr обрушились на государственные органы, финансовые компании, не оставили без внимания и промышленную инфраструктуру. И именно в технологическом сегменте эксперты выявили большое количество уязвимостей, так как долгое время обеспечению ИБ в этой сфере не придавалось должного значения.

Зафиксировано и исследовано вредоносное ПО, предназначенное для атак на физические системы, – CrashOverride/Industroyer. Эксперты пришли к выводу, что оно создано для нарушения рабочих процессов в промышленных системах управления (ICS), в частности, на электрических подстанциях, в сетях которых вирус позволяет управлять выключателями и прерывателями цепи.

— Каковы цели и последствия таких атак?

— Целей множество, среди них можно назвать и угрозу суверенитету государства со стороны экстремистских и террористических групп, борьбу конкурирующих предприятий. Нельзя забывать и о хакерах-активистах, которые таким образом просто изучают промышленные инфраструктуры и «прокачивают» свои знания. Последствия могут быть неописуемыми. Только представьте, если проникнуть в систему управления реактором на АЭС и изменить технологические параметры микроконтроллеров, предна-

значенных для защиты энергоблоков от недопустимых рабочих нагрузок, может произойти взрыв. Это приведет к отключению электроэнергии или даже экологической катастрофе. Вирусные атаки могут остановить процесс производства, обернуться риском для жизни, а также финансовыми и репутационными потерями.

— С какими проблемами чаще всего обращаются к нам клиенты?

— В первую очередь, бизнесу не просто выбрать ИБ-продукт или решение, не только отвечающее требованиям, но также и подходящее по функционалу его инфраструктуре. Автоматизированные системы на большинстве предприятий разные, каждый вид производства имеет свои характерные особенности, поэтому нельзя разработать какой-то готовый шаблон решений, должен быть индивидуальный, комплексный подход. Компания Softline решает эту непростую задачу. Мы проводим независимую экспертную оценку и разрабатываем персональный проект. Силами специалистов Softline решается ряд крупных задач, которые стоят перед руководством предприятия: повышение уровня кибербезопасности, обеспечение выполнения требований регуляторов и ИБ при информационном обмене, автоматизация процессов защиты, обнаружение и предотвращение атак на информационные ресурсы.

— Какие важные изменения произошли в сфере защиты АСУ ТП и КИИ?

— 1 января 2018 г. вступил в силу 187-ФЗ «Об обеспечении безопасности критической информационной инфраструктуры», согласно которому предприятия, попадающие под критерии значимости, указанные в законе, обязаны соблюдать определенные стандарты и регламенты при создании систем безопасности. Нужно отметить, что наши регуляторы основательно подошли к формированию требований по защите, в результате чего под действие данного закона попадает множество отраслей: здравоохранение, наука, транспорт, энергетика, банки, военно-промышленный комплекс и многие другие.

За неисполнение требований 187-ФЗ предусмотрена ответственность: принудительные работы на срок до пяти лет с лишением права занимать определенные должности или даже уголовное наказание от 5 до 10 лет лишения свободы, если инцидент привел к тяжким последствиям.

Softline предлагает полный комплекс услуг по части приведения в соответствие требованиям закона в сфере защиты КИИ и конфиденциальной информации (ПДн). Среди наших клиентов — крупнейшие в мире промышленные компании, предприятия электроэнергетической отрасли, транспортные монополии и многие другие. ▮

Будем рады ответить на ваши вопросы:
SCADAsecurity@softlinegroup.com

Пока что нет четкой картины по выполнению всей цепочки мероприятий, направленных на обеспечение безопасности КИИ, ожидается публикация оставшихся НПА. Но вступившие в силу ФЗ, приказы, постановления дают возможность уже сейчас начать формировать основу для прохождения этапа категорирования.

Транснефть

ООО «Транснефть – Порт Приморск» благодарит компанию Softline за плодотворное и эффективное сотрудничество в рамках реализации проекта по проверке соответствия требованиям регуляторов информационной безопасности АСУ ТП. В результате предприятие получило рекомендации по минимизации ИБ-рисков, которые легли в основу моделирования угроз и технического задания на создание системы защиты АСУ ТП. Мы высоко ценим профессионализм экспертов Softline, их консультативную помощь оперативность проведения работ и рекомендуем компанию как надежного и компетентного партнера в сфере реализации проектов по обеспечению информационной безопасности на предприятии.

ООО «Транснефть – Порт Приморск»

С большой вероятностью можно сказать, что 187-ФЗ — это не «одноразовая акция» для стимуляции индустрии ИБ. Безопасность КИИ предполагает постоянную работу в этом направлении, важно осуществлять мероприятия по обеспечению ИБ, планировать бюджет, расследовать инциденты и взаимодействовать с регуляторами.

Защищенное облако Softline

Удобство облаков и соблюдение закона. Сбросьте груз забот по обеспечению защиты персональных данных!

В 2001 году Россия подписала Европейскую конвенцию «О защите физических лиц при автоматизированной обработке персональных данных». После ратификации конвенции во исполнение международных обязательств наконец-то был принят известный всем Федеральный Закон №152 «О персональных данных» от 27 июля 2006 г. Заканчивая краткий исторический экскурс, стоит отметить еще одну дату – 1 сентября 2015 г., когда начал действовать 242-ФЗ от 21.07.2014, который обязал операторов «обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации».

Благодаря этим законотворческим инициативам мы теперь знаем, что:

- «персональными данными» является «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу»;
- «оператор персональных данных» — государственный орган, муниципальный орган, юридическое или физическое лицо, осуществляющие обработку персональных данных, а также определяющие цели обработки, состав, подлежащих обработке, действия, совершаемые с персональными данными;
- сбор и обработку персональных данных нужно производить на территории РФ (а уже потом можно куда-нибудь передавать, согласно конвенции) и т.д.

Как обеспечить защиту персональных данных

Согласно Статье 19 152-ФЗ, для обеспечения безопасности персональных данных при их обработке требуется ряд серьезных мер как организационного, так и технического плана. При этом в зависимости от «возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, актуальности угроз безопасности персональных данных» установлены четыре уровня защищенности. По мере роста уровня от четвертого к первому возрастают требования к используемым средствам защиты информации.

Отсутствие должной защиты персональных данных может привести не только к серьезным штрафам и личной ответственности руководителей, но и к попаданию сайта организации в реестр запрещенных интернет-ресурсов, что приведет к его немедленной блокировке. Коммерческий риск дополняется имиджевым, и суммарный ущерб для компании может быть непоправимым.

К счастью для бизнеса, п.3 ст.6 152-ФЗ гласит, что «оператор вправе поручить обработку персональных данных другому лицу» и «лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные настоящим Федеральным законом».

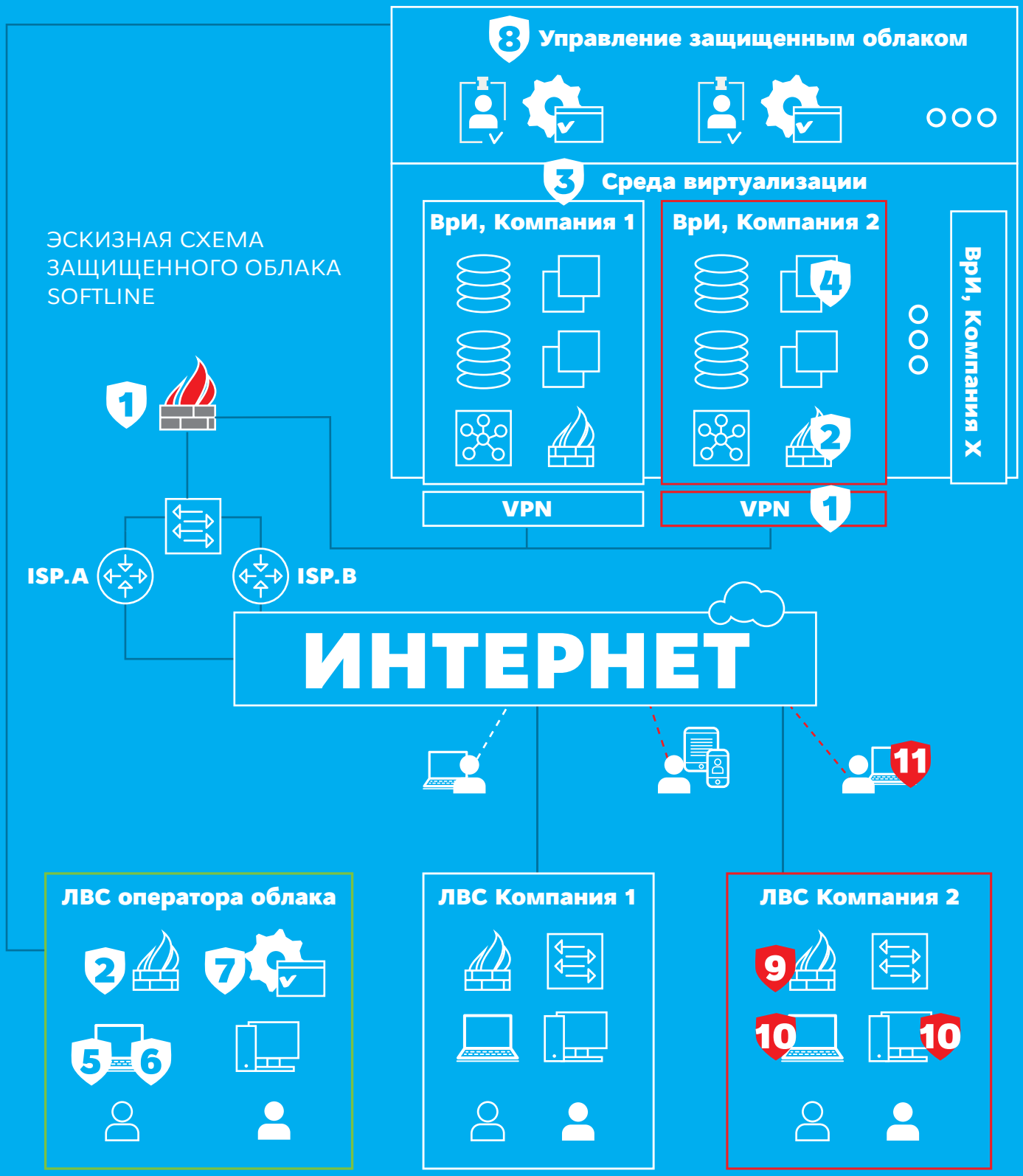
Это и позволяет нашим клиентам сбросить груз забот по обеспечению защиты персональных данных на надежные плечи профессионалов и перенести информационные системы, содержащие персональные данные в «Защищенное облако Softline».

Техническая сторона

Технически «Защищенное облако» (эскизную схему см. справа) построено на сертифицированной платформе FlexPod, в основе которой — вычислительные мощности и коммутаторы Cisco, системы хранения NetApp и программное обеспечение VMware. FlexPod уже много лет эксплуатируется на семи площадках Softline Cloud в разных городах и показал себя безусловно надежно. Безграничные возможности горизонтального масштабирования, отказоустойчивость и гарантированная совместимость оборудования и ПО – залог стабильной работы инфраструктуры клиентов облачной платформы.

Для обеспечения выполнения требований законодательства мы использовали средства защиты информации, являющиеся де-факто стандартами рынка – Лаборатория Касперско-

ЭСКИЗНАЯ СХЕМА ЗАЩИЩЕННОГО ОБЛАКА SOFTLINE



СЗИ в зоне ответственности Softline

1. Межсетевой экран CheckPoint
2. Криптошлюз «С-Терра»
3. Средство защиты виртуальной среды vGate
4. Антивирус «Kaspersky Security для виртуальных сред»
5. Средство защиты от несанкционированного доступа для ОС на ВМ «Secret Net Studio»;
6. СЗИ на АРМ администраторов ИБ
7. Средства управления СЗИ на сервере управления системой ИБ.
8. Средство анализа защищенности «XSpider».

