CIS
Современные Информационные Системы
№ 1 (15) / 2021

ВСЁ ВНИМАНИЕ ЗАЩИТЕ СЕТЕЙ

Стр. 58

Екатерина Чурзина
Руководитель проектов

Аутентификация как она есть

Стр. 32

Анатолий Лебедев
доцент МГТУ им. Н. Э. Баумана

Женщины в IT

Стр. 48

В сферах ИТ и ИБ становится всё больше и больше женщин

Защитите свой бизнес

Стр. 4

при помощи надёжной и безопасной беспарольной аутентификации

ПРЕДИСЛОВИЕ

ПРОДУКТЫ

АНАЛИТИКА

РЕШЕНИЯ

ТЕХНОЛОГИИ

ОПЫТ

СТАНДАРТЫ

ИТ-ГОРОСКОП

СОБЫТИЯ

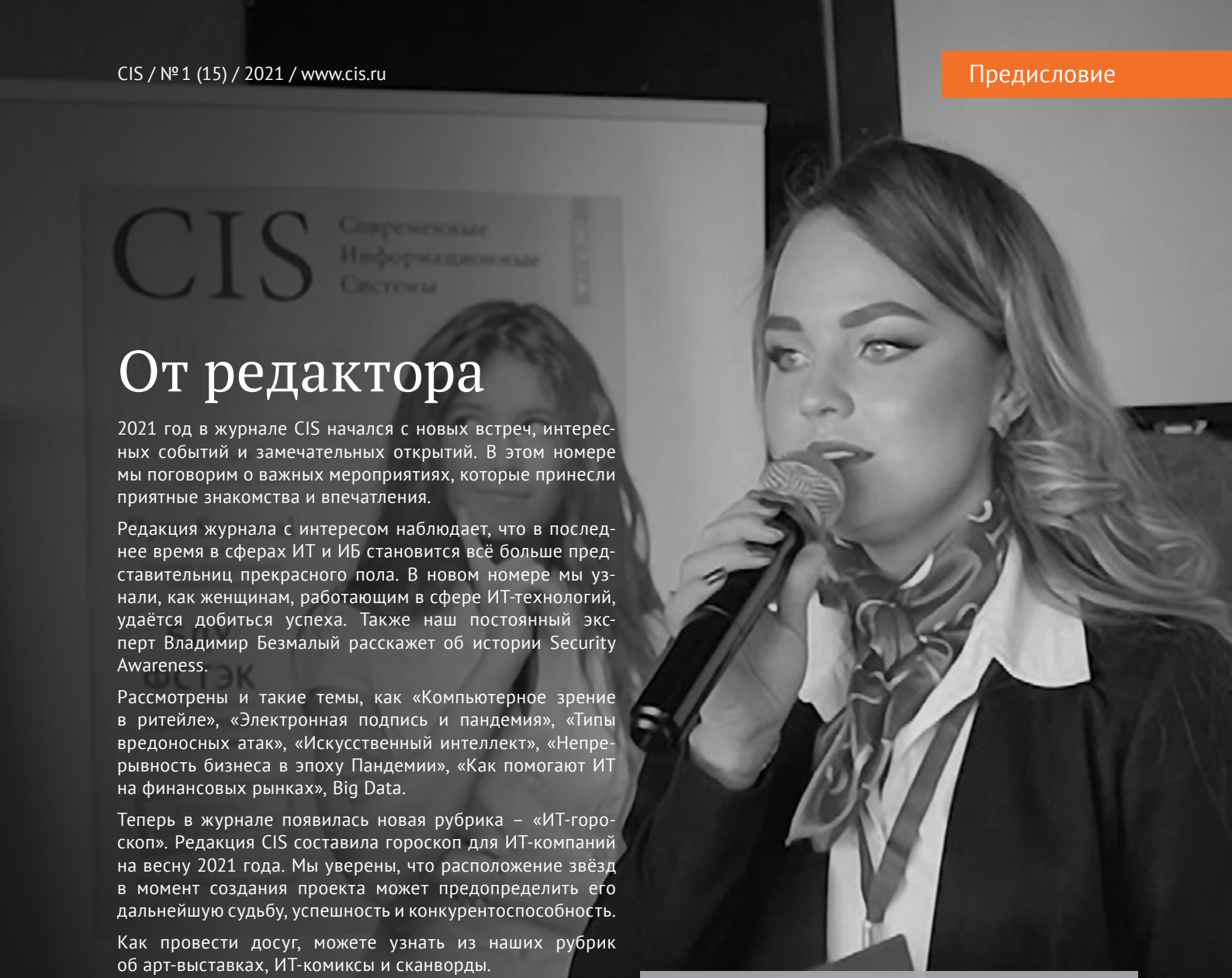
ФОТООТЧЁТ

КУЛЬТУРА

КОМИКСЫ

КАЛЕНДАРЬ

КРОССВОРД



От редактора

2021 год в журнале CIS начался с новых встреч, интересных событий и замечательных открытий. В этом номере мы поговорим о важных мероприятиях, которые принесли приятные знакомства и впечатления.

Редакция журнала с интересом наблюдает, что в последнее время в сферах ИТ и ИБ становится всё больше представительниц прекрасного пола. В новом номере мы узнали, как женщинам, работающим в сфере ИТ-технологий, удаётся добиться успеха. Также наш постоянный эксперт Владимир Безмалый расскажет об истории Security Awareness.

Рассмотрены и такие темы, как «Компьютерное зрение в ритейле», «Электронная подпись и пандемия», «Типы вредоносных атак», «Искусственный интеллект», «Непрерывность бизнеса в эпоху Пандемии», «Как помогают ИТ на финансовых рынках», Big Data.

Теперь в журнале появилась новая рубрика – «ИТ-гороскоп». Редакция CIS составила гороскоп для ИТ-компаний на весну 2021 года. Мы уверены, что расположение звёзд в момент создания проекта может предопределить его дальнейшую судьбу, успешность и конкурентоспособность.

Как провести досуг, можете узнать из наших рубрик об арт-выставках, ИТ-комиксы и сканворды.

С радостью сообщаем, что редакция нашего журнала запустила курсы в Учебном центре CIS. Курсы организованы для специалистов и компаний, работающих в сфере защиты информации. В ходе обучения все желающие получат теоретические знания и научатся создавать надёжные центры информационной безопасности в своей компании.

В начале года ИТ-журнал CIS «Современные Инфосистемы» и клуб ИТ-директоров «я-ИТ-ы» организовали мероприятие «День открытых дверей». Нам удалось в неформальной обстановке продемонстрировать гостям возможности совместного сотрудничества и рассказать о планах на будущее. Участников пригласили на одну из лучших площадок Москва-сити. Отметим, что гости высоко оценили уровень организации бизнес-встречи. В разделе «Фотоотчёт» можно увидеть, как прошёл этот день. Для проведения подобного мероприятия в своей компании, обращайтесь в нашу редакцию.

А ещё у нас отличная новость: конкурс красоты «Beauty & DigITal – 2021» – открылся! В нём примут участие девушки из сферы ИТ и информационной безопасности со всей России. Сайт конкурса – **www.cismiss.ru**.

Также напоминаем об одном из важных событий предстоящего года. Журнал CIS проведёт ИТ-мероприятие в поддержку Фонда Константина Хабенского. Мы будем благодарны всем за активное участие в помощи детям с заболеваниями головного и спинного мозга.

С уважением,
редакция журнала CIS.

Главный редактор: Станислав Понарин.
Фотограф: Нина Жиленкова.
Корректор: Оксана Макаренко.
Отдел рекламы и распространения: info@sovinfosystems.ru.
Сайт: www.cis.ru, интернер-блог: www.cismag.news.
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: 22-й км Киевского ш., (п. Московский), домовладение 4, стр. 1, кор. Б, офис 04, блок 904Б, г. Москва, 108811.
Язык: русский.
Периодичность: 4 раза в год (1 раз в квартал).

Фото на обложке: Екатерина Чурзина.
Тираж 5000 экз. (отпечатанный тираж).
Журнал предназначен для лиц старше 16 лет.

Устройства SafeNet FIDO2

Защитите свой бизнес при помощи надёжной и безопасной беспарольной аутентификации

Вступая в новое десятилетие и внедряя все больше цифровых и облачных технологий, компании сталкиваются с утечками информации, большая часть которых связана с хищением персональных данных. Поэтому многие организации инвестируют в надёжные системы аутентификации, в том числе на основе инфраструктуры открытых ключей (PKI).

Сегодня перед этими же организациями стоит задача обеспечения безопасности в рамках новых сценариев работы – без ущерба для удобства.

Как компаниям обеспечить незаметный и простой вход в систему со всех устройств без паролей? Как эффективно работать в новых условиях, не отбрасывая полностью привычные методы аутентификации? Чтобы помочь решить эти задачи, компания Thales, мировой лидер в области цифровой безопасности, отвечает на эти вопросы, выпуская два новых устройства SafeNet FIDO2: смарт-карту SafeNet IDPrime 3940 FIDO и USB-токен SafeNet eToken FIDO. Новые продукты позволят организациям безопасно переходить на облачные технологии и защищать доступ в гибридные среды с помощью интегрированных функций управления доступом и аутентификации.

Беспарольная аутентификация

Беспарольная аутентификация для подтверждения учётных данных использует вместо пароля иные методы, которые повышают её надёжность и обеспечивают простоту. Такой способ аутентификации получил широкое распространение благодаря значительному упрощению входа в систему для пользователей и отсутствию естественных недостатков текстовых паролей. При этом методе наблюдается меньшее число проблем со входом, он даёт более высокий уровень безопасности для каждого приложения и устраняет проблему устаревания паролей.

Удобство для пользователей PKI

Одно из самых больших преимуществ нового решения состоит в том, что теперь компании, использующие PKI- аутентификацию и находящиеся в процессе цифровой и облачной трансформации, могут пользоваться комбинированной смарт-картой PKI-FIDO, предоставляя пользователям единое устройство аутентификации как для безопасного входа в прежние версии приложений, так и для доступа к сетевым доменам и облачным сервисам.

Единое устройство с поддержкой FIDO2 и PKI

Смарт-карта SafeNet IDPrime 3940 FIDO разработана для приложений на основе PKI и поставляется вместе с мини-драйвером, который обеспечивает беспроблемную интеграцию в существующие системы, в том числе встроенную поддержку сред Microsoft® без какого-либо промежуточного ПО.

Поддерживая связь как через контактный, так и через бесконтактный интерфейс ISO14443, эта смарт-карта также совместима с некоторыми NFC-сканерами.

Смарт-карта SafeNet IDPrime 3940 FIDO имеет сертификацию CC EAL5+/PP для Java-платформ и сертификацию CC EAL5+/PP QSCD для сочетания Java-платформы с PKI-апплетом. SafeNet IDPrime 3940 сертифицирована Национальным агентством кибербезопасности Франции, а также соответствует регламенту eIDAS в отношении приложений электронной подписи и электронной печати. Кроме того, SafeNet IDPrime 3940 FIDO поддерживает стандарты FIDO 2.0 и U2F.

USB-токен с сенсорными функциями

SafeNet eToken FIDO – это USB-токен, который идеально подойдёт компаниям, желающим ввести беспарольную аутентификацию сотрудников. Это компактное USB- устройство с контролем вскрытия и функцией обнаружения присутствия, которая представляет собой третий фактор аутентификации, – наряду с наличием самого физического токена и известного только вам PIN-кода.

Основные преимущества

Устройства SafeNet FIDO2 обеспечивают надёжную и безопасную беспарольную аутентификацию в любой среде.

Среди основных преимуществ этой технологии:

- Безопасность в период перехода на облачные технологии и защищённый доступ в гибридные среды благодаря комбинированной смарт-карте PKI/FIDO
- Безопасный и простой доступ в различные операционные системы
- Доступ к облачным приложениям и сетевым доменам без пароля
- Отсутствие необходимости в отказе от существующей схемы PKI-аутентификации
- Единое средство аутентификации для всех нужд пользователей
- Сертификация по стандарту CC
- Поддержка всех устройств и операционных систем (без промежуточного ПО)
- Возможность настройки всех необходимых параметров
- Идеальное решение для электронных подписей и шифрования электронной почты

Характеристики	**Смарт-карта SafeNet IDPrime 3940 FIDO** 
Память	• Карта SafeNet IDPrime 3940 разработана на основе микросхемы памяти Java Flash 400 Кбайт. Стандартная карта SafeNet IDPrime 3940 FIDO содержит 20 ключевых контейнеров. • Доступно 73 Кбайта памяти, которая может использоваться для хранения сертификатов и других апплетов и данных.
Стандарты	• Мини-драйвер BaseCSP (мини-драйвер SafeNet) • Global Platform 2.21 • Java Card 3.0.4 • ISO 7816 и ISO 14443 • Сертификаты FIDO 2.0 и U2F
Операционные системы	• Приложение FIDO поддерживается Windows 10 и другими совместимыми с FIDO операционными системами. • Приложения PKI-стандарта поддерживаются в Windows, MAC OS X и Linux.
Криптографические алгоритмы	• Хеш: SHA-1, SHA-256, SHA-384, SHA-512. • RSA: до 4096 бит • RSA OAEP и RSA PSS • ECDSA P-256, ECDH. ECDSA P-384 и P-521, ECDH доступны в пользовательских конфигурациях • Генерация асимметричных пар ключей на карте (RSA до 4096 бит и эллиптические кривые до 521 бита) • Симметричные: AES для безопасного обмена сообщениями и 3DES только для Microsoft Challenge/Response
Протоколы связи	• T=1, T=0, PPS, скорость передачи данных до 446 Кбит/с при 3,57 МГц (TA1=97 ч) • T=CL, ISO 14443, Type A, скорость до 848 Кбит/с
Другие характеристики	• Политика встроенного PIN-кода • Поддержка нескольких PIN-кодов • Карты SafeNet IDPrime настраиваются в зависимости от потребностей клиента (физическая конфигурация и программная часть).
Характеристики микросхемы	
Технология	• Встроенный механизм симметричной и асимметричной криптографии
Срок службы	• Минимум 500 000 циклов записи и стирания • Хранение данных минимум 25 лет
Сертификация	• CC EAL6+

Безопасность	• Смарт-карты SafeNet IDPrime имеют множество аппаратных и программных средств противодействия различным атакам — атакам по сторонним каналам, инвазивным атакам, продвинутым атакам на недочеты и другим. • SafeNet IDPrime 3940 FIDO — это одновременно Java-карта CC EAL5+/PP, сертифицированная для Java-платформ, и карта CC EAL5+/PP QSCD для сочетания Java-платформы с PKI-апплетом. Она соответствует стандартам eIDAS для электронных подписей и электронных печатей, а также отвечает требованиям Национального агентства кибербезопасности Франции.

