CIS

Современные Информационные Системы

№ 2 / 11.2017

100 идей контента Digital Signage

Стр. 45

Видеореклама в бизнесе

Путь Samurai

Стр. 18

Защити информацию, уничтожив её

БДУ ФСТЭК

Стр. 25

Практическое использование

Стандарт безопасности

Стр. 28

Как соответствовать?

Разгадай кроссворд – получи приз!

Стр. 51

ПРЕДИСЛОВИЕ

РЕШЕНИЯ

СТАНДАРТЫ

ПРОДУКТЫ

ОПЫТ

КАЛЕНДАРЬ

От редактора

Дорогие читатели, рады сообщить вам о выходе второго номера журнала об информационных технологиях – CIS.

В здоровом теле – здоровый дух! Проводя аналогию, представим себе ваш бизнес или компанию как тело, которое следует всесторонне развивать, укреплять и оберегать для поддержания гармонии с душой – вами. Поэтому тематически этот номер посвящён стандартам безопасности, средствам защиты и базам угроз. Также, на страницах представлены продукты околотематического направления.

В журнале вы найдёте идеи для бизнеса, комментарии экспертов, конкурсы с призами, статьи историй успеха.

Мы очень постарались сделать для вас этот номер максимально интересным, разнообразным и полезным.

На нашем сайте cismag.ru вы всегда сможете скачать свежий номер журнала и подписаться на его бумажную или электронную версию или опубликовать статью со своими продуктами или решениями.

Поскольку приближается новый 2018 год, мы решили сделать для вас приятный бонус – подарить всем желающим большой и очень соблазнительный календарь. Достаточно только написать нам на почту свой адрес (пока только для Москвы) и мы доставим вам его.

Пишите, пожалуйста, сюда: info@sovinfosystems.ru.

Понарин Станислав
главный редактор

Главный редактор: Понарин Станислав.

Корректор: Степанов Артём.

Отдел рекламы и распространения: info@sovinfosystems.ru.

Сайт: www.cismag.ru.

Регистрация журнала: федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Номер свидетельства: ПИ № ФС 77 – 69584.

Дата регистрации: 02.05.2017.

Наименование СМИ: Современные Информационные Системы.

Форма распространения: печатное СМИ, журнал.

Территория распространения: Российская Федерация.

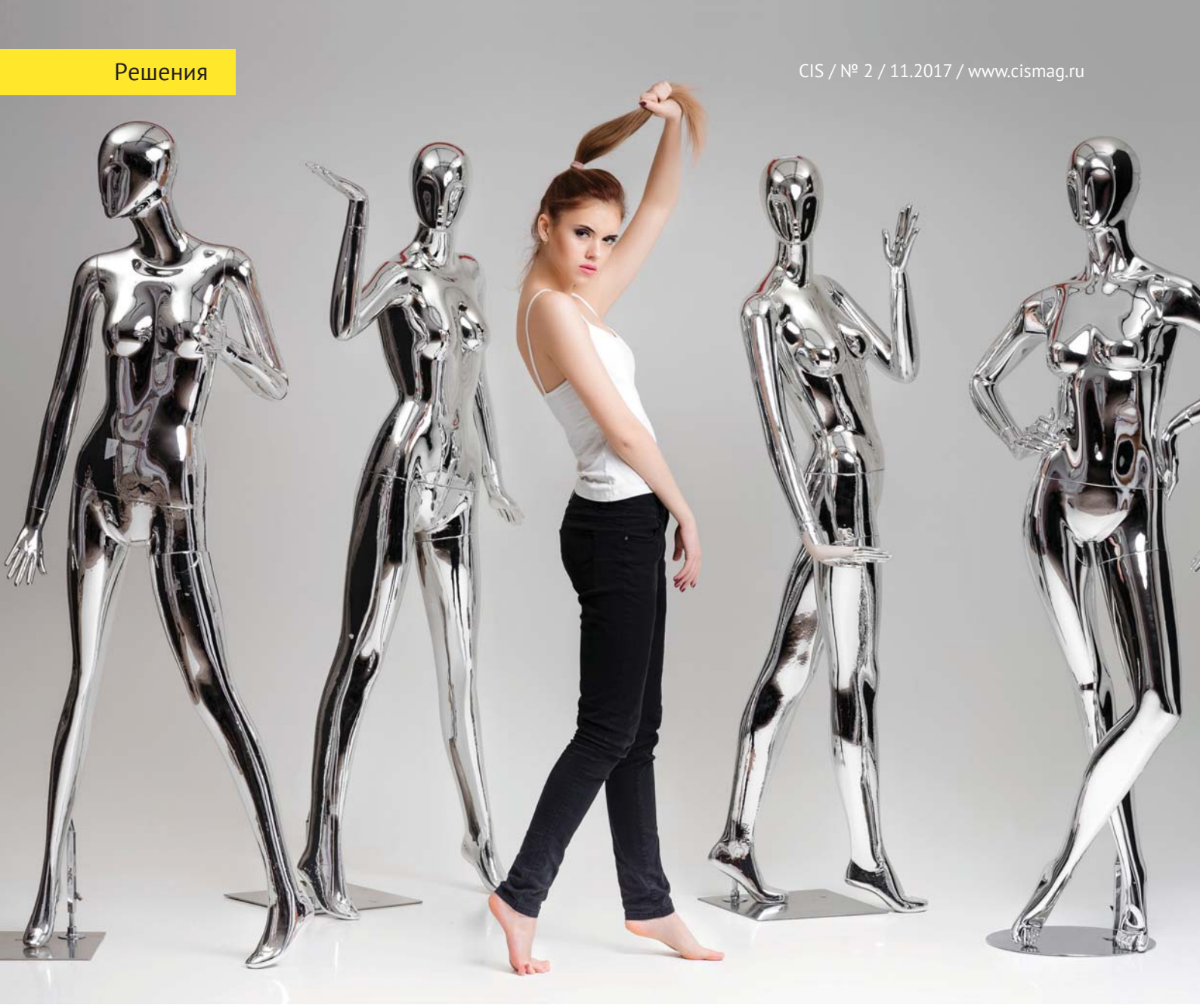
Адрес редакции: Малый Сухаревский пер., д. 9, стр. 1, офис 36, г. Москва, 127051.

Язык: русский.

Периодичность: 4 раза в год (1 раз в квартал).

Тираж 5 000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.



Надёжная аутентификация пользователей на предприятии

Парольная аутентификация доказала свою несостоятельность в контексте обеспечения корпоративной ИТ-безопасности. Главной задачей для ИБ-подразделений в области аутентификации пользователей стал выбор технологий и продуктов, которые должны заменить пароли.

Правда о паролях

В современных компаниях для выполнения бизнес-задач сотрудники используют десятки бизнес-приложений и информационных систем. Им приходится запоминать множество логинов и паролей, а также регулярно менять пароли согласно установленным политикам безопасности. Поэтому сотрудники стараются использовать несложные пароли, дополнительно записывая их на бумажках, которые затем хранят в неподходящих для этого местах.

Кроме того, зачастую пользователи сами сообщают свои пароли коллегам в случае болезни или необходимости выполнения каких-то срочных действий. Поэтому даже если пользователь вводит пароль, это не означает, что он является законным владельцем учётных данных.

«Неудобны» пароли и для специалистов ИТ- и ИБ-служб. Забытые пароли и заблокированные учётные записи требуют дополнительных затрат на восстановление доступа.

Всё это снижает эффективность работы персонала. Но, главное, в такой ситуации возрастает риск несанкционированного доступа к информационным ресурсам компании, а значит, существенно снижается общий уровень безопасности.

Для решения этих проблем используются технологии строгой аутентификации и единого доступа.

Строгая аутентификация

Одним из наиболее эффективных способов решения проблем использования парольного доступа является строгая (многофакторная) аутентификация, основанная на проверке дополнительных данных (факторов) пользователя.

Факторами аутентификации могут быть известная пользователю информация (пароль, PIN-код), имеющееся у пользователя устройство (смарт-карта, токен, генератор одноразовых паролей) или биометрические параметры пользователя, являющиеся его физической особенностью (отпечаток пальца, рисунок вен ладони, лицо).

Аутентификация с применением каждого из этих факторов имеет свои преимущества и недостатки. Однако недостатки отдельных факторов легко устраняются путём применения комбинации нескольких параметров аутентификации. Очевидно, что чем больше факторов используется для аутентификации, тем она надёжнее (наиболее распространённым является применение двух факторов).

Выбор технологий аутентификации является компромиссом между удобством использования, полнотой интеграции, степенью безопасности и ценой итогового решения.

Технология единого входа

Технология единого входа (Single Sign-On, SSO) даёт возможность использовать один набор аутентификационных данных для доступа ко всем (разрешённым) ИТ-ресурсам и системам.

SSO-решения централизованно хранят все пароли пользователя и автоматически подставляют их в запросы аутентификации, когда это требуется.

Для того чтобы выполнить вход в любое доступное приложение, пользователю достаточно лишь предоставить данные для аутентификации (например, приложить палец к считывателю или выполнить какое-то иное действие – в зависимости от используемой технологии аутентификации). Учётные данные (логин и пароль) будут подставлены SSO-системой автоматически без участия пользователя.

Таким образом, пользователи освобождаются не только от необходимости запоминания множества логинов и паролей, но также от необходимости их ручного ввода при аутентификации, что существенно упрощает доступ к приложениям и снижает нагрузку на ИТ- и ИБ-службы.

В концепции SSO также реализуется компонент управления правилами и политиками доступа ко множеству приложений и систем – как для отдельных пользователей, так и для целых групп (отделов, подразделений и проч.), что делает прозрачным процесс управления учётными данными и паролями пользователей. При этом появляется важный «бонус» в виде возможности мгновенной блокировки доступа сразу во все системы в случае такой необходимости.

Решение Indeed Enterprise Authentication

На отечественном рынке технологии строгой аутентификации и единого доступа успешно реализуется программный комплекс Indeed Enterprise Authentication (Indeed EA), разработанный российской компанией «Индид» и предназначенный для построения систем аутентификации сотрудников предприятий.

Данный комплекс поддерживает широкий спектр различных технологий строгой аутентификации (смарт-карты, токены и RFID-карты различных производителей, биометрия, одноразовые пароли), позволяя реализовать различные сценарии многофакторной аутентификации пользователей. Все поддерживаемые технологии можно комбинировать в рамках одной инфраструктуры. Например, можно аутентифицировать пользователей по отпечатку пальца и бесконтактной карте, смарт-карте и OTP и т. д. При этом, если на предприятии уже используются какие-либо способы строгой аутентификации, они могут быть поддержаны данным комплексом, что особенно удобно, поскольку не требует дополнительных затрат на приобретение новых устройств и даёт возможность гибко адаптировать систему аутентификации к потребностям и текущим условиям работы компании.

Подход Single Sign-On в масштабе предприятия реализует компонент Indeed EA Enterprise SSO, входящий в состав комплекса. Система централизованно хранит пароли пользователя от всех приложений, требующих аутентификации, и автоматически подставляет их, когда приложение этого требует. При истечении сроков действия паролей в приложениях система автоматически выполняет их смену.

Indeed EA Enterprise SSO подходит для любых типов приложений, независимо от их архитектуры: однозвенная, трёхзвенная, трехзвенная, «толстый» клиент, «тонкий» клиент, терминальные приложения. При этом организовать доступ можно как в «коробочные» приложения, так и в приложения, разработанные на заказ.

Система также адаптирована к работе в терминальной среде (Remote Desktop, VDI, Citrix), что избавляет сотрудников от явного использования паролей в командировках и других ситуациях, когда работа с приложением выполняется в удалённом режиме.

В компаниях, использующих смарт-карты и токены, Indeed EA Enterprise SSO позволяет связать учётные данные пользователей с жизненным циклом ключевых носителей, интегрировав систему аутентификации с системами управления ключевыми носителями (Card Management System, CMS). Можно отметить, что компания «Индид» также разрабатывает собственную CMS-систему (Indeed Card Management), интегрированную с Indeed EA, хотя при необходимости интеграция возможна и с другими системами данного класса, представленными на рынке.

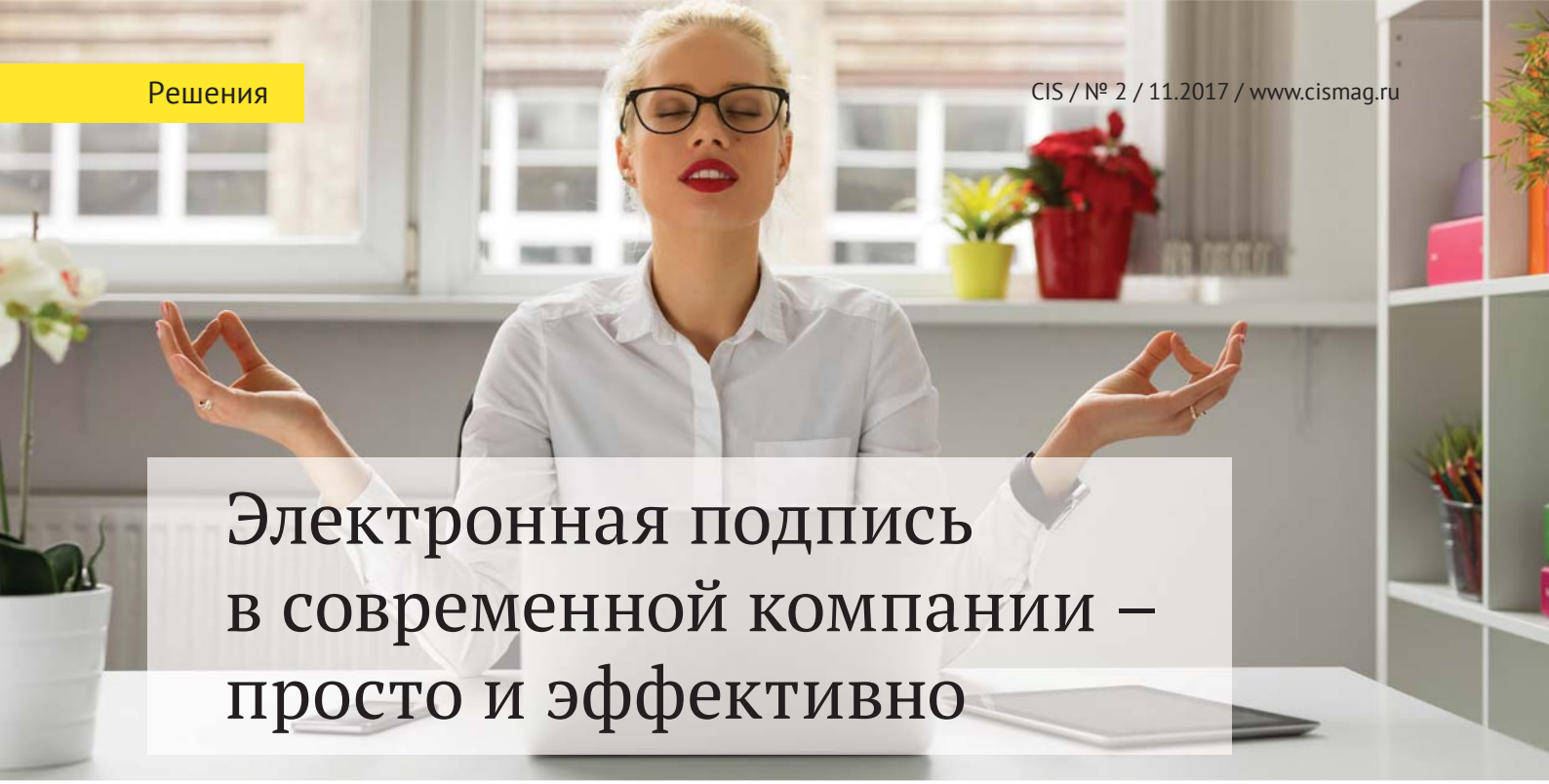
В завершение следует отметить, что все действия администраторов и пользователей фиксируются в специальных журналах событий системы, что существенно упрощает процесс анализа и расследования инцидентов.

INDEED ID

Indeed Identity

Разрабатываемый нами комплекс продуктов предназначен для решения задач по управлению смарт-картами, учётными данными и доступом пользователей к информационным ресурсам компаний и организаций.

www.indeed-id.ru



Электронная подпись в современной компании – просто и эффективно

Зачем это нужно?

Электронная подпись становится неотъемлемым атрибутом даже внутреннего документооборота, цифровые сертификаты являются универсальным средством строгой аутентификации, надёжное шифрование требует использования асимметричной криптографии. Для всех этих задач необходимо развёртывание и сопровождение инфраструктуры открытых ключей (PKI – Public Key Infrastructure).

Со временем сопровождение PKI становится трудоёмкой и сложной задачей. Можно выделить следующие основные проблемы сопровождения PKI:

- с ростом числа используемых цифровых сертификатов возрастает нагрузка на ИТ- и ИБ-службы по контролю срока действия сертификатов и их своевременному обновлению;
- со временем всё сложнее контролировать использование ключевых носителей – смарт-карт и токенов, т. к. устройства теряются, выходят из строя, заменяются и перемещаются между пользователями и офисами;
- использование сертифицированной криптографии ГОСТ для операций КЭП требует ведения журнала СКЗИ по форме согласно требованиям регуляторов;
- с вводом в действие новых удостоверяющих центров линейно возрастают затраты на выпуск и обновление сертификатов.

Перечисленные проблемы требуют грамотного подхода к построению системы управления PKI. Обеспечить такой подход позволяет применение специализированного программного комплекса Indeed Card Management.

Indeed Card Management

Indeed Card Management (Indeed CM) даёт возможность решить указанные проблемы и получить следующие преимущества:

- эффективно управлять жизненным циклом ключевых носителей;
- вести журналирование и аудит действий администраторов и пользователей с ключевыми носителями;
- автоматизировать процессы управления сертификатами пользователей;
- выполнять резервное копирование ключевой информации;
- предоставить сотрудникам механизм самообслуживания для оперативного решения основных задач использования ключевых носителей;
- вести учёт СКЗИ.

Ключевые особенности решения

Поддержка различных производителей смарт-карт

Indeed CM ориентирован на работу с различными смарт-картами, при этом все поддерживаемые карты можно использовать в рамках одной инфраструктуры. Архитектура решения построена таким образом, чтобы иметь возможность оперативной поддержки новых ключевых носителей. На данном этапе поддерживаются следующие ключевые носители:

- Indeed AirKey Enterprise;
- Рутокен компании «Актив»;
- eToken компании SafeNet;
- ESMART компании ISBC;
- JaCarta компании «Аладдин Р. Д.»;
- AvestKey компании «Авест»;
- ID Prime компании Gemalto.

Поддержка КриптоПро УЦ

Indeed CM поддерживает работу с КриптоПро УЦ, а также с КриптоПро CSP. Это даёт возможность применять Indeed CM в инфраструктурах, где требуется шифрование ГОСТ.

Учёт СКЗИ

Indeed CM позволяет вести электронный журнал учёта СКЗИ в соответствии с приказом ФАПСИ №152. Это позволяет выполнить требования регуляторов в части учёта средств криптографической защиты.

Интеграция с Indeed Enterprise SSO

Интеграция Indeed CM с системой управления логическим доступом Indeed Enterprise SSO позволяет связать жизненный цикл смарт-карт и токенов с учётными данными пользователей. В момент выпуска/назначения ключевого носителя администратор имеет возможность сразу

сконфигурировать профиль доступа сотрудника в приложения (профиль Single Sign-On). В результате сотрудник, получая ключ от администратора, уже имеет всё необходимое для полноценной работы. Таким образом, консоль Indeed CM является единой точкой управления жизненным циклом ключей, сертификатов и паролей, упрощая процедуры предоставления и получения доступа в сеть и приложения.

Поддержка принтеров смарт-карт

Использование специализированного принтера смарт-карт позволяет значительно сократить время на персонализацию и выпуск большого количества смарт-карт сотрудникам. Indeed CM позволяет за одну операцию в пакетном режиме выпустить сертификаты и записать их на смарт-карты, а также выполнить персонификацию карт с печатью данных сотрудников на них.

Поддержка КриптоПро DSS

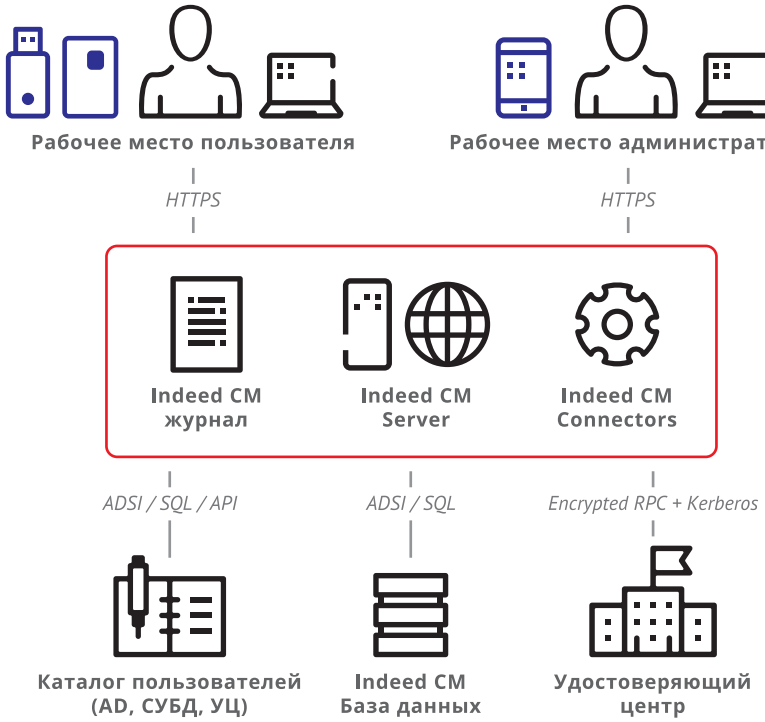
КриптоПро DSS представляет собой централизованный сервис электронной подписи. Решение позволяет применять «облачную» ЭП, что позволяет обходиться без аппаратных носителей (токенов и смарт-карт). Indeed CM поддерживает управление жизненным циклом сертификатами на КриптоПро DSS, что позволяет иметь единую систему управления «облачной» и традиционной электронной подписью.

Результаты внедрения

В завершение хотелось бы отметить ряд преимуществ, которые даёт централизованное управление PKI на базе Indeed Card Management.

Сокращение издержек на сопровождение PKI

Применение в организации инфраструктуры открытых ключей (PKI) требует постоянных затрат на ряд рутинных операций: выпуск новых и обновление истекающих сертификатов, восстановление утерянных устройств, разблокировка заблокированных смарт-карт, учёт устройств и сертификатов и пр. Indeed CM позволяет автоматизировать данные операции и значительно сократить издержки на применение PKI. Система повышает результативность работы как администраторов, так и рядовых пользователей, предоставляя им сервис самообслуживания.



Без привязки к производителю

Организации могут использовать смарт-карты и USB-ключи любых производителей: Indeed CM не накладывает ограничения на парк используемых устройств. Это позволяет, при необходимости, выполнять плавную миграцию с одних устройств на другие.

Виртуальная смарт-карта

Indeed CM поддерживает виртуальную смарт-карту Indeed AirKey Enterprise, которая представляет собой программную реализацию смарт-карты, позволяющую выполнять полный набор операций, доступный аппаратным ключевым носителям. Виртуальная карта может быть доставлена на ПК пользователя в удалённом режиме. Это позволяет, например, оперативно выпустить виртуальный дубликат смарт-карты пользователю, если он забыл или сломал аппаратную карту.