СЗИ в офисе компании-заказчика:

9. Криптошлюз «С-Терра Шлюз» на площадке заказчика «Защищенного облака Softline».
10. СЗИ АРМ сотрудников:
    1. СЗИ от НСД «Secret Net Studio»;
    2. САВЗ «Kaspersky Endpoint Security».

Мобильный пользователь компании-заказчика:

11. СЗИ АРМ мобильных пользователей «Защищенного облака Softline», размещаемых за пределами ЛВС клиентов «Защищенного облака»:
    1. VPN-клиент «С-Терра Клиент»;
    2. СЗИ от НСД «Secret Net Studio»;
    3. САВЗ «Kaspersky Endpoint Security».

го, Код Безопасности, КриптоПро — и построили публичное мультитенантное облако, которое позволяет размещать информационные системы персональных данных уровня защищенности 3 и 4. При необходимости размещения ИСПДн уровней защищенности 1 и 2 инфраструктура выделяется в отдельное частное облако, построенное на схожем технологическом решении.

Защищенное облако Softline аттестовано лицензиатом ФСБ, что является гарантией соблюдения требований законодательства как для нашего клиента, так и для проверяющих органов.

Документы готовы

При размещении ИСПДн в Защищенном облаке предоставляется весь необходимый пакет документов: модель угроз безопасности ПД; акты классификации Защищенного облака; описание подсистемы защиты; приказы об утверждении регламентных документов обеспечения информационной безопасности (модели здоровья, регламент РК и пр.); поручение об обработке ПД (хранение персональных данных и их предоставление для обработки пользователям Заказчика).

Компании-оператору персональных данных остается подготовить требуемую законом организационно-распорядительную документацию, обеспечить защиту канала связи до облака, подключаемых рабочих мест и отправить уведомление в Роскомнадзор.

Но следует помнить, что кроме размещения ИСПДн в Защищенном облаке, требуется соблюдение правил работы организации с персональными данными и с 1 июля 2017 были внесены поправки в ст.13.11 КоАП, ужесточающие требования к обработке ПД и увеличивающие штрафы за нарушения. ▮

Есть вопросы?

Обращайтесь к Сергею Самоукину, департамент облачных технологий Softline
Sergey.Samoukin@softline.com

НАШИ люди, процессы и технологии

Безусловно, за облаками будущее. И мировой, и уже российский опыт показывают, что все больше и больше компаний переносят свои сервисы и бизнес-процессы в облака. При должном подходе к информационной безопасности использование облачных сервисов настолько же безопасно, как и собственный ЦОД (Private Cloud). Более того, модель MSSP (подход аутсорсинга кибербезопасности, заключающийся в привлечении сервис-провайдеров), применяемая сейчас в информационной безопасности, — это прорыв и настоящая, не маркетинговая, инновация, которая в ближайшее время существенно изменит ИБ-ландшафт и в РФ.

На мировом рынке активно позиционируется более 40 крупных MSSP, среди которых не только бывшие поставщики коробочных решений и интеграторы. На путь MSSP встали и крупнейшие вендоры ИБ, консалтинговые компании, включая большую четверку.

Softline имеет большой опыт работы на высококонкурентном рынке. В ИТ- бизнесе выигрывает не тот, кто первый, а тот, кто предложит клиенту лучший продукт, решение или сервис.

Managed Security Services (MSS) — услуги по аутсорсингу информационной безопасности. Компании, предоставляюще такие услуги, называются MSS-провайдерами (MSSP), список предлагаемых ими сервисов весьма широк, и он почти не отличается от того набора продуктов ИБ, которые есть на рынке. Фактически любой продукт, включая даже антивирусную защиту для рабочих станций, можно заказать как сервис с помесячной или поквартальной оплатой и только после отчета провайдера по SLA.

на страже безопасности **ВАШЕЙ** компании

SECaaS — Security as a Service — Информационная безопасность, предоставляемая по модели услуги

SOC — Security Operations Center — Центр мониторинга и реагирования на инциденты ИБ

MSS — Managed Security Service — Услуги по управлению информационной безопасностью

MSSP — Managed Security Services Provider – Компания, предоставляющая MSS

Практически все вендоры, занимающиеся информационной безопасностью, имеют в своей продуктовой линейке так называемые виртуальные аплайнсы (готовые образы виртуальных машин, например, корпоративных брандмауэров или фильтрующих прокси-серверов), не уступающие аппаратным решениям по функционалу, и, в отличие от последних, они легко масштабируются в условиях облачной инфраструктуры. Такие виртуальные образы используются MSSP для предоставления сервисов своим клиентам. Однако облачный вариант зачастую соседствует с гибридным, когда все устройства и ПО физически находятся на стороне заказчика, а управление ими ведется со стороны MSSP по специальным защищенным каналам, при том все управляющие воздействия согласовываются с компанией-клиентом и записываются (логируются).

Внимание к возможностям операционных центров безопасности — Security Operations Center (SOC), с помощью которых осуществляется управление инцидентами информационной безопасности — растет в течение последних нескольких лет. Но по ряду причин полноценный SOC внутри инфраструктуры способна выстроить редкая компания. Организация этих процессов – хороший выход в ситуации, когда важно сэкономить ресурсы и одновременно иметь возможности неограниченного масштабирования, а в условиях РФ это порой единственная возможность получить требуемый функционал.

Услуги MSSP

MSSP, предоставляющие услуги Центра информационной безопасности, способны не только осуществлять мониторинг и бороться с последствиями атак, но и решать целый ряд других задач, среди которых:

- стратегическое планирование, оценка угроз;
- обогащение правил SOC на основе внешних данных и сторонних фидов;

Автор: Виктор Гулевич, руководитель отдела MSSP, департамент информационной безопасности Softline
v.gulevich@softline.com

Почему Softline

К работе сервисов по безопасности мы относимся крайне пристрастно, понимая всю их важность для клиентов. Softline дает все необходимые гарантии по сохранности данных, передаваемых в облака, работает с заказчиками по договору SLA и оказывает консультационные услуги по вопросам, касающимся законодательства в кибербезопасности.

MSS-модель и использование виртуальных аплайнсов решений информационной безопасности дают доступ к передовым технологиям за приемлемые деньги. Больше не надо покупать железо, достаточно добавить мощностей в виртуальном ЦОДе и развернуть виртуальное решение для обеспечения информационной безопасности — например, UTM или WAF. И не нужно нести капитальные затраты, т.к. сервисы ИБ можно оплачивать по подписке, ежемесячно, вместе с оплатой виртуального дата-центра, доступа в интернет и электричества.

И, конечно же, не стоит забывать об управлении сервисами ИБ. Каким бы технологически совершенным ни было решение, его нужно постоянно сопровождать и поддерживать. Возникает вопрос расширения штата и, соответственно, увеличения фонда оплаты труда. Содержать штат своих специалистов, работающих в режиме 24/7, — затратное мероприятие. Не стоит забывать и о желании ИБ-специалистов переходить в другие компании по мере роста их компетенций в поисках более высоких зарплат. Стоимость же сервиса по управлению ИБ сейчас постоянна и существенно ниже, чем стоимость своей команды, а четко прописанный SLA гарантирует качество оказываемых услуг.

- хранение практически неограниченных объемов данных (логов);
- реагирование на инциденты в режиме реального времени;
- автоматизированное реагирование на инциденты;
- поддержка работы граничных систем сетевой безопасности и инфраструктуры;
- отслеживание внутренних угроз, расследование внутренних нарушений;
- тестирование на проникновение;
- и десятки других сервисов.

Необходимо отдельно отметить эффективность корпоративных расследований с привлечением команды профессионалов MSSP Softline. Используя разнообразные инструменты анализа поведения пользователей (UEBA), а также классические системы противодействия утечки информации (DLP) или системы записи действий пользователей в сети и на рабочих станциях, команда экспертов-расследователей выявляет внутренние проблемы организации и доносит их до клиента. Без глубокой аналитики и сопровождения такие системы, как DLP, UEBA, UBA, EMS (employee monitoring software), не стоят потраченных на них денег. С другой стороны, содержать команду расследователей – не по карману большинству компаний. Хорошо, что эта услуга уже доступна от Softline в режиме MSS.

Чем SOC от Softline отличается от конкурентов?

Есть несколько направлений в строительстве SOC. В первом случае провайдер берет у вендора рабочее коммерческое решение SIEM и добавляет в него процессы и политики, необходимые клиентам. Во втором случае провайдер использует open-source решения для гранулярного подхода к своим задачам, содержит команду разработчиков.

Минусы первого подхода видны невооруженным взглядом:

- баснословные платежи вендору, который предоставляет само решение SIEM;
- невозможность планирования бюджета в разрезе даже одного года, так как вендор может поднять цены, или изменится курс рубля;
- жесткая привязка к возможностям конкретного SIEM, имеющих серьезные ограничения по количеству обрабатываемых событий в единицу времени;
- для автоматизирования реагирования также требуется вендорское решение класса IRP (Incident Response Platform), которое значительно увеличивает стоимость сервиса.

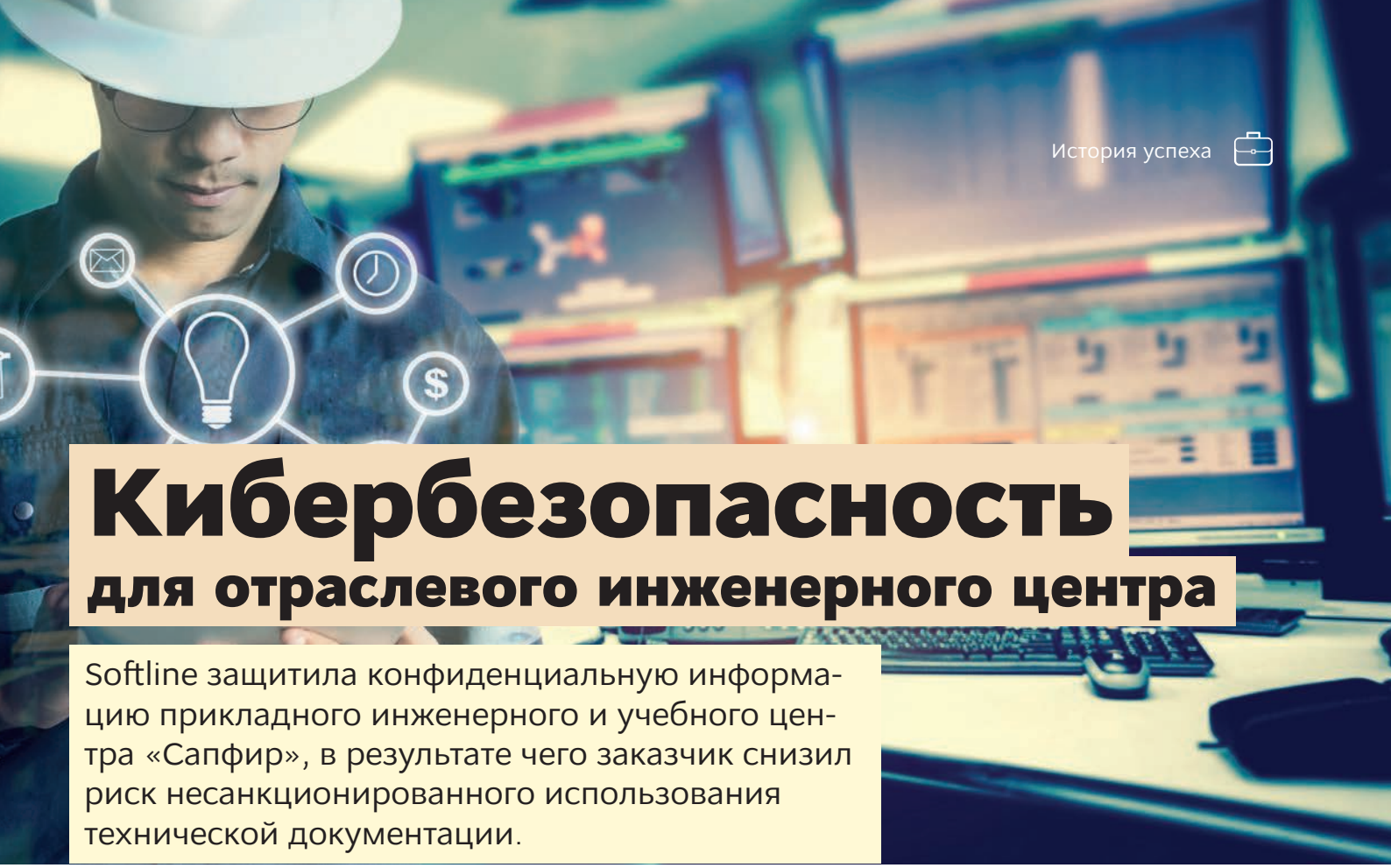
К плюсам можно отнести быструю настройку сбора событий с популярных систем и присутствие сертификатов ФСТЭК у большинства вендоров SIEM.