Характеристики	**Электронный токен SafeNet FIDO** 
Память	• 80 Кбайт
Стандарты	• Поддержка API и стандартов: FIDO 2.0 и U2F
Операционные системы	• Приложение FIDO поддерживается Windows 10 и другими совместимыми с FIDO операционными системами.
Физические характеристики	
Размеры	• 6 x 8 x 40,5 мм
Температура эксплуатации	• от 0 до 70 °C
Температура хранения	• от -40 до 85 °C
Влажность	• от 0 до 100 % без образования конденсата
Сертификат влагозащищённости	• IP X7 (IEC 529)
USB-разъем	• USB Type-A; поддержка USB 1.1 и USB 2.0 (Full-Speed и Hi-Speed)
Корпус	• Жёсткий формованный пластик, контроль вскрытия
Срок хранения данных	• Минимум 10 лет
Перезапись ячеек памяти	• Минимум 500 000 раз
Карта SafeNet IDPrime 3940 FIDO и электронный токен SafeNet FIDO совместимы с учетными записями Microsoft Azure Active Directory.	

Indeed Privileged Access Manager

Управление доступом к привилегированным учётным записям

Привилегированный доступ – угроза безопасности

Постоянное наращивание и усложнение ИТ-инфраструктуры компаний делает управление привилегированными учётными записями одной из важнейших задач информационной безопасности. Увеличивающееся количество информационных систем и разнообразие сценариев доступа к ним затрудняют решение этой задачи. Получив данные административной учётной записи, злоумышленник может нанести предприятию намного более серьёзный ущерб, чем в случае компрометации учётных данных рядового сотрудника. Административные учётные записи могут быть использованы для отключения защиты, остановки работы информационных систем и доступа к конфиденциальной информации. Защитить привилегированный доступ сложнее, решение этой проблемы невозможно с использованием общих подходов к защите учётных данных и требует применения специализированных решений.

Привилегированные пользователи

Иметь повышенные права доступа к важной информации и критичным функциям программного обеспечения и оборудования могут различные категории как штатных, так и внешних сотрудников компании.

Администраторы информационных систем

Каждое устройство и каждое прикладное или системное программное обеспечение имеют свои административные учётные записи. Это самая очевидная группа сотрудников привилегированного доступа, примерами таких сотрудников являются:

- администраторы Active Directory;
- администраторы сетевого оборудования;
- администраторы баз данных;
- администраторы серверов (Windows, Unix/Linux);
- администраторы VDI.

Бизнес-пользователи

Бизнес-пользователи хоть и не обладают административным доступом, но могут иметь широкие полномочия в рамках отдельно взятых информационных систем. Например, они могут иметь возможность выполнять денежные переводы, управлять производственным процессом и получать доступ к коммерческой тайне.

Подрядчики и партнёры

Сотрудники подрядчиков, как правило, выполняют сопровождение специализированных программных и аппаратных комплексов. Это могут быть, например, сотрудники вендора или интегратора. Обычно такие пользователи имеют удалённый доступ в инфраструктуру предприятия, что дополнительно осложняет контроль их работы.

Служебные учётные записи

Служебные учётные записи используются для различной автоматизации процессов. От их имени работают различные службы и демоны, скрипты и другое программное обеспечение. Про такие учётные записи легко забыть, т. к. сотрудники не используют их в явном виде каждый день. Это создаёт дополнительные трудности по управлению ими.

Indeed Privileged Access Manager

Продукт Indeed Privileged Access Manager (Indeed PAM) представляет собой систему управления доступом с использованием привилегированных учётных записей. В основе продукта лежит многолетний опыт компании «Индид» по созданию продуктов в области информационной безопасности. Основные решаемые задачи этого продукта следующие:

- регистрация попыток использования привилегированных учётных записей в журнале доступа с указанием, какой сотрудник, когда и к какой учётной записи получал доступ;
- ведение видео и текстовой записи привилегированных сессий с возможностью просмотра архива сессий;
- обеспечение мультифакторной аутентификации сотрудников при доступе к привилегированным учётным записям;
- хранение паролей привилегированных учётных записей в секрете от сотрудников, регулярная смена паролей на случайные значения.

Indeed PAM состоит из нескольких функциональных и логических модулей.

Политики и разрешения

Политики и разрешения определяют параметры привилегированного доступа:

- кому предоставлен доступ;
- к каким учётным записям предоставлен доступ;
- к каким ресурсам (серверам и оборудованию) предоставлен доступ;
- на какое время (постоянно/временно, в рабочие часы или в любое время);
- какую запись сессий нужно производить (видео и текстовую запись, только текстовую, скриншоты и т. п.);
- какие локальные ресурсы (диски, смарт-карты) будут доступны пользователю в удалённой сессии;
- разрешено ли пользователю просматривать пароль привилегированной учётной записи.

Централизованные политики сокращают затраты на администрирование системы и делают параметры и права доступа прозрачными для специалистов информационной безопасности и аудиторов.

Хранилище привилегированных учётных данных

Учётные данные, необходимые для доступа (логины, пароли, SSH-ключ), хранятся в хранилище, к которому имеет доступ только сервер Indeed PAM. Хранение и передача данных к/от сервера производится в зашифрованном виде с применением стойких алгоритмов шифрования. Доступ к хранилищу ограничен и возможен только для сервера PAM, для реализации этого подхода применяется специальная процедура по «запечатыванию» сервера-hardening сервера базы данных.

Подсистема записи сессий

Все сеансы привилегированного доступа записываются в обязательном порядке и сохраняются в архиве Indeed PAM. В архиве записи хранятся в зашифрованном виде, получить к ним доступ возможно только обладая соответствующими полномочиями в рамках системы PAM. Записи ведутся в следующих форматах:

- Текстовая запись ведётся всегда и фиксирует такие данные:
  - полный ввод и вывод консоли в SSH-подключениях;

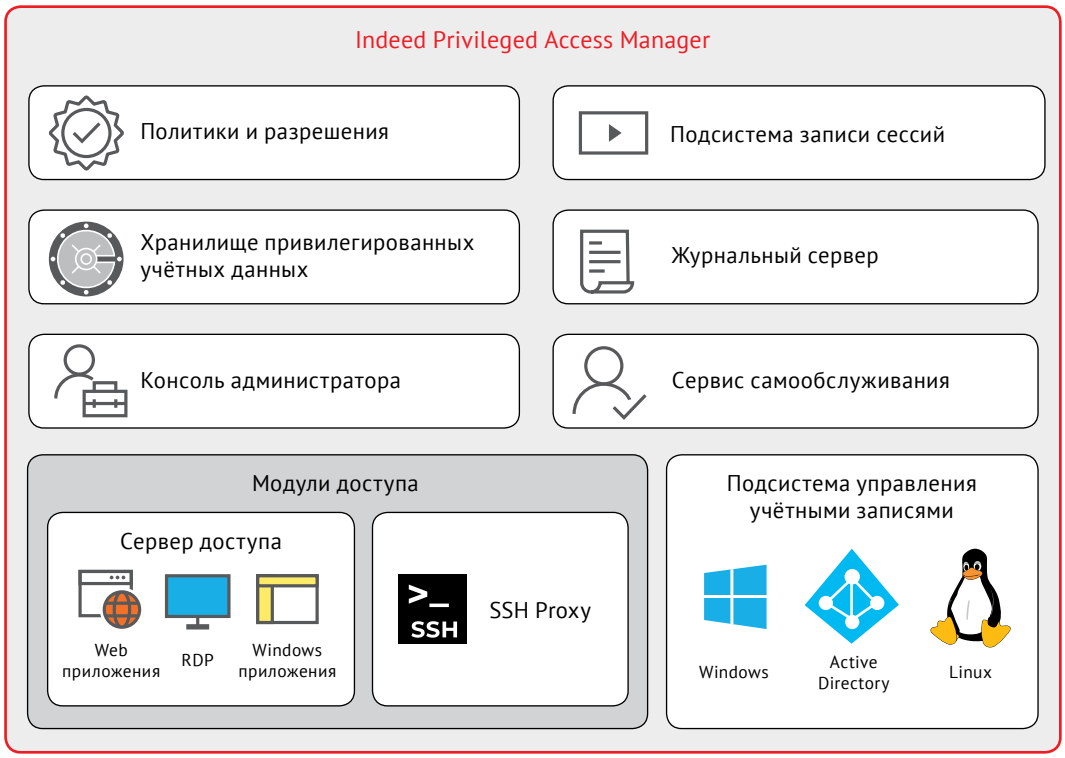


Рисунок 1. Структура Indeed Privileged Access Manager

- все запускаемые процессы, открываемые окна и клавиатурный ввод для RDP-подключений.

- Видеозапись производится как для RDP, так и для SSH-подключений. Видеозапись не обязательна, её включение выполняется администратором PAM с помощью механизма политик. Качество видео настраивается и может быть разным для различных учётных записей, например сеансы администраторов домена могут записываться с максимальным качеством, а сеансы операторов – со сжатием.
- Снятие снимков экрана также производится как для RDP, так и для SSH-подключений.

Сохранение снимков экрана не обязательно, его включение выполняется администратором PAM с помощью механизма политик. Частота снятия и качество снимков экрана задаётся в политиках.

Просмотр активных сессий доступен в режиме реального времени с возможностью разрыва сессии администратором PAM.

Журнальный сервер

Журнальный сервер является выделенным сервисом по сбору событий Indeed PAM. Такие события включают в себя всю активность администраторов и пользователей PAM. Журнал фиксирует, кто и какие параметры системы изменял и кто под какими учётными данными выполнял подключение к целевым ресурсам.

Для удобства интеграции в SEIM и своевременного реагирования на инциденты события могут доставляться по протоколу syslog на сторонний журнальный сервер.

Консоль администратора

Консоль администратора предоставляет интерфейс для настройки, управления и аудита работы системы и выполнена в виде web-приложения. Используя консоль, администратор предоставляет пользователям доступ к учётным данным, настраивает политики доступа и просматривает журналы событий и записи привилегированных сессий. Также консоль позволяет администраторам PAM просматривать активные привилегированные сессии в реальном времени и при необходимости прекращать сеанс работы сотрудника. Доступ в консоль администратора выполняется с помощью двухфакторной аутентификации.

Сервисы самообслуживания

Для получения привилегированного доступа сотрудники используют два инструмента:

- консоль пользователя, выполненная в виде web-приложения. В консоли пользователя сотрудники просматривают доступные им учётные записи и ресурсы, а также запускают привилегированные сессии;
- приложение на сервере доступе. С использованием этого приложения сотрудники получают доступ, минуя консоль пользователя. В этом случае сотрудник подключается напрямую к серверу доступа, где ему предлагается выбрать разрешённое подключение.

В обоих случаях доступ сотрудников защищён двухфакторной аутентификацией с помощью OTP (One-Time Password).

Модули доступа

Модули доступа предоставляют механизмы открытия и записи привилегированных сессий.

Сервер доступа

Сервер доступа реализует централизованную модель получения привилегированного доступа. Сотрудник сначала выполняет подключение к серверу доступа, на котором проверяются его права и выполняется аутентификация по второму фактору, после чего сотруднику открывается сессия на целевом ресурсе.

Сервер доступа работает на базе сервера удалённых рабочих столов Microsoft RDS (Remote Desktop Services), на котором установлено приложение Indeed PAM. Данное приложение выполняет следующие функции:

- проверяет права доступа пользователя – разрешено ли ему получать доступ под запрашиваемой учётной записью на запрашиваемый целевой ресурс;
- производит аутентификацию пользователя – перед открытием сессии пользователь обязан предоставить второй фактор аутентификации;
- ведёт видеозапись сессии и снятие снимков экрана.

Для открытия сессий в целевые системы и приложения на сервере доступа применяется следующее клиентское ПО:

- RDP-клиент Microsoft (mstsc) для доступа на Windows сервера;
- браузер для доступа в web-приложения;
- SSH-клиент PuTTY для доступа на Linux/Unix системы;
- специализированное клиентское ПО для доступа в различные информационные системы с использованием проприетарных протоколов («толстый» клиент).

SSH Proxy

SSH Proxy является альтернативным вариантом получения доступа через Indeed PAM в Linux/Unix системы. Данный метод обладает следующими преимуществами:

- не требуется использование Microsoft RDS;
- возможно использование любого SSH-клиента;
- SSH-клиент работает локально на рабочей станции сотрудника.

SSH Proxy выполняет те же функции, что и сервер доступа:

- проверяет права доступа пользователя;
- производит аутентификацию пользователя;
- ведёт видеозапись сессии и снятие снимков экрана.

При использовании SSH Proxy пользователь инициирует подключение со своего рабочего места с помощью привычного для него SSH-клиента. В качестве сервера подключения сотрудник указывает адрес SSH Proxy. При подключении к прокси у пользователя также запрашивается второй фактор аутентификации, после чего открывается сессия на целевой ресурс.

Подсистема управления учётными записями

При использовании систем класса PAM офицерам информационной безопасности важно понимать, что в инфраструктуре компании нет неучтённых привилегированных записей и доступ к ним контролируется и протоколируется. В рамках Indeed PAM эту задачу решает подсистема управления учётными записями. Подсистема выполняет следующие функции:

- периодический поиск новых привилегированных учётных записей на целевых ресурсах.

Данная мера позволяет защититься от недобросовестного администратора, который создал себе учётную запись для работы в обход системы PAM;

- периодическая проверка паролей и SSH-ключей привилегированных учётных записей.

Данная функция позволяет убедиться, что в хранилище PAM содержатся актуальные учётные данные и недобросовестный администратор не выполнил сброс пароля учётной записи для использования её в обход PAM;

- периодическая смена паролей и SSH-ключей. Indeed PAM генерирует случайные сложные пароли и SSH-ключи для контролируемых привилегированных учётных данных, защищая их от несанкционированного доступа;
- сброс пароля учётной записи после показа его пользователю. Администратор PAM может разрешить сотрудникам просматривать пароль привилегированной учётной записи в тех случаях, когда необходимо явное использование пароля. После того, как сотрудник получит пароль, через заданный промежуток времени Indeed PAM сбросит пароль в новое случайное значение.

Для выполнения указанных функций в состав подсистемы управления учётными записями входят модули подключения (коннекторы) для целевых систем:

- коннектор к Active Directory;
- коннектор к Windows и Windows Server;
- SSH-коннектор для подключения к Linux/Unix системам на базе различных дистрибутивов;
- коннектор к СУБД (MS SQL, Oracle, PostgreSQL и др.).

Основные характеристики Indeed PAM

Протоколы доступа	RDP SSH HTTP(s)
Поддерживаемые типы учётных данных	Имя пользователя + пароль SSH-ключ
Поиск привилегированных учётных записей и управление паролем	Windows Linux Active Directory СУБД (MS SQL, PostgreSQL, My SQL, Oracle и др.)
Поддерживаемые каталоги пользователей	Active Directory
Технологии двухфакторной аутентификации	Пароль + TOTP (программный генератор)
Поддерживаемые типы записи сессий	Текстовый лог Видеозапись Снимки экрана
Технологии удалённого доступа	Microsoft RDS SSH Proxy

INDEED ID

www.indeed-id.ru

Как рассчитать стоимость услуг ИТ-компании?