Поддержка «облачного» КриптоПро УЦ

Работа с «облачным» удостоверяющим центром КриптоПро позволяет организациям сэкономить на установке и настройке УЦ на своей стороне и получить его как услугу. Indeed CM полностью поддерживает такой сценарий работы и позволяет работать пользователям и операторам Indeed CM так же, как если бы УЦ был развернут локально.

Работа с ГОСТ без устройств

Поддерживая такие технологии, как КриптоПро DSS и «облачный» криптопровайдер КриптоПро Cloud CSP, Indeed CM позволяет управлять инфраструктурой «облачной» квалифицированной электронной подписи, что даёт возможность использовать криптографию ГОСТ без аппаратных носителей (смарт-карт и USB-ключей).

Простота взаимодействия конечного пользователя с системой

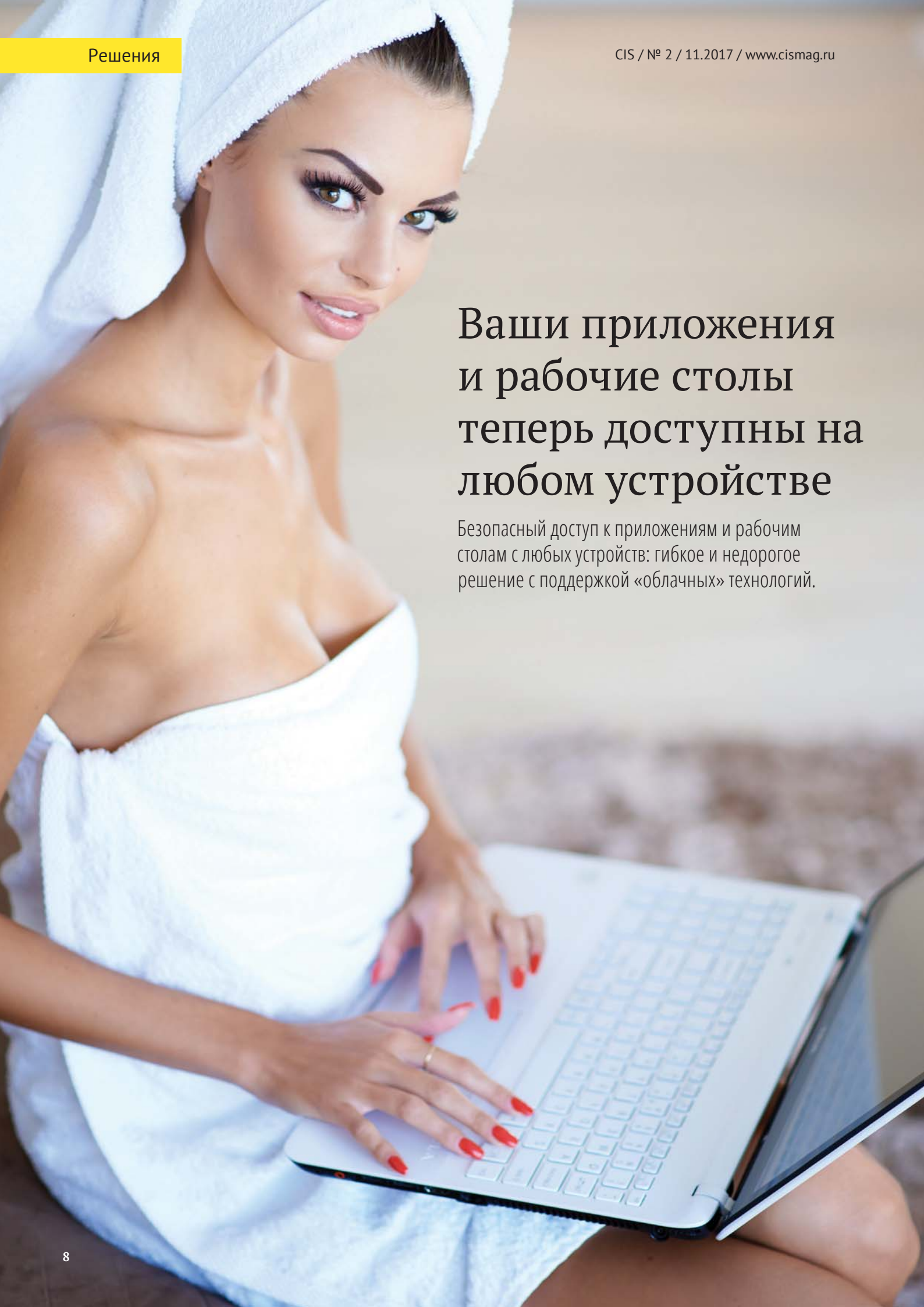
При разработке Indeed CM используются передовые технологии и ориентация на задачи пользователей системы. Это позволяет предоставлять всем участникам процесса удобный и эффективный механизм взаимодействия. Indeed CM имеет удобный и функциональный пользовательский интерфейс, который адаптируется к устройству пользователя. Благодаря этому с системой одинаково удобно работать как на персональном компьютере, так и на планшете или смартфоне.

INDEED ID

Indeed Identity

Разрабатываемый нами комплекс продуктов предназначен для решения задач по управлению смарт-картами, учётными данными и доступом пользователей к информационным ресурсам компаний и организаций.

www.indeed-id.ru



Ваши приложения и рабочие столы теперь доступны на любом устройстве

Безопасный доступ к приложениям и рабочим столам с любых устройств: гибкое и недорогое решение с поддержкой «облачных» технологий.

Решение Parallels Remote Application Server (RAS) поддерживает локальное, гибридное или «облачное» развёртывание на платформах Amazon Web Services и Microsoft Azure. Пользователи устройств под управлением iOS и Android смогут работать с программами Windows так же комфортно, как с обычными мобильными приложениями. Parallels RAS позволяет легко предоставлять доступ к приложениям и рабочим столам благодаря проверенным шаблонам VDI (виртуальный рабочий стол), мастерам настройки и PowerShell API. Контейнеризация приложений поддерживает интеграции с Turbo.net, позволяя одновременно запускать несколько версий приложения на одном сервере.

Основные преимущества Parallels Remote Application Server:

- доступ к приложениям и рабочим столам Windows на любом устройстве в любом месте;
- удобство развёртывания, настройки и управления:
  - пошаговые интуитивно понятные мастера для простой настройки RDSH;
  - мгновенное развёртывание нескольких виртуальных машин и управление ими с помощью утилиты RASprep и проверенных шаблонов;
  - возможность создавать сценарии PowerShell для автоматизации процессов;
- встроенная интеллектуальная балансировка нагрузки, перенаправление печати и сканирования и многое другое;
- множество вариантов доставки приложений и рабочих столов:
  - RDSH и VDI;
  - контейнеры для приложений на основе Turbo.net;
  - использование любого гипервизора: Microsoft Hyper-V, VMware, Citrix, KVM или Nutanix Acropolis;
  - простое лицензирование по модели «всё включено»;
- инновационные мобильные клиенты для iOS и Android, помогающие сотрудникам работать эффективно, где бы они ни находились;
- собственные клиенты для Windows, Mac, Linux, Chrome OS и Raspberry Pi;
- веб-доступ без использования клиента с настраиваемым логотипом и цветовой схемой для HTML5;
- разрешение или ограничение доступа к приложениям и рабочим столам на основе уникальных правил фильтрации.

Удобная работа на мобильных устройствах

Parallels RAS обеспечивает пользователям мгновенный безопасный доступ к приложениям и данным с любых устройств, как если бы эти приложения были разработаны специально для iOS или Android. Сотрудники могут использовать на своих мобильных устройствах привычные сенсорные жесты, такие как прокрутка, перетаскивание, касание или масштабирование, чтобы эффективно выполнять рабочие задачи. Администраторы могут создавать специальные сочетания клавиш для быстрого доступа к командам приложений. Для дополнительного усиления защиты приложений, рабочих столов и данных может использоваться технология Touch ID и коды доступа.

Веб-доступ через HTML5

Сервер Parallels RAS обеспечивает веб-доступ к приложениям, данным и рабочим столам из любого браузера с поддержкой HTML5 на ПК, ноутбуке или мобильном устройстве. Предоставьте своим сотрудникам больше возможностей, создав виртуальное рабочее пространство с доступом к бизнес-ресурсам в любой момент из любой точки мира. Клиент Parallels для HTML5 позволяет вам использовать свой логотип и фирменную цветовую схему. Для каждого пользователя или группы пользователей, указанных в Active Directory, можно использовать персонализированные URL-адреса, темы, приветствия и сообщения о выходе.

Автоматизация

Упростите развёртывание и обслуживание Parallels RAS, воспользовавшись уникальными возможностями для управления инфраструктурой виртуальных рабочих столов (VDI) и службами удалённых рабочих столов Microsoft (RDS). Мастеры настройки, протестированные шаблоны и API PowerShell позволяют ИТ-администраторам быстро вносить необходимые изменения, высвобождая время для более важных задач.

Контейнеризация приложений

Parallels RAS интегрируется с Turbo.net, давая администраторам возможность публиковать приложения в контейнерах и автоматически размещать их на серверах RDSH. Подготовка и установка полностью прозрачны для пользователей и администраторов. Контейнеризация позволяет одновременно запускать на одном сервере разные версии одного приложения или конфликтующие приложения.

Надёжная защита

Parallels RAS поддерживает надёжные механизмы аутентификации – двухфакторную проверку подлинности, доступ по смарт-картам и детализированную фильтрацию устройств и IP-адресов, помогая организациям эффективно управлять доступом к своим ресурсам. Администраторы могут контролировать и ограничивать действия пользователей разными способами, включая удалённую блокировку устройств, запрет операций копирования и вставки, а также контроль подключения USB-устройств.

Улучшенная балансировка нагрузки

Благодаря встроенной балансировке нагрузки на серверы и шлюзы с учётом использования ресурсов решение Parallels RAS позволяет организациям обеспечивать быстрый и надёжный доступ к опубликованным приложениям и рабочим столам в любой момент. Чтобы свести к минимуму простои в работе, вы легко сможете создать среду с многократным резервированием в режимах multi-active/passive или multi-active/active.

Parallels®

Parallels *– новое направление компании: инструмент доставки рабочих столов и приложений Remote Application Server.*

parallels@olly.ru
www.parallels.com/ru

ОЛЛИ ДИСТРИБУЦИЯ

«ОЛЛИ» *– дистрибутор программного и аппаратного обеспечения.*

disti@ollyit.ru
www.ollyit.ru

Оптимизация печати при работе на терминальных серверах

Вопрос печати является одним из важных и критичных для терминальных пользователей. К сожалению, при настройке и управлении процессом печати в терминальном сеансе администраторы довольно часто сталкиваются с множеством трудностей. Среди наиболее распространённых проблем выступают частые сбои в работе спулера печати Microsoft из-за конфликта установленных драйверов печатающих устройств и скорость печати. Также, часто можно слышать о таких задачах, поставленных перед ИТ-отделом, как настройка безопасной печати, сбор подробной статистики по печати, печать с авторизацией пользователя на принтере. Все эти связанные с печатью и не только задачи можно решить с помощью ThinPrint.

Вот уже 18 лет основное решение по организации печати от компании ThinPrint повышает эффективность работы системы печати в компаниях, независимо от их сферы деятельности, размера, региона или имеющейся ИТ-инфраструктуры. Решение относительно просто внедряется и управляется. ThinPrint позволяет увеличить производительность сотрудников, обеспечить оптимальную поддержку процесса печати и заметно сократить расходы путём оптимизации использования ресурсов, отвечающих за печать.

Решение от ThinPrint позволяет оптимизировать систему печати в любом окружении. Неважно, используется ли Microsoft Remote Desktop Services (Terminal Services) или Citrix, Vmware, установлены тонкие клиенты или классические ПК, – решение ThinPrint в сочетании с выделенным сервером печати позволит оптимизировать систему печати для любой ИТ-инфраструктуры.

Основные функции ThinPrint

Быстрая печать с высоким уровнем сжатия

Объём передаваемых данных при печати – очень важный параметр. Часто объём распечатываемого документа больше исходника. ThinPrint анализирует структуру документа и выбирает оптимальный алгоритм сжатия. Благодаря высокому уровню адаптивного сжатия (Advanced Adaptive Compression) ThinPrint сжимает до 98 % от первоначального размера без использования дополнительного программного обеспечения, аппаратных устройств или изменений в ИТ-среде.

Простота администрирования и сокращение сбоев с Driver Free Printing

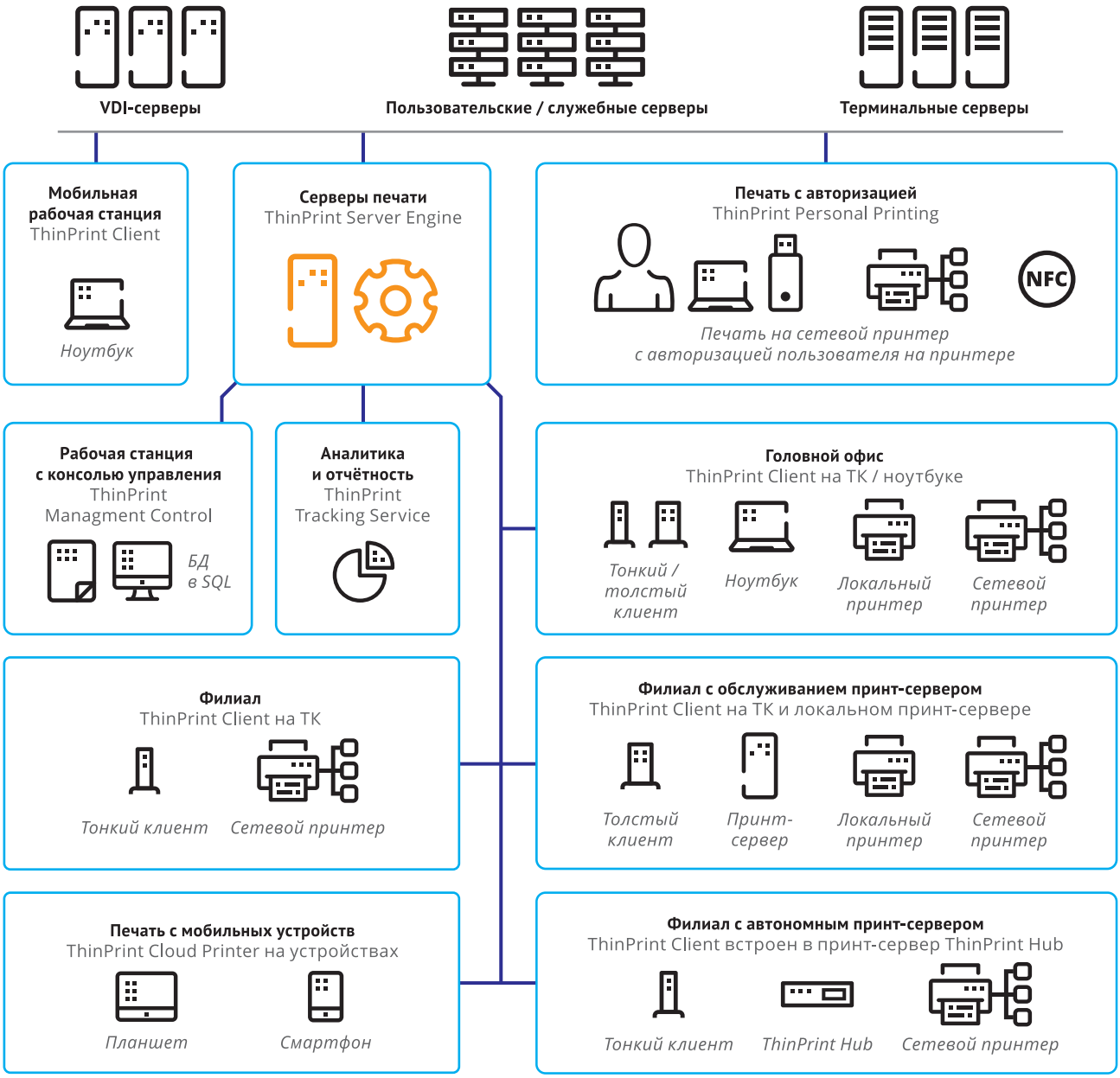
Наличие огромного количества различных драйверов печатающих устройств значительно усложняет работу системных администраторов и службы поддержки. С ThinPrint всё обстоит совершенно иначе: вместо множества драйверов печатающих устройств используется единый виртуальный драйвер – ThinPrint Output Gateway. По-прежнему доступны расширенные настройки печати, при этом ни пользователи, ни администраторы больше не испытывают проблем, связанных с драйверами.

Сокращение серверов благодаря консолидации

Технология ThinPrint позволяет избавиться от локальных серверов печати в филиалах и дочерних предприятиях. Это сокращает расходы на управление, аппаратное обеспечение, энергопотребление и операционную деятельность, дополнительно полностью оптимизируется использование существующих ИТ-ресурсов.

Отказоустойчивость и балансировка нагрузки гарантируют высокую доступность службы печати

Если сервер печати по какой-либо причине недоступен, то все процессы печати автоматически переносятся на другой сервер. ThinPrint проверяет доступность сервера и сразу же реагирует на проблемы с печатью. Благодаря функции балансировки нагрузки, пользователи равномерно распределяются между сервера-



ми печати. Таким образом гарантируется оптимальное использование аппаратных ресурсов, что, в свою очередь, позволяет снизить число используемых серверов печати.

Полный контроль расходов на печать

Модуль ThinPrint Tracking Service собирает статистику по печати в компании: что, где, когда, сколько, стоимость и т. д. Данная информация заносится в базу данных и предоставляется в виде графических отчётов. Это позволяет легко определить основные источники затрат и принять соответствующие меры по их сокращению.

Печать с авторизацией пользователя на принтере

Благодаря решению от ThinPrint возможно построить такую конфигурацию, при которой пользователь будет получать свои распечатки только после авторизации на принтере. Данное решение позволяет обеспечить безопасную печать конфиденциальных данных, значительно сократить затраты на печать за счёт уменьшения количества ошибочных заданий печати и повысить гибкость системы печати. Принцип следующий: документ отправляется на принтер только после того, как пользователь авторизовался на нём. Отметим, что здесь есть несколько способов авторизации. Неоспоримым преимуществом данного решения является то, что на любом сетевом принтере в компании, независимо от производителя и модели, можно настроить печать с авторизацией. Таким образом, данное решение позволяет уменьшить число принтеров в компании, повысив при этом безопасность печати для каждого сотрудника.

ThinPrint®

ThinPrint *– поставщик программного обеспечения и услуг по управлению печатью.*

info@thinprint.com
www.thinprint.com

ОЛЛИ ДИСТРИБУЦИЯ

«ОЛЛИ» *– дистрибутор программного и аппаратного обеспечения.*

disti@ollyit.ru
www.ollyit.ru

SEH – немецкий производитель оборудования для проброса USB через IP

USB по сети от SEH

Виртуализация USB и для чего она нужна

Виртуализация – виртуальная версия аппаратного обеспечения (платформ, устройств, ресурсов и т. п.). Виртуализация USB – проброс USB через IP:

- доступ к USB-устройствам по сети;
- превращение несетевых USB-устройств в сетевые устройства.

Области применения:

- рабочие станции с малым количеством или без USB-портов;
- системы с вычислениями на стороне сервера и среды виртуализации;
- совместное использование устройств.

Представление

3 продуктовых линейки:

- для USB-устройств: myUTNUSB Deviceserver;
- для USB-токенов: myUTNUSB Dongleserver;
- промышленное использование: USB Deviceserver с монтажом на DIN-рейку.

Принцип работы

Подключите сервер UTN к сети и USB-устройство/токен к серверу UTN. Установите ПО SEH UTN Manager на все клиентские машины, где нужен доступ к USB-устройствам/токенам. Создавайте/разрывайте подключение в SEH UTN Manager.

myUTN

- Широкий спектр поддерживаемых USB-устройств/токенов.
- Доступ к USB-устройствам/токенам обеспечивается независимо от местоположения и длины USB-кабелей.
- Не зависит от платформы (ПО SEH UTN Manager поддерживает Windows, OS X и Linux).
- Удобство использования (простая установка, настройка и управление).
- Снижение затрат (создание пулов USB-устройств/токенов).
- Регулярные обновления ПО и техническая поддержка по всему миру.
- Набор эффективных средств безопасности.

myUTN Dongleserver

- Большое количество USB-портов.
- Контроль доступа к отдельным портам и ключам.
- Шифрование передаваемых данных.
- Высокая стабильность работы.
- Поддержка VLAN.
- Сертификация SafeNet, WIBU, Marx, VMWare и Citrix.
- Возможность обеспечить дополнительную физическую защиту токенов, механически закрыв отсек с ними на ключ.
- Работающая поддержка от производителя и его открытость для создания специальных решений с дополнительными функциями для конкретных проектов и заказчиков.
- Полноценная защита сделок по продуктам SEH благодаря эксклюзивному положению компании «ОЛЛИ» в России.

Кому нужна виртуализация USB токенов?

- Центрам обработки данных и «облачным» провайдерам.
- Производственным и любым другим компаниям, которые используют различное специфическое ПО, защищённое лицензионными ключами.
- Финансовым организациям, в которых повсеместно используются банковские ключи.
- Компаниям, где используется виртуализация серверов и рабочих столов.
- Компаниям с высокими требованиями к безопасности.
- Компаниям, у которых не хватает или запрещено использование USB-портов на рабочих станциях.
- Компаниям с работниками вне офиса, которые пользуются защищённым ПО.
- Продавцам лицензионного ПО с защитой на базе аппаратных ключей.

Корпоративная мобильная печать с AirPrint®

- Программная функция от Apple для печати с устройств Apple (Mac, iPhone, iPad).
- Не требуется дополнительное ПО (встроенная функция OS X/macOS и iOS).
- Практически все современные принтеры по умолчанию поддерживают AirPrint.
- Автоматическое обнаружение принтеров.
- Корпоративное решение для мобильной печати – primos.
- Печать с устройств iOS.
- На основе технологии AirPrint.
- Реализовано в виде отдельного устройства.

Выгода

- Поддержка служб каталогов.
- Wide-Area AirPrint.
- Локальные пользователи и группы.
- Безопасный AirPrint.
- Не требуется дополнительное ПО для iOS.
- Без подключения к «облаку».

Сетевая печать с принт-серверами от компании SEH

Принт-серверы – это аппаратные устройства, которые используются для подключения принтеров к сети:

- отдельная коробка;
- встраиваемая плата;
- ПК (принтер с общим доступом).

Задания печати посылаются от клиента (ПК) по сети к принт-серверу, который уже передаёт их на принтер.

Задания печати выстраиваются в очередь (обрабатываются одно за другим).

Почему нужны принт-серверы SEH?

- Общий доступ к устройствам. Пользователи работают с принтерами по сети.
- У принтера нет встроенной сетевой карты.
- Снижение затрат. Не нужно покупать новые принтеры.
- Дополнительные функции (обработка или защита данных печати).
- Простая установка, администрирование и обслуживание.
- Поддержка всех типов интерфейсов (USB, последовательный, параллельный или специальный интерфейс от производителя принтера).
- Поддержка всех типов печатающих устройств (струйные принтеры, лазерные принтеры, принтеры этикеток, принтеры больших форматов, плоттеры, матричные принтеры, принтеры штрих-кодов, МФУ, копиры и т. д.).
- Не зависит от платформы (Windows, OS X/macOS и Linux).
- Регулярные обновления ПО, техническая поддержка по всему миру.