У второго подхода плюсов гораздо больше:

- собственная разработка, гарантирующая гранулярность и внимание к специфике компании-клиента и региона;
- нет привязки к вендорам; используются самые актуальные решения на данный момент, такие как стеки apache и elastic;
- нет узкого «горлышка» на моменте сбора и анализа событий – используются легко масштабируемые Big data решения типа Hadoop;
- наличие собственных разработчиков облегчает создание собственной платформы по автоматизированному реагированию на события ИБ.

Из минусов можно отметить слабое внимание разработчиков к визуализации результатов действий SOC, но это незначительный недостаток.

Softline выбрал второй вариант и ведет работы над улучшением представления данных – визуализацией действий и событий, однако полностью функциональный SOC с командой высококлассных специалистов, с мониторингом 24/7 и предоставлением сервиса на русском и английском языках доступен уже сейчас и обслуживает наших клиентов.



Кибербезопасность
для отраслевого инженерного центра

Softline защитила конфиденциальную информацию прикладного инженерного и учебного центра «Сапфир», в результате чего заказчик снизил риск несанкционированного использования технической документации.

Это обуславливает специфические требования к производственным процессам и высокие стандарты информационной безопасности. Руководство центра «Сапфир» приняло решение внедрить DLP-систему для защиты информации о конструкторских наработках. Партнером на конкурсной основе была выбрана компания Softline, специалисты которой обладают богатым опытом реализации проектов в сфере обеспечения кибербезопасности.

Ситуация

Заказчику было необходимо внедрить систему, которая бы соответствовала как корпоративным требованиям к обеспечению информационной безопасности, так и нормам российского законодательства. Эксперты Softline разработали для центра «Сапфир» политики безопасности, организационно-распорядительную документацию и основные принципы режима коммерческой тайны. После чего развернули в инфраструктуре отечественную DLP-систему InfoWatch Traffic Monitor Standart. Решение анализирует специфические и сложные форматы данных: чертежи, конструкторскую документацию. Оно позволяет категорировать конфиденциальные данные, определять уровень доступа к ним и в режиме реального времени проводить мониторинг их использования. Продукт совместим с пользовательским ПО и не снижает производительность компьютеров.

Результаты

Заказчик получил комплексное решение, которое охватывает организационные, технические и юридические аспекты обеспечения внутренней безопасности компании.

«Деятельность нашей организации предъявляет высокие требования к защите данных. Утечка проектной документации может повлечь серьезные коммерческие, технологические и репутационные издержки. Компания Softline помогла нам выбрать оптимальное решение, внедрение которого позволило оперативно предотвращать инциденты и повышать уровень ответственности персонала, работающего с конфиденциальной информацией», — рассказывает Дмитрий Королев, главный специалист по ИТ инженерного центра «Сапфир».

О компании

ООО «Прикладной инженерный и учебный центр «Сапфир» специализируется на сопровождении проектов в крупной отечественной компании нефтегазовой отрасли.

SAM Cybersecurity для «Пермцветмет»

ПЕРМЦВЕТМЕТ

Эксперты Softline предложили заказчику воспользоваться программой SAM Services для SMB-сегмента.

О компании

«Пермцветмет» производит алюминиевые сплавы для автомобильной промышленности. В штате компании 200 сотрудников.

Мы получили рекомендации по рациональному управлению программными активами и повышению уровня кибербезопасности в компании. Включенные в долгосрочную стратегию развития ИТ-инфраструктуры, эти сведения помогут нам предупреждать киберугрозы и уменьшать материальные и репутационные издержки.

Сергей Мякотников, начальник отдела информационных технологий АО «Пермцветмет»

Ситуация

Компании требовалось повысить уровень кибербезопасности, для чего специалисты компании Softline, которая была выбрана в качестве партнера, проанализировали программные активы организации.
Проект был рассчитан на обзор около 50 ПК. Поэтому эксперты Softline предложили заказчику воспользоваться программой SAM Services для SMB-сегмента.

Решение

«В управлении программными активами в сегменте среднего и малого бизнеса есть нюансы, которые необходимо учитывать. Разобраться в них, определить ключевые направления по совершенствованию ИТ-инфраструктуры и повышению уровня ее безопасности помогают SAM-проекты. Теперь такие программы Microsoft доступны компаниям с парком оборудования от 25 ПК, и больше заказчиков получат возможность оценить эффективность ИТ-инвестиций», – отмечает Татьяна Елисеева, ИТ-консультант департамента бизнес-консалтинга Softline.
Команда Softline выяснила, что «Пермцветмет» использует операционную систему Windows XP, поддержка которой была прекращена вендором. Отсутствие критически важных обновлений создавало угрозу кибербезопасности. Заказчику предложили обновить операционную систему до версии Windows 10. Компании «Пермцветмет» было рекомендовано объединить все устройства в пределах одного домена Active Directory и удалить неиспользуемые учетные записи; применить службу Shadow copy service для оперативного восстановления поврежденных или удаленных файлов; использовать технологию BitLocker для защиты данных от кражи с жестких дисков. Эксперты Softline рассказали заказчику о корпоративных каналах продаж программного обеспечения, которые в сравнении с розничными более выгодны. Заключив лицензионное соглашение, компания сможет привести ИТ-ресурсы в соответствие со своими бизнес-целями и сократить затраты. ▮

Расширенная защита от утечек данных через мессенджеры **и поддержка** цифровых отпечатков в DeviceLock® DLP

Весной 2018 г. компания Смарт Лайн Инк, разработчик программного комплекса DeviceLock DLP Suite, планирует выпустить очередную версию своего продукта — DeviceLock® DLP Suite 8.3. Бета-версия уже доступна для свободного ознакомления.

Программный комплекс DeviceLock DLP Suite предлагает для эффективного решения задачи защиты от утечек данных полнофункциональный набор контекстных и контентнозависимых механизмов эффективного контроля используемых (data-in-use), передаваемых (data-in-motion) и хранимых (data-at-rest) данных. Ключевой особенностью продукта является принцип работы в режиме реального времени, с обеспечением защиты непосредственно на пользовательских компьютерах. Исполнительный агент DeviceLock, функционирующий на уровне ядра операционной системы, поддерживает самый широкий в DLP-отрасли набор контекстных методов предотвращения утечек данных с защищаемых пользовательских компьютеров через их локальные интерфейсы и порты, периферийные, виртуальные и перенаправленные в терминальные сессии устройства ввода-вывода, системный буфер обмена, снимки экрана, а также каналы сетевых коммуникаций.

Защита от утечки данных через мессенджеры

Агент DeviceLock — единственный на мировом рынке агент класса Endpoint DLP со встроенным резидентным модулем, реализующим технологию глубокого анализа и фильтрации сетевых пакетов (deep packet inspection, DPI) непосредственно на защищаемом компьютере. Для большинства мессенджеров, контролируемых DeviceLock DLP Suite, реализованы анализ и фильтрация содержимого сообщений в чате и исходящих файлов, выполняемые «в разрыв» в режиме реального времени.

Для мессенджера WhatsApp DeviceLock DLP на сегодня позволяет задать индивидуальные (или по группам пользователей) политики доступа к WhatsApp Web, а также протоколировать факты его использования. Для мессенджера Viber реализована возможность селективного контроля и протоколирования для чатов и передаваемых файлов, включая теневое копирование, а также протоколирования соединений и голосовых коммуникаций через Viber.

Возможности контроля мессенджера Telegram в DeviceLock намного шире. Прежде всего, детектируется и контролируется использование как web-версии Telegram, так и приложения Telegram Desktop. Для web-версии DeviceLock DLP предоставляет возможность задавать политики контроля доступа и протоколирование соединений. Для Telegram Desktop возможно, помимо селективного контроля доступа, задать детальное событийное протоколирование и создание теневых копий для всех чатов. DeviceLock DLP способен извлекать из переписки в Telegram и сохранять в журнале реальные имена отправителей и получателей для целей протоколирования и вывода в динамическом графе связей.

Использование цифровых отпечатков в контентной фильтрации

Метод использования цифровых отпечатков в DLP-системах, в основе которого лежит сопоставление документов или файлов с так называемыми цифровыми отпечатками, или фингерпринтами — наборами буквенно-цифровых строк (хэшей), является одним из наиболее точных методов идентификации и защиты информации. Особенно эффективен этот метод для идентификации незначительно измененных типовых документов. Например, он позволяют легко идентифицировать заполненные контракты, отличающиеся только данными одной из сторон; или для идентификации финансовых данных, хранящихся в документах MS Office, бизнес-информации, хранящейся в файлах PDF.

DeviceLock DLP снимает цифровые отпечатки с образцов конфиденциальных документов, сохраняя их в собственной базе данных отпечатков, а затем сравнивает их с фингерпринтами проверяемых документов. Если процент соответствия отпечатков превышает требуемый порог в соответствии с настройкой, проверяемые документы считаются конфиденциальными, и к ним в режиме реального времени применяются заданные в DLP-политике действия — блокировка передачи, создание теневой копии, отправка тревожного оповещения в службу ИБ. ▮

Безопасный документооборот

Хотите обеспечить полноценную систему безопасности при работе с документами? Внедрите систему электронного документооборота. Если в ней реализуются все возможности по обеспечению сохранности и конфиденциальности документов, общая безопасность документооборота предприятия усилится десятикратно. Подробнее об этом рассказала Полина Дуйкова, эксперт с 10-летним опытом внедрения СЭД (количество реализованных проектов — более 50), руководитель направления внедрений СЭД/ECM департамента бизнес-решений Softline.

— Полина, какова главная проблема безопасности при работе в системе внутреннего документооборота?

— Сразу отмечу, что задача повышения безопасности работы с документами в рамках внутреннего документооборота стоит перед каждой компанией. Основня проблема, возникающая в разрезе внутренней безопасности, — это отсутствие разграничения доступа к документам и их низкий уровень сохранности. Отсутствие политик безопасности.

Если в компании внедрена система документооборота, то в зависимости от вида электронных документов в рамках большого электронного архива важно распределить при помощи политик безопасности доступ сотрудников на уровне документов внутри системы документооборота и баз данных. При грамотном внедрении системы документооборота в организации обеспечивается целостность системы безопасности при работе с документами и в дальнейшем постоянно поддерживается.

— Кто должен отвечать за безопасность данных?