В контексте постоянно меняющихся условий баланс доходов и расходов не всегда легко просчитать. Во время пандемии многие ИТ-компании столкнулись с неплатёжеспособностью клиентов и были вынуждены приостановить сотрудничество. Круг потенциальных клиентов стал более узким. При этом зарплатные и кредитные обязательства остались. И в ситуации экстренной, и в ситуации повседневной бывает трудно отрегулировать денежный поток и правильно рассчитать стоимость нормочаса к продаже.

Финансовый директор ИТ-компании Reactive Ольга Башкатова разработала модель необходимого и достаточного объёма продаж (МНДОП), которая помогает управлять изменениями в компании и заранее просчитывать экономические последствия.

Я пришла в Reactive осенью 2019-го. Проанализировала все финансовые потоки и поняла, что есть проблемы с балансом расходов и доходов. Компания была в процессе больших изменений, прежние модели оценки бизнеса уже не подходили. У меня возникли три вопроса. Достаточно ли проектов привлекает отдел продаж? Корректна ли на сегодня стоимость нормочаса, которую мы закладываем в договорах? Равномерно ли распределены денежные поступления? В предыдущие расчёты я даже не стала заглядывать. Я математик по образованию, а для математиков важно не замыливать взгляд прежним решением задачи, зачастую неверным, попробовать решить её самостоятельно, с нуля. Иначе ты постоянно возвращаешься к тем же решениям. Мы вместе с руководством решили, что я проведу все расчёты заново.

Ольга Башкатова
Финансовый директор Reactive

Модель содержит в себе две ключевые точки: точку необходимого объёма продаж (ТНОП) и точку достаточного объёма продаж (ТДОП). Благодаря этому, мы понимаем, какой должна быть стоимость услуг и ежемесячная выручка, чтобы деятельность компании была безубыточной или приносила определённую прибыль (например, 20%).

Точка необходимого объёма продаж рассчитывается по формуле:

$$\text{ТНОП} = \text{ОР}/(1 - (\text{П}_1 \times \text{НК} + \text{П}_2 + \text{П}_3 + \ldots + \text{П}_n)),$$

где **ОР** – операционные расходы, включая фонд заработанной платы (в денежном выражении);

$\text{П}_1, \text{П}_2, \text{П}_3, \ldots, \text{П}_n$ – значимые для компании варьируемые параметры, без учёта желаемой прибыли (в доле от объёма продаж);

НК – налоговый коэффициент.

В знаменателе выражение в скобках всегда меньше 1.

ТНОП измеряется в денежном выражении и показывает необходимый объём продаж для выхода компании в ноль, на уровень безубыточности.

Точка достаточного объёма продаж учитывает необходимый уровень прибыли. Мы просто добавляем к варьируемым параметрам значение прибыли (например, 0,2, если это 20%).

На практике важны следствия из этих формул:

Стоимость нормочаса «к продаже» для $\text{ТНОП} = \text{ТНОП}/(\text{К} \times \text{В})$,

Стоимость нормочаса «к продаже» для $\text{ТДОП} = \text{ТДОП}/(\text{К} \times \text{В})$,

где **К** – это количество специалистов IT-отдела;

В – ежемесячная выработка специалиста IT-отдела, час.

Для правильного проведения расчётов необходимо точно оценить операционные расходы компании. Есть расходы, объём которых примерно одинаков каждый месяц. Например, это аренда и содержание офиса, фонд заработной платы, реклама, лизинговые платежи, юридические услуги, амортизация. Такие расходы мы вносим в формулу в денежном выражении. А есть расходы, которые представляют собой процент от валового дохода (выручки). Например, это могут быть премии, налоги, риски. Мы оцениваем их, опираясь на опыт компании, актуальное законодательство и мнения экспертов.

Для наглядности сделаем расчёт для веб-студии Reactive:

Сотрудник	Выработка, ч	Зп	НДФЛ	ПФ	ФФОМС	ФСС	Стоимость для компании
Генеральный директор		100 000	13 000	8 000	4 000	2 200	127 200
Коммерческий директор		100 000	13 000	8 000	4 000	2 200	127 200
Финансовый директор		70 000	9 100	5 600	2 800	1 540	89 040
Бухгалтер		40 000	5 200	3 200	1 600	880	50 880
Ведущий менеджер		70 000	9 100	5 600	2 800	1 540	89 040
Менеджер		60 000	7 800	4 800	2 400	1 320	76 320
Менеджер		60 000	7 800	4 800	2 400	1 320	76 320
Менеджер		60 000	7 800	4 800	2 400	1 320	76 320
Ведущий аналитик	100	60 000	7 800	4 800	2 400	1 320	76 320
Аналитик	100	50 000	6 500	4 000	2 000	1 100	63 600
Аналитик	100	50 000	6 500	4 000	2 000	1 100	63 600
Тим-лид	100	70 000	9 100	5 600	2 800	1 540	89 040
back-end	100	90 000	11 700	7 200	3 600	1 980	114 480
back-end	100	90 000	11 700	7 200	3 600	1 980	114 480
back-end	100	90 000	11 700	7 200	3 600	1 980	114 480
back-end	100	90 000	11 700	7 200	3 600	1 980	114 480
full steck	100	80 000	10 400	6 400	3 200	1 760	101 760
full steck	100	80 000	10 400	6 400	3 200	1 760	101 760
full steck	100	80 000	10 400	6 400	3 200	1 760	101 760
Арт-директор	100	80 000	10 400	6 400	3 200	1 760	101 760
Верстальщик	100	50 000	6 500	4 000	2 000	1 100	63 600
Верстальщик	100	50 000	6 500	4 000	2 000	1 100	63 600
Дизайнер	100	50 000	6 500	4 000	2 000	1 100	63 600
Копирайтер	100	50 000	6 500	4 000	2 000	1 100	63 600
Фонд ЗП							**2 130 000**

Расчётные данные	
Выручка (доля от выручки)	1
Фонд ЗП	2 130 000
Прочие операц. расходы	300 000
Премия команды менеджеров	0,07
Желаемая прибыль	0,20
Налог	0,06
Риски	0,10

Левая часть уравнения (для ТНОП)	0,74
Левая часть уравнения (для ТДОП)	0,55
Правая часть уравнения	2 430 000
Точка необходимого объема продаж	3 300 000
Точка достаточного объема продаж	4 500 000

ТНОП Reactive = (2 130 000 + 300 000)/(1 – (0,07 × НК + 0,06 + 0,01)) = 3 300 000,

где **2 130 ООО** — фонд заработной платы со всеми налоговыми отчислениями (см. таблицу);
300 ООО — другие операционные расходы;

П$_3$ — премия команды (7% от валового дохода);

НК — налоговый коэффициент (налоговые отчисления на премии);

П$_2$ — налог по УСНО/доход (6%);

П$_1$ — риски (технические трудности на крупных проектах – 10% от валового дохода).

ТНОП Reactive = (2 130 000 + 300 000)/(1 – (0,07 × НК + 0,06 + 0,01 + 0,2)) = 4 500 000,

Всё то же самое, только добавляем в знаменатель желаемую прибыль в виде четвёртого параметра (**П**$_4$ = 20%).

Стоимость нормочаса «к продаже» для **ТНОП Reactive** = 3 300 000/(16 x 100) = 2 100;
Стоимость нормочаса «к продаже» для **ТДОП Reactive** = 4 500 000/(16 x 100) = 2 900.

Итак, при ежемесячном объёме продаж в 3,3 млн доходы Reactive полностью покроют расходы. Прибыль компании будет равной 0. Стоимость нормочаса к продаже в этих условиях – 2100.

При ежемесячном объёме продаж в 4,5 млн прибыль компании составит 20% от валового дохода, стоимость нормочаса к продаже – 2900.

Модель помогает решить несколько экономических задач:

- определить минимальный объём продаж – такой, при котором компания останется на плаву и не будет нуждаться в заёмных средствах;
- обеспечить равномерный ежемесячный приток денежных средств: корректируются формы и сроки выплат по контрактам;
- проанализировать финансовое состояние компании и уровень её платежёспособности. Если уровень точки необходимого объёма продаж пройден – компания точно получит прибыль, если же эта точка не достигнута – компания несёт убытки. Чем дальше компания от ТНОП, тем в большей степени она финансово устойчива.
- прогнозировать экономические последствия повышения зарплаты, расширения штата сотрудников, приобретения имущества, увеличения других видов расходов. Мы просто подставляем в формулы новые значения (новый уровень зарплаты) и видим, какой объём выручки нужен для таких изменений. Если текущие проекты, договоры обеспечивают такую выручку в необходимом временном диапазоне, то зарплату можно смело поднимать;
- определить стоимость нормочаса, которая обеспечит компании отсутствие убытков или необходимую прибыль. Это один из самых интересных и сложных экономических вопросов. Большинство ИТ-компаний испытывают трудности с правильным расчётом цены;
- принимать верные решения о новых активах: покупать, арендовать или отказаться.

К тому же математика помогает в работе с клиентами: имея формулы под рукой, проще и быстрее обосновать стоимость проекта.

После внедрения в практику таких расчётов мы сбалансировали входящие денежные потоки по договорам, отказались от убыточных проектов. Стоимость услуг стала более понятной и прозрачной – это порадовало заказчиков. Конечно, по-прежнему имеют место имиджевые проекты, которые дают возможность выйти на новый рынок, получить признание, претендовать на премию в сфере digital. Мы рассчитали новые плановые показатели для менеджеров, ориентированные на прибыль 20%. Экономически обосновали возможность покупать имущество в лизинг, расширять штат сотрудников и повышать зарплаты. В 2019 году наша компания смогла полностью отказаться от привлечения заёмных средств, закрыть год с прибылью и индексировать заработные платы всех сотрудников.

В планах предстоит оценить рентабельность персонала и разработать новое премиальное положение. Рассчитать экономическую эффективность всего кейса проектов и отказаться от наиболее трудозатратных, но менее рентабельных.

Эта модель подходит для большинства компаний. Главное – правильно учесть все возможные издержки. Необходимо разделить их по категориям и либо экспертно оценить, либо рассчитать. Модель разработана специально для студии Reactive с учётом потребностей компании, но мы готовы делиться опытом и помочь адаптировать её под запрос любой организации. Мы открыты для дискуссий и обсуждений.

Ольга Башкатова
Финансовый директор Reactive

www.rktv.ru

CIS / № 1 (15) / 2021 / www.cis.ru

Big Data: перспективы развития и объёмы рынка больших данных

Глобальный рынок Big Data ежегодно демонстрирует положительную динамику, увеличившись по итогам 2019 года на 12% и достигнув 189,1 млрд долл. О показателях мирового и российского рынка Big Data, сценариях развития и главных трендах в области данных и аналитики – в статье экспертов Группы «ДЕЛОВОЙ ПРОФИЛЬ».

Большие данные представляют собой массивы информации, характеризующиеся колоссальными объёмами, стремительно растущей скоростью накопления, разнообразием их формата представления как в виде структурированной, так и неструктурированной информации. Big Data также включают в себя комплекс инновационных методов и способов хранения и обработки информации с целью автоматизации, оптимизации бизнес-процессов, обеспечения принятия наиболее эффективных решений на основе накопленной информации.

Таким образом, большие данные характеризуются тремя основными признаками:

- большой объём информации,
- высокая скорость изменения информации,
- разнообразие и разнородность данных.

Ниже представлены ключевые элементы, составляющие аналитику больших данных (рис. 1).

Структура и объём рынка больших данных

В 2018 году объём глобального рынка Big Data и бизнес-аналитики (global big data and business analytics market) достиг 168,8 млрд долл. В соответствии с оценкой IDC, по итогам 2019 года объём глобального рынка больших данных увеличился на 12%, по сравнению с показателями предыдущего года, и достиг 189,1 млрд долл. Кроме того, в период 2018-2022 гг. предполагается рост рынка со среднегодовым темпом (CAGR) на уровне 13,2%. Таким образом, объём рынка может увеличиться до 274,3 млрд долл. к 2022 году.

ResearchAndMarkets прогнозирует возможные темпы роста глобального рынка Big data на уровне 19,7% ежегодно на период 2019-2025 гг. (рис. 2).

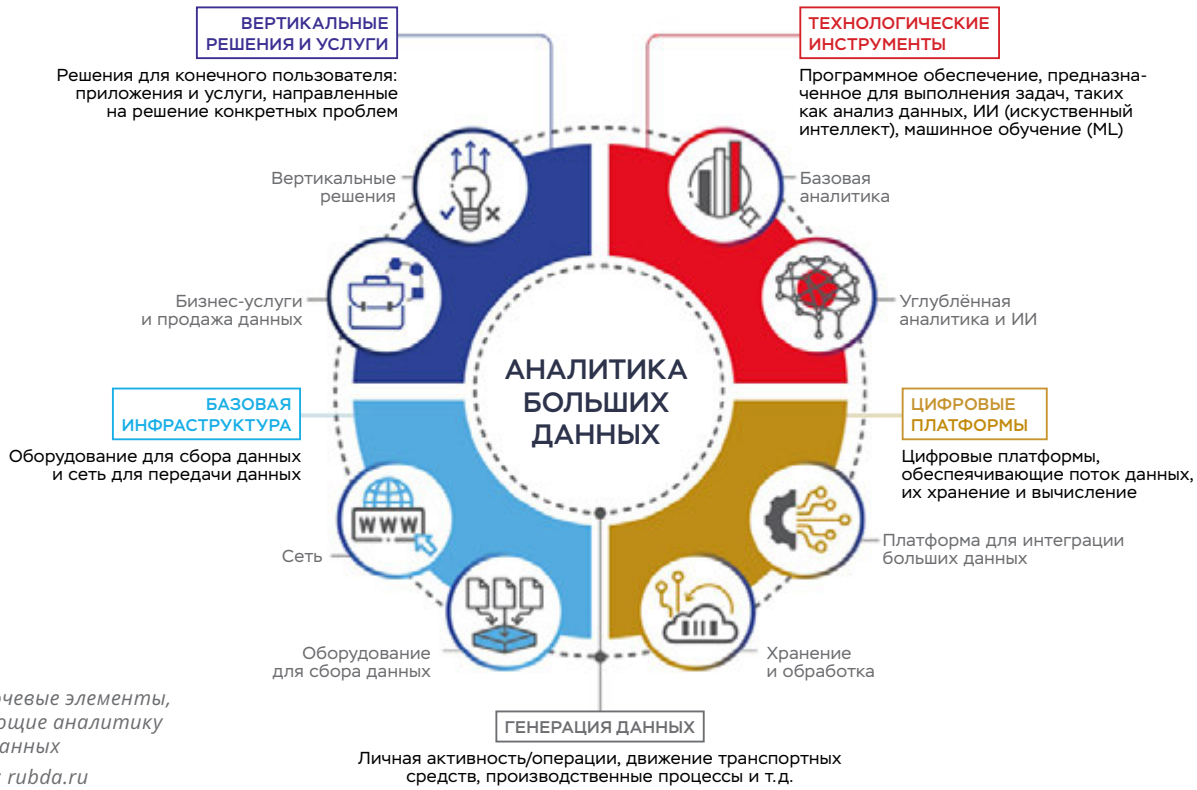


Рис. 1. Ключевые элементы, составляющие аналитику больших данных

Источник: rubda.ru

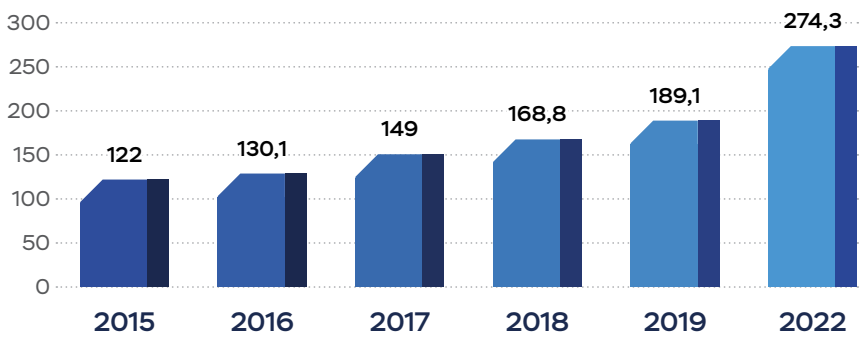


Рис. 2. Динамика роста рынка больших данных, млрд. долл.