Протоколы печати

Socket printing, IPP/IPPS, LPD/LPR, HTTP/HTTPS, ThinPrint.

Безопасность

Шифрование заданий печати (SSL/TLS), IPSec, Аутентификация (802.1X), сертификаты, контроль доступа.

Обработка данных печати

- Задержка в приёме заданий.
- Редактирование (например, поиск и замена).
- Фильтры (например, логические принтеры, ASCII или Hex).

Сценарии использования

Второй сетевой интерфейс

- Требуется во многих проектах.
- Безопасность (два различных уровня безопасности, например, публичный и частный).

Принтеру не хватает средств безопасности

- Аутентификация 802.1X.
- Интеграция IPSec.
- Проекты, где требуется высокий уровень безопасности.

SEH – один из редких производителей принт-серверов, оставшихся на рынке

- Производители принтеров требуют, чтобы принт-серверы поддерживали их функции.
- Производители принтеров рассчитывают на высочайшее качество и поддержку.

SEH

SEH Computertechnik GmbH

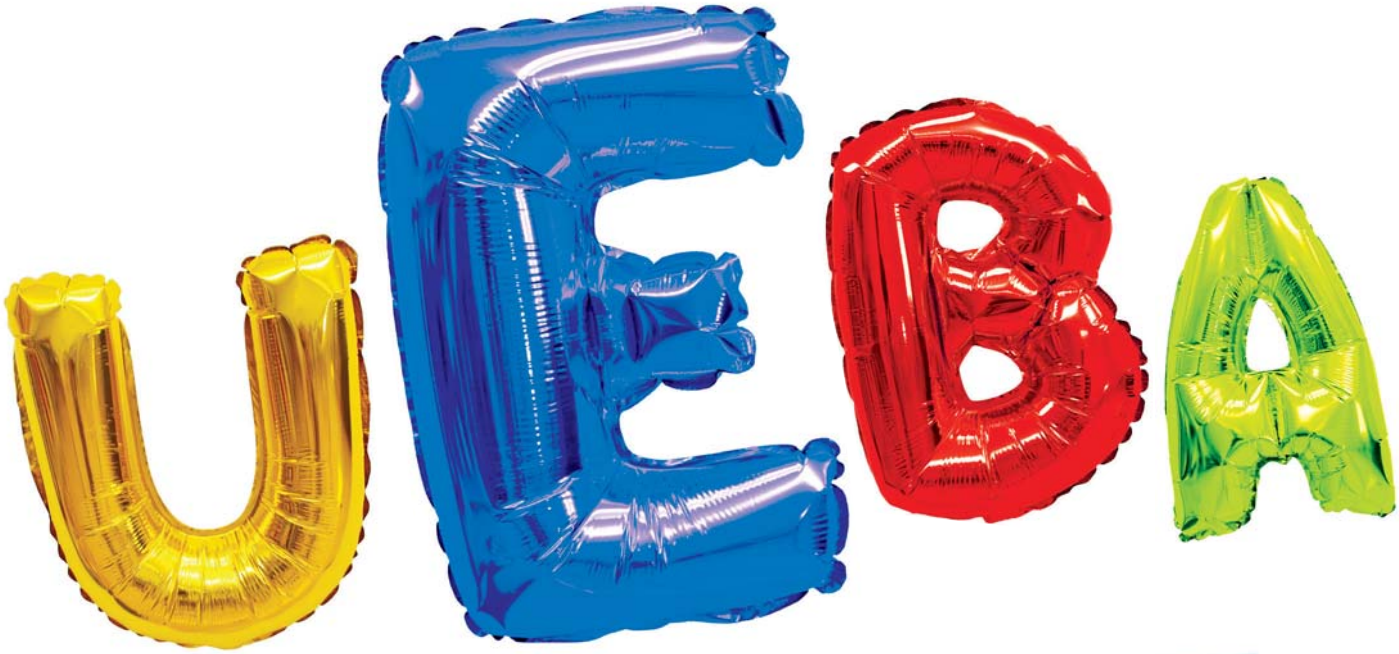
Производитель оборудования для проброса USB через IP.

www.seh.de

ОЛЛИ ДИСТРИБУЦИЯ

«ОЛЛИ» – дистрибутор программного и аппаратного обеспечения.

disti@ollyit.ru
www.ollyit.ru



Что же значит буква «E»?

Ни для кого не секрет, что в настоящее время существующая реальность ИБ связана с аналитикой колоссального объёма данных. Рынок инструментов аналитика растет, появляются всё новые и новые решения «Next Generation» (следующее поколение). В классе решений UBA (User Behavior Analysis) следующим поколением являются системы класса UEBA (User & Entity Behavior Analysis).

Решения UBA, как правило, опираются на статическую модель поведения конкретного пользователя. Это ваша учётная карточка, в которой обозначены «имя, фамилия, рост и вес». Но в данной анкете нет данных о вашем взаимодействии. Нет данных о процессах, о среде, в которой вы работаете.

В свою очередь, решения UEBA позволяют построить динамическую модель поведения пользователей. Данная модель строится с учётом изменения среды, в которой находится пользователь. Предполагается, что система работает по принципу превентивности.

Рассмотрим пример. Поисковый запрос: повышение привилегий в ОС Ubuntu.

Для системы класса UBA данный запрос останется строкой в логах, конечно же, если пользователь не начнет использовать советы из результатов поискового запроса. Но решения класса UEBA учтут, что пользователь не эксплуатирует ОС Ubuntu, что данному пользователю не требуется привилегий для исполнения служебных обязанностей, и на основе этой информации создадут предупреждение.

Примерами в частном случае могут послужить запросы следующего характера: повышение привилегий в ОС, удаление логов в ОС и тому подобные. В данном случае ОС и является той самой средой, той самой Entity.

Вам остаётся решать, важна ли буква «E» для вашей компании, а Next-Generation SIEM это уже совсем другая история...

Эдуард Яровой, независимый эксперт.

Система ePlat4m Security GRC

Программный комплекс, обеспечивающий автоматизацию процессов ИБ и их интеграцию в систему управления организацией.

Автоматизация СУИБ

Любая современная система управления информационной безопасностью (СУИБ) помимо средств защиты информации включает в себя поддерживающие их процессы информационной безопасности (ИБ), объединяемые на основе выбираемой модели управления ИБ. В связи со сложностью используемой ИТ-инфраструктуры, наличием актуальных многовекторных угроз ИБ и ограниченными ресурсами, направляемыми предприятием на защиту своих корпоративных активов, говорить о возможности построения эффективной СУИБ без автоматизации процессов обеспечения и управления ИБ не приходится.

Security GRC

Решение ePlat4m Security GRC относится к классу специальных информационно-аналитических систем, автоматизирующих процессы обеспечения и управления ИБ корпоративной СУИБ. В западной терминологии этот класс решений принято называть GRC (Governance – стратегическое управление, Risk – риски, Compliance – соответствие требованиям). В России решения класса GRC применительно к тематике ИБ принято также именовать решениями Security GRC класса. Security GRC – это концепция управления организацией (Governance) в сфере информационной безопасности (ИБ) на основе оценки рисков (Risk) и в соответствии с нормативными правовыми и корпоративными требованиями по защите информации (Compliance), а также технология по реализации данной концепции. Все три вида деятельности связаны между собой, оказывают влияние друг на друга и позволяют в совокупности принимать руководству эффективные управленческие решения в области ИБ во взаимосвязи с другими корпоративными системами управления.

Опыт внедрения

Исходя из практического опыта внедрения системы ePlat4m Security GRC в России, можно выделить следующие выгоды от внедрения системы на предприятии:

- снижение рисков, связанных с регулирующими органами в области ИБ: ФСТЭК России, ФСБ России, Банка России – за счёт полного и эффективного учёта и контроля соблюдения различных нормативных требований по ИБ;
- повышение уровня защищённости ИТ-активов за счёт повышения зрелости процессов управления и обеспечения ИБ;
- упрощение проведения аудита предприятия на соответствие требованиям по ИБ, за счёт централизованного хранения и повторного использования его результатов;
- предоставление сводных аналитических данных по ИБ в понятном и наглядном виде для поддержки принятия управленческих решений;
- построение корпоративной СУИБ на основе риск-ориентированного подхода.

Создание системы

При создании системы ePlat4m Security GRC был учтён опыт ведущих мировых производителей решений класса GRC, поэтому система ePlat4m Security GRC включает в себя:

- реляционную базу данных, которая хранит и осуществляет контекстное преобразование данных по управленческой деятельности в рамках организации;
- механизм потока работ (workflow), который позволяет выстраивать GRC-процессы;
- механизм управления контентом, который поддерживает единый жизненный цикл неструктурированной информации (контента) GRC различных типов и форматов;

- механизм формирования отчётности, который позволяет представить информацию GRC в удобном для восприятия и анализа виде для лиц, принимающих решения;
- механизм управления доступом;
- механизм генерации и отправки уведомлений о событиях системы пользователям;
- механизмы анкетирования и тестирования персонала, позволяющие создавать и управлять опросными листами и тестами;
- механизм создания пакетов для переноса изменений между средами разработки, тестирования и производства, установления обновлений и передачи в службу поддержки;
- инструменты разработки собственных приложений и их объединения в отдельные модули;
- инструменты по интеграции со смежными системами.

Модули автоматизации

Модули	Функции
Управление классификацией ИТ-активов	Автоматизирует процессы учёта и классификации информационных и физических ИТ-активов.
Управление рисками ИБ	Автоматизирует процессы идентификации, анализа, оценки и обработки рисков ИБ.
Управление инцидентами ИБ	Автоматизирует процессы регистрации, обработки инцидентов ИБ, оповещения о них, хранения статистики и результатов расследования инцидентов.
Управление персоналом и третьими сторонами по вопросам ИБ	Автоматизирует процессы доведения организационно-распорядительных документов по ИБ до работников и контрагентов Заказчика, контроль знаний работниками Заказчика требований по ИБ.
Управление соответствием требованиям по ИБ	Автоматизирует процессы внутреннего аудита и оценки соответствия системы ИБ Заказчика требованиям по ИБ.
Управление защитой персональных данных	Автоматизирует процессы защиты ПДн (ведение перечня ПДн и ИСПДн, формирование описания процессов обработки ПДн, работа с обращениями субъектов ПДн, формирование частной модели угроз и модели нарушителя и др.).
Мониторинг эффективности процессов ИБ	Автоматизирует процессы оценки результативности и эффективности процессов обеспечения и управления ИБ.
Управление документацией по ИБ	Автоматизирует процессы хранения, согласования, определения актуальности документации системы ИБ Заказчика.
Управление аудитами ИБ	Автоматизирует процессы планирования аудитов ИБ, определения перечня проверяемых требований, учёта выявленных замечаний и автоматизированного контроля их устранения.
Управление уязвимостями	Автоматизирует процессы централизованного учёта всех выявленных уязвимостей, оповещения о них, планирования и контроля за устранением уязвимостей.

В поставку могут быть включены модули, обеспечивающие автоматизацию определённых процессов обеспечения или управления ИБ.

Подведём итоги

В случае принятия положительного решения о внедрении на предприятии системы класса Security GRC следует обратить внимание на следующие ключевые факторы успеха проекта внедрения:

- поддержка проекта внедрения системы Security GRC со стороны руководства предприятия и подразделения ИБ;
- наличие у организации эффективной организационной структуры, обеспечивающей управление ИБ на предприятии в рамках корпоративной СУИБ;
- прохождение необходимого обучения эксплуатации системы Security GRC в авторизованном учебном центре;
- соответствие системы Security GRC требованиям регуляторов – наличие системы в государственном реестре российского программного обеспечения, а также наличие сертификатов соответствия ФСТЭК России или ФСБ России;
- вовлечение в автоматизируемые с помощью системы Security GRC процессы управления ИБ всего необходимого персонала: руководства организации, ИТ-подразделения, подразделений внутреннего аудита и риск-менеджмента и др.;
- наличие у системы Security GRC гибкости и возможности настройки прикладных модулей с использованием инструментов платформы без необходимости привлечения программистов;
- выделение необходимого финансирования на внедрение, развитие и сопровождение системы Security GRC.

Путь Samurai: как защитить информацию, уничтожив её

На что сделал ставку владелец «Рантеха» Евгений Цацура, чтобы отвоевать себе место на рынке флэшек.

Набирая код на приборчике размером чуть больше пачки жевательной резинки, Евгений Цацура поясняет: «Бывают ситуации, когда отсутствие информации лучше, чем её присутствие. Представьте себе, что вы потеряли флэшку, а там важная информация. Если кто-то попытается её достать, данные будут стёрты».

Принадлежащая Цацуре компания «Самурай» выпускает под брендом GuardDo несколько моделей флэш-накопителей и внешних жёстких дисков, а также B2B-системы для защиты информации Samurai. В год такие устройства приносят «Самураю» 80 млн рублей выручки. Около 40 % продаж приходится на флэшки и диски. Если конкуренты завлекают покупателей возможностями хранения, то фирма Цацуры, наоборот, – безвозвратного уничтожения информации. Её рекламный слоган: «Когда уничтожить важнее, чем сохранить». Оправдала ли себя стратегия продвижения от противного?

В середине 2000-х москвич Евгений Цацура, инженер-приборостроитель по специальности, учредил компанию, взявшуюся торговать импортным оборудованием для защищённого хранения информации. Как-то летом в 2007 году Евгению позвонил взволнованный приятель – у него украли из автомобиля сумку с личными вещами, среди которых находилась флэшка с важными документами. «Он меня спросил тогда, нельзя ли создать флэшку, которая бы безвозвратно стирала информацию при попытке взлома пароля», – вспоминает предприниматель.

Хотя зарубежные варианты таких флэшек существовали, на российском рынке о них мало кто знал. А отечественное устройство могло составить им конкуренцию по цене. У «Самурая» на тот момент была своя сборка систем хранения информации с функцией экстренного уничтожения. Цацура попробовал применить имевшуюся разработку в компактном виде. Потратив 150 000 $ на производственное оборудование и аренду помещения в технопарке «Строгино», Цацура приступил к созданию флэшки-уничтожителя. В 2008 году он запатентовал портативные накопители информации с особой защитой: при неверном наборе пароля более шести раз на все ячейки памяти подаётся сигнал и состояние носителя приводится к исходному.

Правда, флэшка получилась дорогой – около 10 000 рублей, почти как у британских и американских аналогов. «Но она работала, и клиентов цена не смущала», – улыбается Цацура. За год компания продала 1500 флэшек, предлагая их как постоянным, так и потенциальным заказчикам. Свои системы защищённого хранения «Самурай» предлагал за 150 000 рублей – немалые деньги. И Евгений Цацура решил демонстрировать возможности технологии с помощью флэшки. Клиентам предлагали купить такой накопитель, убедиться в его эффективности, а затем уже прийти за более мощным оборудованием.

Всем устройствам дали название Samurai. «С одной стороны, самурай хозяина защищает, с другой – уничтожает себя, если оказался в позорной ситуации, – объясняет Евгений Цацура. – Благодаря слогану внимание на себя мы обратили. А затем уже разъясняли, в чём наши преимущества». Учтя пожелания пользователей, собранные путем опроса на сервисе HabrHabr (пришло около 4000 ответов), команда Цацуры в конце 2013 года подготовила вторую версию флэшки. Она выглядела более стильно, не требовала подключения через USB-кабель, а управлять её состоянием можно было с помощью клавиатуры на корпусе.

Розничную цену владелец «Самурая» решил установить на уровне 100 $ – как у самых дешёвых импортных аналогов. Производителя корпусов он нашел в Китае. Собирали и прошивали флэшки сотрудники «Самурая». Накопители второй версии продавали покупателям, приходящим по рекламе в интернете, и в мелкой рознице – на «Горбушке» и Митинском радиорынке. В первой произведенной партии обнаружилось около 25 % брака. Наладив качество, Цацура задумался о крупной рознице.

Для работы с крупными ретейлерами нужна товарная линейка. Предприниматель дополнил флэшки внешними жёсткими дисками. Специалисты из брендингового агентства ради придания престижности и отражения ключевых качеств новых продуктов предложили название GuardDo: «guard» – защита, а «do» в английском языке означает «действие», в японском – «путь». Товарным знаком стал силуэт рукояти меча с гардой как символ надёжной, но не грубой защиты. Слоганом – фраза «Защита информации любой ценой».

Сегодня в линейке Samurai GuardDo пять продуктов – флэшки с разными объёмами памяти, USB-накопитель, карманный жёсткий диск и два жестких диска большего объёма. Для каждой модели Цацура подобрал имена из фехтовальных терминов: Touche (лёгкий укол шпагой), Volte (уклонение от удара противника) и т. д.

«Самурай» продаёт 80 % своей продукции – как B2B-системы, так и линейку GuardDo – через дистрибьюторов. «До Samurai у нас уже был опыт продажи таких устройств. Они пользуются спросом, а Samurai к тому же имеет чуть более приятную цену, – говорит Станислав Вацуев, категорийный менеджер отдела закупок интернет-магазина iCover. – Объёмы, естественно, несравнимы с более массовыми обычными внешними жёсткими дисками. Но сейчас, например, есть несколько заказов на накопители Samurai объёмом до 25 штук».

Евгений Цацура называет свой продукт флэшкой для внимательных. Если пользователь забыл пароль, достать информацию с накопителя уже невозможно. «К нам не раз обращались клиенты с просьбой взломать за любые деньги. Но технически это невозможно», – разводит руками предприниматель. В некоторой степени это сдерживающий фактор для продаж. Но важнее цена. «Это специфичная продукция, и массовый покупатель, в том числе и в корпоративном сегменте, вряд ли оценит преимущества таких носителей информации, – комментирует представитель сети „Связной“ Сергей Тихонов. – Ключевым моментом является цена гаджета. В „Связном“ стоимость внешнего жёсткого диска начинается от 2990 рублей, в то время как самое доступное устройство от „Самурай“ предлагается почти за 6000 рублей».

Флэшки и жёсткие диски GuardDo продаются в 40 онлайн- и офлайн-магазинах Москвы и регионов. Корпоративных клиентов, пользующихся оборудованием «Самурая», Евгений Цацура не называет, ссылаясь на соглашения о конфиденциальности, но говорит, что их около пятнадцати. Хотя 60 % выручки «Самурая» приходится на крупное оборудование (от импорта компания почти отказалась), его доля, уверяет предприниматель, постоянно уменьшается.

В планах Цацуры выход на крупнейших сетевых продавцов электроники, таких как «М.Видео» и re:Store. «Мы видим спрос на такие товары со стороны компаний, которые будут закупать их для своих сотрудников, либо со стороны энтузиастов, – замечает представитель „М.Видео“ Юлия Зотова. – Но массовым продуктом их назвать сложно. К тому же в I квартале 2015-го продажи флэш-накопителей упали на 12,7 % по сравнению с 2014 годом. Как и любую другую продукцию, защищённые флэшки необходимо продвигать на рынке, а это большие вложения для производителей».

Евгений Цацура признает: пока очень мало людей знают о таких продуктах, а у GuardDo нет значительного маркетингового бюджета (основные рекламные каналы – выставки, конференции, интернет). Но он надеется, что проблемные случаи, потребность в защите и сарафанное радио сделают своё дело. «*Многие считают, что им защита информации не пригодится,* – рассуждает создатель Samurai. – *А это как подушка безопасности в машине: лучше не пользоваться, но спокойнее, когда она есть*».

GUARD'DO

«Самурай24»

Разработка высокотехнологичных комплексных решений для эффективной защиты корпоративной информации от потерь, кражи или от несанкционированных действий злоумышленников.

www.samurai24.ru

Способы защиты данных при высокоскоростном доступе в интернет

Введение

Скоростной доступ в интернет – требование времени, однако обеспечение безопасности такого доступа может влететь в копеечку, а администрирование может быть чрезвычайно затруднено. Также, операции шифрования могут снизить скорость доступа. Эта статья посвящена тому, как избежать подобных неприятностей.

Приведённые в статье сведения также могут пригодиться в следующих случаях:

- необходимо увеличить скорость доступа в интернет;
- нужно оптимизировать расходы на интернет;
- нужно упростить управление безопасностью;
- работа приложений является причиной высокой загрузки сети организации.

Увеличение спроса на высокоскоростной доступ

Всё большему количеству организаций требуется высокоскоростной доступ в интернет. Возникает необходимость не только в «толстых» каналах, но и в способах эффективного управления ими. Ethernet позволяет масштабировать полосу пропускания до 100 Гбит/с, при этом затраты на порт ниже, чем при использовании обычных WAN-технологий.

Поэтому различные организации имеют возможность платить за фактическое использование пропускной способности, при этом затраты могут расти постепенно – в зависимости от реального использования полосы пропускания. Это основная причина, почему организации предпочитают использоваться свой Ethernet, чтобы передавать данные по WAN.

Ethernet позволяет обеспечивать соединение на высокой скорости между различными зданиями в черте большого города, а также между несколькими населёнными пунктами или в пределах глобальной сети. Также, службы Ethernet позволяют укрупнить инфраструктуру LAN до глобальной сети, предоставляя возможность гибкого администрирования. Сейчас скорость обмена данными между региональными концентраторами при взаимодействии между дата-центрами превышает 1 Гбит/с.

Сайты восстановления информации, для работы которых необходима скоростная синхронизация сети хранения данных, требуют ещё большую скорость сети. Для этих целей используются соединения с малой задержкой E-LAN или E-Line.

«Облачные» приложения для коллективной работы также требуют повышения пропускной способности. Технология IP MPLS может стать причиной задержек, поэтому она не годится для передачи, например, аудио и видео в реальном времени.

К списку задач, для которых требуется высокоскоростное соединение, можно отнести обработку брокерских транзакций, а также передачу медицинских данных (например, снимков). Ethernet позволяет повысить скорость передачи за меньшие средства, если сравнивать с другими технологиями.

Таким образом, технология Ethernet завоёвывает популярность среди организаций, которым нужен высокоскоростной обмен данными. Немалую роль в этом играет простое управление. Одно из неоспоримых преимуществ этой технологии – возможность масштабирования в рамках организации без потери значительных ресурсов.

Чем привлекает технология Ethernet:

- позволяет масштабировать полосу пропускания;
- снижает сложность администрирования;
- снижение стоимость использования;
- предоставляет возможность контроля безопасности;
- совместимость разных производителей на основе принятых стандартов.

Шифрование и защита данных

Так как компании передают конфиденциальные сведения, используя внешние сети, встаёт вопрос защиты этих сведений. Провайдеры не торопятся предоставлять свои способы защиты – обычно это просто изолирование трафика. Этот способ не может обезопасить компании, например, от прослушивания в случае подключения к каналам связи посторонних лиц.

Также, с одной стороны, злоумышленники постоянно совершенствуют свои навыки, с другой – по сети передаётся всё большее количество конфиденциальных данных, возможная утечка которых приведёт к потерям компании, финансовым и репутационным.

Специалисты в области ИТ прикладывают множество усилий, чтобы поднять уровень безопасности в системах управления данными и дата-центрах. В самих приложениях и ОС уровень безопасности неуклонно растёт, однако сетевая безопасность по-прежнему оставляет желать лучшего.

Внедрение IPv6 происходит медленно – хотя эта версия протокола позволяет передавать криптографическую информацию в заголовке, его повсеместное использование ожидается нескоро. В настоящее время стандартом обмена данных является IPsec с IPv4.

Где проходит ваш кабель?