— Я всегда рекомендую разделять данные по зонам ответственности. На мой взгляд, их три, и вводить их нужно при создании положения об электронном документообороте в организации.

За персональные данные должен отвечать HR-директор, поскольку именно на отделе кадров лежит ответственность за прием и увольнение сотрудников. HR инициирует заявки на подбор персонала, появление сотрудника в информационном пространстве.

Служба безопасности отвечает за сохранность коммерческой тайны внутри компании. Сотрудники ИТ-департаментов организуют базу данных и следят за сохранностью информации внутри бизнеса, отвечая за ее целостность и структурность, а также за защиту от вирусных атак.

Служба безопасности, помимо того, что проверяет благонадежность контрагентов, должна внутри системы документооборота проверять протоколирование всех действий с документами: смотрел ли тот или иной сотрудник определенный файл, когда и т.д. С помощью настройки маячковых верификаторов можно отслеживать действия пользователей и их действия с определенными документами.

— Какие существуют возможности обеспечения сохранности документов в системах DIRECTUM и ТЕЗИС?

— Эти системы дают высокую надежность хранения документов и быстрый доступ к ним — в зависимости от выданных правил безопасности.

Документ имеет жизненный цикл — от инициации до конечного исполнения. Если не внедрена система документооборота, то количество копий, которые хранятся локально на компьютерах, достигает колоссальных значений. И эту информцию, какая бы она ни была, можно скачать и отправить куда угодно, с любого мессенджера, на любую личную почту.

В системе DIRECTUM можно включать механизмы, которые помогают системам документооборота запретить отправку файлов по различным метрикам вовне.

Внутри DIRECTUM и ТЕЗИС можно ограничить доступ к документам посредством различных клиентских приложений с двойной аутентификацией, смс-уведомлений. Также могут быть внедрены смарт-карты, биометрические устройства. Для этого дополнительно к стационарным компьютерам добавляют оборудование, позволяющее осуществлять вход в устройство по сетчатке глаза или отпечатку пальца.

Доступ пользователей к документам может быть открыт только на чтение, на изменение, а может быть предоставлен и полный доступ для переназначения на документы, и полный запрет. Если регламентно права на просмотр документа не выданы, человек никогда не найдет этот документ внутри системы. Неважно какие запросы он будет применять, он даже не узнает о существовании файла.

— Кто и как может контролировать обеспечение подлинности документа внутри системы документооборота?

— Согласно внутреннему регламенту положения об электронном документообороте, в каждой компании есть особые правила по использованию электронно-цифровых подписей. Они бывают квалифицированные и неквалифицированные. По Закону об электронной подписи, внутри компании можно использовать обычную бесплатную подпись. Документ может быть подписан одним или несколькими пользователями. При подписании, как и в случае с шифрованием документов, могут применяться сертифицированные средства криптозащиты.

За выдачу сертификатов отвечает системный администратор. Подписи выдаются согласно определенной роли сотрудника в компании. Здесь важно не сделать ошибки. Например, не выдать ненадежному сотруднику роль на согласование бюджета. А такое может произойти, особенно в крупной, территориально-распределенной компании. Ситуация крайне нежелательная, ведь когда документ подписан, он является фактом неизменности.

Поэтому обеспечение подлинности документов во многом завязано на действиях ИТ-департамента.

— Расскажите о мобильных пользователях, которым нужно удаленно работать с системой документооборота.

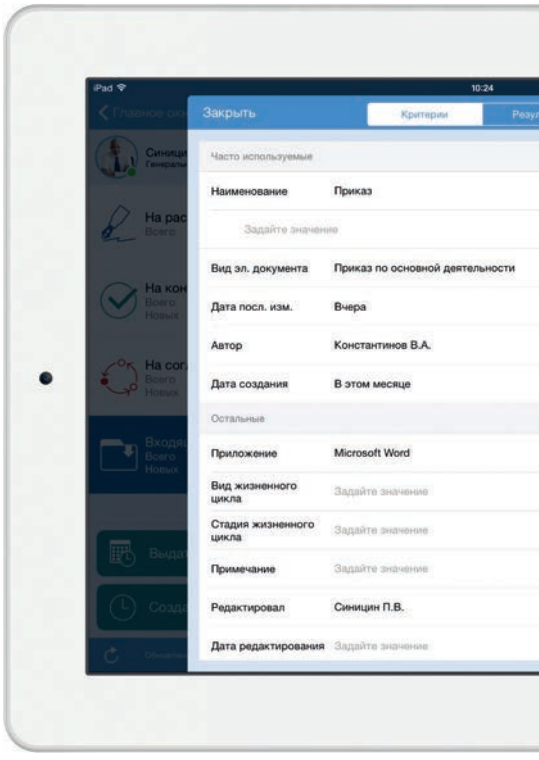
— Различают два уровня внешнего доступа — для всех пользователей и для топ-менеджеров. Последние – привилегированные пользователи, которым я рекомендую использовать решения, позволяющие работать не в онлайн-режиме, а скачивать документы, работать с ними на устройстве и затем передавать по шифрованным каналам, как только появляется доступ к интернету, на основной сервер, где развернута система документооборота.

Есть и два «массовых решения» — DIRECTUM Jazz и DIRECTUM Solo. Это мобильные приложения, которые дают доступ к контенту вне офиса с возможностью запуска новых бизнес-процессов и занесения документов в систему.

DIRECTUM Solo особенно пригодится руководителям, которые пользуются планшетами на iOS и Android.

Приложения позволяют рассматривать входящие документы, выносить резолюции, ставить и контролировать ход выполнения задач и т.д. Интерфейс отображает всю необходимую информацию на одном экране, а возможность работы без интернета и локального рецензирования документов обеспечивает максимальную мобильность. При появлении сети все изменения будут синхронизированы. Это позволяет руководителям работать откуда угодно, эффективно и быстро. ▮

Если в компании не внедрена система документооборота, количество копий, хранящихся локально на компьютерах, достигает колоссальных значений.



Остались вопросы?

Продолжите беседу с Полиной напрямую!

Пишите: Polina.Duykova@softlinegroup.com

Звоните: +7 (351) 222 40 10, доб.3656

Восстановить **за 60 секунд**

Вирусные атаки 2017 года показали истинную ценность данных очень многих корпораций.

От зловредов Petya, WannaCry и других компании теряли накопленную информацию — о клиентах, контрагентах и разработках — и приобретали огромное количество репутационных проблем и сложностей, связанных с восстановлением нормального функционирования бизнес-процессов.

Именно резонансные и крайне болезненные с точки зрения непрерывности бизнеса вирусные атаки привели владельцев предприятий к пониманию того, что необходимо иметь как минимум одну резервную копию данных, чтобы в случае какого-то инцидента иметь возможность восстановить важные сведения. Главная проблема такой схемы – длительное время восстановления информации. Если для вашей компании простой даже в несколько часов критичен (например, крупная торговая сеть не может на два дня остановить работу кассовых аппаратов), альтернативой создания «холодных» (без возможности непрерывного доступа) резервных копий для вас может стать репликация с возможностью аварийного восстановления (disaster recovery).

Как работает репликация?

Репликация (от лат. Replico — «повторяю») — это тиражирование изменений данных с главного сервера на одном или нескольких зависимых серверах. До недавнего времени, эта задача решалась строительством резервного центра обработки данных, в котором хранились базовые сервисы. Получается долго и дорого, ведь дата-центр нужно не только построить, но и обслуживать. Сейчас у компаний появилась возможность решить эту проблему с помощью использования специального программного обеспечения и разместить реплики в об-

Если ваши бизнес-процессы позволяют предоставить данные только за последние 4 часа до происшествия, то последняя резервная копия должна быть сделана не позднее четырех часов назад.

лаке, используя решение Disaster Recovery-as-a-service («Аварийное восстановление как сервис», или DRaaS). Стоимость решения от сервис-провайдера зависит от того, насколько велики риски при том или ином времени простоя. Для кого-то некритичен час простоя, а кто-то многое потеряет даже при остановке работы сервисов на 15 минут. Заказчик выбирает тариф в зависимости от того, как часто серверу на его стороне необходимо синхронизироваться с сервером провайдера и создавать новую реплику. Тариф можно менять, что особенно удобно для владельцев сезонного бизнеса, когда три месяца в году новый клиент приходит каждые десять минут, а в «несезон» — раз в несколько часов.

Как выбрать способ восстановления данных?

Основные параметры, на которые ориентируется провайдер, подбирающий для вас сервис — RTO и RPO.

RPO (допустимая точка восстановления) — это допускаемый уровень потери данных в случае прерывания операций. Это последняя точка во времени, с которой можно восстановить данные. Например, если ваши бизнес-процессы позволяют предоставить данные только за последние 4 часа до происшествия, то последняя резервная копия должна быть сделана не позднее 4-х часов назад. Сначала восстанавливаются данные из резервной копии, затем добавляется информация за последние 4 часа. Если возможно «вручную» восстановить данные за несколько дней, RPO может быть больше. Таким образом, RPO определяет количество данных, которые могут быть потеряны, т.к. их всегда можно восстановить.

RTO (допустимое время восстановления) — это показатель, который определяется временем неработоспособности сервиса в случае прерывания операций. Оно показывает раннюю точку времени, после которой операции могут быть продолжены.

Чем ниже показатели RPO и RTO, тем более дорогой сервис вам необходим.

Сервисы аварийного восстановления от Softline

Softline предлагает сервисы DRaaS двух типов. Тем клиентам, которые уже разместили свои сервисы в облаке Softline, компания предлагает дополнительно застраховать себя от потери данных, создав реплику в другом дата-центре (он может располагаться в том же или в другом городе). В этом случае, если по каким-то причинам доступ к основному дата-центру временно будет потерян, клиент может оперативно подключиться к резервному ЦОДу и избежать существенного простоя. Доступность сервисов для клиента при этом оказывается выше, чем этого требует стандартный SLA.

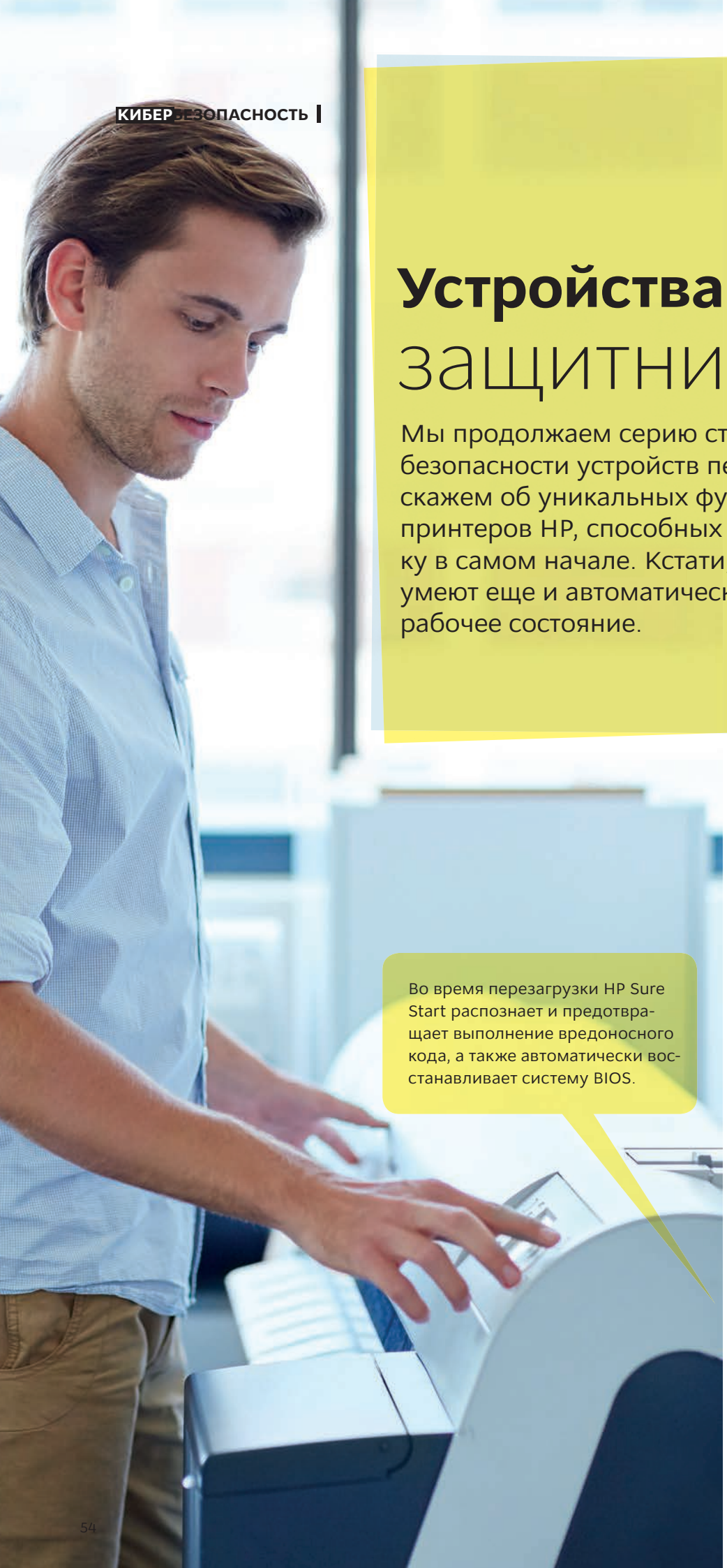
Тем клиентам, которые уже разместили свои сервисы в облаке Softline, мы предлагаем дополнительно застраховать себя от потери данных, создав реплику в другом дата-центре.