Источник: Global big data and business analytics revenue from 2015 to 2022: statista.com

В 2018 году выручка на рынке программного обеспечения больших данных составила 60,7 млрд долл. На конец 2019 года более половины выручки BDA обеспечили доходы, полученные от IT- и бизнес-сервисов – 77,5 млрд долл. и 20,7 млрд долл. соответственно. Размер выручки в сегменте аппаратного обеспечения составил около 23,7 млрд долл. Доход от программного обеспечения больших данных достиг 67,2 млрд долл. По данным IDC, ожидаемые темпы роста (CAGR) в период с 2018-2023 гг. в этом сегменте поднимутся до отметки в 12,5%.

Согласно исследованию Fortune Business Insights, объём глобального рынка технологий Big Data, оценённый в 2018 году в 38,6 млрд долл., увеличится к 2026 году до 104,3 млрд долл., демонстрируя темпы роста (CAGR) на уровне 14% в период с 2019 по 2026 гг. (рис. 3).

По данным Grand View Research, к 2025 году глобальный рынок Big Data как услуги (global big data as a service (BDaaS)) достигнет 51,9 млрд долл., при этом CAGR составит 38,7% в период 2019-2025 гг.

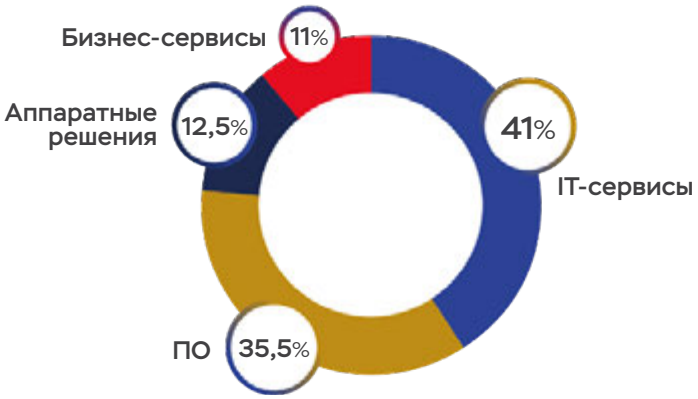


Рис. 3. Доля сегментов рынка в общем объёме выручки, %

Источник: Big Data Technology Market Size, Share, Demand & Growth: fortunebusinessinsights.com

География рынка Big Data

С географической точки зрения по результатам 2019 года наиболее крупным стал рынок США с объёмом доходов в 100 млрд долл. Второе и третье место по объёму заняли Япония (9,6 млрд долл.) и Великобритания (9,2 млрд долл). Также в пятёрку крупнейших рынков вошли КНР (8,6 млрд долл.) и Германия (7,9 млрд долл.).

В Аргентине и Вьетнаме наблюдаются наиболее высокие показатели прироста за пятилетний период (CAGRs – 23,1% и 19,4%). Третье место по уровню CAGR занял Китай (19,2%), что к 2022 году может обеспечить выход этой страны на второе место по уровню доходов (рис. 4).

Драйверами рынка больших данных и бизнес-аналитики выступают 5 отраслей, на которые, по оценке IDC, приходится около половины инвестиций (91.4 млрд долл.):

- банковская сфера,
- дискретное производство,
- специализированные услуги,
- непрерывное производство,
- федеральное/центральное правительство.

При этом наибольший рост рынка в будущем обеспечат такие направления, как розничная торговля (15,2% CAGR), а также операции с ценными бумагами и инвестиционные услуги (15,3% CAGR) (рис. 5).

Рис. 4. Доля стран-лидеров в общем объёме рынка больших данных, %

Источник: 9 IDC Forecasts Revenues for Big Data and Business Analytics Solutions Will Reach $ 189.1 Billion This Year with Double-Digit Annual Growth Through 2022: idc.com

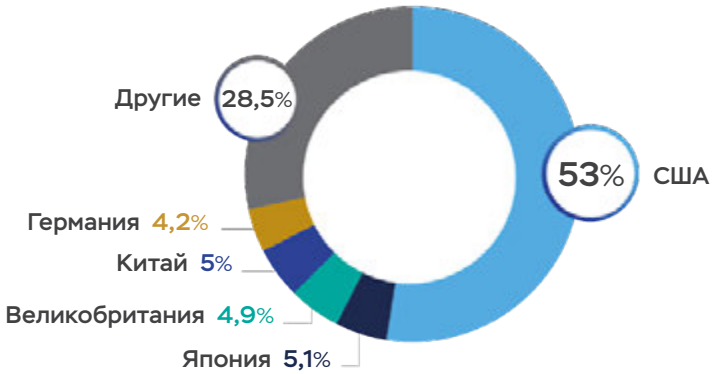


Рис. 5. Инвестиции в технологии больших данных по отраслям, %

Источник: 9 IDC Forecasts Revenues for Big Data and Business Analytics Solutions Will Reach $ 189.1 Billion This Year with Double-Digit Annual Growth Through 2022: idc.com

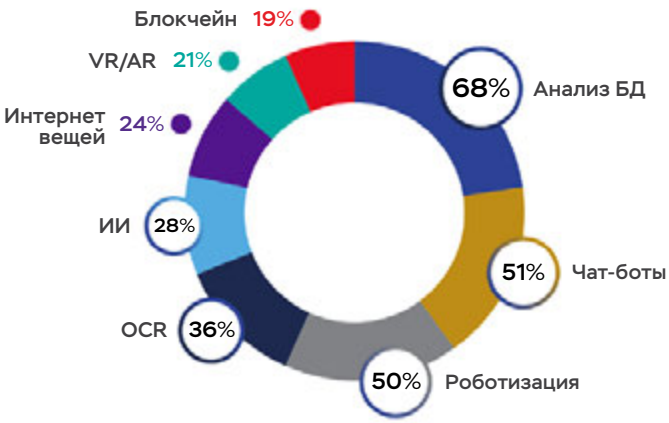
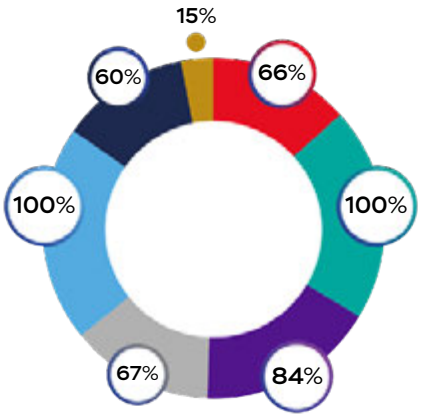


Рис. 6. Технологии, используемые среди российских компаний, %

Перечень инструментов, используемых для анализа больших данных, формируется в зависимости от отрасли компании.



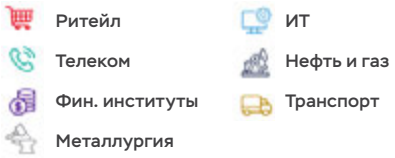


Рис. 7. Индустрии использования больших данных в России, %

Крупнейшие поставщики на рынке больших данных

Согласно отчёту Wikibon (2018 Big Data and Analytics Market Share Report), в 2018 году (по данным 2017 года) в пятёрку крупнейших поставщиков решений на рынке Big Data вошли такие компании, как IBM, Splunk, Dell, Oracle и AWS. И, по данным исследования Global Big Data Market Forecast 2019-2027, проведённого Inkwoodresearch, в 2019 году эти компании сохранили свои позиции в качестве лидеров рынка.

Российский рынок Big Data

Российский рынок пока занимает незначительную долю в мировом предложении и потреблении информационных технологий. Однако в 2018-2019 гг. было принято немало решений и реализовано достаточное количество законодательных инициатив, способствующих развитию отечественного рынка Big Data.

По результатам опроса, проведённого International Data Corporation (IDC) и Hitachi Vantara в ходе исследования «Аналитика больших данных как инструмент бизнес-инноваций», **более 55% российских организаций выделяют бюджет на внедрение технологий больших данных** (участие приняли более 100 компаний со штатом от 500 чел.).

По состоянию на конец 2019 год Boston Consulting Group оценивает объём российского рынка больших данных **в 45 млрд руб. с темпом прироста 12% в течение последних пяти лет.**

Крупнейшие российские игроки рынка больших данных

В Ассоциацию больших данных (АБД), образованную в 2018 году, входят организации, представляющие собой наиболее крупных участников российского рынка Big Data:

- ПАО «Сбербанк»,
- АО «Газпромбанк»,
- АО «Тинькофф Банк»,
- АО «КИВИ Банк» (QIWI),
- ООО «Яндекс»,
- ООО «Мэйл.ру»,
- ПАО «Мегафон»,
- ООО «Единыйфактор» («oneFactor»),
- ПАО «Ростелеком».

В июле 2019 года было объявлено о присоединении к Ассоциации Аналитического центра при Правительстве РФ.

Объём российского рынка больших данных

Согласно данным, приведённым Ассоциацией участников рынка больших данных, **объём рынка Big Data в России составляет 10-30 млрд руб.** При этом, в соответствии с усреднёнными прогнозами отечественных и иностранных экспертов, **предполагается рост этого показателя в 10 раз – до отметки 300 млрд руб. к 2024 году.**

Основные потребители технологий Big Data в России

Сегодня лидерами по внедрению технологий в российских компаниях являются такие инструменты цифровизации, как роботизированная автоматизация бизнес-процессов, использование чат-ботов, инструментов анализа больших данных и предиктивной аналитики.

Технология анализа больших данных является наиболее часто внедряемой технологией среди российских компаний: 68% организаций на конец 2019 года уже опробовали внедрение инструментов анализа больших данных (рис. 6, 7).

Сценарии развития рынка Big Data в России

В 2019 году участниками Ассоциации совместно с привлечёнными внешними специалистами (в т.ч. Boston Consulting Group) была разработана стратегия развития рынка до 2024 года, включающая 5 возможных сценариев:

- пессимистичный,
- сценарий «бездействия»,
- базовый,
- оптимистичный,
- «сценарий мечты».

В соответствии с разными вариантами прогноза рынок больших данных может обеспечить от 0,3% до 2,4% прироста ВВП, а объёмы отрасли

могут увеличиться на сумму от 20 до 230 млрд руб., по сравнению с показателями 2019 года (табл. 1).

Реализация стратегии развития российского рынка Big Data

АБД будет продвигать 6 инициатив: 3 дадут умеренный эффект, остальные – более агрессивные по сложности имплементации и эффекту от БД.

Умеренный эффект:

1. Упрощённый доступ и обработка данных

- Позволить пользователям одновременно и дистанционно давать согласие на несколько целей использования их данных;
- Позволить компаниям обрабатывать персональные данные для широкого круга целей при соблюдении определённых требований;
- Запустить массовую государственную цифровизацию в областях, релевантных для БД, с фокусом на стандартизацию данных.

3. R&D песочницы для исследования Больших Данных

- Определить законом контролируемую среду экспериментирования с ослабленным регулированием;
- Обеспечить вовлечение регуляторов для оптимизации одобрений при последующем крупномасштабном развёртывании;
- Обеспечить «озера данных» со стандартизированными данными и технологические библиотеки.

5. Стратегии Больших Данных традиционных индустрий

- Создать стандарт для внедрения Больших Данных в компании с государственным участием;
- Ввести ориентированные на результат стимулы для компаний частного сектора;
- Создать проектный и технический кадровый резерв, чтобы помочь компаниям внедрять Большие Данные и обучать их команды.

Агрессивный эффект:

2. Обеспечение возможности обмена/обогащения данных

- Позволить игрокам делиться анонимными персональными данными на коммерческой основе;
- Поощрять обмен отраслевыми данными внутри и между отраслями через саморегулируемые стандарты;
- Позволить государству делиться определёнными типами релевантных данных с частным сектором.

4. Финансирование инноваций и ресурсная экосистема

- Обеспечить инновационные команды выделенным доступом к «озёрам данных» с труднодоступной отраслевой информацией;
- Оптимизировать процессы бэк-офисного типа путём предоставления доступа к юристам, бухгалтерам и специалистам по патентам;
- Внедрить инвестиционную платформу, соединяющую квалифицированных инвесторов с отобранными инициативами.

6. Внутренние стимулы для инновационных отраслей

- Внедрить упрощённый процесс получения необходимых сертификатов и патентов для продуктов и услуг на основе Больших Данных;
- Устранить выборочные барьеры для экспорта продуктов и сервисов, построенных на технологиях Больших Данных;
- Провести кампании по повышению осведомлённости об экспортном потенциале продуктов на технологиях Больших Данных.

Согласно базовому сценарию, в 2024 году в России эффект от внедрения продуктов и технологий больших данных увеличится на 1,2% как доля от ВВП (рис. 8).

Меры, направленные на реализацию стратегии, объединены в три основных блока:

- повышение доступности данных,
- проведение исследований в области больших данных (R&D),
- масштабирование рынка.