Сейчас злоумышленник может приобрести прибор, с помощью которого он может прослушивать оптоволоконный кабель без нарушения его целостности. Огромное количество данных может быть скомпрометировано за ничтожное количество времени. При этом специальные детекторы, предназначенные для обнаружения подключений, нечувствительны к таким подключениям. Разумеется, чтобы интерпретировать полученные данные, злоумышленнику потребуется определённая сноровка и опыт, однако принципиального препятствия для злоумышленника это не представляет.

Каким должно быть шифрование?

Кроме собственно шифрования с целью защиты данных может возникнуть требование соблюдения правил, определённых, например, на уровне закона. Используемые средства шифрования должны соответствовать этим требованиям, а также предоставлять широкие возможности аудита.

Продуктивность

Для шифрования необходима высокая производительность процессора, так как использование шифрования может сказаться на работе других приложений. Выбранный в организации вариант подключения к интернету может ещё больше сказаться на производительности. Так, при использовании туннелирования, для которого требуется большая пропускная способность, производительность может превосходить значение собственно шифрования.

Сеть с передачей аудио- и видеоданных

Организации нуждаются в шифровании, которое бы позволило работать с мультимедийными данными с минимальными потерями скорости.

Масштабируемость

Организации применяют сети в большинстве видов бизнеса – начиная с телефонных служб и заканчивая интернет-эквайрингом, поэтому необходимо обеспечить надёжное шифрование и безопасность таким образом, чтобы они не мешали стабильному соединению. Такие технологии как GRE/IPsec VPNs и IPsec VPNs нельзя назвать простыми в администрировании. Соответственно, при увеличении охвата сети организации сталкиваются с трудностями.

Гибкое планирование сети

Используемые механизмы шифрования не должны мешать сетевому подключению. Также, они должны быть совместимы с текущей и предполагаемой организацией сети. Это является основной причиной, по которой компании избегают негибких механизмов шифрования, препятствующих планированию сети. Всегда стоит выбор между комплексными механизмами шифрования, которые интегрируются в ИТ-инфраструктуру организации, и специфическими механизмами шифрования, способными обеспечить защиту на определённых участках.

Администрирование

Приоритетным выбором механизма шифрования должна быть простота администрирования и внятная ролевая модель, что избавило бы организацию от необходимости нанимать персонал с высоким уровнем технической компетенции. Внутренние средства шифрования должны управляться легко и быть понятны администраторам. Также, механизмы шифрования должны взаимодействовать с механизмами администрирования отказов.

Выбор типа сетевого шифрования

Распространены два типа наиболее популярных решений. В первом из них используется возможность шифрования в маршрутизаторах. Второй тип использует для целей шифрования специальные устройства, которые устанавливаются отдельно от остальных компонентов сети. Может показаться, что интегрированные механизмы шифрования предпочтительнее, однако это является заблуждением.

Организации предпочитают интегрированные механизмы шифрования, потому что на первых порах они дешевле – например, ввиду единого производителя. Кроме того, возможное снижение скорости доступа, а также совместимость с текущей организацией сети также входит в ряд особенностей, на которые админи-

страторы должны обратить внимание. Поэтом немало компаний предпочитают шифрование «на борту» маршрутизатора. Однако специализированные устройства для шифрования имеют ряд неоспоримых и часто недооценённых преимуществ.

Интегрированное шифрование может привести к ряду проблем, некоторые из которых мы рассмотрим ниже. После мы разберём второй тип шифрования, в котором используются специальные шифраторы канального уровня, после чего сравним два решения.

Для большого количества организаций стало настоящим сюрпризом узнать действительные затраты на шифрование внутри маршрутизаторов. Для средних пакетов, наиболее распространённых в сетях, в которых передаются данные мультимедиа, расходы IPsec достигают половины пропускной способности, что выливается в тесячедолларовые траты в месяц. Тогда как шифрование Ethernet обеспечивает хорошую пропускную способность, оптимизирует механизмы безопасности и упрощает администрирование, что позволяет снизить стоимость обслуживания.

Скоростное шифрование с Gemalto

Предлагаемое SafeNet решение позволяет зашифровать содержимое сетевого канала, основываясь на источнике и назначении MAC-адресов. Это позволяет, используя IPv4 или IPv6, прозрачно передавать данные с высокой скоростью. Механизмы шифрования Ethernet можно применять в различных сетевых средах организации. Так, организация может использовать их, чтобы обеспечить шифрование на высокой скорости внутри всего периметра этой организации, связывая в единую сеть дата-центры и офисы. Список применения высокоскоростного шифрования не исчерпывается вышеуказанным. Оно также используется для городских сетей, а также для сетей, в которых передаются данные мультимедиа. Шифрование находит применение и в процессе централизации серверов, включая сети хранения данных. Кроме того, эти механизмы шифрования могут использоваться, чтобы обезопасить сетевые магистрали.

Компания Gemalto может предложить улучшенные решения шифрования, позволяющие избежать различных трудностей, которые неизбежно возникают при использовании маршрутизаторов в качестве устройств шифрования. При этом качество шифрования не страдает.

Преимущества использования специализированных устройств шифрования:

- низкие финансовые расходы:
  - более широкий канал связи;
  - простота в обслуживании и администрировании;
  - самое дешёвое решение для агрегирования нескольких сайтов;
- высокая производительность:
  - снижение использования ресурсов;
  - снижение времени на передачу данных;
  - позволяет избавиться от общей инкапсуляции маршрутов (GRE) и запутанных схем качества обслуживания;
- масштабируемость в пределах организации:
  - качественное сетевое взаимодействие;
  - упрощение администрирования архитектурой до тысяч устройств;
  - прозрачность – поддерживаются протоколы IPv4, IPv6, а также устаревшие версии.

Шифровальные устройства SafeNet позволяют достичь максимальной пропускной способности, усилить защиту, упростить администрирование и снизить расходы. Устройства SafeNet High Speed Encryptors (SHSE) с наибольшей эффективностью и быстротой передают данные на канальном уровне, что само по себе снижает расходы на безопасность сети.

Устройства SHSE, которые выполнены в виде сетевого дополнения и управляются через единый централизованный центр управления, лучше всего подходят для создания масштабной архитектуры шифрования в сети. Они выполняют свою работу на скоростном канальном уровне и подходят для удалённого создания резервных копий, для сетей хранения данных, дата-центров, кроме того, они способствуют бесперебойность бизнес-процесса и позволяют легко восстановиться после сбоев.

Снижение расходов

В первую очередь снижение расходов происходит за счёт того, что шифровальные устройства канального уровня позволяют экономить средства на пропускную способность.

Сокращаются также траты на администрирование. Т. к. они работают на канальном уровне, устройства SHSE просты в установке и администрировании. Если сравнивать с шифрованием на сетевом уровне, SHSE-устройства управляются только частью переменных и настроек. Тогда как при использовании шифрования на сетевом уровне головной болью администраторов является поддержка VPN-политик, равно как туннелирвоание данных из точки в точку.

Главные возможности шифровальных устройств SafeNet:

- дуплексное шифрование Ethernet до 100 Гбит/с;
- соответствие FIPS 140 2, HATO, UC APL и соответствие требованиям CAPS;
- устройство готово к подключению к существующим сетевым средам;
- низкие задержки;
- стандартная проверка подлинности, электронные сертификаты и администрирование криптографическими ключами;
- централизованная настройка, слежение и администрирование;
- низкие расходы на управление и низкая стоимость обладания.

К примеру, при добавлении всякого нового устройства в сеть с ячеистой структурой каждое соединение нужно сконфигурировать в таблицах маршрутизации. Тогда как если изменение произойдёт в структуре, где используется безопасность канального уровня, нужно будет только добавить цифровой сертификат, который позволит остальным устройствам обмениваться сообщениями с только что добавленным. Так что в список преимуществ входит простота развёртывания, администрирование и снижение общей цены владения.

Для администрирования устройств SHSE используется Win32-приложение. Это приложение позволяет изменять политики управления SHSE-устройств, а также позволяет осуществлять проверку и слежку за устройствами, что необходимо для обеспечения ИБ.

Администраторы могут в удалённом режиме конфигурировать выполнять мониторинг и обновление устройств SafeNet. Им также предоставлена возможность задавать настройки безопасности, которые можно применить к нескольким шифраторам, что снижает затраты на администрирование.

Соответствие требованиям

Проверка устройств SHSE на соответствие требует меньше усилий, чем использовании шифрования на сетевом уровне. В распоряжении администратора централизованный архив логов, упрощающий проведение отчётности по соответствию регулятивных требований. Шифровальные устройства SafeNet прошли сертификацию FIPS и соответствуют 140-2 уровня 3, что позволяет соблюсти большое количество государственных требований и требований бизнеса. Некоторые из предлагаемых Gemalto шифров прошли сертификацию NATO, UC APL и CAPs (UK), Common Criteria, а также FIPS 140-2 L3. Также, компания Gemalto является поставщиком услуг безопасности, обслуживающим нужды правительственных и коммерческих сетей. Более 80 % переводов между банками производится на шифровальных устройствах компании SafeNet, которая была приобретена Gemalto.

Рост производительности

Шифровальные устройства SafeNet производят шифрование всего IP-пакета, при этом дополнительный IP-заголовок шифруется отдельно. Это значит, что когда фрагмент данных канального уровня путешествует по промежуточным сетям, MAC-адрес исходного фрагмента данных остаётся неизменным. Так как маршрутизаторы, которые работают на сетевом уровне, меняют MAC-адрес, фрагмент данных, подвергшийся шифрованию, неспособен пройти через маршрутизатор до расшифрования.

Шифровальные устройства SafeNet прекрасно подходят для соединений WAN ввиду меньшей сложности и большей эффективности. После того как данные подверглись шифрованию на канальном уровне, скоростной фрагмент данных а также все проходящие через сеть данные уже зашифрованы. Также, после замены IPsec-шифрования на шифрование с помощью устройств SafeNet существенно (почти в два раза) увеличивается пропускная способность, а задержка через IPsec-соединение, в свою очередь, сокращается в более чем 10 раз. Это гораздо лучше, чем покупать или брать в аренду дорогой канал с большими расходами.

Архитектура

Ввиду несложной реализации, устройства SHSE позволяют осуществлять гибкие подходы к развёртыванию. Это позволяет выполнить развёртывание сети с ячеистой структурой с наименьшими затратами.

Доступная совместимость

Если устанавливать устройство SHSE в качестве дополнительного устройства, то это не сказывается на инфраструктуре. Поэтому системы в рамках сети работают, как прежде. Компании получают гибкость в администрировании и большую отдачу от сделанных вложений, а также позволяют эффективно планировать дальнейшее развитие инфраструктуры.

Ниже представлен список сетей, с которыми могут работать шифровальные устройства SafeNet.

- VLAN, QinQ;
- Jumbo Frames;
- Carrier High Speed (E-Line/E-LAN);
- High Speed II, IEEE 802.3;
- High Speed over OTN (G.709);
- High Speed over MPLS;
- DWDM/Dark Fibre.

Влияние шифрования на сетевом уровне на пропускную способность

Исследование Рочестерского технологического института показало, что выгоды дорогих скоростных сетей могут быть значительно снижены за счёт потери пропускной способности. Результаты исследования говорят о том, что шифрование с помощью шифровальных устройств SafeNet на канальном уровне гарантируют отличную пропускную способность и существенно снижают задержку по сравнению с операциями IPsec VPN сетевом уровне. Взглянем подробнее на некоторые различия.

IP-заголовок

В транспортном режиме IPsec содержит меньшее количество служебной информации, но не гарантирует конфиденциальность для IP-заголовка сетевого уровня. Это значит, что конфиденциальные сведения об адресе внутренней сети могут быть злонамеренно получены путём обзора общей сети.

Туннельный режим IPsec позволяет закрыть эту брешь, ведь IP-пакет шифруется и включается в состав другого пакета. Этот другой IP-пакет имеет только адреса шифровальных устройств в конечных точках, но не адреса хостов.

Несмотря на то, что режим туннелирования ликвидирует брешь безопасности транспортного режима IPsec, вместе с тем он добавляет существенное количество служебной информации. Обработка IP-заголовка сказывается на производительности, увеличивая задержки.

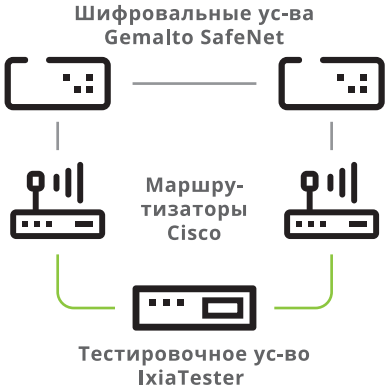
Шифровальные устройства SHSE позволяют избежать проблем, которые появляются в режиме туннелирования IPsec, т. к. они находятся «с краю» сети и обеспечивают шифрование всего IP-пакета целиком, при этом не добавляют служебную информацию дополнительного IP-заголовка.

Тестирование решений

Рочестерский технологический институт в своих тестах использовал следующие устройства:

- две сетевых карты Cisco Gigabit Ethernet (эти карты были установлены в двух шасси Cisco Catalyst 6509 высокой производительности);
- два модуля Cisco Services IPsec VPN Services;
- два выделенных устройства шифрования SafeNet канального уровня;
- тестовая платформа Ixia 250.

Всё это было соединено простой сетью.



При тестировании установили базовую инфраструктуру, позволяющую учитывать сужение полосы

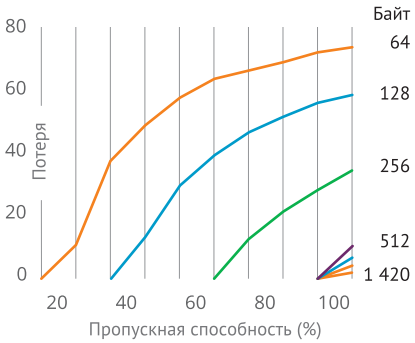
пропускания за счёт служебной информации протокола Ethernet. После в измерения были включены потери фрагментов данных, задержку и пропускную способность зашифрованной и незашифрованной информации для различных размеров фрагментов данных.

Потери фрагментов данных

Потеря фрагментов данных представляет собой различие между числом фрагментов, которое передаётся одним интерфейсом, и числом фрагментов, полученных другим интерфейсом. Тесты, которые производил Рочестерский технологический институт, выявляли наибольшую скорость работы устройств без потери фрагментов данных.

Шифратор SHSE показал потери менее 1/1000-го из 1 % потерь фрагментов данных для всякого заданного размера фрагмента данных. Этот показатель незначителен с точки зрения статистики и фактически означает, что средняя потеря фрагмента данных равна 0 для 100 % скорости канала.

Если сравнить с решением IPsec, то потери последнего существенны для всех размеров фрагментов данных. Если увеличивать нагрузку, потеря фрагментов данных была также зарегистрирована. При уменьшении фрагментов данных наблюдалась логарифмическое увеличение потери фрагментов. При фрагменте в 64 байта больше 40 % потерь фрагментов зарегистрировано при 30 % наибольшей в теории пропускной способности.



Это существенно ограничивает возможную полосу пропускания в условиях шифрования IPsec.

Доступная пропускная способность

Обычный фрагмент данных Ethernet может передавать полезную нагрузку в 1500 байт. Ethernet содержит преамбулу размером 8 байт в начале фрагмента и разрыв между фрагментами 12 байт – всё это снижает общую пропускную способность.

В ходе тестов было установлено, что скоростные устройства шифрования SafeNet не сказываются на пропускной способности в каком бы то ни было направлении, невзирая на размер фрагмента данных. При этом пропускная способность держится на уровне 100 % от наибольшей возможной.

IPsec-шифрование использует дополнительно 57 байт служебной информации, включённой в IP-заголовок пакета. Таким образом, при небольших размерах фрагмента данных (кадра/фрейма) дополнительные 57 байт существенно влияют на пропускную способность.

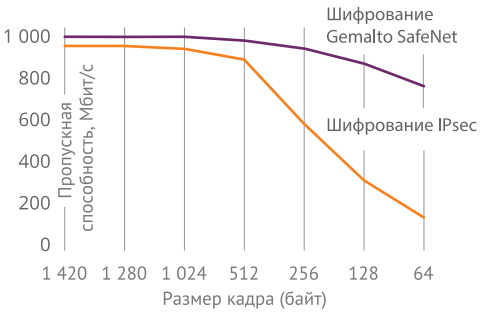
IPsec-шифрование не позволяет использовать наибольшую теоретическую пропускную способность при маленьких размерах фрагментов данных. Размеры от 512 до 1280 байт позволяли достичь примерно 100 % наибольшей теоретической пропускной способности. Однако, если фрагменты данных были размером 256 байт, производительность составляла только 73 % и далее только снижалась, составив только 27 % при фрагменте данных в 64 байта.

Задержка

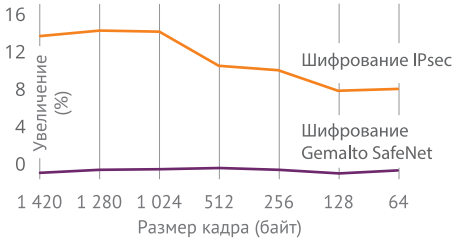
В тестах Рочестерского технологического института замерялось время, которое необходимо, чтобы первый бит фрагмента данных прошёл тестовую сеть от точки передачи к точке прибытия. Результаты сравнивались в виде процентного увеличения задержки, если сравнивать с задержкой, которая происходит без шифрования.

Есть ожидание, что каждое новое устройство в сети увеличивает задержку. Средняя задержка для данных, отправленных через тестовую сеть, разнилась от 1,2 мс для фрагментов в 64 байта до 1,3 мс для фрагментов размером 1420 байт. Использование устройств шифрования SafeNet увеличило показатель задержки менее чем на 1 %.

Усреднённые показания шифрования IPsec говорят о задержке, в 13 раз превышающей задержку, которая возникала при использовании скоростных устройств шифрования SafeNet.



Сравнение пропускной способности при шифровании данных



Сравнение задержек при шифровании с IPsec и с помощью SafeNet

Итоги

В теории производительность шифрования на канальном уровне превосходит производительность шифрования сетевого уровня. Проведённые тесты подтверждают теорию, т. к. при шифровании на сетевом уровне задержки вызваны добавлением служебной информации к фрагменту данных.

Устройства шифрования SafeNet, в отличие от ситуации с IPsec-шифрованием, работают на линейной скорости и почти не провоцируют задержки, оставляя полосу пропускания насколько возможно широкой.

При тестировании также не было замечено существенных потерь фрагментов данных при шифровании с помощью шифраторов SafeNet, а вот при использовании IPsec-шифрования потеря фрагментов и снижение скорости передачи были существенными.

Также, зафиксированная латентность Cisco IPsec в условиях шифрования превысила латентность устройств шифрования SafeNet в 13 раз. В архитектурах, где Ethernet-шифрование подходит для нужд компании, его производительность смотрится намного более выгодно на фоне IPsec-шифрования.

TESSIS

TESSIS *– официальный дистрибьютор Gemalto в России.*

www.tessis.ru

БДУ ФСТЭК – практическое использование

В рамках статьи рассмотрены основные возможности, которые специалистам по защите информации предоставляет Банк данных угроз (БДУ) ФСТЭК России, а также проведено экспресс-сравнение с альтернативными источниками информации по уязвимостям и угрозам.

Банк данных угроз безопасности информации (БДУ – www.bdu.fstec.ru), запущенный в 2015 году ФСТЭК России (Федеральная служба по техническому и экспортному контролю) и ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (Государственный научно-исследовательский испытательный институт проблем технической защиты информации), на сегодняшний день насчитывает **205** угроз и **17 391** уязвимость.

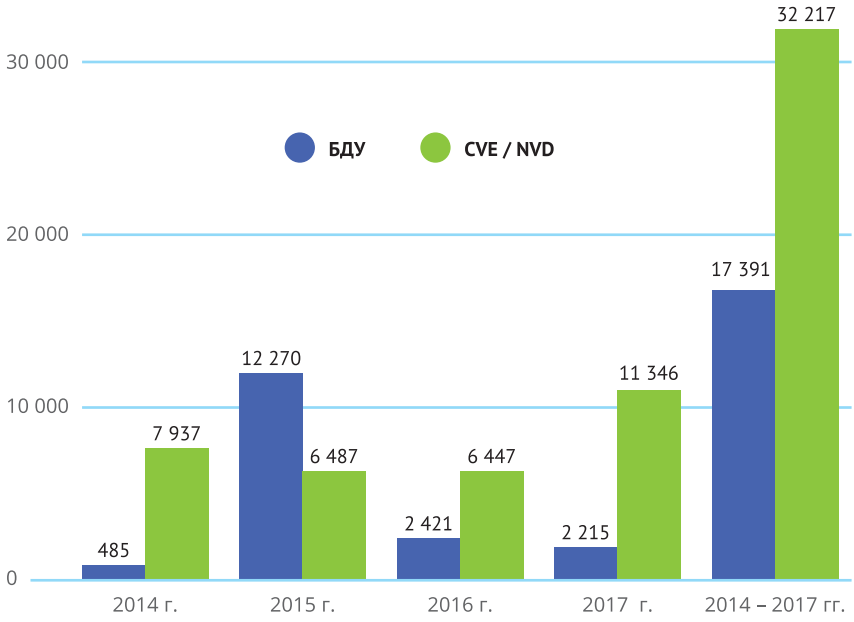
База уязвимостей и База угроз – это далеко не все возможности, которые предоставляет БДУ, однако это именно те разделы сайта, которые на практике, пожалуй, используются чаще всего.

База уязвимостей

ФСТЭК, как уже отмечалось выше, начала вести свою базу уязвимостей в 2015 году, когда в мире существовало уже более 60 различных баз схожей направленности.

Самой обширной и содержательной на тот момент была открытая независимая база Open Source Vulnerability Database (OSVDB). OSVDB насчитывала более 120 000 уязвимостей, однако 5 апреля 2016 года её деятельность была прекращена, по мнению многих – не в последнюю очередь из-за роста популярности программ Bug Bounty, позволяющих исследователям заработать деньги с помощью продажи найденных ими уязвимостей. Бесплатная публичная база уязвимостей, по всей видимости, не оправдала себя во всё более коммерциализируемом мире.

Из других крупных баз уязвимостей можно отметить популярную Common Vulnerabilities and Exposures (CVE), поддерживаемую The MITRE Corporation и являющуюся основой для американской национальной базы U.S. National Vulnerability Database (NVD). Также стоит упомянуть базы X-Force компании IBM и SecurityFocus компании Symantec, китайскую China National Vulnerability Database of Information Security (CNNVD) и японскую Japan Vulnerability Notes (JVN iPedia).



Сравнение динамики добавления новых уязвимостей в базы БДУ и CVE / NVD за последние 4 года.

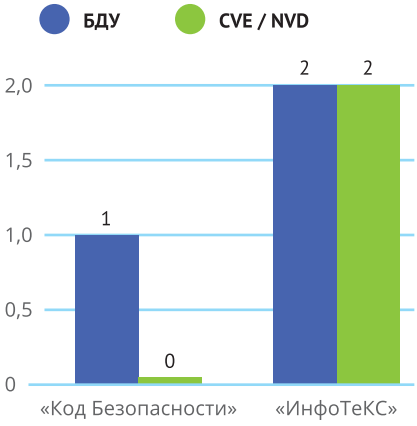
Все упомянутые и государственные, и принадлежащие частным корпорациям базы существенно превышают БДУ ФСТЭК как по количеству уязвимостей, так и по скорости обновления.