Если же у заказчика есть собственный дата-центр, Softline может предложить им недорогой, но при этом качественный сценарий DRaaS, создав реплику базы клиента в свое облако. Благодаря гибкости инструментов управления сервисов, вы можете выбрать оптимальный тариф для вашей компании. ▮

Материал опубликован на http://nsk.dk.ru

Остались вопросы?

Вам ответит Антон Нагов, руководитель направления развития бизнеса, департамент облачных технологий
Пишите: Anton.Nagov@softlinegroup.com
Звоните: +7 (495) 232-00-23 доб. 1382



Устройства печати — защитники сети

Мы продолжаем серию статей об обеспечении безопасности устройств печати. В этот раз расскажем об уникальных функциях безопасности принтеров HP, способных остановить кибератаку в самом начале. Кстати, модели HP Enterprise умеют еще и автоматически восстанавливать свое рабочее состояние.

Во время перезагрузки HP Sure Start распознает и предотвращает выполнение вредоносного кода, а также автоматически восстанавливает систему BIOS.

Принтер имеет очень много общего с обычным ПК. Его так же можно атаковать или использовать как «ворота» в ИТ-инфраструктуру предприятия. Функция непрерывного мониторинга в устройствах HP существует для обнаружения проблем в реальном времени. Она распознает и пресекает атаки во время работы устройства и перегружает его, чтобы восстановить систему.

HP Sure Start

Около трех лет назад решение HP Sure Start было внедрено в персональные компьютеры. Оно проверяет BIOS в момент загрузки устройств (к сожалению, большинство поставщиков игнорирует данную проверку). При обнаружении повреждения BIOS устройство перезагружает систему, удалив BIOS и восстановив его исправленную копию. Эта технология самовосстановления — надежная защита от киберугроз.

Проверка настроек

HP уже давно оснащает устройства печати встроенным веб-сервером, с помощью которого можно ограничить доступ к устройству, используя уникальные сертификаты. Сертификат устанавливается на устройство через центр сертификации; на это уходит примерно 15-20 минут.

Как этот процесс автоматизировать? Используйте HP JEtAdvantage Security Manager — приложение для управления сертификатами. Они будут в считанные минуты установлены на все устройства печати в организации. Решение проверяет и исправляет настройки безопасности принтеров во время перезагрузки. Кроме того, в этом приложении можно ознакомиться с отчетными данными. Проводите ли вы проверку безопасности или ИТ-директор просто хочет узнать, как используется сеть компании, вы можете получить отчет, где будет указано точное количество устройств в сети, как они используются, какие политики безопасности применяются. Вот так HP JetAdvantage Security Manager поможет управлять безопасностью всего парка устройств в вашей компании.

Проверка микропрограммы

Микропрограммное обеспечение устройств тоже нуждается в защите. Если в ходе загрузки микропрограммы обнаружены повреждения, загрузка мгновенно прекращается и запускается безопасная «золотая» копия. И вновь устройства пользователей защищены от киберугроз, а далее проблему можно перенаправлять в службу безопасности.

Технология Whitelisting гарантирует загрузку в память только подлинного кода HP, в случае нарушения безопасности устройство перезагружается и высылает уведомление ИТ-специалистам.

HP Runtime Intrusion detection

Эта функция защиты от вторжений постоянно работает в момент перезагрузки устройств печати, проверяя их на наличие возможных вирусов или вредоносных программ. В случае обнаружения угрозы устройство будет отключено. Об инцидентах сообщается службе безопасности, при этом используются различные инструменты управления событиями информационной безопасности (SIEM). После этого устройство возвращается в сеть, и пользователи могут продолжить работу.

Как еще можно контролировать безопасность?

Устройства HP имеют более 250 настроек безопасности, которые специалисту-новичку, возможно, будет сложно сразу освоить. Но с помощью решения, которое встраивается в микропрограммное обеспечение, — технологии HP Instant-on — все становится гораздо проще. Благодаря HP Instant-on устройство при подключении в сеть сообщает о себе, находит сервер с политиками безопасности, которые загружаются, задавая конфигурацию всех 250 настроек безопасности.

По сути, решение представляет собой комбинацию внутреннего микропрограммного обеспечения и внешнего ПО, с помощью которого можно контролировать настройки безопасности.

Принцип действия следующий: ИТ-специалисты вашей компании создают и проверяют политику безопасности в соответствии с необходимыми внутренними требованиями. Теперь можно добавлять устройства. С помощью HP Instant-on все подключаемые в сеть принтеры и МФУ сообщают о себе. Если устройство по какой-то причине перестало соответствовать политике, или вы развертываете новые устройства в сети, в момент их появления к ним применяется соответствующая политика.

Следующий шаг – текущий мониторинг устройств. Получив доступ к устройствам, мы видим всю сеть и можем проверить конфигурацию устройств в ней, а также соответствие политик безопасности заданному уровню. Если степень защиты устройства не соответствует политике компании, это можно быстро исправить и таким образом обеспечить надлежащий уровень защиты. ▮

SOLIDWORKS
Впереди — лучшее

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

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

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

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

Значительное расширение партнерской сети произошло за счет нашего сотрудничества с Softline

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

BI-СИСТЕМА для промышленной компании

В связи с постоянным ростом объемов данных в организации появилась потребность в мощном инструменте бизнес-аналитики. Необходимо было обеспечить регулярное построение аналитической отчетности и единую точку доступа к достоверной информации для повышения оперативности принятия управленческих решений.

Ситуация

К развертыванию BI-платформы компания шла давно. В течение года было реализовано несколько пилотных проектов с разными партнерами для полного понимания того, как информационно-аналитические системы будут работать в корпоративной среде. В итоге исполнителем была выбрана компания Softline, которая предложила решение, максимально соответствующее требованиям заказчика по функционалу.

До внедрения

«Отчетность в компании, конечно, была обширная – производственная, финансовая, коммерческая. Она строилась в учетной системе 1С и в Microsoft Excel, — рассказывает Станислав Воронин, руководитель направления внедрений систем бизнес-аналитики Softline. — Более половины отчетности специалистам приходилось выгружать и соединять именно в Excel. Когда проводили предпроектное обследование, обнаружили, что 80% всех отчетов реализовывались в табличном виде».

Периодичность получения актуальных данных со стороны высшего руководства составляла порядка одного раза в неделю. Еженедельно проводились оперативные совещания, однако лишь единичные отчеты составлялись по итогам ежедневного регламента и каждый день рассылались управляющим.

Большая проблема состояла в том, что отчетности на стыке функциональных подразделений не существовало. Исключение составляли отчеты по продажам и производству, которая демонстрировала соотношение выполнения планов.

Решение

Для внедрения была выбрана BI-система Qlik, одна из лучших на рынке в своей функциональной области, позволяющая осуществлять гибкий бизнес-анализ больших объемов любых разрозненных данных с высокой скоростью. Проект был масштабным и охватил все технологические и вспомогательные службы: производство, финансы, продажи, маркетинг, транспорт, персонал, ИТ, ремонт, клиентский сервис — всего 14 функциональных областей. Все существующие в компании службы были так или иначе задействованы.

В ходе проекта в компании была обеспечена «единая версия правды», что позволило гарантировать централизованную работу с данными, повысить их качество в системах оперативного учета и решить проблему с разрозненностью показателей по одному и тому же вопросу. Специалисты Softline реализовали ряд отчетов, которые по объему обрабатываемой информации практически невозможно было сформировать в учетной системе, теперь отчеты строятся за несколько секунд с любой детализацией. BI-проект позволил заказчику проана-

лизировать узкие места в производственных процессах, которые находятся на стыке подразделений, и определить точки управленческого воздействия.

«В качестве примера приведу интересный кейс. В компании работают два производственных департамента, один из которых поставлял продукт на переработку в другой. В процессе передачи на конвейер продукта сотрудники отмечали в нем ряд специфических проблем, которые ухудшали категорию продукции и снижали ее стоимость. Ряд реализованных отчетов позволил проанализировать дефекты на каждой конкретной единице продукта и сделать факторный анализ. Это позволило понять, в зоне ответственности каких подразделений находится причина того, что продукция теряла в категории», — говорит Станислав Воронин.

Результат

Компания получила инструмент, который очень четко «подсвечивает» проблемные области и точки роста за счет глубоких кроссфункциональных отчетов. Среди функциональных преимуществ Qlick — понятный user-friendly интерфейс, позволяющий пользователям быстро начать работу. Затраты на обучение — минимальны.

Работы длились 9 месяцев, однако уже через 2 месяца с начала проекта еженедельные оперативные совещания проводились на основе сформированных в аналитической системе отчетов, поскольку не осталось никаких расхождений в данных и их оценке. Использование «единой версии правды» и широких возможностей визуализации позволило сократить время планерок и повысить их эффективность. По оценке руководства компании, еще до своего окончания BI-проект окупил затраченные средства и минимизировал влияние человеческого фактора на принятие управленческих решений. ▮

О компании

Сегмент: крупный бизнес
Отрасль: пищевая промышленность (производство и продажа)

Небезопасность публичных Wi-Fi сетей

В наше время, когда беспроводные Wi-Fi сети есть практически везде: на вокзалах, в кафе, ресторанах и даже глубоко под землей в вагонах метро, далеко не все знают об угрозах информационной безопасности, которые касаются каждого пользователя, включившего Wi-Fi на своем устройстве.

Что такое ARP?

ARP — протокол, который используется для связи IP-адреса устройства с его MAC-адресом. Другими словами, он помогает определить MAC-адрес устройства, зная его IP-адрес. После того, как ARP-ответы будут получены устройствами и соответствующая информация будет добавлена в ARP-таблицу, весь трафик пойдет через ноутбук злоумышленника.

Перехват трафика

Если вы подключены к публичной Wi-Fi сети, злоумышленник может легко перенаправить весь трафик между вашим устройством и роутером через свой ноутбук, тем самым он получит доступ ко всем данным, которые вы передаете или загружаете. Для этого злоумышленник может использовать давно известную атаку типа MitM («человек посредине») — ARP-spoofing. Эта атака основана на уязвимостях протокола ARP.