Таблица 1 – Сценарии развития рынка больших данных в России

	Доступность данных	Исследования и идеи	Масштабирование	Вклад БД в ВВП, 2024 г. против 2019 г.	Отрасль БД в 2024 г. против 2019 г., млрд. руб.
Пессимистичный сценарий	Активные ограничения на использование данных	Отсутствует адресная поддержка	Отсутствует адресная поддержка	+0,3%	+20
Сценарий бездействия	Установленные регулятором ограничивающие прецеденты	Отсутствует адресная поддержка	Отсутствует адресная поддержка	+0,5%	+40
Базовый сценарий	1. Упрощённый доступ и обработка	3. R&D – «песочницы» для исследования БД	5. Стратегия БД традиционных индустрий	+1,2%	+100
Оптимистичный сценарий	2. Обеспечение возможности обмена/обогащения данных	4. Финансирование инноваций и ресурсная экосистема	6. Внутренние стимулы для инновационных отраслей	+1,8%	+160
Сценарий мечты	Платформы для крупномасштабного обмена данными	Специализированные государственные инвестиционные программы	Финансовая поддержка экспорта	+2,4%	+230

Источник: Российские сценарии для Big Data: rspectr.com

Рис. 8. Базовый сценарий эффективности внедрения инструментов больших данных
Источник: Минэкономразвития РФ

1. Базовый сценарий Минэкономразвития в постоянных цехах. 2. Анализ BCG на основе практического опыта, интервью с экспертами, открытых источников. 3. Цветовая кодировка на основе текущего состояния отрасли на 2019 г.

Стратегия предусматривает создание R&D – «песочницы» для проведения экспериментов, внедрения мер по изменению законодательства, центра компетенций и др.

Согласно прогнозу IDC, к 2025 году общий объём цифровых данных, генерируемых во всём мире, вырастет более чем вчетверо – до 175 Зеттабайт с 40 Зеттабайт в 2020 году, в том числе благодаря растущему количеству IoT-устройств и датчиков. В соответствии с описанием главных атрибутов больших данных как «трёх «V» (объём, многообразие, скорость), которое даёт Gartner, эта нарастающая лавина данных будет всё больше характеризоваться разнообразием типов информации, причём большая часть будет представлять собой постоянно меняющиеся потоки данных в реальном времени. Как результат, задача управления данными и их анализа значительно затрудняется. И это обусловливает многие из трендов, которые, по всей видимости, будут преобладать в ближайшие три года.

Ключевые технологические тренды Big Data

Gartner отмечает следующие 11 технологических трендов в области данных и аналитики, которые потенциально окажут значительное влияние на дальнейшее развитие рынка в течение последующих 3-5 лет:

1. «Расширенная» (дополненная) аналитика (Augmented analytics) – совершенствование процесса анализа за счёт автоматизации процесса поиска, обработки данных с использованием технологий машинного обучения (Machine Learning (ML)) и искусственного интеллекта (Artificial Intelligence (AI)). Отмечается, что к 2020 году расширенная аналитика станет драйвером в области закупок инструментов бизнес-аналитики, а также платформ обработки информации. По данным ResearchAndMarkets, ожидается, что рынок расширенной аналитики вырастет с 4,8 млрд долл. в 2018 году до 18,4 млрд долл. к 2023 году при совокупном годовом темпе роста (CAGR) 30,6%.

2. «Расширенное» (дополненное) управление данными (Augmented data management) – применение технологий AI и ML, позволяющих осуществлять автоматизацию и самонастройку процесса управления корпоративными данными (включая управление метаданными, качеством данных, интеграцию данных и баз данных). К 2022 году предполагается снижение объёма «ручного» управления данными компаний на 45%.

3. Технологии обработки естественного языка (Natural language

processing (NLP) and conversational analytics) – согласно прогнозу экспертов, к 2021 году внедрение средств NLP повысит уровень распространения технологий интеллектуального анализа данных с 35% до 50%. Технология обработки естественного языка позволяет компьютерам понимать человека. Как результат, рядовые бизнес-пользователи смогут делать запросы к сложным массивам данных обычными словами и фразами – голосом или вводом с клавиатуры и получать такие же легко понимаемые результаты бизнес-анализа. По прогнозу Gartner, к концу 2020 года 50% аналитических запросов будут делаться на естественном языке или с помощью привычного поиска либо генерироваться автоматически. А по данным Ventana Research, 33% организаций ожидают, что к 2021 году запросы и ответы на естественном языке будут стандартной функцией инструментов бизнес-анализа.

4. Аналитика графов (Graph analytics) – по оценке Gartner, применение методов обработки графической информации и графических баз данных будет увеличиваться на 100% ежегодно в течение последующих 5 лет. Бизнес-аналитики создают всё более сложные запросы к структурированным и неструктурированным данным, часто из нескольких приложений и источников. Выполнение таких сложных запросов в больших масштабах с использованием традиционных инструментов и языков запросов представляет собой очень трудную задачу. Графовые базы данных и инструменты аналитики и визуализации помогают справиться с этой задачей, показывая связи, существующие между узлами – людьми, локациями и объектами материального мира. Gartner прогнозирует, что использование графовой обработки и графовых баз данных будет удваиваться ежегодно в последующие несколько лет, что позволит «ускорить подготовку данных и создать более сложные и адаптивные методы анализирования данных».

5. Коммерческие инструменты искусственного интеллекта и машинного обучения (Commercial AI and machine learning) – переход от использования платформ с открытым исходным кодом к применению специально разработанных коннекторов, подключающихся к open-source экосистеме, позволит реализовать функции управления моделями, проектами, а также предоставит возможность для преобразования и многократного использования данных, обеспечит интеграцию и прозрачность, недоступные в рамках open-source платформ. Разработчики ПО анализа данных всегда стремились предоставить возможности своей технологии более широкой аудитории обычных бизнес-пользователей и всех работающих с информацией. И это уже происходит благодаря так называемой интеллектуальной (augmented) аналитике. Gartner определяет интеллектуальную аналитику как использование технологий искусственного интеллекта, машинного обучения и обработки естественного языка для содействия в подготовке данных, понимании и трактовке результатов анализа, то есть в качестве расширения возможностей человека и традиционных способов формирования и использования аналитического контента. Интеллектуальная аналитика поможет специалистам и обычным сотрудникам, работающим с информацией, автоматизировать многие аспекты изучения данных, а также разработки и использования моделей данных. К 2022 году 75% решений для конечных пользователей будут создаваться с использованием коммерческих, а не открытых платформ.

6. Матрица данных (Data fabric) – подходы к интеграции данных в виде логически организованной структуры для облегчённого доступа и обмена в распределённой среде данных.

7. Объясняемый искусственный интеллект (Explainable AI) – возможность формирования описательной модели на естественном языке, позволяющей обосновать автоматически сгенерированные решения и результаты, полученные на базе технологий AI. К 2023 году более 75% крупных организаций будут нанимать специалистов по поведению AI, обеспечению конфиденциальности и доверительных отношений с клиентом для снижения репутационных рисков.

8. Блокчейн в области данных и аналитики – реализует взаимосвязь транзакций, активов, обеспечивает прозрачность и гарантии в сложных сетях взаимодействия участников.

9. Непрерывная интеллектуальная обработка данных (Continuous Intelligence) – подход, при котором результаты аналитики в реальном времени интегрируются в бизнес-операции, происходит обработка потоковой контекстной информации, поступающей с датчиков IoT, и исторических данных, позволяющий моментально реагировать на изменения и предписывать поведение моделей. К 2020 году прогнозируется наличие функции непрерывного интеллектуального анализа в более чем 50% бизнес-систем.

10. Серверы «постоянной» памяти (Persistent memory servers) – технология сохранения данных при отключении питания позволяет решить проблему ограниченности объёмов памяти при возрастающем количестве данных; предоставляет возможность анализировать больше данных в оперативной памяти и в режиме реального времени; повышает энергоэффективность, операции с данными становятся более рациональными за счёт уменьшения дублирования.

11. Ужесточение регулирования в сфере обращения с данными. Многие компании уже ощутили на себе ужесточение регулирования в обращении с данными с вступлением в силу Генерального регламента о защите данных (GDPR) в Евросоюзе в мае 2018 года. В 2020 году, с вводом Закона штата Калифорния о защите конфиденциальности потребителей (CCPA) и в свете растущих призывов ввести такие правила в масштабах всей страны, компании и организации в США встанут перед необходимостью внедрить строгий контроль за данными, обеспечением их защищённости и конфиденциальности. Всё это окажет влияние на практику сбора, обработки, хранения и использования данных компаниями, и, в первую очередь, это касается данных потребителей. К 2021 году 25% организаций создадут новые центры передовых технологий управления данными и безопасности, что поможет снизить риск неправомерного использования или утечки, по прогнозу Ventana Research. Исследователи в сфере технологий управления данными и бизнес-анализа призваны сыграть ключевую роль в разработке и внедрении эффективных и надёжных методов.

DELOVOY PROFIL
A member of mgiworldwide

Пашкевич Александра
Ведущий маркетолог Группы «ДЕЛОВОЙ ПРОФИЛЬ»

pashkevich@delprof.ru

www.delprof.ru

Чтобы видеть

Компьютерное зрение в ритейле

Мы смотрим, чтобы видеть. Принцип работы глаза человека и компьютера сравнительно одинаков. Видеокамера – такой же орган зрения компьютера, как глаз у человека. Увиденное попадает в компьютерный «мозг» – сложную нейронную сеть, которая идентифицирует, классифицирует и учится реагировать на то, что «видит».

В ритейле технологии компьютерного зрения используются в системах управления информацией о товарах (PIM). Это помогает понимать, как люди перемещаются по торговым залам, на что они обращают внимание, выявить шаблоны поведения покупателей. Все эти данные накапливаются и становятся основой для принятия стратегических и операционных решений.

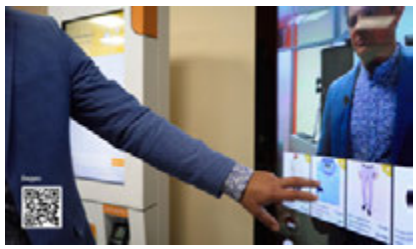
Тепловые карты перемещения покупателей по торговому залу позволяют спроектировать оптимальную планировку магазина. Система знает, какие товары лучше располагать рядом, а какие должны лежать на других полках.

Всё это ведёт к увеличению доходности магазина.

Автопилот

Как и автомобили с автопилотом, новые «автопилотируемые» магазины без продавцов появляются в США, Европе, Азии. Помимо очевидной выгоды от экономии на персонале, такой магазин точно знает, сколько товаров осталось на полках, как и когда их покупают. Это даёт возможность решать и маркетинговые задачи, предлагая покупателям новый уровень сервиса.

Совсем недавно в Москве открылся полностью автоматизированный магазин «Пятерочка #налету». Простота и скорость обслуживания всё больше и больше привлекают внимание как владельцев розничных сетей, так и покупателей.



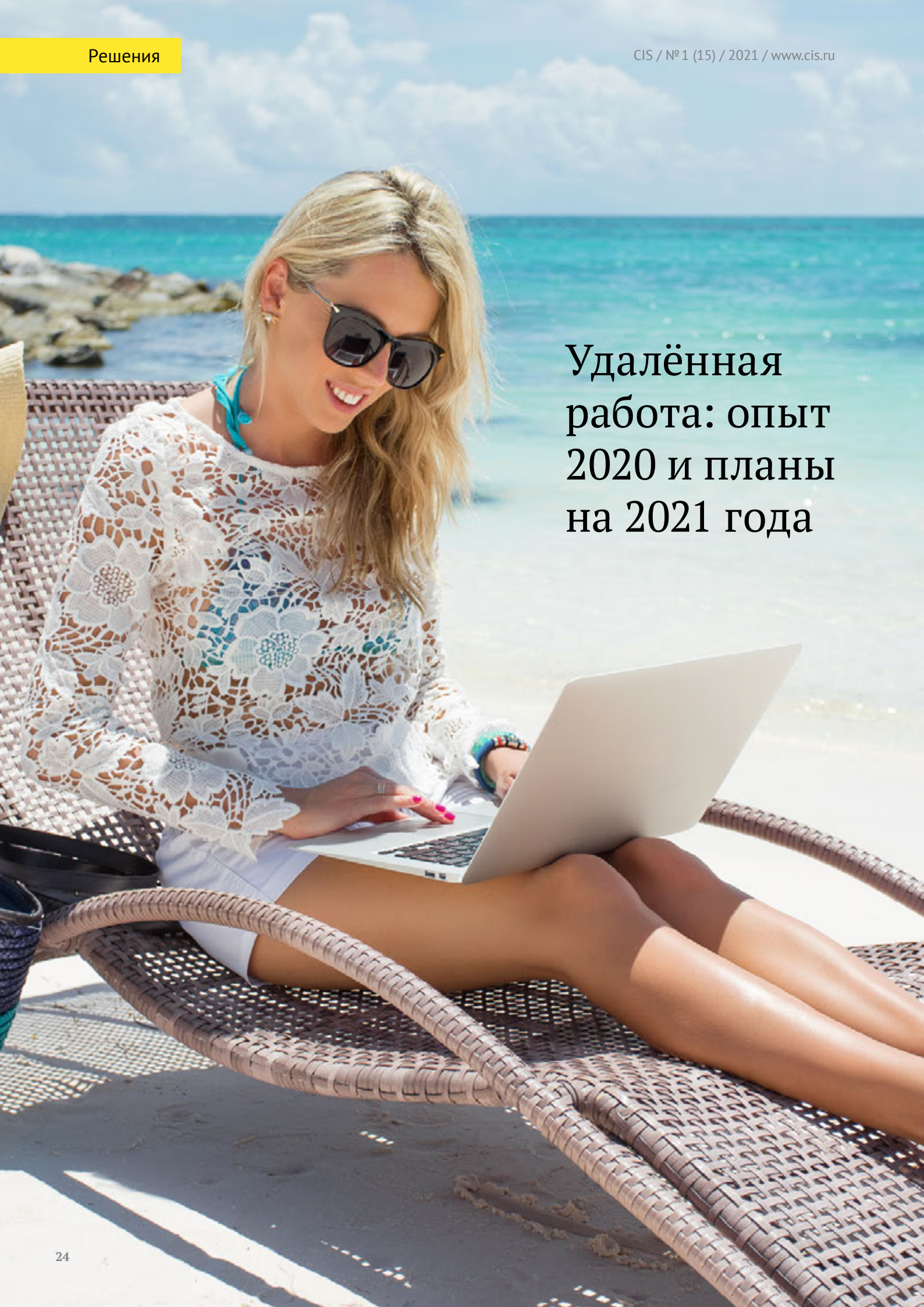
Узнаю «по походке»

В индустрии моды процесс покупки также активно трансформируется. Проанализировав внешний вид и даже настроение человека, «виртуальное зеркало» подбирает те модели одежды из ассортимента магазина, которые с высокой вероятностью понравятся покупателю.