Говоря о базах уязвимостей, нельзя не упомянуть российский проект Vulners, также стартовавший в 2015 году и стремительно набирающий популярность. В некоторых источниках его называют «Google для хакера», так как Vulners автоматически собирает информацию из популярных баз уязвимостей, бюллетеней безопасности, тематических ресурсов и других источников, а также позволяет искать по ним. Из-за многообразия источников и видов представленной информации общее число записей, выдаваемых при поиске, на сегодня превышает 600 000 штук. Среди плюсов Vulners – открытый программный интерфейс (API), встроенный расширенный язык поисковых запросов и даже собственный Telegram-бот @vulnersBot.

На таком общем фоне БДУ ФСТЭК выглядит далеко не всеобъемлюще и отчасти несовременно, однако у данного источника есть два неоспоримых преимущества.

Во-первых, БДУ ФСТЭК – самая крупная база уязвимостей на русском языке. Понятные описания и понятный интерфейс дорогого стоят – на одном из мероприятий по информационной безопасности наполовину в шутку, а наполовину всерьёз из зала прозвучала фраза: «Уязвимости, опубликованные в базе ФСТЭК, для нас весомее, чем такие же, но в западных источниках».

Второй плюс БДУ ФСТЭК – ориентация в том числе на уязвимости в отечественном программном обеспечении. Уже сейчас представлены около 80 уязвимостей 11 отечественных производителей, таких как НПП «РЕЛЭКС», «Лаборатория Касперского», «ОВЕН», «1С», «1С-Битрикс» и других. Важным следствием из такой ориентации является наличие уникальных уязвимостей, которые в других базах могут быть не представлены.



Для наглядной иллюстрации были изучены уязвимости отечественных производителей средств защиты информации «ИнфоТеКС» и «Код Безопасности». Обе известные уязвимости в решениях «ИнфоТеКС» представлены и в базе CVE/NVD. Однако важная уязвимость в продукте Secret Net компании «Код Безопасности» в ней отсутствует до сих пор.

Среди других доступных для выбора, но пока не имеющих опубликованных уязвимостей на сайте БДУ ФСТЭК значатся также отечественные производители «НПО РусБИТех», «ТЕКОНГРУП», «АСКОН», «Интеллектуальные Системы Автоматизации Технологии», «Нанософт», «Новые электронные технологии», «НТЦ ИТ РОСА» и другие.

В своих публичных выступлениях сотрудники ФСТЭК заявляли, что публикуют уязвимости только после выпуска производителями соответствующих обновлений. Возможно, наличие указанных выше производителей среди доступных для выбора как раз говорит о том, что в их продуктах есть известные уязвимости, исправление которых ФСТЭК ожидает для их публикации в БДУ.

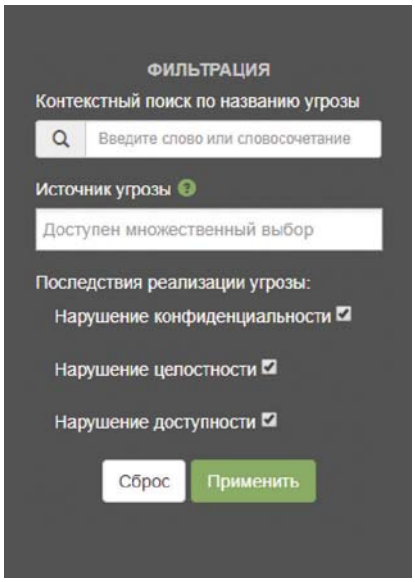
База угроз

Второй важный компонент БДУ ФСТЭК – это каталог уязвимостей. Из широко известных аналогов можно назвать разве что каталог угроз Федерального ведомства по информационной безопасности Германии: BSI IT-Grundschutz-Kataloge. Данный каталог обновляется раз в год или два, последнее обновление (версия 15) было в мае 2016 года, тогда же было заявлено, что форма подачи материала (сейчас это единый PDF-файл с 5000 страницами) будет изменена для упрощения её практического использования. Текущая версия IT-Grundschutz-Kataloge доступна на немецком и английском (черновик) языках и, помимо описания угроз, содержит общие рекомендации по нивелированию угроз (в том числе физическими, организационными и техническими мерами). Каталог отлично структурирован, имеет сквозную нотацию, а общее число описанных угроз превышает 700.

Как указано в описании БДУ ФСТЭК: *«Угрозы безопасности информации, включённые в состав банка данных угроз, не являются элементами иерархической классификационной системы угроз, а представляют собой обобщённый перечень основных угроз безопасности информации, потенциально опасных для информационных систем»*.

Каталог угроз в БДУ ФСТЭК пока позволяет искать только по названию угрозы и применять фильтры по источнику угрозы и последствиям

реализации угрозы (нарушение конфиденциальности, целостности и/или доступности).



Окно фильтрации на сайте БДУ

Равно как и для Базы уязвимостей, важнейшим преимуществом Базы угроз от ФСТЭК является детальное описание угроз на русском языке. С другой стороны, порой это описание избыточно и затрудняет, наравне с уже упомянутым отсутствием структурированности, практическое использование, так как, по сути, для каждой из 205 угроз нужно провести анализ и обосновать её актуальность либо неактуальность для конкретной информационной системы.

Так как все угрозы с их описанием и другими имеющимися полями можно просто выгрузить в виде табличного документа (для уязвимостей можно сделать то же самое), на практике работа с БДУ существенно упрощается ручным укрупнением разделов Базы угроз путём объединения схожих угроз в группы, что позволяет исключать из рассмотрения, например, все угрозы, связанные с технологиями виртуализации, если в рассматриваемой информационной системе они не применяются. Такую «доработку» БДУ обычно достаточно сделать один раз, после чего применять в своей повседневной работе, время от времени дополняя структуру новыми угрозами, публикуемыми ФСТЭК.

Дополнительные разделы и возможности

Помимо важных и полезных Базы уязвимостей и Базы угроз, сайт БДУ ФСТЭК предлагает дополнительные инструменты, которым также можно найти применение в типовой деятельности специалиста по информационной безопасности. Впрочем, справедливости ради, стоит отметить, что большинство дополнительных разделов пока скорее ближе к прототипам, чем к полноценным инструментам.

Термины и определения

Данный раздел задуман как глоссарий с официальными (выбранными из различных стандартов) определениями основных терминов и ссылкой на источник. К сожалению, раздел пока так и остался в зачаточном состоянии – 66 определений (не для всех из которых, к слову, указан источник) вряд ли можно считать хорошим подспорьем. Документация среднего размера проекта может содержать больше терминов.

Документы

Опять-таки, просто отличная задумка – собрать в одном месте (да ещё и систематизировать) всю требуемую в работе специалиста по защите информации документацию (ГОСТы, приказы, методические рекомендации и проч.), но текущая реализация снова оставляет желать лучшего: 9 документов, с поиском которых и так особых проблем не возникает. Да и выложены не сами документы, а ссылки на них. Похоже, корректнее раздел было бы назвать «Ссылки на документы».

Калькуляторы CVSS

Интерактивные калькуляторы, позволяющие, не покидая сайт ФСТЭК, быстро получить оценку CVSS – вещь удобная. Впрочем, существенным образом скопированная с калькулятора на сайте NIST идея уступает в реализации: у NIST гораздо информативнее, но зато только на английском языке.

Инфографика

Отличный раздел, который позволяет в красивом графическом представлении посмотреть топ-10 производителей, в программном обеспечении (ПО) которых обнаружено максимум уязвимостей (на первых трёх местах: свободное ПО, Red Hat, Inc. и Adobe Systems Incorporated), такой же топ-10, но уже по числу критических уязвимостей (в лидерах – та же тройка, только чуть в другом порядке) и, наконец, распределение уязвимостей по типам ошибок, уровням опасности и типам ПО.

Участники и Обратная связь

Задуманная как доска почёта таблица с информацией о частных исследователях, сообщивших об уязвимостях, содержит информацию о 17 переданных через форму обратной связи уязвимостях от 7 человек. Подраздел «Организации» заполнен логотипами тех, кто помогает ФСТЭК в наполнении базы. Опыт работы с формой обратной связи показывает, что она действующая и запросы – по крайней мере, о выявленной уязвимости – обрабатываются оперативно.

Обновления

Чтобы завершить с второстепенными разделами, стоит отметить возможность получения информации об обновлениях: непосредственно на сайте (в разделе «Новости»), через подписку на RSS-ленту и, наконец, через официальный аккаунт в «Твиттере» – @gniiiptzi

Заключение

В качестве основного пожелания дальнейшего развития Банка данных угроз к уже высказанному, пожалуй, можно было бы добавить предложение разработать соответствующие методики по работе с БДУ и, прежде всего, методику по работе с Базой угроз.

Вместе с тем, несмотря на имеющиеся недостатки, Банк данных угроз от ФСТЭК и ГНИИИ ПТЗИ является лучшим на сегодняшний день отечественным русифицированным инструментом для работы специалиста по защите информации с перечнями угроз и уязвимостей. Пусть пока не все задачи можно решить исключительно с помощью реализованных механизмов, БДУ развивается как в плане полноты охвата, так и по числу предоставляемых возможностей.

Алексей Комаров
автор блога по информационной безопасности www.zlonov.ru

Новый стандарт ИТ-безопасности: как соответствовать?

В данной статье мы рассмотрим изменения, касающиеся только усиления функции аутентификации, и возможные способы решения задач, связанные с проверкой подлинности идентификатора для соответствия стандарту PCI DSS.

Стандарт безопасности данных индустрии платёжных карт PCI DSS, разработанный Советом по стандартам безопасности индустрии платёжных карт, не стоит на месте и продолжает развиваться, адаптируясь к новым технологиям и тенденциям в сфере информационной безопасности.

Так, новая версия стандарта повлекла за собой не только изменения в терминологии, но и усиления требований в ряде механизмов защиты. Срок действия стандарта PCI DSS 3.1 истекает 31 октября 2017 года, а новые нормативные требования, определённые в спецификации PCI DSS 3.2, вступают в силу с 1 февраля 2018 года.

Новые требования

Изначально требования по усилению к механизмам аутентификации (использование двухфакторной аутентификации) предъявлялись только при организации удалённого доступа из-за периметра сети для пользователей и администраторов, а также представителей сторонних компаний, осуществляющих поддержку. Теперь требуется использовать многофакторную аутентификацию для администраторов при выполнении неконсольного доступа, а также при любом удалённом доступе к среде данных о держателях карт.

Под многофакторной аутентификацией в документе понимается выполнение минимум двух из трёх факторов аутентификации:

1. фактор знания (например, пароль или парольная фраза);

2. фактор владения (например, токен или смарт-карта);

3. фактор свойства (например, биометрические данные).

Некоторые специалисты ошибочно игнорируют важное обстоятельство, указанное в документе – использование одного фактора дважды (например, два отдельных пароля) не попадает под понятие многофакторной аутентификации. Поэтому можно утверждать, что классическая модель двухфакторной аутентификации (фактор знания и фактор наличия) полностью удовлетворяет требованию стандарта. Интересно отметить также следующие допущения в стандарте.

- В России принято разделять механизмы аутентификации по классам: базовая аутентификация (парольная), усиленная (с использованием одноразовых паролей), строгая (на основе инфраструктуры открытых ключей).

В западной литературе усиленная и строгая аутентификация попадают в одну группу – строгая аутентификация (двухфакторная аутентификация, которая требует выполнения минимум двух факторов списка факторов аутентификации, представленного выше). Следовательно, и стандарт PCI DSS не разделяет данные понятия.

- Если среда не подвержена сегментации путём выделения подсети, содержащей среду данных о держателях карт, то администратор вправе использовать механизм многофакторной аутентификации либо при входе в сеть со средой держателей карт, либо при входе в систему. Если же среда сегментирована, то многофакторная аутентификация требуется при доступе извне в среду данных о держателях карт.
- Многофакторная аутентификация может осуществляться на уровне сети, системы/приложений.

Все эти дополнения к механизмам аутентификации в части организации неконсольного (или удалённого) входа для администраторов обусловлены перенаправлением активности подразделения информационной безопасности на усиление аутентификации рядового удалённого пользователя. При этом не рассматриваются потенциальные риски при аутентификации пользователей с высоким уровнем привилегий, даже в условиях контролируемого периметра.

Способы решения

Исходя из требований стандарта и допущений, можно определить два пути решения задачи.

Первый из них – использование двухфакторной аутентификации на основе инфраструктуры открытых ключей (инфраструктуры PKI). При условии применения данного подхода требуется развернуть внутри компании удостоверяющий центр, приложение для управления жизненным циклом ключей и смарт-карт и, в завершение, убедиться в возможности интеграции механизма аутентификации по сертификатам в требуемом сервисе.

Первые два пункта мы опустим, так как хотя они и представляют некоторые сложности, но решаемы. А вот вопрос с интеграцией стоит достаточно остро. Скорее всего, интеграция электронных ключей будет осуществляться через протокол PKCS11 (если она вообще реализуема), который хоть и реализован во многих системах, но требует ювелирного совпадения версий библиотек и окружения. С этим часто приходится сталкиваться при организации двухфакторной аутентификации при входе в операционную систему. Для платформы Microsoft выглядит всё гладко, но как только возникает потребность в организации аутентификации в системах Linux/UNIX/BSD , вот тут начинается.

Дальше встаёт вопрос о возможности использования токенов и смарт-карт на рабочем устройстве – не каждое устройство оборудовано считывателем смарт-карт или имеет USB-разъём, к которому может быть подключён токен. Да и с точки зрения безопасности – невозможность использования USB-разъёма снимает вопрос о несанкционированном копировании на внешние устройства. Как результат, строгая аутентификация остаётся строгой, но накладывает ряд ограничений, которые не всегда могут быть применимы в компании.

Второй вариант решения вопроса – это применение бесконтактных аутентификаторов, работающих на основе одноразовых паролей.

Принцип интеграции бесконтактных аутентификаторов в 90 % случаев не привязан к среде, а опирается на стандартные протоколы, такие как RADIUS и SAML 2.0. В этом случае сервис выступает в роли некоего фронтенда, за которым скрыт механизм аутентификации на основе стандартного протокола. Некритично, если требуется интегрировать двухфакторную аутентификацию в продукт собственной разработки. Несколько строк кода позволяют внедрить в сервис RADIUS-клиент (на сегодня в сети доступна реализация RADIUS на клиента на всех популярных языках программирования), который, в свою очередь, предоставит пользователям аутентификацию с использованием одноразовых паролей.

Оптимальное решение

Задача поставлена, выбор сделан – сервер аутентификации на основе одноразовых паролей. Но что и как стоит выбирать?

В качестве объекта исследований мы возьмём решение от компании Gemalto – SafeNet Authentication Service (далее по тексту – SAS). Сразу бросается в глаза особенность в названии продукта – не Server, а Service. И это действительно так – решение представлено на рынке в 2 вариантах исполнения. Первый – сервер аутентификации, который разворачивается внутри компании, второй – сервер аутентификации, который предоставляется поставщиком услуг из своего дата-центра.

Рассмотрим параметры, которые выделяют решение Gemalto на фоне конкурентов.

Любое решение по безопасности вносит изменения в привычное функционирование системы для пользователя. И нередко приходится слышать от клиентов, что сервисом становится просто невозможно пользоваться из-за неудобств, с которыми сталкивается клиент. В части аутентификации, с чем приходится иметь дело – это разного рода аутентификаторы (генераторы одноразовых паролей). В продуктовой линейке аутентификаторов можно подобрать генератор, который оптимально подойдёт для использования, исходя из угроз безопасности, удобства эксплуатации и

цены. Так, аппаратные генераторы по-прежнему остаются наиболее востребованными для защиты критически важных объектов инфраструктуры (обусловлено это тем, что генерация значения пароля происходит изолированно от среды функционирования самого сервиса). Помимо этого, всегда можно подобрать оптимальный форм-фактор для аутентификатора – начиная от брелока с PIN-кодом для защиты устройства и заканчивая генератором в виде смарт-карты.

Большую популярность стали приобретать программные генераторы одноразовых паролей, которые могут быть установлены на мобильный телефон, тем самым превратив его в аутентификатор. Развитие таких токенов также обусловлено и развитием мобильных технологий в целом. Так, например, в линейке программных аутентификаторов Gemalto представляет приложение MobilePass+, которое поддерживает технологию PUSH OTP (на сегодняшний день данная технология поддерживается только в «облачной» версии SAS). Данная технология состоит в том, что после ввода идентификатора в сервисе, куда необходимо получить доступ, на мобильный телефон приходит PUSH-уведомление. Пользователю необходимо разблокировать мобильное приложение MobilePass+ (используя PIN-код или биометрию) и выбрать одну из кнопок: «DENY» или «APPROVE». При нажатии кнопки «APPROVE» приложение само передаст значение одноразового пароля, не требуя дополнительных действий со стороны пользователя.

Интересным решением также является применение графического аутентификатора. Он представляет собой матрицу повторяющихся цифр, в которой пользователь знает определённую им траекторию. На основании данной траектории пользователь сам составляет значение одноразового пароля. Каждый раз значения цифр в матрице новые, что позволяет избежать формирования одинакового пароля.

В завершение списка линейки аутентификаторов стоит отметить, что решение поддерживает также доставку одноразовых паролей в виде SMS или на электронную почту.

Ожидаем от читателя вопрос: одноразовые пароли хотя и представляют собой динамические значения, но где же та самая двухфакторная аутентификация? Аутентификатор обеспечивает только то, «что я имею», а где то, что «я знаю»? Решение SAS позволяет для каждого аутентификатора задать свой PIN-код. PIN-код может быть как для защиты самого аутентификатора (например, для формирования значения пароля или разблокировки приложения пользователь должен ввести PIN-код), так и дописываться к значению одноразового пароля при вводе его на сервисе, то есть динамический пароль будет иметь вид «PIN-код + значение одноразового пароля». Данная комбинация позволяет использовать решение SAS как полноценный сервер двухфакторной аутентификации.

Для снижения нагрузки на отдел технической поддержки и ускорения решения вопросов, связанных с аутентификаторами пользователей, решение SAS предоставляет портал самообслуживания. На данном портале пользователь может самостоятельно, без привлечения сил IT-специалистов, решить такие задачи, как запрос на аутентификатор, синхронизация аутентификатора в случае рассинхронизации токена, изменение значения PIN-кода, изменение траектории для графического аутентификатора, изменение личных параметров пользователя. Дополнительно, портал может быть кастомизирован (сохраняется только нужная для пользователя функциональность), брендирован (на портале используется логотип, стиль и цвета, принятые в компании), локализован (все записи переводятся на русский язык и переименовываются для облегчённой работы пользователя с порталом).

YouTube

SAS PUSH OTP – генератор одноразовых паролей (видеоролик)

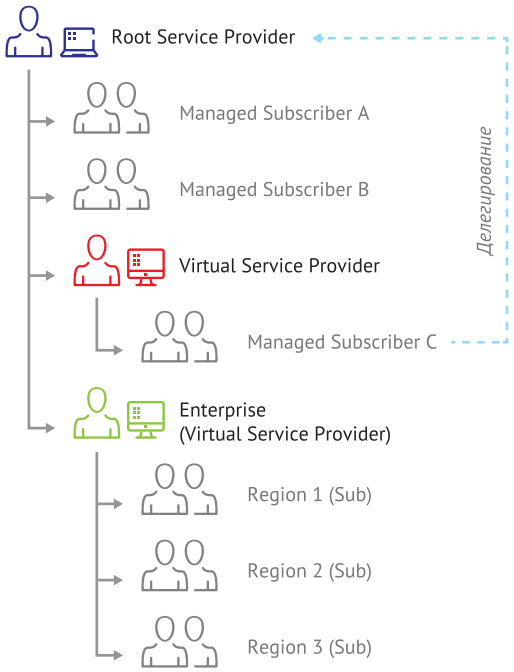
Аутентификаторы Gemalto

Отдельно стоит отметить процедуру назначения аутентификаторов пользователям. Процедура не сложнее регистрации в социальных сетях. Администратор SAS или же сама система SAS в случае выполнения правил автоматического назначения аутентификатора отправляет пользователю почтовое сообщение со ссылкой на активацию токена. Пользователю необходимо перейти по ссылке и в случае аппаратного токена – ввести его серийный номер и значение одноразового пароля для синхронизации с сервером, в случае с графическим токеном – задать траекторию, а во всех остальных случаях система всё сделает сама. С учётом времени развёртывания сервера SAS и данной процедуры активации аутентификаторов настройка механизма двухфакторной аутентификации для 20 000 пользователей займёт не более 15 минут.

Особенности сервера

Сервер SAS представляет собой веб-приложение и набор сервисов, функционирующих на платформе Microsoft Windows. Решение легко масштабируемо за счёт простой интеграции отдельных экземпляров SAS в кластер, что позволяет выполнять балансировку нагрузки при большом количестве пользователей системы. Исключительной особенностью решения является то, что оно поддерживает архитектуру Multi-Tier Multi-Tenant – когда на одном экземпляре сервера аутентификации можно развернуть древовидную структуру из нескольких дочерних серверов аутентификации с возможностью наследования определённых параметров (например, настройка почты или SMS-шлюза), но позволив при этом серверу существовать автономно – использовать собственного администратора сервера аутентификации, выполнять синхронизацию пользователей из различных источников, таких как Active Directory, LDAP, таблицы баз данных, а также задавать собственные политики безопасности. Такая архитектура позволяет сделать SAS единой точкой аутентификации пользователя для предприятий различных размеров.

Для любой системы аутентификации очень остро стоит вопрос интеграции с внешними сервисами. Можно говорить, что в 90 % случаев SAS интегрируется «из коробки». SAS использует готовые агенты для платформы Microsoft Windows. В список сервисов входят агенты для входа на рабочие станции и серверы (с возможностью работы в автономном режиме без доступа к серверу SAS), Microsoft IIS, Microsoft OWA, Microsoft SharePoint, Microsoft RDP, Microsoft RDWeb Gateway, Microsoft ADFS. Если агенты неприменимы, интеграция с сервисами может быть выполнена через протоколы RADIUS и SAML, которые уже реализованы в решениях, где требуется двухфакторная аутентификация, либо может быть добавлена их поддержка в решения собственной разработки.



Архитектура Multi-Tier Multi-Tenant

Любое решение, связанное с безопасностью, должно предоставлять механизмы аудита. В этом направлении SAS также предоставляет широкую функциональность, которая реализуется двумя способами. Первый из них состоит в возможности формирования по запросу или по расписанию отчётов на основе существующих шаблонов (на текущий момент существует порядка 50 шаблонов) с возможностью их просмотра непосредственно в самой системе или отправки на почту. Второй способ состоит в отправке записей аудита во внешние системы, к которым относятся: файловое хранилище, Microsoft Event Viewer, syslog (включая интеграцию с SIEM-системами).

Что в итоге

Представленные выше функции решения SAS позволят легко и быстро внедрить двухфакторную аутентификацию как для рядовых пользователей, так и для администраторов систем. Использование одноразового пароля позволит упростить процедуру аутентификации, снизив риски, которые были при использовании статического пароля. При необходимости, список сервисов, которые будут требовать использование одноразовых паролей, можно расширить за счёт использования стандартных протоколов аутентификации RADIUS и SAML. Автоматизация и механизмы аудита позволят бесшовно внедрить усиленную аутентификацию, обеспечив тем самым как усиление системы безопасности, так и соответствие новым требованиям стандарта PCI DSS.

ThinPrint®

SIMPLY BETTER PRINTING

Ведущее решение печати для бизнеса!