Злоумышленник отправляет ложные ARP-ответы

Создание поддельных точек доступа

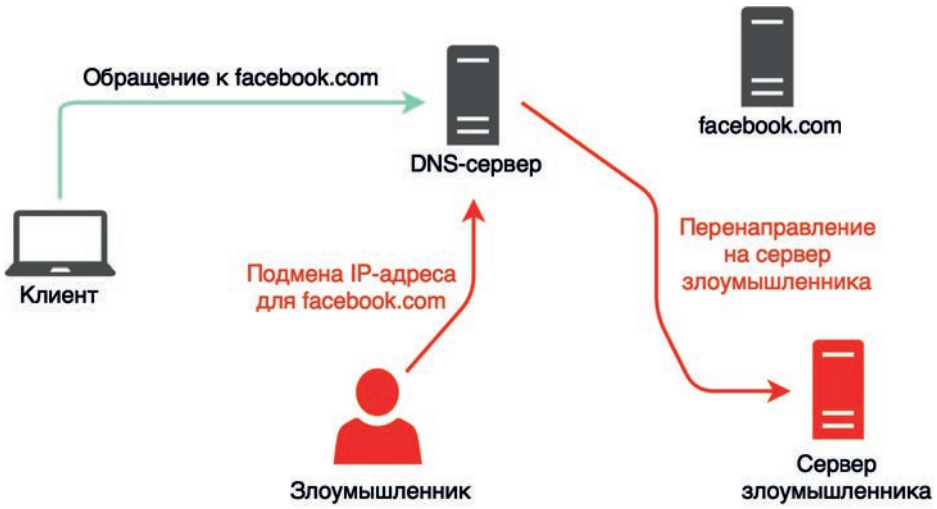
Большинство смартфонов, ноутбуков и планшетов автоматически ищут Wi-Fi сети и подключаются к ним. В первую очередь такие устройства будут искать сети со знакомыми названиями, такими как MosMetro_Free или MT_FREE. Во время поиска устройства отправляют запросы, так называемые probe requests.

Злоумышленник может видеть их и создавать сети, с зарегистрированными названиями, или же создать сеть с произвольным именем, например, с названием кафе, в котором он сейчас находится.

Несомненно, многие сервисы используют протокол HTTPS для шифрования трафика, но, несмотря на это у злоумышленника существует множество возможностей для обхода шифрования и перехвата трафика.

DNS Spoofing

Следующая атака — DNS Spoofing. Она заключается в подмене данных кэша доменных имен таким образом, чтобы вернуть пользователю ложный IP-адрес. Например, злоумышленник может подменить данные кэша так, что переход пользователя по доменному имени facebook.com направит его на сервер киберпреступника.



Пример реализации атаки DNS Spoofing

На своем сервере злоумышленник может развернуть копию сайта facebook.com и собирать учетные данные ни о чем не подозревающих пользователей.

Captive portal

Captive portal — это то самое окно, которое появляется у вас при подключении к публичной сети, где, как правило, необходимо выполнять какие-либо действия, например, нажать «Войти». Используются эти окна для аутентификации, показа рекламы и взимания платы за доступ в Интернет.

Злоумышленник может использовать эту технологию для того, чтобы показать жертве подобную страницу, на которой будет форма ввода банковской карты, учетной записи от социальной сети или же это может быть просто страница с обновлением, которое необходимо срочно установить. Правда установка таких обновлений может предоставить злоумышленнику полный доступ к устройству ничего не подозревающего пользователя.

Как защититься?

Необходимо быть бдительными, когда вы используете публичные сети. Если вы все же подключились к публичной Wi-Fi сети, вы можете использовать VPN. Для того, чтобы работать через VPN, вы можете обратиться к VPN-провайдерам, поднять свой VPN-сервер или использовать Traffic Inspector Next Generation. Он из коробки поддерживает различные виды VPN, включая OpenVPN и IPsec.

Более того, Traffic Inspector Next Generation может использоваться для объединения географически удаленных филиалов компании (в режиме «сеть-сеть»), а также для подключения удаленных сотрудников к головному офису, или просто для организации безопасного канала связи для выхода в интернет из недоверенной сети (в режиме «узел-сеть»). Именно использование режима «узел-сеть» может предотвратить утечку критичных данных (паролей, номеров карт, персональных данных) в публичных сетях Wi-Fi.

Самый популярный способ организации подключения по VPN — OpenVPN максимально удобно реализован в Traffic Inspector Next Generation. Графический интерфейс устройства позволяет легко генерировать необходимые для подключения CA, сертификаты и ключи.

Вы можете за несколько нажатий настроить себе собственный VPN-сервер на устройстве Traffic Inspector Next Generation и больше не беспокоиться о безопасности данных, передаваемых вами внутри публичной Wi-Fi сети

Готовые решения для увеличения прибыли интернет-магазинов

GIFTD

Платформа включает в себя 10 готовых решений. У каждого решения своя специфика. Вместе они обеспечивают рост продаж интернет-магазинов до 35% и позволяют обрабатывать входящий трафик с большей эффективностью.

Среди клиентов компании самыми популярными являются мотивационный, реферальный и макси-корзина виджеты.

Мотивационный виджет

Увеличит конверсию в 2 раза, продавая уходящим посетителям с помощью скидки.

Что получает магазин:

- Увеличивает количество оформленных заказов за счет предоставления скидки уходящим посетителям;
- Возвращает посетителей на сайт за счет серии персонализированных триггерных писем со спецпредложением на просмотренные товары;
- Собирает контактные данные посетителей.

Макси-корзина

Повышает средний чек на 20% и более за счет увеличения количества товаров в корзине.

Что получает магазин:

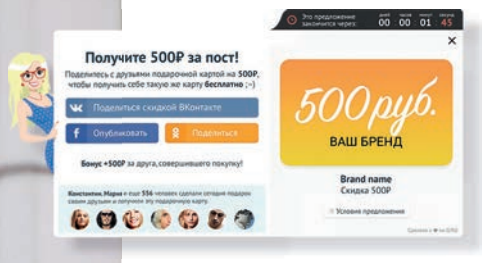
- Увеличивает средний чек заказов за счет интеллектуальной реакции при клике на кнопку «Купить»;
- Меньше брошенных корзин, т.к. мы совершаем контакт с клиентом в ключевой точке;
- Умные Up-sell сценарии: величина скидки предлагается автоматически в зависимости от цены товаров в корзине.

Реферальный виджет

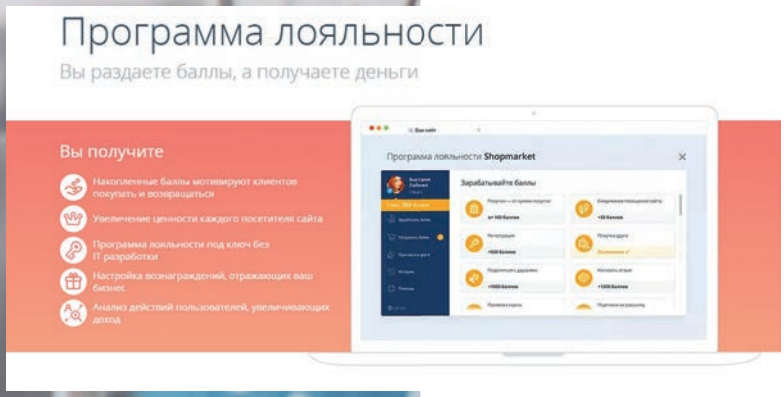
30% посетителей сделают пост в соцсеть о вашем магазине — это лучшая рекомендация.

Что получает магазин:

- Привлекает новый трафик с постов ваших посетителей в соцсетях;
- Эффективная и бесплатная реклама в соцсетях от ваших посетителей своим друзьям;
- Постоянные упоминания вашего бренда в соцсетях служат мощным сигналом ранжирования в поисковых системах.



SaaS-платформа GIFTD предназначена для вознаграждения посетителей интернет-магазинов и управления лояльностью.



Отдельно стоит сказать о GIFTD.Лояльность. Интернет-магазин выбирает события, за которые он готов начислять баллы — например, покупка, приглашение друга, отзыв и т.д. Покупатели в свою очередь зарабатывают баллы и могут использовать их для получения скидок и призов. Уникальность решения GIFTD состоит в абсолютной гибкости — интернет-магазин может создавать новые условия для получения баллов, тем самым повышая уникальность и эффективность своей программы лояльности.

Программа лояльности BitRewards

Александр Егоров, основатель GIFTD, уверен, что использование технологий распределенного децентрализованного реестра (блокчейн) и машинного обучения, а также внимание к запросам растущей криптоаудитории, позволят вывести программы лояльности на принципиально новый уровень.

Так родилась идея BitRewards — программы лояльности на блокчейне. BitRewards даст покупателям возможность получать бонусы и скидки в виде токенов BIT за покупки, совершенные как самими покупателями, так и их друзьями. Помимо этого, клиенты смогут получать бонусы не только за покупки, но также за любые действия, которые могут быть интересны для интернет-магазина — например, активности в социальных сетях, отзывы, рекомендации и т.д. Идея получила самые высокие отзывы от участников рынка, уже почти закрыв soft cap по сборам на предпродаже без существенных затрат на рекламу и продвижение. ∎

Сервис GIFTD работает в своей нише более 5 лет. Компания была одной из первых в России, кто запустил сервис по выпуску электронных подарочных карт. До GIFTD механизмы поведенческого маркетинга с эффективным конверсионным потенциалом были доступны только большим компаниям с внутренними ИТ-отделами, которые разрабатывали его годами. Благодаря GIFTD доступ к подобным инструментам имеют также малый и средний бизнесы.

allsoft.ru®

Вы можете приобрести решения GIFTD в интернет-магазине Allsoft

Юрий Зайцев: «В цифровой экономике побеждает тот, кто готов и умеет экспериментировать с технологиями»

Руководитель цифровой лаборатории Softline о перспективах онлайн-торговли, персонализации, чат-ботах и других технологиях, меняющих облик традиционного ретейла.

— Каково текущее состояние рынка e-commerce в России и его потенциал? Как в ближайшие годы будет расти объем российского рынка цифрового ретейла? Каковы будут основные сегменты роста: одежда, бытовая и цифровая техника и т.д.?

— Рынок активно развивается и имеет значительный потенциал роста. Онлайн и мобильная торговля растут намного быстрее традиционной и в ближайшей перспективе будут оставаться ключевыми драйверами ретейла. Лидирующие «традиционные» ретейлеры больше не считают онлайн-торговлю еще одним небольшим каналом продаж. Это заметно не только по заявлениям первых лиц ведущих компаний, но и по проектным активностям и запуску новых digital-сервисов. Потребительские тренды и меняющееся

Изменения – это всегда сложно. К ним могут быть не готовы как руководство компании, так и менеджеры среднего звена.

потребительское поведение действительно открывают новые возможности для развития онлайн каналов, что делает диджитализацию клиентского опыта необходимостью для успешного развития бизнеса.

На международном рынке есть хорошие примеры успеха: компания Tesco осуществляет 15% своих продаж в digital-каналах. Это действительно высокий показатель. Если российские ретейлеры будут следовать примеру западных коллег и наращивать продажи в цифровых каналах, то, по оценке Цифровой лаборатории, уже к 2020 году доля онлайн-торговли может достичь 7% от российского рынка ретейла. Важно понимать, что шансы на успех не равны для всех. Так в 2017 году один из лидеров ретейла в сегменте бытовой техники добился выдающихся результатов даже на фоне международных лидеров в диджитал: средняя доля интернет-продаж за год превысила 15% оборота компании.