Системы компьютерного зрения не один год успешно применяются в интеллектуальном видеонаблюдении, банковском ритейле и прочих сферах. Во всём мире насчитывается немало компаний, разрабатывающих системы машинного зрения. Мы сотрудничаем с одним из ведущих разработчиков таковой в России, компанией Тевиан (Tevian).

С возникновением в нашей жизни новых проблем, таких как пандемия COVID-19, скорость развития и распространения систем компьютерного зрения возросла, как и скорость решения юридической стороны применения этих технологий.

Насколько мы правы в том, что отдаём машинным алгоритмам решение многих задач, в том числе тех, что сейчас прочно закреплены за человеком, покажет время. Очевидными плюсами, ещё 10 лет назад возможными только в кино, уже можно воспользоваться. Будущее наступило!



Удалённая работа: опыт 2020 и планы на 2021 года

В начале 2020 года мало кто мог предположить, какие изменения произойдут в ИТ-инфраструктурах предприятий. До этого момента о преимуществах удалённой работы говорили уже больше 10 лет, но всегда находились объяснения тому, почему в данной конкретной компании невозможно или нецелесообразно вводить такую практику.

Часто это было поле битвы между подразделениями ИТ и ИБ, и в результате такая возможность предоставлялась в основном Топ-менеджерам и особо ценным сотрудникам. Но с наступлением пандемии и принятием на государственном уровне ряда ограничительных мер во многих странах возможность работы из дома стала критически важной для выживания многих компаний. Можно сказать, что пандемия и правительственные ограничения сделали для пропаганды удалённой работы за один год гораздо больше, чем все маркетинговые мероприятия за прошедшее десятилетие.

Как только стало понятно, что государственные органы вводят или в самое ближайшее время введут строжайшие ограничения на перемещения людей, предприятия стали срочно искать возможности по организации удалённой работы. Бизнес-подразделения быстро заставили ИТ и ИБ договориться между собой и обеспечить возможность удалённой работы для всех пользователей. В зависимости от используемых ранее технологий, готовности и уровня зрелости в области ИТ компании стали внедрять или расширять различные решения.

Фактически можно выделить 4 возможных варианта. Опишем их с точки зрения решений, предоставляемых компанией Citrix Systems.

1. Компании, использовавшие ранее решения по VPN-доступу, стали наращивать пул VPN-концентраторов, обновлять лицензии, увеличивая пропускную способность решений для обслуживания резко увеличившегося количества пользователей. Поставщики решений, у которых, как у Citrix, существует возможность масштабирования пропускной способности устройства за счёт изменения лицензии или предоставляющие VPN-решения не только как аппаратные комплексы, но и как виртуальные устройства под различные платформы виртуализации, смогли быстро помочь своим клиентам найти выход из этой проблемы.
2. Компании, у которых уже были в той или иной мере внедрены решения по терминальному доступу или виртуализации десктопов и требуемое количество дополнительных по сравнению с уже существующими пользователями было небольшое, просто увеличили количество лицензий на используемые решения и предоставили удалённую работу всем пользователям. Это можно было сделать или за счёт уплотнения имеющихся пользователей, или перераспределив серверные мощности, временно освободив серверы, которые не предоставляют критически важных сервисов внутри компании. В ряде случаев компании закупали небольшое количество оборудования (серверы и системы хранения данных), что на рынке, где то же самое требовалось всем компаниям, сделать было очень сложно. Для помощи своим заказчикам компания Citrix представила специальную программу лицензирования – годовые лицензии с 50% скидкой.
3. Те компании, которые принимают идеологию облачных сервисов, резко нарастили использование облачных ресурсов. В зависимости от используемого подхода заказчики или полностью получали сервис Citrix из облаков Azure, AWS, Google Cloud, или интегрировали свои площадки в гибридные схемы. В таком случае можно было разделять приложения и сервисы таким образом, чтобы полностью соответствовать требованиям локального законодательства по работе с данными. В эту модель также успешно встраивались локальные сервис-провайдеры, которые на своих мощностях разме-

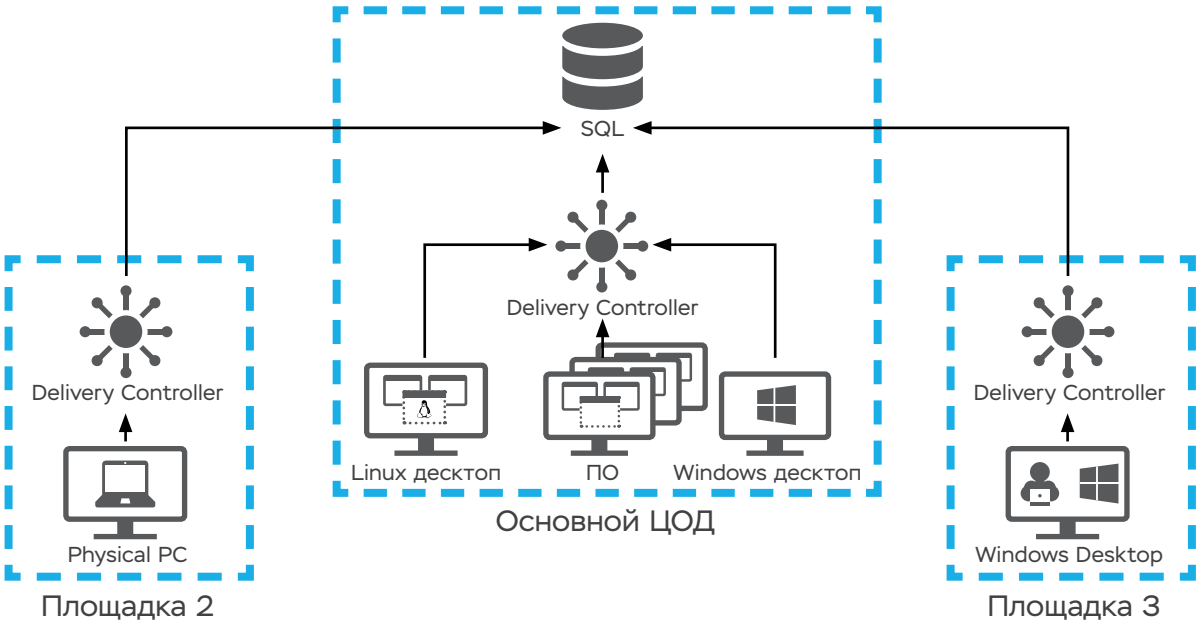


Рисунок 1. Наращивание инфраструктуры Citrix Virtual Apps and Desktops за счёт увеличения количества площадок с ресурсами для конечных пользователей

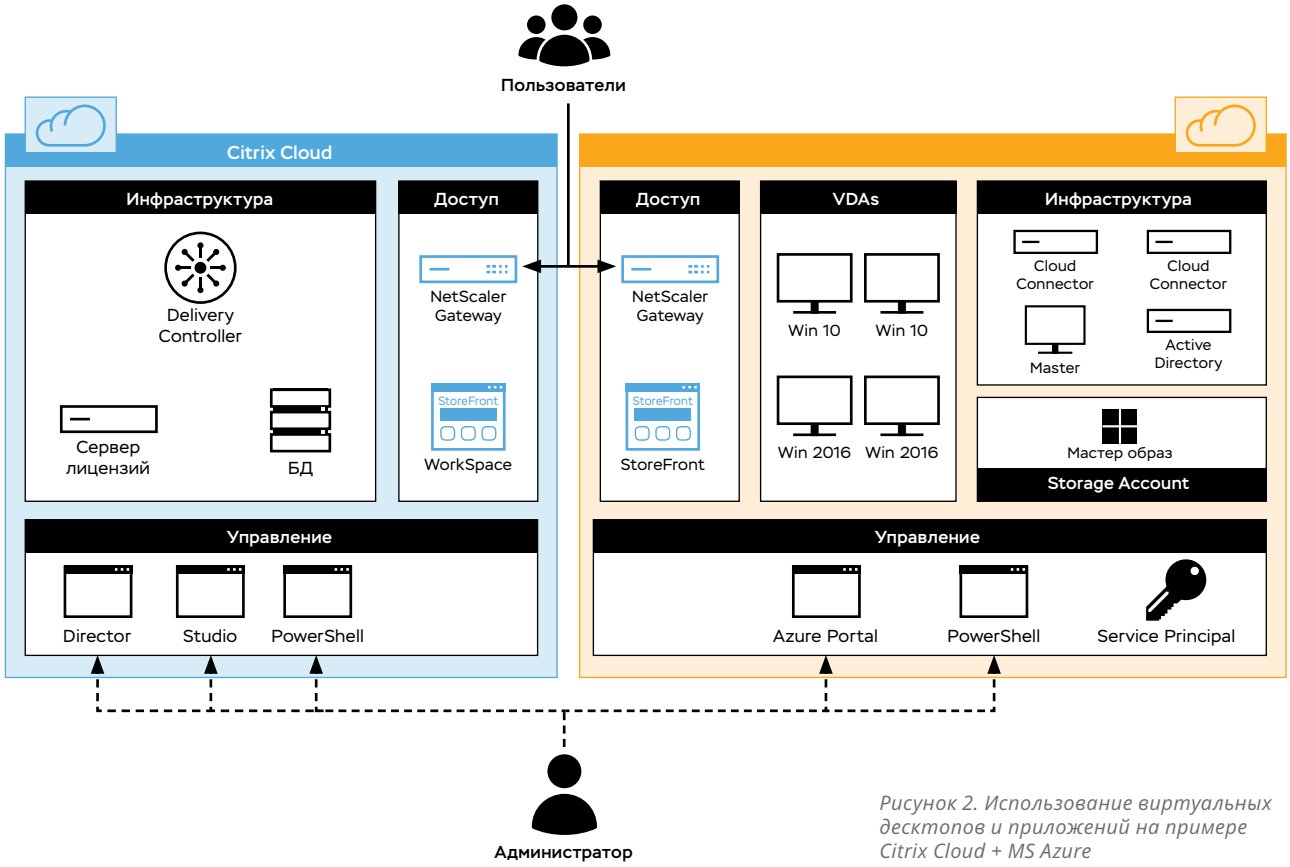


Рисунок 2. Использование виртуальных десктопов и приложений на примере Citrix Cloud + MS Azure

щали приложения и виртуальные десктопы заказчиков и обеспечивали наиболее близкое сетевое размещение к конечному пользователю. Как и раньше, компания Citrix старалась помочь своим заказчикам максимально полно использовать сделанные инвестиции и при этом обеспечить максимальную гибкость и комфортность работы конечных пользователей.

4. Одним из самых быстрых и, наверное, наименее затратных вариантов организации удалённой работы для больших групп пользователей стало предоставление удалённого подключения к их физическим ПК, оставшимся в опустевших офисах на рабочих столах. Используя личные устройства пользователей и функционал RemotePC в рамках решения Citrix Virtual Apps and Desktops ИТ департамент обеспечивал возможность подключиться к офисным устройствам, на которых уже было установлено всё необходимое ПО. При этом использовался протокол Citrix HDX потребляющий меньшую полосу пропускания по сравнению с другими протоколами, применялись политики Citrix Virtual Apps and Desktops, обеспечивающие безопасность и комфортность работы пользователей. В качестве успешных примеров использования такой технологии можно привести действительно быстрый (чуть больше недели) перевод более 25000 пользователей одной из компаний на удалённую работу. При этом заказчику не потребовалось приобретать СХД и дополнительные серверы для обеспечения работы такого количества пользователей.

Если рассмотреть проблемы, которые возникали у конечных пользователей, переведённых на работу из дома, то их можно подразделить на три группы: технические, организационные и психологические. К слову сказать, самыми простыми для решения были технические задачи, так как организации и пользователи для удалённой работы в основном применяли знакомые инструменты. Основная проблема была связана с приобретением требуемого количества оборудования и лицензий. Гораздо более сложными оказались организационные проблемы: договорённости между ИТ и ИБ, а также обеспечение конечных пользователей оборудованием для работы из дома. Эта задача оказалась очень важной, что можно заметить по практически исчезнувшим с прилавков магазинов ноутбуков в нижнем ценовом