- Создание отказоустойчивой системы печати
- Печать без драйверов (Driver Free Printing)
- Контроль полосы пропускания, пакетная передача данных
- Высокий уровень сжатия данных, отправленных на печать
- Автоматический маппинг принтеров для пользователей виртуализации
- Контроль расходов на печать подразделений или пользователей
- Сохранение электронных копий распечатанных документов

ОЛЛИ ДИСТРИБУЦИЯ

+7 (812) 703-30-69 +7 (495) 139-89-60 disti@ollyit.ru www.ollyit.ru

Тестируйте 30 дней бесплатно!

Антивирус Grizzly Pro – пока другие думают, мы действуем!

Инновационная антивирусная разработка всестороннего действия. Её защита основана на обнаружении всех видов вирусных угроз.

Технологии быстро развиваются и всё больше влияют на жизнь людей, а значит, киберугрозы становятся проблемой мирового масштаба. И поскольку ИТ-индустрия приобретает особую важность во всём мире, экспертный опыт и знания в сфере ИТ-безопасности становятся вдвойне необходимыми.

Grizzly Pro знает всё о киберугрозах, а наши эксперты обладают глубокими знаниями и опытом в обнаружении и нейтрализации всех видов вредоносных программ. Свою квалификацию мы наработали за годы борьбы с крупнейшими ИТ-угрозами, и это наш самый ценный актив.

Новый игрок на поле боя

Среди множества антивирусных программ выделяется одна новая, современная разработка от компании Grizzly Pro. Grizzly Pro разрабатывает защитные компоненты с 2012 года, и сейчас на рынке представлены решения антивирусной защиты для разных целей. Стремительному развитию компании способствует желание как можно полно и надёжно решить проблемы клиента, то есть выстроить защиту таким образом, чтобы у злоумышленников не осталось ни одного шанса на проникновение в ПК.

Разработчики Grizzly Pro – это профессионалы, имеющие современные взгляды и методы решения проблем, связанных с информационными угрозами.

Игра стоит свеч

Антивирус Grizzly Pro был задуман, чтобы сочетать в себе все лучшие свойства традиционных и новейших противовирусных систем. Разработчики учли все недоработки и лаги предшествующих программ и создали новейшего робота. Его цели заключаются в:

- контроле поступающих потоков информации;
- обнаружении и блокировке подозрительных объектов;
- оповещении клиента о возможных и имеющихся атаках;
- удалении вредоносных компонентов, сохранении в базе данных сведений о них;
- выстраивании уникальной защиты с учётом обновлений.

Наш продукт понятен на интуитивном уровне и прост в применении. Команда разработчиков Grizzly Pro создала несколько ключевых компонентов антивирусной защиты под нужды каждого клиента:

- для бизнеса;
- для дома;
- профессиональный.

Каждый пользователь выбирает подходящее программное обеспечение, включающее набор важных компонентов информационной безопасности.

Наша цель – лидировать в разработке, развитии и совершенствовании программного обеспечения в сфере информационной безопасности. Помогать с помощью передовых технологий, защищать бизнес и персональные данные наших клиентов по всему миру.

Всё и сразу

Мы обеспечиваем безопасность персональных устройств и сохранение личных данных наших клиентов. Именно это мы довели до совершенства.

- Широкий спектр действия антивирусной программы, эффективность программного обеспечения не влияет на работоспособность устройства, а сканирование системы происходит на рекордных скоростях.
- В отличие от традиционных и современных программ, мы разработали целую линейку узкоспециализированной защиты. В разделе профессиональной антивирусной защиты можно найти такую версию Grizzly Pro, которая будет соответствовать рабочей направленности (для бухгалтеров, фотографов, переводчиков, программистов и других специализаций).
- Любую из версий можно установить бесплатно на 35 дней. Затем антивирус продлевается на 3, 6 или 12 месяцев (в зависимости от потребностей клиента).
- Клиенту не нужно переплачивать за активацию дополнительного ключа, любой продукт рассчитан на 2 или 4 устройства.
- Всесторонняя защита: ПК, флэш-карты, защита при пользовании интернетом.

GRIZZLY PRO
INTERNET SECURITY

Grizzly PRO

Современная компания в сфере информационной безопасности.

8 (800) 200-59-71
sale@grizzly-pro.ru
www.grizzly-pro.ru

Тонкий Клиент Atrust t180L

Atrust

Atrust

Компания-производитель тонких клиентов, серверов и систем управления своими продуктами.

www.atrustcorp.com

ОЛЛИ ДИСТРИБУЦИЯ

***«ОЛЛИ»** – дистрибутор программного и аппаратного обеспечения.*

disti@ollyit.ru
www.ollyit.ru

Atrust t180L – это тонкий клиент с ОС Linux, специально разработанный для клиент-серверных инфраструктур. Встроенное ПО ACS (Atrust Client Setup) разработки Atrust помогает эффективно управлять клиентами t180L. Поддержка Citrix ICA/HDX, Microsoft RDP с RemoteFX, VMware Horizon View с PCoIP и Red Hat SPICE позволяет реализовывать всевозможные сценарии работы с различными средами виртуализации. t180L предлагает полноценную работу, как за ПК, при которой приложения, включая мультимедиа высокого разрешения, выглядят, воспринимаются и работают так, как будто они выполняются локально.

Особенности Atrust t180L

- Поддержка двух мониторов.
- Тихий и надёжный.
- Простое управление.
- Тонкий и прочный корпус.
- Низкое энергопотребление.
- Низкая стоимость владения.
- Поддержка различных протоколов: Citrix ICA/HDX, Microsoft RDP с RemoteFX, VMware Horizon View с PCoIP и Red Hat SPICE.

Процессор	Intel® Bay Trail Quad Core 1.83 ГГц
Оперативная память	1 ГБ
Флэш-память	4 ГБ
Сетевой интерфейс	10/100/1000 Мбит
Разрешение	1920x1200
Поддерживаемые протоколы	Citrix ICA/HDX, Microsoft RDP, VMware Horizon View с PCoIP и Red Hat SPICE
Операционная система	Atrust Linux®
Размеры	39.5 x 103 x 143 мм
Интерфейсы	3 x USB 2.0, разъём для наушников и микрофона, DVI-I, DVI-D, USB 3.0, RJ-45 LAN, DC IN, разъём Kensington lock

Нулевой клиент Atrust m321

Atrust m321 – это оконечное устройство для систем с распределением ресурсов, таких как MultiPoint Server или Userful Multiplatform. Это решение позволяет на основе одного сервера сделать много независимых рабочих станций, каждая из которых состоит из хаба (нулевого клиента) с подключёнными к нему клавиатурой, мышкой и монитором. В результате много пользователей делят между собой вычислительные ресурсы одного сервера. Сервер обеспечивает привычную независимую рабочую среду Windows с использованием обычного Ethernet-соединения.

Особенности Atrust m321

- Низкая стоимость владения.
- Простая установка.
- Бесшумная работа в компактном корпусе.
- Подключение по локальной сети.
- Лёгкое управление и обслуживание.

Процессор	SOC SMSC UFX6000
Сетевой интерфейс	10/100/1000 Мбит
Разрешение	1920 x 1080
Поддерживаемые операционные системы	Windows MultiPoint Server 2012 Userful Multiplatform 6.0
Сертификаты	CB, FCC, CE, BSMI, NRTL
Размеры	120 x 80 x 26 мм
Интерфейсы	DVI-I, 2 x USB тип A (для клавиатуры и мышки), 2 x USB тип A (для других USB устройств), Gigabit Ethernet (для подключения к серверу), разъём для наушников и микрофона, Kensington lock

Atrust

Atrust

Компания-производитель тонких клиентов, серверов и систем управления своими продуктами.

www.atrustcorp.com

ОЛЛИ ДИСТРИБУЦИЯ

***«ОЛЛИ»** – дистрибутор программного и аппаратного обеспечения.*

disti@ollyit.ru
www.ollyit.ru

myUTN-80

С лёгкостью пользуйтесь USB-ключами по всей сети!

Коммутатор USB-ключей myUTN-80 – это безопасное место для этих ключей, открывающее доступ к ним для нескольких пользователей.

Использование USB-ключей без вопросов и сомнений

Использование аппаратных лицензионных USB-ключей в организациях связано с некоторыми трудностями: USB-ключи могут быть потеряны или переставлены, или отдельные проблемы могут возникать в средах виртуализации с ПО, защищённом ключами.

Коммутатор USB-ключей SEH myUTN-80 позволяет оставить все эти ограничения в прошлом! До 8 USB-ключей могут получить доступ к сети через данное устройство, легко и безопасно. Запускайте защищённое ключами ПО как обычно – только не подключая USB-ключ непосредственно на своём рабочем месте – и используйте полную функциональность данного программного обеспечения.

Помимо этого, myUTN-80 предлагает множество дополнительных функций, упрощающих использование USB-ключей в сети: виртуализируйте ваш коммутатор USB-ключей и привяжите его к разным отделам. Для этого есть 2 способа: либо через VLAN путём присвоения IP-адреса каждому порту коммутатора USB-ключей, либо с помощью функции контроля портов для ключей, которая позволяет присваивать пароли каждому порту. Только пользователи с верными паролями могут получить доступ к соответствующим ключам.

Таким образом, одно устройство myUTN-80 с лёгкостью может быть превращено в 8 виртуальных коммутаторов USB-ключей!

USB-ключи всегда под контролем

Коммутатор USB-ключей myUTN-80 значительно упрощает управление подключёнными USB-ключами. Через веб-интерфейс ПО myUTN Control Center администраторы ИТ полностью контролируют все USB-ключи и могут легко управлять всеми портами. С точки зрения пользователя работа с приложениями не меняется: нужно просто запустить программу и myUTN-80 автоматически подключит требуемый USB-ключ.

Естественно, myUTN-80 также обеспечивает максимальную безопасность: он предоставляет широкий набор функций безопасности, включая шифрование, защиту паролем и многое другое!

Область применения

- Предприятия, использующие защищённое ключами ПО.
- Защита для комплектов ключей в университетах, больницах и т. п.
- Идеально для сред с вычислениями на стороне сервера (CitrixXenApp, Microsoft Remote Desktop Services/ Terminal Services) и сред виртуализации (VMware, Citrix XenDesktop или серверная виртуализация).

Преимущества

- Идеальное решение для сред виртуализации.
- USB-ключи всегда готовы к использованию по сети.
- USB-ключи доступны для нескольких пользователей без необходимости повторного подключения.
- Независимость от USB-интерфейсов на компьютерах.
- Каждый USB-ключ может быть присвоен отдельным пользователям, департаментам и т. д.

myUTN-800

Корпоративное решение для управления USB-ключами

Коммутатор USB-ключей SEH myUTN-800 обеспечивает доступ по сети к USB-ключам в количестве до 20 штук – идеальный вариант для случаев, когда имеется много пользователей и большое количество ключей. Кроме того, централизованное хранение ключей в закрытом коммутаторе защищает их от потери, повреждения, износа и кражи.

Работает это следующим образом: пользователь подключает нужные ключи через ПО SEH UTN Manager и локально работает с лицензионными приложениями. При этом подключённые ключи недоступны для других пользователей. Как только он перестает работать со своими приложениями и деактивирует ключи, они оказываются доступны для других пользователей.

Этот подход работает с любыми защищёнными приложениями и гарантирует законность действий пользователей, так как лицензионные правила не нарушаются. Такое управление лицензиями также позволяет сократить расходы на лицензии, так как пользователи не всегда одновременно работают с одним и тем же ПО.

Дополнительные функции ПО UTN Manager позволяют автоматизировать и упростить многие действия. Например, активация и деактивация USB-ключей может происходить автоматически при запуске/остановке приложений.

Для обеспечения максимальной надёжности коммутатор myUTN-800 имеет 2 блока питания и 2 сетевых интерфейса. Помимо этого, есть возможность сохранения настроек на карту SD для их последующего быстрого переноса на другой коммутатор myUTN-800. А наличие многосегментного индикатора ошибок позволяет оперативно диагностировать проблемы, например, неисправность карты SD или неисправность блока питания.

Для коммутаторов myUTN-800 доступна дополнительная опция myUTN-800 Serviceplus, которая продлевает гарантию до 60 месяцев и обеспечивает оперативную замену неисправных устройств. Для установки коммутатора myUTN-800 в стойку 19″ используется опциональный набор креплений Rack Mount Kit (RMK3).

Области применения

- В центрах обработки данных.
- У «облачных» провайдеров.
- В средах виртуализации.
- В крупных компаниях, которые используют много разных лицензионных ключей.
- В образовательных учреждениях.
- В компаниях с высокими требованиями к безопасности.
- Когда не хватает USB-портов на рабочих станциях.
- Для выделения USB-ключей работникам вне офиса.

Коммутатор USB-ключей myUTN-800 – это продвинутое устройство, предназначенное для установки в серверных крупных компаний.

SEH Computertechnik GmbH

Производитель оборудования для проброса USB через IP.

www.seh.de

«ОЛЛИ» *– дистрибутор программного и аппаратного обеспечения.*

disti@ollyit.ru www.ollyit.ru

Устройства для безопасного хранения и переноса информации

Защищённый флэш-накопитель USB 3.0 GuardDo Touche

Характеристики

- Материал: алюминий
- Объём памяти: 16 Гбайт, 32 Гбайт
- Порт: USB 3.0
- Аппаратное шифрование по алгоритму AES, 256 бит
- Встроенный литий-ионный аккумулятор ёмкостью 65 мАч
- Размеры: 80x24x8 мм

Преимущества

- Шифрование в реальном времени
- Аппаратная клавиатура на корпусе
- Не требуется установка дополнительного ПО
- Защита от воды и пыли
- Пароль администратора даёт доступ ко всем функциям устройства, а пароль пользователя – только к чтению данных
- Ввод пароля с аппаратной клавиатуры

Накопитель USB 3.0 1,8" GuardDo Masquer

Характеристики

- Материал: алюминий
- Объём памяти: 64 Гбайт, 128 Гбайт, 256 Гбайт, 480 Гбайт
- Порт: USB 3.0
- Аппаратное шифрование по алгоритму AES, 256 бит
- Размеры: 90x55x12 мм

Преимущества

- Шифрование в реальном времени
- Аппаратная клавиатура на корпусе
- Не требуется установка дополнительного ПО
- Ультратонкий дизайн
- Размеры не более визитной карточки, прочная и надёжная конструкция
- Высокая скорость передачи данных
- Высокоскоростной порт USB 3.0 со скоростью передачи данных до 5 Гбит/с

Защищённый жёсткий диск 2,5" GuardDo Attache

Характеристики

- Материал: алюминий
- Объём памяти: 500 Гбайт, 1 Тбайт и 2 Тбайт
- Порт: USB 3.0
- Аппаратное шифрование по алгоритму AES, 256 бит
- Размеры: 127x77x15 мм

Преимущества

- Шифрование в реальном времени
- Клавиатура на корпусе
- Защита от перенапряжения с лимитом 10 % до отключения
- Защита от повреждения жёсткого диска под действием скачков напряжения
- Защита от низкого напряжения срабатывает при недостаточном напряжении питания
- Поддержка жёстких дисков SSD/HDD 2,5″ с интерфейсом SATA I/II/III и объёмом памяти до 2 Тбайт

Защищённый жёсткий диск 3,5" GuardDo Croiser

Характеристики

- Материал: качественный алюминий для эффективного отвода тепла
- Объём памяти: 2 Тбайт, 4 Тбайт
- Порт: USB 3.0
- Аппаратное шифрование по алгоритму AES, 256 бит
- Размеры: 210x120x38 мм

Преимущества

- Шифрование в реальном времени
- Поддержка HD 3,5″ с объёмом памяти до 6 Тбайт
- Клавиатура на корпусе
- Не требуется установка дополнительного ПО

GUARD'DO

«Самурай24»

www.samurai24.ru

Защита мобильной связи

Специальный абонентский терминал (CAT)

С появлением комплексов перехвата разговоров в системе GSM никто не может быть застрахован от прослушивания разговора третьими лицами.

Решить проблему предупреждения и защиты от прослушивания можно с использованием специального абонентского терминала.

Преимущества

- Защита от активных и пассивных комплексов (перехват переговоров и дистанционное управление телефоном).
  - Обнаружение дистанционного включения микрофона.
  - Обнаружение понижения уровня кодирования.
- Удаление информации о звонках из памяти телефона.
- Невозможность локализации телефона и определения номера основного телефона и связанных с ним номеров других телефонов.
- Функция смены IMEI.

Смартфон для анонимности и безопасности

Хранение личных данных на серверах стало нормой; мир наводнился мобильными гаджетами с GPS-приёмниками и GSM-модулями, способными рассказать практически всё об их владельцах.

Представляем вам смартфон, который позволит оставаться анонимным в таких условиях.

Преимущества

- Установлен VPN от одного из лидеров услуг (сервис оплачен на 2 года).
- Трафик на подключение только через VPN.
- Шифрование данных телефона SSE.
- Удалены все сервисы от Google.
- Установлена программа для загрузки открытого программного обеспечения.
- Дополнительно запущена сеть Tor (опция).
- На смартфоне предустановлены и настроены все необходимые программы для анонимного общения и веб-сёрфинга.
- Функция смены IMEI.

Оборудование для безопасного хранения и уничтожения данных

Samurai HS

Системы защищённого хранения и экстренного уничтожения информации на жёстких дисках.

Преимущества

- Защита корпуса от несанкционированного вскрытия.
- Управление и мониторинг по GSM.
- Система протоколирования событий.
- Автономное питание до 48 часов.
- Уничтоженная информация не подлежит восстановлению.

Риски, связанные с возможностью силового доступа к вашей конфиденциальной информации. Незаконные действия конкурентов при попытке получить информацию.

Для решения подобных проблем создана серия устройств SAMURAI HS с функцией уничтожения информации в серверных стойках, при этом процесс монтажа настолько прост, что каждый пользователь без специальных знаний способен установить это устройство. Подобные системы давно используются во многих организациях.

Оперативное уничтожение информации с жёсткого диска без возможности восстановления производится дистанционно по решению владельца (по радиоканалу, мобильному телефону или по проводному каналу) или автоматически при определённых заранее технических условиях.

ATX

Система для самостоятельной установки на персональных компьютерах.

Преимущества

- Проводная кнопка, возможность подключения управления и мониторинга по GSM.
- Возможность подключения дистанционного управления.
- Система протоколирования событий.
- Автономное питание до 48 часов.

Защита персонального компьютера финансового директора и бухгалтера

Персональные компьютеры финансовых директоров и главных бухгалтеров так же часто, как и серверы, становятся объектами атаки.

Главный бухгалтер может выполнять функции финансового директора, обрабатывая информацию о финансовых потоках, данные об активах и другие сведения, составляющие полную картину финансово-экономического состояния компании.

GUARD'DO

«Самурай24»

Разработка высокотехнологичных комплексных решений для эффективной защиты корпоративной информации от потерь, кражи или от несанкционированных действий злоумышленников.

www.samurai24.ru

DATAPK – программно-аппаратный комплекс оперативного мониторинга и контроля на защите АСУ ТП

Программно-аппаратный комплекс DATAPK™, сертифицированный ФСТЭК России, обеспечивает оперативный мониторинг и контроль состояния защищённости систем автоматизации критически важных объектов (КВО) и объектов критической информационной инфраструктуры (КИИ), в частности, автоматизированных систем управления технологическими процессами (АСУ ТП).

Подход к обеспечению ИБ

И хочется, и колется – как подойти к вопросу обеспечения информационной безопасности автоматизированных систем управления технологическими процессами?

Сегодня мы получаем всё больше аргументов в пользу актуальности вопроса обеспечения информационной безопасности (ИБ) в автоматизированных системах управления (АСУ) технологическими процессами (ТП): это и растущая популярность вредоносных программ-вымогателей в АСУ ТП, и ужесточение требований законодательства РФ, и результаты аудитов ИБ, проведённых многими владельцами АСУ ТП. Но при этом до сих пор остаётся актуальным вопрос – что и как применять для защиты АСУ ТП? Нередко можно услышать, что АСУ ТП отличаются от традиционных офисных систем, а значит, и подходы к обеспечению ИБ должны отличаться, но как именно?

Зачастую отмечают, что для АСУ ТП традиционная триада «конфиденциальность, целостность, доступность» меняется на «доступность, целостность, конфиденциальность», так как в АСУ ТП гораздо важнее обеспечить работоспособность системы, а не сохранить в секрете тот или иной сигнал или содержимое экранной формы. Также необходимо отметить, что свойства доступности, целостности и конфиденциальности в АСУ ТП надо рассматривать не в отношении информации, циркулирующей в системе, а в отношении системы в целом, так как основная задача АСУ ТП – корректная работа функций, заложенных в неё разработчиком.

Функции АСУ ТП имеют достаточно жёсткие требования по точности, времени выполнения и пр. Именно поэтому многие решения по обеспечению ИБ воспринимаются представителями подразделений автоматизации в штыки – они вносят изменения в работу функций (дополнительная задержка, вносимая межсетевым экраном в передачу сигналов технологической сети, может привести к нарушению временного норматива работы функции, ПО для защиты рабочих станций или серверов может привести к отказу того или иного программного блока из-за ложного срабатывания и т. д.).

Позицию подразделений по автоматизации можно понять: все смежные системы, не имеющие отношения к основной АСУ ТП (к которым относятся, например, системы промышленной безопасности, выявляющие пожары, утечки ядовитых веществ и прочие критичные для безопасности объекта факторы), как правило, не могут влиять на неё в автоматическом режиме (исключение, когда эти системы интегрированы в единую систему силами одного разработчика) – тогда почему система обеспечения ИБ должна быть более привилегированной в этом вопросе?

Принимая во внимание вышеперечисленное, подход к обеспечению ИБ в АСУ ТП целесообразно строить, исходя из следующих принципов:

- система обеспечения ИБ АСУ ТП должна быть направлена на выявление любых изменений в системе, которые могут привести к нарушению работы функций системы;
- система обеспечения ИБ АСУ ТП должна быть направлена в первую очередь на обнаружение реализации угрозы ИБ и информирование ответственных работников организации, которые уже могут применять меры в отношении выявленной угрозы ИБ.

Одним из вариантов построения системы обеспечения ИБ, удовлетворяющей приведенным выше принципам, является специализированный программно-аппаратный комплекс DATAPK производства компании «Уральский центр систем безопасности» (УЦСБ).