Мы наблюдаем пики активности в различных сегментах. Пищевой ретейл в России долгое время занимал выжидающую позицию. Если 17 лет назад компания «Утконос», старейший онлайн-гипермаркет, не имела прямых конкурентов, то сейчас наблюдается «лавинный» эффект, и все больше и больше игроков вынуждены создавать и развивать различные e-commerce решения. Только в этом году несколько крупных food-ретейл сетей запустили онлайн-сервисы по продажам продуктов. Fashion-ретейл показывает самые интенсивные темпы роста: все крупные игроки уже создали свои электронные площадки — как гиганты marketplace Lamoda и Wildberries, так и монобренды Zara, H&M и прочие. Но есть и исключения: компания Gloria Jeans с многомиллиардным оборотом не имеет своего онлайн-канала продаж. Сложно прогнозировать, но компании, которые не идут по пути цифровой трансформации, постепенно начнут терять долю на рынке, у них ухудшатся финансовые показатели, и со временем все может закончится крайне печально.

Безусловно у компаний с видением перспективы развития цифрового ретейла, готовых инвестировать в создание совершенного клиентского опыта и обладающих передовыми компетенциями создания диджитал-сервисов, шансы на успех выше. Это история не одного проекта и не одного года.

— С какими проблемами наиболее часто сталкивается российский e-commerce на текущем этапе развития? Какие решения для интернет-торговли являются наиболее перспективными на данном этапе? Какие технологические драйверы роста наиболее активно разрабатываются и применяются в России: Big Data, облачные технологии, боты и т.п.?

— Компаниям, которые не начали заблаговременно готовиться к цифровой трансформации, будет очень сложно адаптироваться в современном мире: несмотря на лояльную аудиторию, барьер входа на рынок онлайн-торговли очень высок. Требования потребителя очень разнообразны, и затраты, которые потребуются для запуска успешного проекта, могут быть высоки. Компаниям, без большого опыта на рынке e-commerce, сложно догнать лидеров и создать что-то действительно релевантное. У маленьких игроков преимущество: они вынуждены экспериментировать и искать новые ниши. Они вынуждены думать, как создать большую ценность для клиента. Крупные компании могут испытывать проблемы с трансформацией: им сложно оперативно принимать решения, добиваться процесса согласования и дальнейшей реализации.

Изменения – это всегда сложно. К ним могут быть не готовы как руководство компании, так и менеджеры среднего звена. Для сегодняшних задач ретейлеров практически не осталось простых решений – ты должен экспериментировать и быть готовым меняться в условиях неопределённости. В цифровой экономике побеждает тот, кто готов и умеет экспериментировать с технологиями в рамках всей цепочки создания ценности.

Технологии, которые используются в интернет-торговле, могут быть уникальными, а могут использоваться и в других отраслях. Многое зависит от бизнес-модели конкретно взятого магазина. Сегодня для того, чтобы создать конкурентоспособную компанию e-commerce недостаточно просто создать ассортимент, удобный интерфейс. Нужно продумать логистику,

Если российские ретейлеры будут следовать примеру западных коллег и наращивать продажи в цифровых каналах, то по оценке Цифровой лаборатории, уже к 2020 году доля онлайн-торговли может достичь 7% от российского рынка ретейла.

разобраться с поставщиками, продумать медийную стратегию и прочее. Все движется в сторону персонализации: решения основываются на знаниях, технологии упрощают жизнь компаниям и клиентам. Например, у компании Amazon треть продаж совершает рекомендательный сервис – искусственный интеллект, в основе которого лежат обработка больших данных и алгоритмы машинного обучения.

Чат-боты сейчас на вершине популярности, но для того, чтобы успешно их использовать, требуется не только знание самой технологии, которая не является новой, но и понимание болей и проблем клиента. Если просто заменить всех людей чат-ботами, это скорее создаст проблемы для бизнеса. Чат-боты полезны для решения точечных задач — они решат проблемы транзакционных издержек, оптимизации взаимодействия с клиентом.

— Можно ли говорить о том, что российские онлайн-площадки не отстают от зарубежных аналогов по используемому софту? В чем заключается польза облачных решений для интернет-торговли?

— Однозначной позиции нет. Софт не является решающим фактором, который определяет успешность компании. Уровень доступности технологий одинаковый для любого предприятия электронной торговли. Все находятся в равных условиях. Другой вопрос в наличии компетенций для использования этих технологий. Передовые практики построения цифровой платформы ретейлера сводятся к созданию «невидимой инфраструктуры», сервисно-ориентированной архитектуры и индивидуального клиентского опыта. Для решения этой задачи вопрос используемого софта не является определяющим. Польза облачных решений для онлайн-ретейла, по опыту Цифровой лаборатории, очевидна для большинства компаний: безграничная масштабируемость вычислительных мощностей для обработки больших данных. Если к вам придет весь Интернет, то облачная инфраструктура без проблем обработает все запросы пользователей.

— Ваших клиентов условно можно отнести к трем группам: крупные корпоративные клиенты, средний и малый бизнес и государственные компании. Можно ли говорить в связи с этим, что в период рецессии спрос на софт со стороны какой-либо из трех групп сократился? Или, напротив, увеличился? Все ли цели на текущий год были достигнуты, и какие задачи Вы ставите себе на следующий год?

— Мы не видим явного тренда на падение или рост спроса во время рецессии. Компании, которые осознают необходимость цифровой трансформации, стараются повысить вложения в технологии, соответственно их затраты растут.

В 2018 году мы хотим масштабировать модель цифровой лаборатории, поскольку видим, что количество запросов на рынке увеличивается. На основании работы с нашими клиентами мы убедились, что те компетенции, которые мы аккумулируем в цифровой лаборатории, те услуги, которые мы предлагаем, востребованы на рынке. Запрос на цифровую трансформацию существует практически у всех компаний. Когда создавалась Цифровая лаборатория, мы ставили очень амбициозные цели, и в некоторых областях мы выполнили план на 200%. Мы очень хорошо продвинулись в реализации бизнес-модели, собираемся наращивать мощности и двигаться только вперед.

Материал опубликован на https://marketing.rbc.ru/articles/10122/

SOICA

Мощная платформа для решения любых задач по оцифровке документов, их классификации, разделению и потоковому вводу данных. Полностью российское ПО. Полезно компаниям любой сферы деятельности с документооборотом от 10 000 страниц в год.

В портфель решений SOICA входит набор продуктов для успешного решения любых задач по оцифровке документов по заранее настроенным инструкциям. Основой для движка распознавания данных служат новейшие технологии со свободным исходным кодом Google, доработанные российскими специалистами.

Процент распознавания

Зависит от качества распознаваемого документа и стремится к 100%, если это оригинал без испорченных символов. Если на документе присутствуют следы неисправности оборудования (полоса от лампы, рассыпанная краска картриджа, отсутствие части документа – порван, прожжен и т.д.) — процент распознавания снижается. Но, в случае если документ испорчен, у SOICA есть функционал, позволяющий выполнить предобработку изображения перед его распознаванием, т.е. очистить шумы, убрать пятна, восстановить контрастность текста, целостность линий.

Поскольку недостаточно просто распознать данные из документа, их нужно правильно сопоставить и занести в целевую систему для дальнейшего учета и использования, SOICA поддерживает автоматическую классификацию и разделение документов, очистку и коррекцию картинки перед распознаванием. Важно, что изображение чистится многократно, и вы можете получить интерпретацию одного и того же документа в разных графических форматах. SOICA может сравнить их все и передать вам самый корректный результат.

Поиск

В SOICA есть интеллектуальный поиск данных без шаблонов, что позволяет использовать гибкие настройки поиска данных и их сопоставления. Решение работает не с зонами, а с форматами, с представлением данных. Поиск графических цветных объектов (ссылок, печатей) пригодится, если бизнес-процессы вашей компании не позволяют принять в обработку документы без печати. SOICA проверит наличие печати, и в случае ее отсутствия не пропустит документ в целевую систему.

Решение позволяет сопоставлять данные —например, номенклатуры, имена, товарные позиции, единицы измерения — с различными базами и справочниками.

Автоматизация ручного труда

Большое преимущество решения. Помогает не только сократить время обработки документов, но и исключить ошибки ручного ввода. Для этого в SOICA реализовано настраиваемое правило для автоматической валидации. ▮

Эффект от внедрения

- Увеличение скорости обработки документов на всех этапах.
- Исключение ошибок, связанных с человеческим фактором.
- Возможность применения в компаниях с территориально-распределенной структурой.
- Окупаемость проекта от полугода.

SOICA поддерживает многопоточную обработку данных. При полном задействовании современных серверных процессоров, 1 страница обрабатывается менее чем за одну секунду.

Расписание курсов в учебном центре Softline

Вендор		Город	Курс	Даты
Cisco	О	Ростов-на-Дону	IP-коммутация на базе оборудования Cisco	23-27 апреля
Cisco	О	Санкт-Петербург	IP-коммутация на базе оборудования Cisco	23-27 апреля
Cisco	Д	Ростов-на-Дону	IP-коммутация на базе оборудования Cisco	23-27 апреля
Cisco	Д	Санкт-Петербург	IP-коммутация на базе оборудования Cisco	23-27 апреля
Cisco	Д	Москва	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.3.0 Part 2)	23-27 апреля
Cisco	О	Москва	Использование сетевого оборудования Cisco. Часть II (Interconnecting Cisco Networking Devices v.3.0 Part 2)	23-27 апреля
Cisco	О	Уфа	IP-коммутация на базе оборудования Cisco	14-18 мая
Cisco	Д	Уфа	IP-коммутация на базе оборудования Cisco	14-18 мая
Citrix	Д	Москва	Расширенное администрирование XenApp and XenDesktop 7.1x	14-18 мая
Citrix	О	Москва	Расширенное администрирование XenApp and XenDesktop 7.1x	14-18 мая
ITIL	О	Казань	Операционная поддержка и анализ	14-17 мая
ITIL	О	Нижний Новгород	Основы ITILv3 - 2011	14-16 мая
ITIL	О	Ростов-на-Дону	Основы ITILv3 - 2011	14-16 мая
ITIL	О	Самара	Основы ITILv3 - 2011	14-16 мая
ITIL	Д	Нижний Новгород	Основы ITILv3 - 2011	14-16 мая
ITIL	Д	Ростов-на-Дону	Основы ITILv3 - 2011	14-16 мая
ITIL	Д	Самара	Основы ITILv3 - 2011	14-16 мая
ITIL	Д	Казань	Операционная поддержка и анализ	14-17 мая
Microsoft	О	Казань	Подготовка инфраструктуры с System Center Virtual Machine Manager	23-27 апреля
Microsoft	О	Москва	SharePoint 2013 для конечных пользователей	23-25 апреля