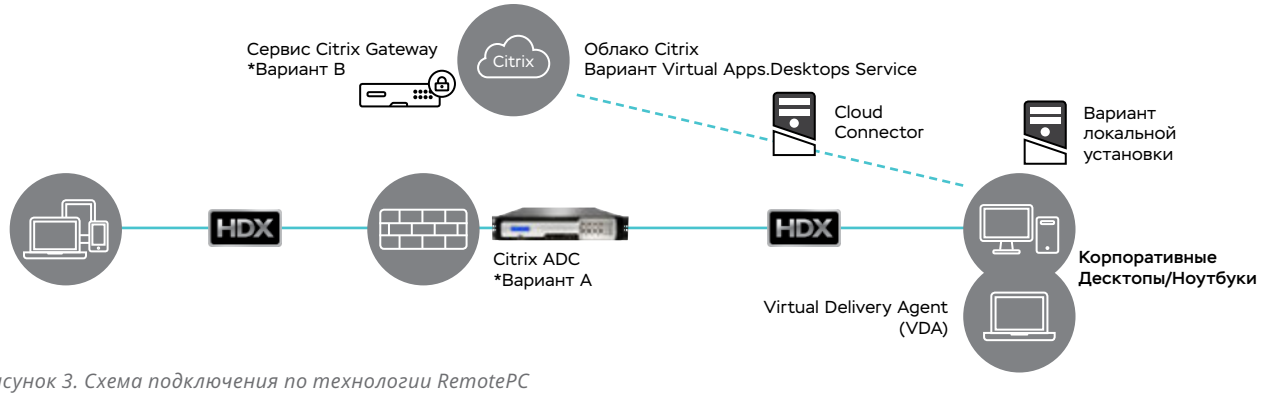


Рисунок 3. Схема подключения по технологии RemotePC

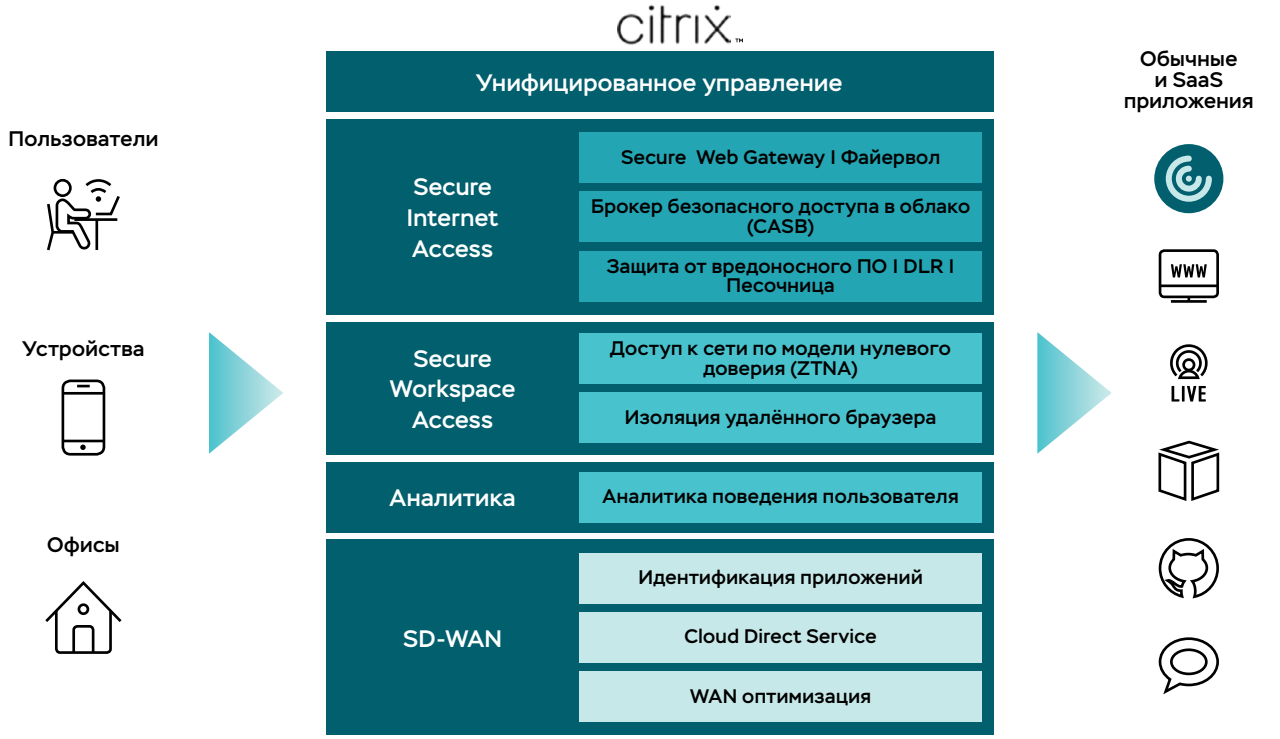


Рисунок 4. Концепция SASE с точки зрения предлагаемых решений и сервисов Citrix

сегменте, что подтверждается и отчётами IDC по росту продаж оконечного оборудования. Некоторые компании привозили на дом сотрудникам офисные ПК и ноутбуки, кто-то перевозил и тонкие клиенты, остальные пытались «выжить» в конкуренции за устройства со своими домочадцами. Затем оказалось, что конкуренция идёт не только за устройства, но и за полосу пропускания интернет-канала, и тут требования серьёзно выросли после перевода на удалённую работу не только родителей, но и детей на удалённую учёбу в школах и вузах. Школьники и студенты активно использовали решения по видео-конференциям, которые создавали серьёзную нагрузку на каналы передачи данных, что часто приводило к деградации изображения и проблемам с передачей звука и, как следствие этого, сложностям с прохождением занятий и уроков. А по прошествии определённого времени на первое место вышли психологические и социальные проблемы, связанные с резким снижением социальных коммуникаций между сотрудниками. В результате многие компании для своих работников стали проводить психологические тренинги, открыли горячие линии по психологической поддержке, организовывали дополнительные онлайн встречи, не связанные с выполнением заданий, а с целью дополнительного персонального общения между ними.

За последнее время аналитические агентства и поставщики различных решений и сервисов провели множество опросов для понимания, что нас ждёт дальше и как выходить из сложившейся ситуации по мере снятия противоэпидемических ограничений. Эти опросы чётко сигнализируют, что мир изменился и абсолютного возврата к до «Ковидной» картине не будет. Мир переходит на гибридные схемы работы, когда одна часть сотрудников останется полностью на удалённой работе, другая – вернётся в офис, а третья – будет делить своё рабочее время между офисной и удалённой работами. ИТ-руководители всё больше полагаются на использование облачных сервисов, что позволяет им гибко реагировать на изменения с точки зрения нагрузки и масштабирования ресурсов. В то же время в связи со значительным использованием не управляемых компаниями устройств (BYOD) возникают новые задачи по обеспечению защиты корпоративных ресурсов, что подтверждается опросами руководителей ИТ и ИБ. В ответ на эти вызовы Citrix предлагает своим заказчикам дополнительные решения и сервисы по защите удалённых пользователей от различных типов угроз. В 2019 году компания Gartner выделила новое направление – граничные сервисы безопасности SASE, которые представляют собой комбинацию сетевых решений и сервисов по информационной безопасности.

Такой подход обеспечит защиту удалённых пользователей, оказавшихся за пределами корпоративного периметра.

Таким образом, в ближайшей перспективе можно ожидать большой спрос на решения по обеспечению безопасности удалённой работы; перенос рабочей нагрузки в облака, как публичные, так и гибридные, с использованием различных облачных сервисов; повышение комфортности работы, в том числе и с мобильных устройств; поиск оптимального соотношения гибридной работы – офис/дом; трансформацию офисных пространств и правил посещения и работы в офисе. Также компании будут внимательнее подходить к составлению планов по обеспечению непрерывности работы бизнеса с учётом полученного в 2020 году опыта и их регулярному пересмотру и актуализации.

citrix

Халяпин Сергей Николаевич,
главный инженер Citrix

www.citrix.ru

CIS / № 1 (15) / 2021 / www.cis.ru

Электронная подпись как главный помощник во время пандемии

На сегодняшний день для всех основной целью является обеспечение безопасности здоровья своего и своих близких в условиях пандемии COVID-19. Но работу никто отменял, как и потребность в получении государственных услуг, связанных с физическим контактом с другими людьми.

Многие компании до сих пор сохраняют дистанционный режим работы для большинства своих сотрудников. Как же оптимизировать деятельность организации в таком режиме? И как граждане смогут получать государственные услуги, не выходя из дома? Ответ прост: здесь пригодится электронная подпись, которую многие до сих пор называют «ЭЦП».

Что это такое?

Для многих электронная подпись до сих пор остаётся непонятной штукой, хотя создание ЭЦП уходит корнями в середину 70-х годов прошлого столетия. Её активное использование началось только с развитием интернета. Говоря простым языком – это аналог собственноручной подписи, состоящий из уникального набора цифровых символов. С помощью неё можно подписывать различные договоры и подтверждать свою личность на государственных порталах.

Документ, который необходимо удостоверить, может иметь не только текстовый формат rtf- или pdf-файла, но и любой иной компьютерный файл, содержащий графику, звук, видео, программу. С помощью электронной подписи можно не только защитить их от внесения изменений, но и подтвердить авторство.

Какие операции можно совершать с помощью ЭЦП?

Обычные граждане или, как принято говорить, физические лица, могут:

- оформить российский или заграничный паспорта;
- работать с документами в Росреестре для сделок с недвижимостью;
- оформить трудовой договор;
- произвести регистрацию по месту жительства;
- подать заявление в ЗАГС;
- зарегистрировать транспортное средство;
- подать документы в ВУЗ.

Юридические лица и индивидуальные предприниматели могут выполнять следующие операции:

- встать на учёт в налоговом органе;
- сдавать отчётность в различные государственные структуры;
- регистрировать онлайн-кассы в ФНС;
- участвовать в электронных торгах;
- обмениваться документами с помощью системы ЭДО.

И это далеко не весь список операций, которые можно делать с помощью электронной подписи.

Где получить ЭЦП?

Квалифицированный сертификат электронной подписи имеют право выпускать только аккредитованные Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации удостоверяющие центры (далее – УЦ). Актуальный список аккредитованных УЦ можно найти на официальном сайте ведомства.

Чтобы получить ЭЦП, заявителю необходимо предоставить три основных документа:

- паспорт;
- СНИЛС;
- ИНН.

Безопасность в использовании

Для обработки электронной подписи используется пара криптографических ключей:

- закрытый (секретный) – он позволяет зашифровать содержание подписываемого документа в уникальную последовательность символов, то есть заверить документ;
- открытый – позволяет расшифровать подпись и тем самым её проверить.

Квалифицированная электронная подпись имеет высокую степень защиты благодаря специальному коду шифрования, ключ от расшифровки которого находится у владельца.

Число вариантов ключей и их сочетаний столь велико, что сегодня подобрать подходящие к конкретному документу даже с использованием самых мощных компьютеров (из числа имеющихся) практически невозможно. То есть злоумышленник не сможет подделать чужую подпись или незаметно изменить содержание документа.

Срок действия электронной подписи, как правило, составляет двенадцать месяцев с момента создания сертификата и в обязательном порядке указывается в сертификате ключа проверки электронной подписи. Для продолжения работы с электронной подписью по окончании указанного в сертификате срока необходимо обратиться в УЦ для формирования новой ЭЦП.

Как работают УЦ в период пандемии?

Для знакомства с УЦ в Москве мы выбрали Национальный удостоверяющий центр (НУЦ) и узнали о тонкостях работы из первых рук от ведущего специалиста отдела внешних и внутренних коммуникаций Полторацкой Алины.

В первую очередь отметим, что в офисе НУЦ соблюдаются все рекомендуемые меры безопасности: работники обслуживают клиентов строго в масках и перчатках, а если у пришедшего человека нет средств индивидуальной защиты, УЦ предоставляет маску и пару перчаток. Во время «первой волны» приём клиентов осуществлялся только по предварительной записи, чтобы не допускать большого скопления людей и нарушения рекомендованной социальной дистанции.

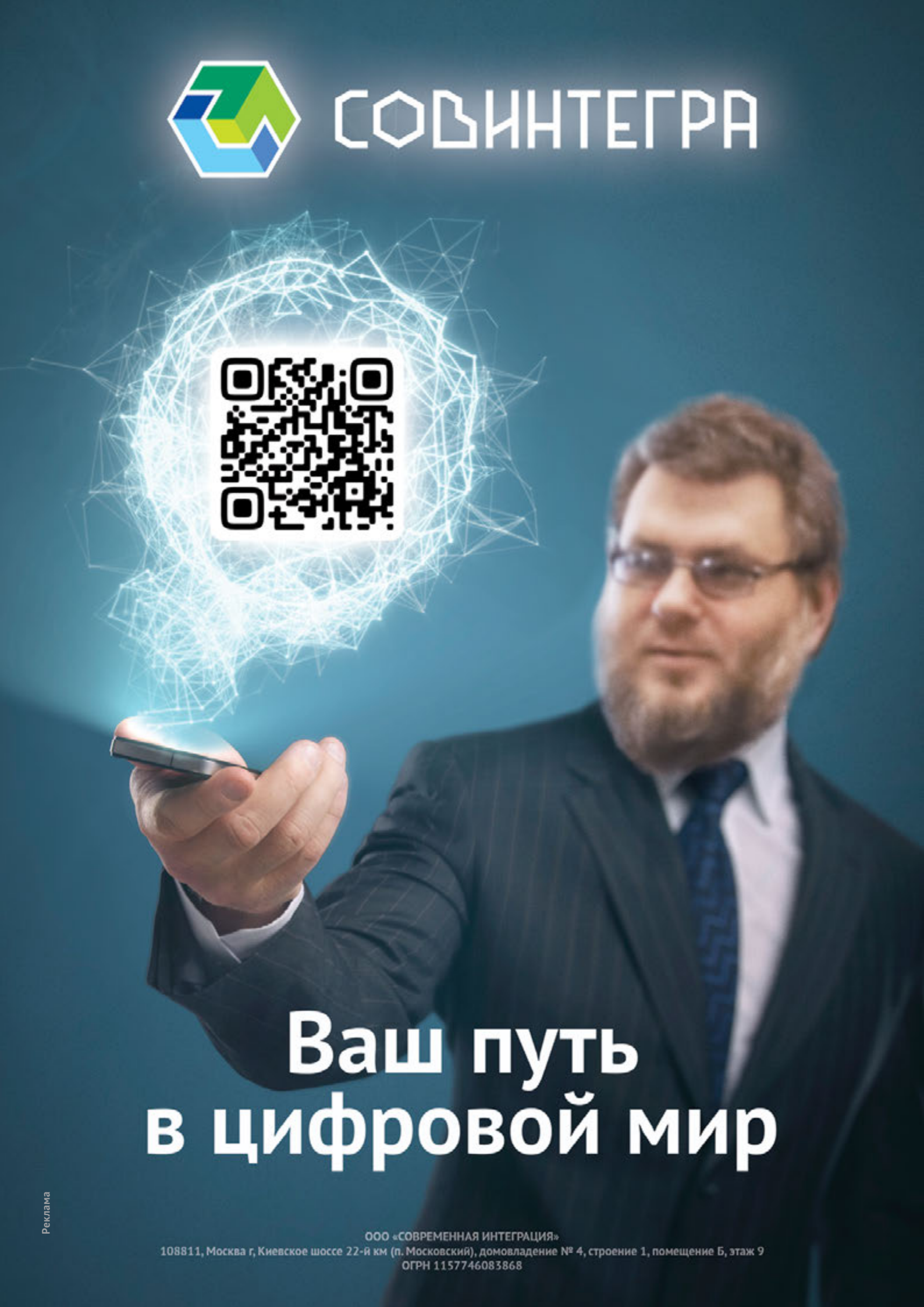
Сейчас УЦ обходится без неё, поскольку оборудовал ещё одно помещение для приёма клиентов. Также в целях улучшения качества обслуживания центральный офис (который находится по адресу: г. Москва, ул. Авиамоторная, д. 8, стр. 1) увеличил своё время работы до 21:00 с понедельника по четверг.

Как вы поняли, электронная подпись является действительно важным и удобным средством для решения различных задач в повседневной и деловой среде. Выбор – использовать ЭЦП или нет – всегда остаётся за вами.

НАЦИОНАЛЬНЫЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР

«Национальный удостоверяющий центр»

www.nucrf.ru



Аутентификация как она есть

Анатолий Лебедев
доцент МГТУ
им. Н. Э. Баумана

Аутентификация (от англ. – authentication) или подтверждение подлинности – это процедура проверки соответствия субъекта информационной системы тому набору характеристик, который полностью представляет (однозначно определяет) его в рамках данной информационной системы.

Обычно такая проверка производится с помощью некой уникальной информации, имеющейся у субъекта (секретного пароля, кода доступа или криптографического ключа) или неотторжимого индивидуального свойства субъекта (например, некоторой биометрической характеристики субъекта-человека: отпечатка пальца, рисунка вен кисти руки, рисунка сетчатки глаза и т. п.), или способности производить определённые действия (например, возможности открыть ключом механический замок или вычислить электронную подпись под заданным блоком данных), которой может обладать только этот субъект.

Фактически вся защита информации в современных информационных системах начинается именно с процедуры аутентификации пользователей. Каждый пользователь современных информационных систем сталкивается с процедурами аутентификации многократно в течение рабочего дня.

Все известные способы несанкционированного доступа к информации или ресурсам информационных систем так или иначе опираются на методы нарушения самого процесса аутентификации или на методы обхода системы аутентификации субъектов информационной системы.