ПАК DATAPK

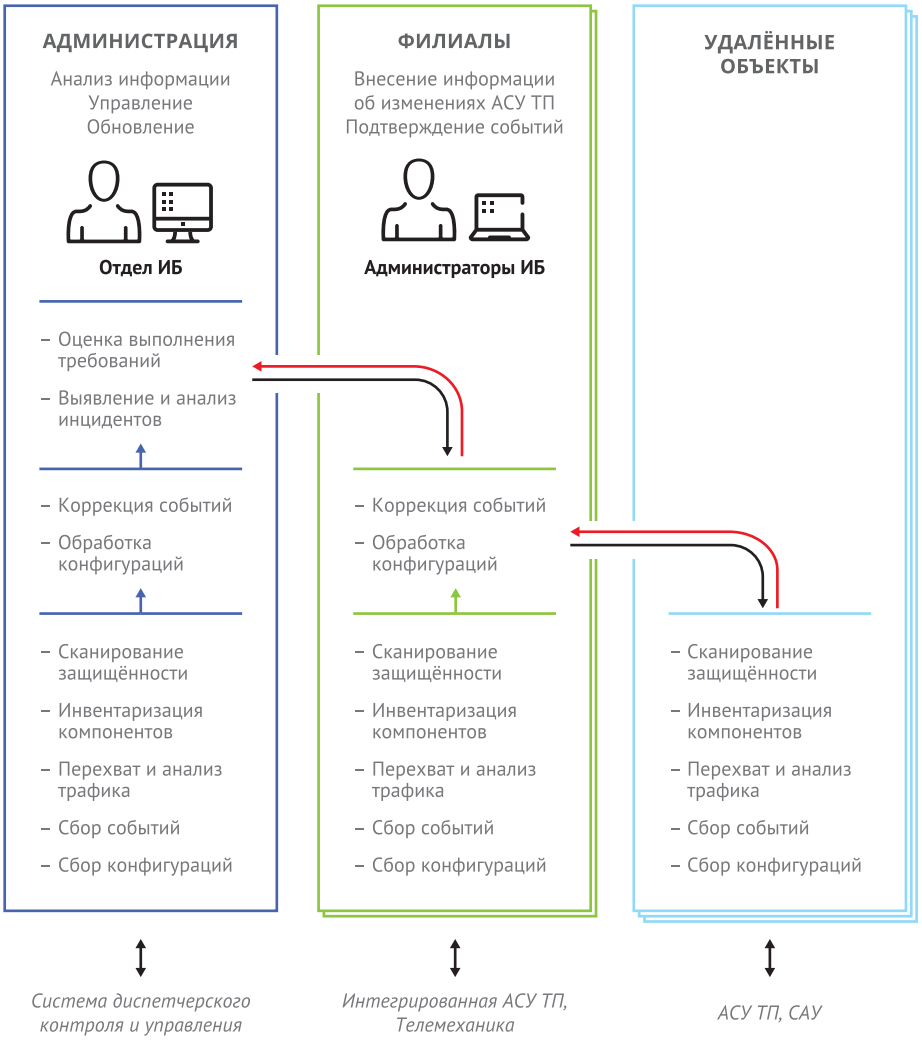
Непрерывный контроль изменений АСУ ТП без вмешательства в работу системы.

DATAPK обеспечивает оперативный мониторинг и контроль состояния защищённости компонентов АСУ ТП. Решение DATAPK предназначено для выявления предпосылок реализации угроз ИБ и недопущения возникновения инцидентов ИБ в АСУ ТП путём оперативного информирования персонала организации, ответственного за реагирование на инциденты ИБ.

DATAPK позволяет создавать распределённые системы обеспечения ИБ, повторяющие иерархическую структуру АСУ ТП организации. При этом модульная структура DATAPK позволяет выстраивать систему максимально эффективно с экономической точки зрения: на нижних уровнях иерархии используется минимальный набор модулей, обеспечивающих только сбор информации, а интеллектуальная обработка информации осуществляется уже на более высоких уровнях.

Среди основных преимуществ DATAPK можно перечислить возможность работы без установки дополнительных программных агентов на компоненты АСУ ТП, отсутствие воздействия на работу АСУ ТП, а также модульность и интеграцию с внешними системами управления и обеспечения ИБ.

Весной 2017 года интегратор УЦСБ объявил о завершении сертификационных испытаний программного комплекса оперативного мониторинга состояния информационной безопасности и контроля состояния защищённости производственно-технологических комплексов DATAPK. В результате проведённой работы DATAPK получил сертификат соответствия №3731 Федеральной службы по техническому и экспортному контролю (ФСТЭК России).



Сертификат соответствия №3731 ФСТЭК России подтверждает, что DATAPK является программным средством контроля (анализа) защищённости информации, не содержащей сведений, составляющих государственную тайну, а также соответствует требованиям технических условий при выполнении указаний по эксплуатации.

В настоящее время DATAPK проходит апробацию у ряда заказчиков УЦСБ из ТЭК, металлургии и других отраслей. Кроме того, DATAPK используется в качестве элемента лабораторного стенда, на котором проходит обучение студентов ЮФУ.

DATAPK может быть использован для автоматизированного контроля реализации требований Приказа ФСТЭК России от 14 марта 2014 г. N 31 «*Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды*».

Основные модули DATAPK

Модуль управления конфигурацией объектов защиты обеспечивает:

- ведение каталога объектов защиты (под объектом защиты в DATAPK понимается устройство АСУ ТП, подключённое к технологической сети передачи данных), автоматическое выявление изменений в составе объектов защиты (появление ранее неизвестных или наоборот – пропадание ранее наблюдавшихся объектов защиты) путём анализа сетевого трафика технологической сети передачи данных;
- контроль сетевого взаимодействия между объектами защиты, выявляющий ранее неизвестные информационные потоки между объектами защиты (при этом конфигурация DATAPK позволяет в качестве отдельного информационного потока описать конкретные команды промышленного протокола, например, команды, меняющие ПО программируемого логического контроллера);
- контроль конфигураций объектов защиты, выявляющий изменения аппаратной и программной части объекта защиты (например, подключение съёмных носителей информации к АРМ, создание нового пользователя в ОС или ПО SCADA и пр.).

Модуль сбора и анализа событий ИБ обеспечивает:

- сбор событий ИБ с объектов защиты посредством различных протоколов передачи событий ИБ (syslog, Windows Event Log, чтение событий из файлов или базы данных и пр.);
- представление событий ИБ от всех источников в едином интерфейсе DATAPK;
- анализ и корреляцию событий ИБ по заданным правилам.

Модуль оценки соответствия требованиям ИБ и поиска уязвимостей обеспечивает:

- оценку соответствия конфигурации объектов защиты заданным требованиям по обеспечению ИБ (требования могут быть заданы внутренними нормативными документами, проектной документацией и пр.);
- поиск известных уязвимостей объектов защиты.

Оценка соответствия и поиск уязвимостей производится на базе описаний, использующих язык OVAL, что позволяет использовать описания, сформированные в других решениях, поддерживающих этот язык.

Построение системы обеспечения ИБ на базе DATAPK

Насколько сложно внедрить DATAPK для мониторинга состояния защищённости АСУ ТП? Ответ на вопрос зависит от многих факторов, но для примера рассмотрим ситуацию, близкую к идеальной: требуется защитить АСУ ТП, расположенную на территории одного технологического комплекса (небольших размеров), при условии, что АСУ ТП сопровождается разработчиком/проектировщиком и на неё есть вся актуальная документация.

В такой ситуации порядок внедрения DATAPK будет следующим.

1. Необходимо обеспечить подключение DATAPK в технологическую сеть передачи данных двумя способами: первое подключение должно обеспечить передачу копии всего сетевого трафика для анализа информационных потоков (это реализуется с использованием технологии SPAN на современных коммутаторах или с помощью ответвителей сетевого трафика – TAP), второе подключение должно обеспечить возможность взаимодействия DATAPK с объектами защиты (в случае сегментированной с помощью VLAN сети это может быть транковый порт, который обеспечит доступ во все VLAN технологической сети).

2. Необходимо наполнить каталог объектов защиты DATAPK, описав все сетевые устройства и их информационные потоки. Эта задача легко решается при наличии актуальной проектной и эксплуатационной документации на АСУ ТП – так как там приведён состав (и конфигурация) объектов защиты, сведения о способах их взаимодействия между собой и со смежными системами.

3. На объектах защиты необходимо создать служебные учётные записи, которые позволят DATAPK осуществлять сбор событий и конфигураций.

4. После сбора текущих конфигураций объектов защиты DATAPK уже готов к непрерывному мониторингу состояния защищённости. По мере эксплуатации решения, конфигурация может расширяться источниками событий ИБ, дополнительными правилами анализа и корреляции событий ИБ, правилами контроля соответствия объектов защиты требованиям ИБ.

«Уральский центр систем безопасности»

Компания УЦСБ специализируется на создании, модернизации и обслуживании базовых инфраструктурных элементов предприятий и организаций.

+7 (343) 379-98-34
info@ussc.ru
www.ussc.ru

Средства управления тонкими клиентами Atrust

Продукты управления позволяют работать одновременно с ТК Atrust разных моделей и на разных платформах. Atrust открыт для внесения дополнений по просьбам заказчиков. Все продукты управления предоставляются покупателям оборудования Atrust абсолютно бесплатно.

Atrust Device Manager

Серверный продукт для централизованного управления:

- объединение ТК в группы и создание профилей;
- настройка ТК;
- установка обновлений и сертификатов;
- включение/выключение и удалённый мониторинг ТК;
- планировщик заданий;
- поддержка работы с внешними СУБД.

Atrust Auto Setup

Система автоматической настройки:

- установка настроек и обновлений на ТК «из коробки» без участия администраторов;
- особые настройки для конкретных ТК и конкретных пользователей;
- специализированное ПО для создания конфигурационных файлов.

Atrust Deployment Server

Продукт для распределённого хранения файлов обновлений:

- содержит прошивки, образы систем и WES пакеты;
- подключается и управляется через основной сервер ADM;
- устанавливается в филиалах;
- убирает необходимость передавать файлы обновлений для каждого удалённого ТК с центрального сервера ADM.

Atrust Package Creator

Продукт для создания WES-пакетов:

- упаковка в пакеты необходимых дополнительных приложений и настроек Windows;
- централизованная установка и удаление пакетов через ADM;
- не требуется обновлять прошивку ТК на WES целиком.

Atrust Client Setup

Встроенное ПО для локальной настройки ТК:

- управление подключениями (RDP, Citrix, VMware, SPICE, Parallels, SSH);
- настройка интерфейса пользователя;
- управление подключёнными устройствами;
- сетевые настройки.
- системные настройки и подключение к продуктам управления.

Atrust

Atrust

Компания-производитель тонких клиентов, серверов и систем управления своими продуктами.

www.atrustcorp.com

ОЛЛИ ДИСТРИБУЦИЯ

«ОЛЛИ» *– дистрибутор программного и аппаратного обеспечения.*

disti@ollyit.ru
www.ollyit.ru

Контроллер видеостен Userful

Компания Userful предлагает простые и доступные решения для централизованного управления устройствами отображения информации.

Видеостена

Userful позволяет создавать разнообразнейшие видеостены и инсталляции digital signage с широким функционалом, поддержкой различных источников контента и с возможностью быстрого расширения или масштабирования системы на основе обычного компьютерного оборудования, что ведёт к существенной экономии на проекте.

По миру насчитывается более 1 миллиона дисплеев, работающих под управлением Userful, в более чем сотне стран. Инсталляции Userful включают в себя реализации интерактивных видеостен, художественных мозаичных видеостен, видеостен ситуационных центров, а также VDI-решений.

Возможности

- Создание дизайнерских видеостен с возможностью комбинирования мониторов любого размера и поворота мониторов под любым углом.
- Создание предустановленных конфигураций для простого переключения режимов работы видеостены.
- Масштабируемость до 100 мониторов на один ПК/сервер.
- Режим multi-window (PiP).
- Полное управление видеостеной через API.
- Широкий спектр поддерживаемых систем управления контентом (CMS).
- Поддержка разрешения до 8K.
- Высокая доступность.
- Поддержка русского языка в ПО.

Архитектура

ПО Userful ставится на ПК. Контент крутится либо на самом этом ПК (с жёсткого диска, USB-flash, DVD или из виртуальных машин), либо получается по сети (из CMS, с помощью RTSP, по RDP, из «облака» или web browsing), или пробрасывается с помощью карт захвата. Затем, после обработки Userful, видеоинформация передаётся по сети Ethernet через маршрутизатор на нулевые клиенты (практически видеокарты, подключённые к сети), которые отображают её на подключённых к ним мониторах.

Примеры применения видеостен Userful

- Транспорт и промышленность (ситуационные центры).
- Индустрия развлечений.
- Торговля, гостиничный бизнес, медицина.

---

userful™

Userful *предлагает простые и доступные решения для централизованного управления устройствами отображения информации.*

userful@olly.ru
www.userful.com

ОЛЛИ ДИСТРИБУЦИЯ

«ОЛЛИ» *– дистрибутор программного и аппаратного обеспечения.*

disti@ollyit.ru www.ollyit.ru

100 идей контента Digital Signage почти для любой отрасли

Если ваша организация использует цифровые видеопанели, одной из сложнейших задач является планирование идей для нового контента, чтобы трансляции продолжали быть интересными.

Поиск в Google может занять массу времени, при этом в итоге результаты будут довольно скромными. Использование устаревших, традиционных образов с листовок и плакатов не выглядит достаточно современным. Вы, конечно, можете обойти окрестности, рассматривая в поисках идей цифровые видеопанели других организаций, но контент, который подходит для вашей ближайшей доставки пиццы, может совсем не подойти для вас.

Для того чтобы помочь решить эту задачу, и был составлен список из 100 идей контента для видеорекламы. Список поделён по отраслям, чтобы легче было понять – какой тип контента работает для какого бизнеса.

Любое направление деятельности

1. Вдохновляющие цитаты – цитаты можно найти в Google, Goodreads или на сайте BrainyQuote. Оформите их, используя Canva или Word Swag.

2. Каталог.

3. Карта вашего помещения.

4. Часы работы.

5. Предстоящие праздники, когда заведение будет закрыто.

6. Метеосводка.

7. Обзоры/отзывы.

8. Пресса – транслируйте недавние упоминания о вашей организации в прессе.

9. Реклама – транслируйте ваши последние рекламные ролики, чтобы укрепить узнаваемость бренда.

Внутренняя связь

10. Мотивационные фразы – обратитесь за вдохновением к Startup Vitamins.

11. Вдохновляющие цитаты ваших любимых предпринимателей – опять же, на Startup Vitamins.

12. Напоминания.

13. Объявления.

14. Предстоящие события в жизни коллектива – часы скидок, выездные мероприятия и другое.

15. Поздравления с днём рождения.

16. Ключевые события в жизни компании – обращайте внимание на ключевые события, такие как достижение определённого количества продаж, новый этап финансирования, получение прибыли и т. п.

17. Годовщины – отмечайте годовщины создания компании, первой продажи, первого выпуска продукта и т. п.

18. Сведения о компании – интересные факты или история компании.

19. Рассказывайте о своих сотрудниках – транслируйте анкеты своих сотрудников и помогайте коллегам узнать их лучше.

20. Достижения сотрудников.

21. Панель KPI – панель KPI (key performance indicators – ключевые показатели эффективности) представляет обзор показателей, которые наглядно демонстрируют эффективность работы вашей компании. Мы рекомендуем использовать Geckoboard для создания такой панели и затем отображать эту панель с помощью приложения для системы цифровых видеопанелей на веб-странице.

22. Профили компании в социальных сетях – выводите на дисплее трансляции вашей компании в социальных сетях. Это продвигает внутренний маркетинг и информирует вашу команду о том, чем компания делится с остальным миром.

23. Профили конкурентов в социальных сетях – лёгкий способ следить за конкуренцией.

24. Лента хэштегов, относящихся к направлению деятельности или к бизнесу – транслируйте ленту публикаций в социальных сетях, тематически связанную с направлением

деятельности вашей компании; это позволяет проследить современные тенденции и «слушать» клиентов.

25. Коллективные фото сотрудников – способствуйте развитию сильной корпоративной культуры, демонстрируя слайды с коллективными фотографиями сотрудников. Транслируйте фотографии, демонстрирующие сплочённость, как внутри, так и вне офиса.

26. Новости индустрии – транслируйте RSS-ленту новостей, относящихся к направлению деятельности вашей компании.

Здравоохранение

27. Советы, как сохранить здоровье и самочувствие.

28. Новости медицинской сферы – используйте RSS-трансляцию.

29. Рассказывайте о своих сотрудниках – представьте своих сотрудников дайте понять, что здоровье пациентов находится в надёжных руках. Вы можете представить общие сведения о своих сотрудниках, об их образовании или опыте.

30. Реклама лекарственных препаратов – рекламируйте лекарственные препараты, которые предлагает ваша компания.

31. Разъясняйте медицинские процедуры – если ваша медицинская организация проводит операции или иные медицинские процедуры, используйте текст, видео и/или графику, чтобы объяснить их суть.

32. Фотографии «до и после» – если ваша медицинская организация предлагает косметические процедуры, используйте ленту Instagram или обычные слайды, чтобы продемонстрировать сравнения состояний до и после этих процедур.

33. Время ожидания – пусть пациенты будут знать предполагаемое время ожидания приёма.

Розничная продажа

34. Описание продукции – предоставьте подробные сведения о продукции, которую вы продаёте.

35. Предстоящие распродажи – все любят скидки.

36. Советы по стилю – вдохновляйте покупателей стилем.

37. Тренды – сделайте упор на последних трендах, используя фото и видео.

38. Показы мод – транслируйте подиумные видео с последних показов мод, в которых участвовал ваш бренд.

39. Рассказывайте о дизайнерах одежды – если вы продаёте дизайнерскую одежду, помогите покупателям познакомиться с дизайнерами и их работой.

Салоны и спа

40. Услуги и цены.

41. Демонстрация продукции – транслируйте обучающее видео о том, как использовать продукцию для волос и косметические средства, которые вы продаёте.

42. Фотографии ваших лучших работ – транслируйте фотографии клиентов, которые демонстрируют свои новые причёски.

43. Рассказывайте о стилистах – познакомьте клиентов с вашими стилистами и их работой.

44. Рекомендации по использованию продукции.

45. Советы по сохранению причёски – вооружите своих клиентов советами по стилю, чтобы они отлично выглядели, даже покинув ваш салон.

46. Советы по уходу за волосами – помогите своим клиентам добиться того, чтобы у них были самые здоровые волосы.

47. Фотографии клиентов из Instagram – попросите своих клиентов поделиться фотографиями своей новой причёски в Instagram, используя определённый хэштег, после чего отображайте их на экранах через трансляцию этого хэштега.

Рестораны

48. Меню – показывайте привлекательное, яркое цифровое меню.

49. Аппетитные фотографии ваших блюд.

50. Диетологические сведения.

51. Сведения об аллергенах – клиенты должны знать, если в ваших блюдах есть какие-либо распространённые аллергены.

52. Рекламные страницы в Instagram – еде в Instagram уделяют много внимания. Отображайте кнопку для перехода на основной сайт, попросив клиентов поделиться фотографиями еды из вашего ресторана с определённым хэштегом.

53. Лента хэштегов Instagram – транслируйте Instagram-ленту ваших клиентов, используя хэштег, указанный в настройках кнопки перехода на основной сайт.

54. Видео приготовления еды – вам необязательно выдавать секретные рецепты, но подумайте о демонстрации коротких видео своих поваров за работой.

55. Рассказывайте о своих шеф-поварах – представьте клиентам кулинарных мастеров, готовящих так полюбившиеся клиентам блюда.

56. Другие заведения – если ваш ресторан сетевой, расскажите клиентам, где ещё они могут найти его.

57. Расскажите о ваших блюдах – предоставьте больше сведений о тех пунктах меню, которые появились недавно или заслуживают особого внимания.

Гостиницы

58. Сведения о гостиничном баре – где-то сейчас пять часов.

59. Сведения о ресторане в гостинице.

60. Сведения о гостиничном бассейне.

61. Сведения о других удобствах и услугах – пусть клиенты будут в курсе всех удобств, которые предлагает гостиница, таких как спа-процедуры или услуги прачечной.

62. Достопримечательности поблизости – превратите свою видеостену в цифрового консьержа.

63. Инструкции по заселению и выселению из гостиницы.

64. Правила – транслируйте наиболее важные правила своей гостиницы, чтобы персоналу не пришлось постоянно повторять их клиентам.

65. Предстоящие мероприятия в гостинице.

66. Сведения об особых мероприятиях – если в вашей гостинице проходит мероприятие, такое как торго-

вая выставка или тематический слёт, предоставьте участникам сведения, которые им нужны.

67. Сведения о транспорте.

Недвижимость

68. Реестры имущества.

69. Рассказывайте об агентах – представляйте клиентам своих агентов недвижимости и укрепляйте доверие.

70. Продвигайте услуги вашей фирмы – воодушевляйте продавцов на то, чтобы они размещали сведения о продаже в вашей фирме.

71. Сведения об открытых показах – рекламируйте предстоящие открытые показы.

72. Новости рынка недвижимости – что там с рынком? Сейчас хорошее время, чтобы покупать или продавать? Используйте RSS-ленту, чтобы транслировать последние новости рынка недвижимости.

73. Виртуальные осмотры – используйте видео или слайды, чтобы потенциальные клиенты могли совершить виртуальный осмотр собственности, выставленной на продажу.

Образование

74. Правила безопасности и правила поведения в экстренных случаях – безопасность очень важна в кампусах учебных заведений. Учащиеся должны знать, куда обратиться за помощью и как вести себя в случае чрезвычайной ситуации.

75. Расскажите о составе факультета и его администраторах – помогите учащимся узнать их учителей и администрацию кампуса.

76. Рассказывайте об учащихся – выделяйте учащихся, которые достигли выдающихся результатов.

77. Предстоящие мероприятия.

78. Студенческие группы – помогайте студентам принимать участие в социальную жизнь кампуса, показав им, в какие группы и клубы они могут вступить.

79. Социальная инфраструктура – ознакомьте учащихся и посетителей кампуса с объектами социальной инфраструктуры, такими как рестораны, фитнес-центры, музеи и т. д.

80. Объявления о строительстве или ремонте – кампусы печально известны тем, что в них постоянно что-то строят или ремонтируют. Предупредите учащихся и посетителей.

81. Упоминания в новостях – пусть учащиеся гордятся, увидев положительные упоминания своего учебного заведения в новостях.

82. Последние сроки, которые важны – академический год вращается вокруг последних сроков. Сделайте учащимся одолжение и напомните им об этих сроках.

83. Рекламный материал – покажите перспективным учащимся и их родителям, почему они должны посещать ваше заведение.

84. Рассказывайте о выпускниках – хвастайтесь успехами тех, кто учился в вашем заведении.

85. Спортивные достижения – стимулируйте развитие командного духа и гордости, рассказав о спортивных достижениях учебного заведения, неважно, были ли эти достижения в далёком прошлом или недавно.

86. Сведения об учебном заведении – поделитесь историей учебного заведения и интересными фактами о нём.

87. Вакансии в кампусе – включите в трансляцию описание работ и инструкции для соискателей.

88. Информационные ресурсы – информируйте учащихся о полезных информационных ресурсах, таких как онлайн-порталы, библиотеки, дополнительные занятия.

Праздники

89. Распределение праздничных дней в году – найдите эти сведения здесь.

90. Поздравления – создайте и транслируйте красивые поздравления с пожеланием счастливого праздника.

91. Виртуальный камин – скачайте видео горящих поленьев и транслируйте, превратив свою видеостену в виртуальный камин.

Фитнес-центры

92. Советы по фитнесу.

93. Правила и этикет – транслируйте дружественные напоминания о правилах и этикете, принятых в вашем фитнес-центре.

94. Расписание занятий.

95. «Фитнес-вдохновение» – контент, связанный с фитнесом, вдохновляющий клиентов на действие. Вы можете поискать примеры на Pinterest.

96. Реклама продукции – если в вашем фитнес-центре продаётся собственная продукция или продукция партнёров, рекламируйте её на цифровых экранах.

Банки

97. Советы по управлению финансами.

98. Рекламируйте продукты и услуги – расскажите клиентам о финансовых продуктах и услугах, которые вы предлагаете.

99. Курсы обмена валют.

100. Финансовые или экономические новости – используйте RSS-ленту или социальные сети.

А красочно, эффектно и экономично вывести всю эту информацию на ваши устройства отображения информации поможет видеоконтроллер на базе ПО Userful.