Вендор		Город	Курс	Даты
Microsoft	О	Москва	Создание запросов к Microsoft SQL Server 2014	23-27 апреля
Microsoft	О	Москва	Виртуализация серверов с использованием Hyper-V и System Center	23-27 апреля
Microsoft	О	Москва	Администрирование System Center Configuration Manager и Intune	23-27 апреля
Microsoft	О	Москва	Обеспечение безопасности Windows Server 2016	23-27 апреля
Microsoft	О	Омск	Конфигурация, управление и устранение неисправностей работы организации Microsoft Exchange Server 2010	7-11 мая
Microsoft	О	Хабаровск	Администрирование Windows Server 2012 R2	7-11 мая
Microsoft	О	Хабаровск	Администрирование Microsoft Exchange Server 2016	7-11 мая
Microsoft	О	Нижний Новгород	Внедрение System Center 2012 Configuration Manager	7-10 мая
Microsoft	О	Самара	Возможности идентификации в Windows Server 2016	7-11 мая
Microsoft	О	Самара	Администрирование Microsoft Exchange Server 2016	7-11 мая
Microsoft	О	Владивосток	Администрирование Windows Server 2012 R2	7-11 мая
Microsoft	Д	Самара	Возможности идентификации в Windows Server 2016	7-11 мая
Microsoft	Д	Владивосток	Администрирование Windows Server 2012 R2	7-11 мая
Microsoft	Д	Хабаровск	Администрирование Windows Server 2012 R2	7-11 мая
Microsoft	Д	Самара	Администрирование Microsoft Exchange Server 2016	7-11 мая
Microsoft	Д	Хабаровск	Администрирование Microsoft Exchange Server 2016	7-11 мая
Microsoft	О	Казань	Планирование и администрирование SharePoint 2016	14-18 мая
Microsoft	О	Омск	Автоматизация администрирования с использованием Windows PowerShell	14-18 мая
Microsoft	О	Хабаровск	Базовые решения Microsoft SharePoint Server 2013	14-18 мая
Microsoft	О	Хабаровск	Проектирование и развертывание Microsoft Exchange Server 2016	14-18 мая
Microsoft	О	Нижний Новгород	Развертывание рабочих станций с Windows и корпоративных приложений	14-18 мая
Microsoft	О	Екатеринбург	Установка и конфигурирование Windows Server 2012 R2	14-18 мая
Microsoft	О	Екатеринбург	Администрирование System Center Configuration Manager и Intune	14-18 мая
Microsoft	О	Санкт-Петербург	Разработка решений Microsoft Azure	14-17 мая

Вендор		Город	Курс	Даты
Microsoft	О	Санкт-Петербург	Сетевые возможности Windows Server 2016	14-18 мая
Microsoft	О	Самара	Проектирование и развертывание Microsoft Exchange Server 2016	14-18 мая
Microsoft	О	Новосибирск	Введение в базы данных SQL	14-16 мая
Microsoft	О	Новосибирск	Установка и конфигурирование Windows Server 2012 R2	14-18 мая
Microsoft	О	Владивосток	Базовые решения Microsoft SharePoint Server 2013	14-18 мая
Microsoft	Д	Новосибирск	Введение в базы данных SQL	14-16 мая
Microsoft	Д	Санкт-Петербург	Разработка решений Microsoft Azure	14-17 мая
Microsoft	Д	Санкт-Петербург	Сетевые возможности Windows Server 2016	14-18 мая
Microsoft	Д	Екатеринбург	Установка и конфигурирование Windows Server 2012 R2	14-18 мая
Microsoft	Д	Омск	Автоматизация администрирования с использованием Windows PowerShell	14-18 мая
Microsoft	Д	Владивосток	Базовые решения Microsoft SharePoint Server 2013	14-18 мая
Microsoft	Д	Хабаровск	Базовые решения Microsoft SharePoint Server 2013	14-18 мая
Microsoft	Д	Самара	Проектирование и развертывание Microsoft Exchange Server 2016	14-18 мая
Microsoft	Д	Хабаровск	Проектирование и развертывание Microsoft Exchange Server 2016	14-18 мая
Microsoft	Д	Казань	Планирование и администрирование SharePoint 2016	14-18 мая
Microsoft	Д	Екатеринбург	Администрирование System Center Configuration Manager и Intune	14-18 мая
Microsoft	Д	Москва	Администрирование Microsoft Exchange Server 2016	14-18 мая
Microsoft	Д	Москва	Администрирование Windows Server 2012 R2	14-18 мая
Microsoft	Д	Нижний Новгород	Развертывание рабочих станций с Windows и корпоративных приложений	14-18 мая
Microsoft	Д	Новосибирск	Установка и конфигурирование Windows Server 2012 R2	14-18 мая
Microsoft	Д	Москва	Разработка баз данных SQL	14-18 мая
Microsoft	Д	Москва	Создание информационных хранилищ с помощью Microsoft SQL Server 2014	14-18 мая
Microsoft	Д	Москва	Сетевые возможности Windows Server 2016	14-18 мая
Microsoft	О	Москва	Администрирование Microsoft Exchange Server 2016	14-18 мая

Вендор		Город	Курс	Даты
Microsoft	О	Москва	Администрирование Windows Server 2012 R2	14-18 мая
Microsoft	О	Москва	Разработка баз данных SQL	14-18 мая
Microsoft	О	Москва	Создание информационных хранилищ с помощью Microsoft SQL Server 2014	14-18 мая
Microsoft	О	Москва	Сетевые возможности Windows Server 2016	14-18 мая
Oracle	О	Новосибирск	Oracle Database 12c: Administration Workshop Courseware	23-27 апреля
Oracle	Д	Новосибирск	Oracle Database 12c: Administration Workshop Courseware	23-27 апреля
Oracle	Д	Москва	База данных Oracle: SQL I НОВЫЙ	7-10 мая
Oracle	О	Москва	База данных Oracle: SQL I НОВЫЙ	7-10 мая
VMware	О	Екатеринбург	VMware vSphere: Оптимизация и масштабирование (VMware – Optimize & Scale v.6.0)	23-27 апреля
VMware	Д	Екатеринбург	VMware vSphere: Оптимизация и масштабирование (VMware – Optimize & Scale v.6.0)	23-27 апреля
VMware	Д	Москва	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.6.5)	23-27 апреля
VMware	О	Москва	VMware vSphere: Установка, настройка, управление (VMware vSphere: Install, Configure, Manage v.6.5)	23-27 апреля
Код безопасности	Д	Москва	Администрирование АПКШ «Континент» Версия 3.7. Базовый курс	23-25 апреля
Код безопасности	Д	Москва	Администрирование АПКШ «Континент» Версия 3.7. Расширенный курс	26-27 апреля
Код безопасности	О	Москва	Администрирование АПКШ «Континент» Версия 3.7. Базовый курс	23-25 апреля
Код безопасности	О	Москва	Администрирование АПКШ «Континент» Версия 3.7. Расширенный курс	26-27 апреля
Лаборатория Касперского	Д	Москва	Kaspersky Endpoint Security and Management. Управление системами	19 апреля
Лаборатория Касперского	Д	Москва	Kaspersky Endpoint Security and Management. Управление мобильными устройствами	20 апреля
Лаборатория Касперского	О	Москва	Kaspersky Endpoint Security and Management. Управление системами	19 апреля
Лаборатория Касперского	О	Москва	Kaspersky Endpoint Security and Management. Управление мобильными устройствами	20 апреля

О Очный Д Дистанционный

Лицензия на образовательную деятельность
№ 035264 от 30 июня 2014 года.

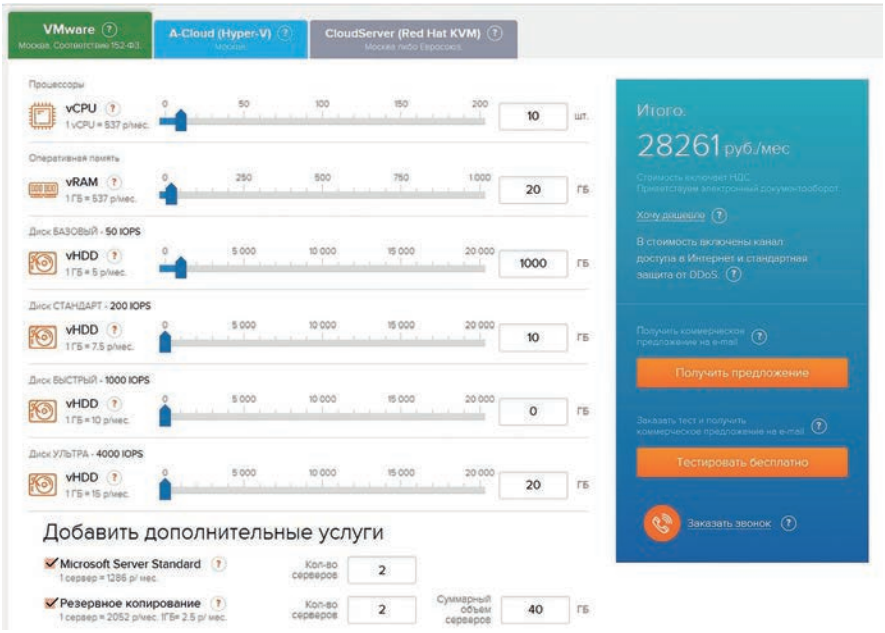
115088, Москва, 2-ой Южнопортовый проезд, дом 31, стр. 1

Звоните: 8-800-505-05-07

Пишите: edusales@softlinegroup.com

Новый сайт ActiveCloud делает облака ближе

Облачный провайдер запустил новую версию сайта **www.activecloud.ru.** Веб-ресурс стал более информативным и полезным, его «изюминка» — онлайн-калькулятор для расчета и заказа широкого спектра облачных услуг.



Что нового?

Новую версию сайта отличает простая навигация, четко структурированная подача информации, современный легкий дизайн. Новинка сайта — калькулятор, максимально упрощающий заказ виртуальных ИТ-мощностей по модели IaaS. Он позволяет выбрать нужное количество процессоров, объем оперативной памяти, размер дискового пространства и скорость его работы. Дополнительно можно заказать лицензии по программе Microsoft SPLA для виртуальных машин, услугу резервного копирования данных, указать требуемый уровень технической поддержки и приобрести антивирусную защиту для виртуальных машин, локальных рабочих станций и серверов.

В чем суть?

Посетитель сайта сразу сможет увидеть стоимость нужного ему объема облачных услуг, а нажав кнопку «Получить предложение», на электронную почту придет сформированное коммерческое предложение согласно выбранным параметрам. На этой же вкладке потенциальный заказчик может послать запрос на тестирование.
Ряд сервисов, связанных с веб-хостингом пользователи могут протестировать или заказать полностью автоматически без участия менеджера.

Один из ведущих международных провайдеров облачных решений для бизнеса. Компания работает на рынке с 2003 года. В 2010 году ActiveCloud вошла в группу Softline. ActiveCloud обслуживает более 50 тыс. клиентов и предоставляет полный спектр облачных решений, от хостинга сайтов до построения частных и виртуальных частных облаков.
Дата-центры компании расположены в Москве (2 площадки), Минске, Ташкенте, а также в Вильнюсе и в Дубае. По итогам 2017 года компания входит в ТОП-5 поставщиков услуг IaaS в России по версии IDC.

«В нашем портфеле решений несколько облачных инсталляций, созданных на базе 3-х технологий виртуализации. С одной стороны, это позволяет предлагать клиентам максимально подходящий для них вариант, а с другой — затрудняет самостоятельный подбор решения. Функционал нового сайта помогает пользователям подобрать то, что им нужно и автоматически сформировать готовое коммерческое предложение, описывающее весь комплекс и стоимость выбранных услуг.»

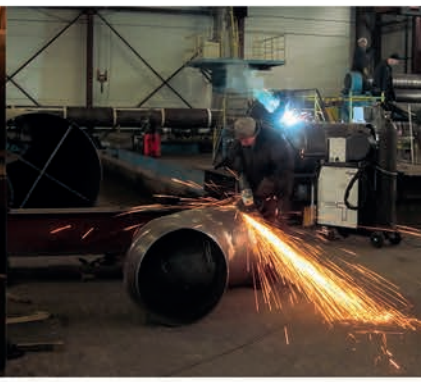
Татьяна Гапоненко,
руководитель отдела маркетинга компании ActiveCloud

STATiSTiCA

IoT - Analytics!

Аналитические исследования Интернета Вещей

Постигаем Умные Данные Интернета Вещей в Промышленности!



academy StatSoft

IoT-Аналитика, Курсы Академии Анализа Данных!

Закажите прямо сейчас: sale@statsoft.ru

+7 (495) 78 777 33 | www.statsoft.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