Средство от рейдеров: как заработать на уничтожении данных

Бывают ситуации, когда в дверь стучат, и информацию нужно уничтожить за считаные секунды. Супруги Евгений и Ольга Цацура решили эту проблему – они зарабатывают миллионы на быстром и безвозвратном уничтожении данных.

Российский рынок защиты информации объёмом в 553 млн долларов США, по данным IDC за 2014 год, весьма конкурентный: свои услуги на нём предлагают несколько десятков компаний, в том числе такие гранды, как LETA и InfoWatch. Но супруги Ольга и Евгений Цацура нашли на нём свою нишу – безвозвратное уничтожение данных – как последний шанс защитить их от незаконного использования. Потребность в этом на вполне законных основаниях испытывают банки, медицинские клиники и научные центры. В прошлом году компания «Самурай», через которую супруги Цацура ведут свой бизнес, получила выручку в 80 млн рублей.

От плюшек к электротехнике

Основатель «Самурая» Евгений Цацура в 1997 году окончил МГТУ им. Баумана по специальности «приборостроение». Ещё будучи студентом, он открыл свою пекарню. Но быстро понял, что далёк от кондитерского дела, и решил вернуться к электротехнике. В 1999 году Цацура занялся дистрибуцией оборудования специального назначения – металлодетекторов, блокираторов телефонного сигнала, подавителей диктофонов. Законодательство менялось, многие виды техники для прослушивания запрещались, но это не останавливало продавцов жучков и ручек со скрытыми камерами. «*Мы всегда были на светлой стороне – пытались защитить людей от незаконного вторжения в их частную жизнь,* – рассказывает Цацура в интервью. – *Большого заработка дистрибуция не приносила, нам просто было интересно решать эксклюзивные задачки*». Постепенно от продажи техники сторонних производителей компания Цацуры перешла к решениям под ключ. Выполнение некоторых задач походило на шпионские фильмы: заказчики имитировали затопление офиса, чтобы во время ремонта установить необходимое оборудование, не афишируя это среди сотрудников.

Цифры «Самурая»

50 млн долларов США – объём российского рынка технологий по защите данных

200–700 устройств и систем продаёт компания в месяц

450 В – напряжение, которое подается на катушку-излучатель для запуска процесса уничтожения данных

80 млн руб. – годовая выручка компании в 2014 году

12 человек составляет штат компании

148–275 тыс. руб. составляет стоимость системы для уничтожения данных с жёстких дисков

6–16 тыс. руб. стоят защищённые флэш-накопители компании

На пятый год существования компании Евгений решил открыть собственное производство. Первоначальные инвестиции – несколько сотен тысяч рублей – Евгений взял из оборотного капитала дистрибуционного бизнеса. На них предприниматель арендовал офис 15 кв. м и помещение 10 кв. м в подвале для цеха; собрал команду из четырёх инженеров и закупил первую партию отечественных комплектующих. Партнером по бизнесу стала супруга – Ольга Цацура, которая с тех пор выступает «переводчиком» между клиентами и инженерами «Самурая».

Штырь на всю катушку

Идею создания системы для экстренного уничтожения данных Евгению Цацуре подсказал один из клиентов в 2004 году. На тот момент данные можно было удалить только физическим воздействием – жёсткий диск протыкался металлическим штырём. Цацура решил разработать технологию, которая позволяла уничтожать информацию «цивилизованно», с помощью электромагнитного импульса. Подобные технологии уже существовали в военном сегменте, но не были распространены на гражданке. «*Поступил заказ с предоплатой,* – вспоминает Ольга Цацура. – *Мы подумали: ничего себе – столько денег – 5 тысяч долларов! Оставалось их отработать. Ребята сидели трое суток подряд без сна, а я носила им кофе и бутерброды*». «*Представьте, что у вас на тарелке рисунок из риса – если тарелку тряхнуть, то рисунок пропадет, хотя сам рис никуда не денется,* – приводит пример Цацура. – *Так же происходит и с намагниченными областями диска – после направленного электромагнитного импульса первоначальный уникальный рисунок исчезает, восстановить его нельзя*». Разработанный прибор представлял собой электромагнитный излучатель, который монтируется в корпус системного блока компьютера прямо над жёстким диском. В случае отключения электричества устройство работает от аккумулятора в течение 48 часов. Подать устройству сигнал об уничтожении данных можно несколькими способами: нажать кнопку под столом, на автомобильном брелоке или отправить СМС с уникальным кодом. Возможно и автоматическое уничтожение данных в случае несанкционированного проникновения в помещение, в котором находится компьютер. «*При тестировании устройства мы обнаружили, что электромагнитный импульс буквально отрывает головки жёстких дисков*», – говорит Николай Хозяйнов, генеральный директор компании R-Lab, специализирующейся на защите информации.

Цацура говорит, что система экстренного уничтожения данных – товар штучный и подстраивается под каждого клиента индивидуально. Цена вопроса – от 148 тыс. до 275 тыс. руб. за систему. Ежемесячно устанавливается около 15 подобных систем (за 2014 год продано 210 систем).

Свою разработку назвали «Самурай». Разработчики посчитали, что это название хорошо отражало концепцию технологии, которая, как и японский воин, должна защищать хозяина ценой своей жизни. Спустя несколько месяцев супруги Цацура поняли, что этот бренд показался удачным не только им – запрос в поисковике выдавал несколько десятков видов продуктов и услуг с аналогичным названием. Так, «Самурай» превратился в «Самурая 24».

Хозяйнов из R-Lab подтверждает, что система «Самурая» уничтожает данные безвозвратно. «К нам часто приходят клиенты с просьбой посмотреть их очищенные жёсткие диски. Практически во всех случаях мы с легкостью могли восстановить всю информацию, – рассказывает он. – Мы проверяли «Самурай 24» на собственных дисках, хорошо защищённых от внешнего воздействия, но после электромагнитного импульса на них ничего не сохранилось, хотя мы несколько дней пытались восстановить данные».

Большинство клиентов используют «Самурай 24» не из-за боязни рейдерского захвата бизнеса или обыска компетентных органов: намного чаще оно востребовано во вполне мирных целях. Сотрудники банков, медицинских клиник, научных организаций часто работают с персональными данными или секретной информацией, которая не может попасть третьим лицам. Простое стирание данных не позволяет полностью уничтожить данные, поэтому прежде чем утилизировать жёсткие диски, информация на них должна быть уничтожена. «*Способы утилизации бывают разными, но, как мне кажется, наиболее „экологически чистое“ решение – это электромагнитный импульс*», – считает директор по информационно-технологическим проектам Modulbank Илья Титов. «*Иногда данные важнее уничтожить, чем сохранить*», – резюмирует Евгений Цацура. Он не раскрывает клиентов, купивших «Самурай 24».

Защита от паяльника

Но самый популярный товар «Самурая» – не дорогие системы уничтожения данных на жёстком диске, а защищённые флэшки. По словам Ольги Цацура, идея их разработки родилась почти случайно. Сотрудник компании-клиента вынес из офиса флэшку с важной информацией, работать с которой по регламенту можно было только на рабочем месте. В этот же вечер у клиента украли сумку вместе с этой флэшкой. В результате в «Самурае» решили создать внешний накопитель с защитным кодом – кнопки располагаются прямо на корпусе флэшки, код программируется во время первого использования гаджета. После пяти безуспешных попыток ввести пароль информация безвозвратно удаляется. «*Дальше был азарт – ребята думали: а что, если данные настолько важны, что их владелец может оказаться в опасности? Что если к нему придут с паяльником?*» – вспоминает Ольга. Так появилась функция «пароль под принуждением»: есть возможность назвать запасной код, который либо откроет область флэшки без ценных данных, либо автоматически удалит всю информацию на ней.

В «Самурае» понимали, что продать свои разработки без привлекательной упаковки будет очень сложно. Спаяв платы для первой партии флэшек «с секретом», инженеры компании обмотали их термоусадкой – получился кустарный корпус с USB-входом. Себестоимость флэшки составила около 2 тыс. руб. В таком виде постоянные клиенты «Самурая» раскупили три десятка устройств, но о том, чтобы выводить их в таком виде в розничную продажу, речи быть не могло. Евгений Цацура обратился в одну из московских фирм, специализирующихся на промышленном дизайне, с заказом на разработку внешнего вида флэшек. Счёт на 1,5 млн руб. поверг его в шок, и он нашел фрилансера, сделавшего макет за 40 тыс. руб. Пластик заменили на алюминий. Пробную партию в 1,5 тыс. шт. (из пластика) отлили на одном из крупных заводов, но из-за неточностей пресс-формы кнопки не нажимались. «*На заводе нам предложили поковырять отверткой и срезать лишнее ножом, чем мы и занимались всей командой в течение нескольких дней*», – рассказывает Евгений. Эту партию флэшек Цацура продавал через небольшие интернет-магазины по цене 8 тыс. руб. Продажи шли вяло. Проведя опрос на своей странице на habrahabr.ru, Евгений выяснил, что оптимальная для покупателей цена держится в районе 3 тыс. руб. Цацура решил снизить цены, увеличив объёмы производства. Продажи взлетели, но через несколько месяцев на компанию посыпались жалобы о браке (бракованными оказались около 20 % флэшек). Тогда он принял решение предоставлять пожизненную гарантию на свою продукцию. «*К нам подходили люди на выставках, хвалили продукт, но жаловались, что флэшка вышла из строя,* – говорит Евгений. – *Мы раздавали новые прямо там, не спрашивая документов и чека*».

Новому продукту решили дать иное название – GuardDo (от английского «guard» – охранник и «do» – действие). Сейчас защищённые флэш-карты «Самурая 24» представлены в трёх вариантах: первое, самое простое, поколение оснащено защитным кодом, второе защищает карту от принудительной записи или стирания информации (актуально, если придётся вставлять флэшку в чужой компьютер), в третьем есть функция «пароль под принуждением» и специальная магнитная метка, которая не позволяет вынести флэшку из помещения. Флэшек и внешних дисков «с секретом» «Самурай» продает в месяц около 600 штук по цене от 6 до 16 тыс.

«*Полное уничтожение данных, когда на жёстком диске байт за байтом пишутся сплошные нули – дело довольно долгое, и если компания дорожит своими данными и репутацией, ей будет неплохо обзавестись подобным девайсом,* – считает Дмитрий Кузнецов, глава отдела „Оборудование и сети“ группы компаний „Компэл“. – *Большинство крупных компаний хранят базы в удалённых дата-центрах и не могут обеспечить защиту доступа к носителям. Чёрт его знает, кто в Голландии сегодня моет полы в серверной. И защитить данные стоимостью в миллионы долларов и репутацию компании ценой пары жестких дисков – дело правое*». По словам Кузнецова, целевая аудитория такого сервиса может быть очень широкой. «*Налоговики настолько разуверились в „белых“ компаниях, что при проверках подметают всё: ноутбуки, кипы бумаг, стикеры с мониторов,* – отмечает он. – *Полное отсутствие информации – неплохой выход из ситуации*». Эксперт предлагает «Самураю» разработать «Самурай 24» для мобильных устройств – ноутбуков, планшетов и телефонов, поскольку всё большую часть деятельности предприниматели ведут не за стационарными компьютерами.

GUARD'DO

«Самурай24»

www.samurai24.ru

«Транскапиталбанк» внедрил Netwrix Auditor for Active Directory для контроля ИТ-инфраструктуры

Компания Netwrix успешно завершила проект внедрения Netwrix Auditor for Active Directory в целях контроля ИТ-инфраструктуры «Транскапиталбанка». Система обеспечивает оперативное выявление и реагирование на инциденты, возникающие в сфере информационной безопасности, что существенно повышает управляемость ИТ-инфраструктуры в целом.

«Транскапиталбанк» работает на рынке финансовых услуг с 1992 года и стабильно входит в топ-50 крупнейших и топ-30 самых надёжных российских банков. В целях обеспечения безопасности хранения данных банк уделяет большое внимание защите своей ИТ-инфраструктуры с учётом принятых в финансовых системах стандартов ИБ.

Ситуация

Необходимость контроля действий выделенных пользователей и оповещения об изменениях в Active Directory и групповых политиках

Обслуживание ИТ-инфраструктуры банка выполняется коллективом специалистов с разными административными полномочиями и сферами ответственности, действия которых тесно связаны между собой.

«*Мы сталкивались с ситуациями, когда изменение в Active Directory, внесённое одним из администраторов, вызывало определенный сбой работы бизнес-приложений или служб, за которые отвечал другой технический специалист. Мы пробовали решать проблему на административном уровне, для чего был разработан соответствующий регламент согласования проведения технических работ. Однако потребность в автоматизированном инструменте, фиксирующем изменения в Active Directory и групповых политиках, а также оперативно оповещающем об этом, продолжала оставаться актуальной*», – отмечает Олег Ржевский, заместитель начальника управления технической поддержки «Транскапиталбанка».

Решение

Netwrix Auditor for Active Directory для контроля ИТ-системы в режиме онлайн

Процесс выбора решения проходил в несколько этапов. Изначально специалисты «Транскапиталбанка» рассматривали вариант использования встроенных средств Windows для аудита объектов Active Directory и журналов событий на контроллерах домена. Но вскоре стало понятно, что этих данных недостаточно. В ходе тестирования выяснилось: стандартные средства аудита не предоставляют полную информацию об изменениях, а именно не отображают состояние объекта до модификации, что усложняет процесс оперативного восстановления работы приложений.

«*Один из моих коллег прислал статью о продуктах Netwrix. Нас привлёк тот факт, что Netwrix Auditor не устанавливает дополнительное программное обеспечение на контроллеры домена, полагаясь исключительно на штатные функции аудита. Недостающую информацию Netwrix Auditor for AD получает посредством периодического создания снапшотов – моментальных снимков AD*», – комментирует Олег.

На заключительном этапе был запущен пилотный проект с использованием пробной версии решения Netwrix Auditor for Active Directory (ранее Netwrix Active Directory Change Reporter), которое обладает всеми функциями коммерческого программного обеспечения. По окончании тест драйва была развернута полнофункциональная версия продукта, что не потребовало больших временных и трудовых затрат.

Результат

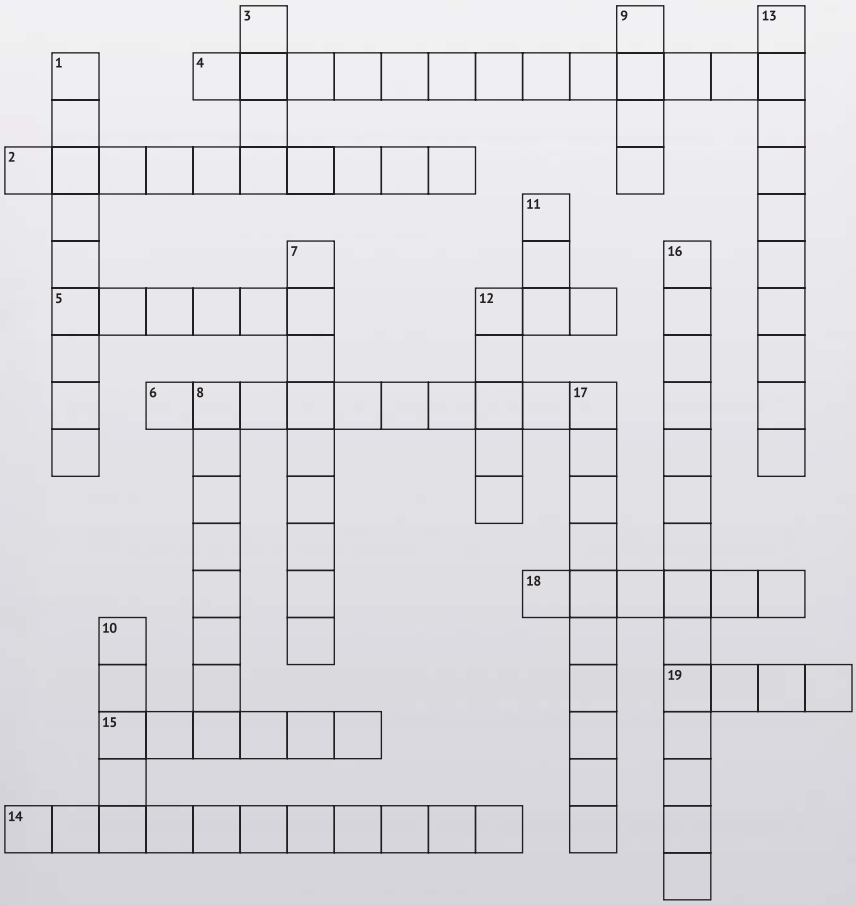
Оперативное выявление инцидентов информационной безопасности, непрерывность бизнес-процессов

Использование программных продуктов Netwrix позволяет получать максимально полную картину состояния ИТ-системы в определённые периоды. Появляется возможность не только отслеживать изменения в инфраструктуре или отдельных приложениях, но и иметь представление о доступе к корпоративной информации, отслеживать историю работы с файлами. Средства аудита Netwrix позволяют получать оповещения об изменениях в режиме реального времени, что снижает нагрузку на ИТ-отделы, позволяет избежать ненужных рисков и сбоев в работе.

«*Проект по внедрению Netwrix Auditor оправдал наши ожидания. Теперь администраторы, работающие с AD, находятся в курсе всех изменений. Каждое планируемое действие становится более взвешенным и ответственным*», – заключил Олег Ржевский.

Кроссворд с призами!

Первые 50 человек, приславшие разгаданный кроссворд, получат приз – годовую лицензию на антивирус Grizzly Pro!



По вертикали:

1. CPU.

3. Сетевой информационный ресурс.

7. Оператор связи.

8. Команда перенаправления.

9. Программа для модернизации.

10. Вредоносная программа.

11. Персонаж из м/ф «Аладдин» с потребностью везде доминировать и постоянно искать выгоду.

12. Имя пользователя.

13. Программа для ЭВМ.

16. Процедура проверки подлинности.

17. Сведения.

По горизонтали:

2. Устройство соединения фреймов.

4. Устройство, пересылающее пакеты между различными сегментами сети.

5. Программа для сбора, просмотра и анализа всего проходящего трафика.

6. Технические права учётной записи.

12. Журнал регистрации событий.

14. Набор данных для установки программы.

15. Вид вредоносной программы.

18. Количество информации, переданное по цифровой линии связи.

19. Команда, отдаваемая нажатием кнопки мыши.

Приз ждёт вас!

Разгаданный кроссворд присылайте на почту ниже в любом удобном для вас виде.
info@sovinfosystems.ru

Календарь мероприятий

24–26 ноября
Санкт-Петербург • Хакатон
Всероссийский хакатон neuromedia 2017 по разработке продуктов на стыке информационных технологий, медиа и нейронных сетей
a.baranova@spb.gs.ru

24 ноября
Москва • Конференция
Droidcon Moscow 2017
smitrjakova@apps4all.ru

25 ноября
Минск • Конференция
Smart Taler 2017
smart-taler.by

25–26 ноября
Москва • Выставка
Robotics Expo 2017
goo.gl/4QfMiw

25 ноября
Москва • Конференция
Ladies Code: время технологий
ok@zucker.studio

28–30 ноября
Екатеринбург • Выставка
Выставки по автоматизации и электронике «ПТА-Урал 2017» и «Электроника-Урал 2017»
www.pta-expo.ru

28 ноября
Москва • Конференция
Криптоконференция 2017
pr@cryptoconf.su

28 ноября
Новосибирск • Курс
Курсы Тестирования ПО
academ@suhorukov.com

29 ноября
Москва • Конференция
Технологии баз данных. Практическая конференция
kon@osp.ru

29 ноября
Москва • Конференция
Russian Startups Go Global 2017
iidf.vc/goglobal/2017

30 ноября
Москва • Форум
Федеральный форум «Smart Cars & Roads – цифровая трансформация экосистемы «автомобиль-дорога» в Российской Федерации»
ns@comnews.ru

30 ноября
Москва • Конференция
Вторая международная конференция ISPRAS Open 2017
an@ispras.ru

30 ноября
Вебинар
Изменения в ИТ-подразделении при движении в сторону DevOps
a.lipova@cleverics.ru

1 декабря
Екатеринбург • Конференция
CONVERT.2017
ekaterina@it-people.ru

4 декабря
Курс
Курс веб-разработки (front-end)
academ@suhorukov.com

8–9 декабря
Москва • Конференция
Гейзенбаг 2017 Moscow – конференция по тестированию
zeller@krasfair.ru

9 декабря
Киев • Конференция
BACon AllStars – конференция бизнес-аналитиков
arthur.seletskiy@gmail.com

9–10 декабря
Киев • Конференция
Games Gathering 2017
alexander.khrutsky@gmail.com

9–10 декабря
Санкт-Петербург • Тренинг
1 модуль курса «Руководство проектами в IT»: Модели, стандарты и методологии проектного управления в области информационных систем
s.orlova@scout-gps.tu

9 декабря
Санкт-Петербург • Курс
Руководство проектами в области информационных-технологий
Организатор: JUG.ru Group
s.orlova@scout-gps.ru

9 декабря
Москва • Конференция
Лекционный день по игровой индустрии в ВШБИ
gamedevday.hsbi.ru

10–11 декабря
Москва • Конференция
HolyJS 2017 Moscow – конференция для JavaScript-разработчиков
tickets@holyjs.ru

10 декабря
Санкт-Петербург • Тренинг
Рабочая документация тестировщика
academy.scout-gps.ru/events/tester/

14 декабря
Санкт-Петербург • Конференция
Первый IoT-Forum в Санкт-Петербурге
iotforum2017@gmail.com

18 декабря
Санкт-Петербург • Курс
Системный и бизнес анализ в разработке ПО. Интенсивный курс
info@levelp.ru

19 декабря
Москва • Конференция
Moneymakers
ms@moneymakers.events

13–14 января
Санкт-Петербург • Тренинг
2 модуль курса «Руководство проектами в IT»: Подготовка проекта
s.orlova@scout-gps.ru

16 января
Тренинг
Тренинг по тестированию ПО
academ@suhorukov.com

20–21 января
Санкт-Петербург • Тренинг
Недирективные коммуникации
s.orlova@scout-gps.ru

17–18 февраля
Санкт-Петербург • Тренинг
3 модуль курса «Руководство проектами в IT»: Управление требованиями
s.orlova@scout-gps.ru

20 февраля
Санкт-Петербург • Конференция
VI Ежегодная Конференция День Информационных Технологий
solomina@svega-computer.ru

ОЛЛИ
ДИСТРИБУЦИЯ

Дистрибуция «облачных» технологий

Компания «ОЛЛИ» специализируется на дистрибуции «облачных» технологий, поставке программного и аппаратного обеспечения в сегменте B2B: продуктов для построения платформ виртуализации серверов, приложений, рабочих станций и продуктов, обеспечивающих эффективную работу пользователей с виртуальными окружениями.

Благодаря многолетнему опыту работы на рынке виртуализации, «ОЛЛИ» является экспертом и обладает высоким уровнем компетенции в данной области. Оказывает техническую поддержку в виде предпродажных консультаций и реализации пилотных проектов для заказчиков партнёров, проводит обучение и сертификацию специалистов, считает важным защищать инвестиции своих партнёров в проекты, регулярно организует маркетинговые программы и мероприятия.

CITRIX® ThinPrint® Atrust atlantis COMPUTING Parallels®

userful™ netwrix® zscaler® SEH

ОЛЛИ
ДИСТРИБУЦИЯ

+7 (812) 703-30-69 +7 (495) 139-89-60 disti@ollyit.ru www.ollyit.ru