Термины и определения

В современных учебниках по информационным технологиям и в действующих нормативных документах обычно принимаются следующие термины и определения из области аутентификации.

Идентификация – это процедура распознавания субъекта в рамках информационной системы по некоторому его идентификатору (формальному имени), действующему в рамках данной системы.

В процессе первичной регистрации в рамках конкретной информационной системы субъект формирует (самостоятельно или с помощью администратора системы) свой идентификатор, который регистрируется в базе идентификаторов субъектов системы. В дальнейшем при каждом обращении субъекта к ресурсам информационной системы он предъявляет свой идентификатор, а служба идентификации информационной системы проверяет наличие этого идентификатора в базе данных идентификаторов субъектов системы. Субъекты информационной системы, идентификаторы которых известны системе, считаются легальными (законными), остальные субъекты относятся к нелегальным.

Аутентификация – это процедура проверки подлинности субъекта в рамках информационной системы, позволяющая достоверно убедиться в том, что субъект, предъявивший некоторый зарегистрированный в системе идентификатор, на самом деле является именно тем субъектом, идентификатор которого он использует.

Для этого он должен подтвердить не только факт обладания данным идентификатором, но также дополнительно подтвердить факт обладания некоторым материальным объектом (например, ключом от сейфа, смартфоном, банковской картой или аппаратным токеном) или некоторой информацией, которые могут быть доступны только легальному субъекту информационной системы с данным идентификатором (код доступа, пароль, криптографический ключ, биометрические данные и т. д.).

Авторизация – это процедура предоставления субъекту информационной системы определённых прав доступа к ресурсам этой информационной системы (привилегий) только после успешного прохождения им процедуры аутентификации.

Для каждого субъекта в информационной системе определяется конкретный набор прав (привилегий), которыми он может воспользоваться при обращении к её ресурсам.

Для того, чтобы обеспечить управление и контроль над данными процедурами, дополнительно используются процессы администрирования и аудита в рамках информационной системы.

Администрирование – это процесс управления доступом субъектов к ресурсам информационной системы.

Данный процесс включает в себя:

- создание идентификатора субъекта (создание учётной записи пользователя) в рамках данной системы;
- управление данными субъекта, используемыми для его аутентификации (смена кода доступа или пароля, выпуск сертификата криптографического ключа и т. п.);
- управление правами доступа субъекта к ресурсам системы.

Аудит – это процесс контроля (мониторинга) доступа субъектов к ресурсам информационной системы, включающий протоколирование действий субъектов при их доступе к ресурсам системы с целью обеспечения возможности обнаружения несанкционированных действий.

Пять элементов аутентификации

В любой системе аутентификации всегда присутствует пять основных *элементов аутентификации* и происходят определённые события.

Первый элемент аутентификации – это субъект аутентификации – конкретный человек или группа людей, или компьютерная программа, устройство, или процесс, которые должны проходить аутентификацию.

Второй элемент аутентификации – *отличительная характеристика* (опознавательный знак, аутентификатор), которая отличает конкретного субъекта аутентификации от других в рамках данной информационной системы.

Третий элемент – *владелец системы* (администратор), который управляет ею и несёт ответственность за использование информационной системы, полагаясь на выбранный механизм аутентификации в процессе разграничения авторизованных субъектов от всех остальных.

Четвёртый элемент – *механизм аутентификации,* который позволяет проверить присутствие у субъекта информационной системы именно той отличительной характеристики, которая выделяет его среди всех других. При успешном прохождении аутентификации субъекту информационной системы должны быть присвоены (выданы) некоторые права (привилегии).

Для этого служит пятый элемент – *механизм управления доступом*. С помощью этого же механизма субъект лишается прав (привилегий), если аутентификация была неуспешной.

Примеры этих элементов процесса аутентификации приведены в таблице.

Элемент процесса аутентификации	**Авторизация пользователя компьютерной системы**	**Пользователь (клиент) по отношению к интернет-сервису**	**Интернет-сайт по отношению к клиенту**
Субъект аутентификации: человек, процесс, программа или устройство	Легальный пользователь компьютерной системы (человек)	Легальный пользователь (клиент) интернет-сервиса (человек)	Интернет-сайт (его владелец)
Отличительная характеристика, опознавательный знак, аутентификатор	Секретный персональный пароль пользователя, программное или аппаратное (токен) средство вычисления электронной подписи под запросами сервиса аутентификации, содержащее закрытый ключ ЭП субъекта аутентификации	Секретный персональный пароль пользователя, одноразовый цифровой код (push code), высылаемый пользователю сервисом по дополнительному каналу (например, по каналу мобильной связи), банковская карта и персональный идентификационный номер, программное или аппаратное (токен) средство вычисления электронной подписи под запросами сервиса аутентификации, содержащее закрытый ключ ЭП, биометрические характеристики субъекта аутентификации – человека (отпечатки пальцев, фотография или видео лица или фигуры, рисунок вен кисти руки, рисунок радужной оболочки или сетчатки глаза и т.д.)	Открытый ключ проверки электронной подписи владельца сайта в его цифровом сертификате, выданном лицом или организацией, вызывающей доверие пользователя сайта
Служба аутентификации, администратор, хозяин, владелец системы	Лицо, организация, которой принадлежит или которой обслуживается компьютерная система	Лицо, организация, которой принадлежит или которой обслуживается данный интернет-сервис	Орган, выдающий цифровые сертификаты открытых ключей владельцев (администраторов) интернет-сайтов
Механизм аутентификации	Программное обеспечение, проверяющее подлинность паролей легальных пользователей системы или электронных подписей под ответами пользователей системы на запросы сервиса аутентификации	Специальная аппаратура или программное обеспечение, проверяющие подлинность паролей, одноразовых цифровых кодов (push code), электронных подписей клиентов под запросами сервиса аутентификации, подлинности данных банковской карты и ПИН-кода клиента банка или платёжной системы, биометрических характеристик субъекта аутентификации – человека	Системное программное обеспечение операционной системы компьютера, планшета или смартфона клиента, проверяющее подлинность электронной подписи владельца сайта под его содержимым в целом или под отдельными его разделами
Механизм управления доступом	Процесс регистрации пользователей и управления доступом к ресурсам компьютерной системы	Разрешение на выполнение той или иной операции в рамках конкретного Web-сервиса, в частности, разрешение на проведение банковской транзакции	Метки браузера клиента, сообщающие ему о защищённом или незащищённом статусе сайта

Факторы аутентификации

Выделяют всего три типа факторов аутентификации, используемых на практике в различных комбинациях при аутентификации субъектов различных информационных систем. Все типы факторов приведены в таблице.

Тип фактора аутентификации	**Классификация типов факторов аутентификации по NCSC-TG-017**[1]	**Примеры факторов аутентификации**
На основе знания чего-либо	Type 1: Authentication by Knowledge	• Пароль или парольная фраза • PIN-код (Personal Identification Number) • Одноразовый пароль, присылаемый субъекту по каналам сотовой связи
На основе обладания чем-либо	Type 2: Authentication by Ownership	• Физический (механический) ключ • Карта с магнитной полосой • Микропроцессорная смарт-карта • OTP-токен, генерирующий одноразовый пароль • Аппаратный модуль шифрования • Аппаратный токен, вычисляющий электронную подпись
На основе биометрических характеристик	Type 3: Authentication by Characteristic	• Отпечаток пальца • Фотография лица • Голос • Рисунок сетчатки глаза • Рисунок вен кисти руки • Клавиатурный почерк • Движения руки при работе со смартфоном • Движения губ человека при произнесении парольной фразы • Форма ушных раковин человека • Импульсы коры головного мозга человека

В некоторых компаниях организуется так называемый «строгий контроль» доступа в помещение, т.е. в определённые помещения доступ предоставляется только ограниченному числу лиц. Например, в серверную комнату может войти только администратор или в комнату финансового отдела компании могут иметь доступ только его сотрудники. Если при этом установить для компьютеров, находящихся в этих помещениях, строго определённые IP-адреса, то тогда появляется возможность усиления аутентификации при доступе сотрудников к ресурсам компьютерной сети. Им предоставляется доступ к определённым действиям или данным только в том случае, если они это делают в строго обозначенном помещении и, соответственно, с определённых компьютеров, имеющих определённые IP-адреса.

В этом случае иногда говорят об использовании «четвёртого» типа фактора аутентификации – *аутентификации на основе места проведения процедуры*. Он не считается дополнительным типом факторов аутентификации, так как не может использоваться отдельно от других факторов для аутентификации субъекта. Поскольку, как правило, на практике эффективно нельзя обеспечить, чтобы только определённый сотрудник работал на строго определённом рабочем месте (компьютере), данный «фактор» нецелесообразно выделять как дополнительный тип фактора аутентификации.

В последнее время наметилась тенденция интеграции логических средств аутентификации и средств контроля и управления доступом (СКУД).

Смарт-карты, используемые для аутентификации пользователя при попытке доступа к ресурсам компьютерной системы, интегрируются с метками RFID (радиочастотной идентификацией). В этом случае появляется возможность дополнительно использовать их для аутентификации человека при его физическом доступе в различные помещения. По-прежнему в этом случае речь будет идти об использовании аутентификации «на основе обладания чем-либо». Это расширяет возможности использования смарт-карты, даёт дополнительные удобства для пользователя, но не усиливает аутентификацию.

Процедура аутентификации может быть реализована с использованием одного из перечисленных трёх типов факторов аутентификации. Например, в процессе аутентификации у пользователя может быть запрошен пароль, либо потребуется представить отпечаток пальца.

Многофакторная аутентификация

Аутентификация, в процессе которой используется только один тип факторов аутентификации, называется *однофакторной,* несколько типов – *многофакторной*.

1. NCSC-TG-017 – документ A Guide to Understanding Identification and Authentication in Trusted Systems, опубликованный U.S. National Computer Security Center. Руководство содержит комплект рекомендуемых инструкций по процедурам идентификации и аутентификации.

Например, если в процессе аутентификации пользователь должен использовать смарт-карту и дополнительно пароль (или PIN-код), то такая аутентификация считается двухфакторной.

Также используются понятия двухфакторной и трёхфакторной аутентификации при использовании в её процессе комбинации двух и трёх различных типов аутентификационных факторов, соответственно.

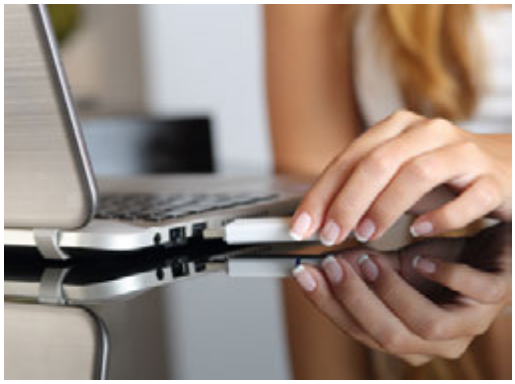
В цитированном выше документе NCSC-TG-017 вводятся термины для различных видов многофакторной аутентификации: аутентификация типа 12, типа 23, типа 13 и типа 123. *Аутентификация типа 12* – аутентификация, в процессе которой используются два фактора аутентификации: первый (на основе знания чего-либо) и второй (на основе обладания чем-либо).

Соответственно, определяются и другие типы двухфакторной аутентификации: *аутентификация типа 13* и *аутентификация типа 23*. Также определена трёхфакторная аутентификация, в процессе которой используется комбинация факторов аутентификации всех трёх типов («на основе знания чего-либо», «на основе обладания чем-либо» и «на основе биометрических параметров субъекта»). Такую аутентификацию называют *аутентификацией типа 123*.

Считается, что процедура, использующая в процессе аутентификации только один тип факторов, с большей вероятностью может быть уязвима по отношению к внешним атакам. Комбинация в процедуре аутентификации двух и более типов факторов аутентификации обеспечивает большую безопасность ресурсов информационной системы.

На практике наиболее широко распространено использование комбинации двух типов факторов аутентификации. Например, при аутентификации пользователя банковской карты в банкомате или торговом терминале, а также при покупках в интернете требуется одновременно использовать карту с магнитной полосой или чипом и CVV-код пользователя этой карты, или же в дополнение к нему ещё и присылаемый по каналам сотовой связи одноразовый пароль для выполнения конкретной транзакции.

При аутентификации пользователей компьютерных систем часто используется процедура аутентификации типа «логин-пароль» в сочетании с аппаратным токеном пользователя, подключаемым к USB-порту компьютера.



Два принципиально разных подхода

В мире в настоящее время выделяются два принципиально различающихся подхода к использованию биометрического фактора аутентификации людей как субъектов распределённых информационных систем.

Первый состоит в том, чтобы этот фактор аутентификации как наиболее чувствительный с точки зрения нарушения их прав и требований защиты персональных данных, *использовался только локально*.

То есть субъект может аутентифицироваться по биометрическим данным только на устройствах, которые находятся непосредственно в его личном распоряжении и никогда не передаются посторонним вместе с зафиксированными в их памяти его биометрическими параметрами.

Например, это может быть процесс аутентификации пользователя при использовании его персонального мобильного телефона, планшета или ноутбука. Но при этом вся информация о биометрических параметрах пользователя остаётся только в памяти его персонального гаджета и не участвует непосредственно (то есть не передаётся на серверы службы аутентификации) при дистанционной аутентификации его как субъекта распределённой информационной системы.

При таком подходе удаётся достигнуть разумного компромисса между требованиями надёжности системы аутентификации, её удобства для «простого» пользователя, который не в силах запоминать или хранить в надёжно защищённом виде периодически сменяемые сложные пароли или длинные ПИН-коды, и соблюдением всех требований приватности и защиты персональных данных субъекта.

Биометрические характеристики субъекта никогда не покидают устройств, находящихся под его непосредственным контролем, и уж тем более не передаются на удалённые серверы информационных систем и не собираются на них в огромные базы данных. Они служат лишь для допуска к локальным устройствам. Последние же могут на них использоваться после первичной аутентификации субъекта для реализации надёжных процедур дистанционной строгой аутентификации на удалённых серверах уже при помощи сложных вычислительных процедур цифровой аутентификации типа шифрования, хэширования или электронной подписи.

Именно такой подход был положен в основу так называемой универсальной инфраструктуры аутентификации (Universal Authentication Framework, UAF), а также в основу протоколов применения универсального второго фактора аутентификации (Universal 2-nd Factor, U2F) – компактного аппаратного внешнего модуля (токена), подключаемого к персональному компьютеру пользователя именно для целей строгой двухфакторной аутентификации.

Этот подход был впервые предложен международным альянсом по удалённой аутентификации FIDO Alliance (Fast IDentity Online), созданным в 2012 году, и с тех пор успешно развивается во многих странах. Его первоначальными участниками были корпорации Google, Yubico, Microsoft, Visa, Master Card, American Express, PayPal и др.

Со стороны пользователя протокол двухфакторной строгой аутентификации выглядит так (рис. 1).

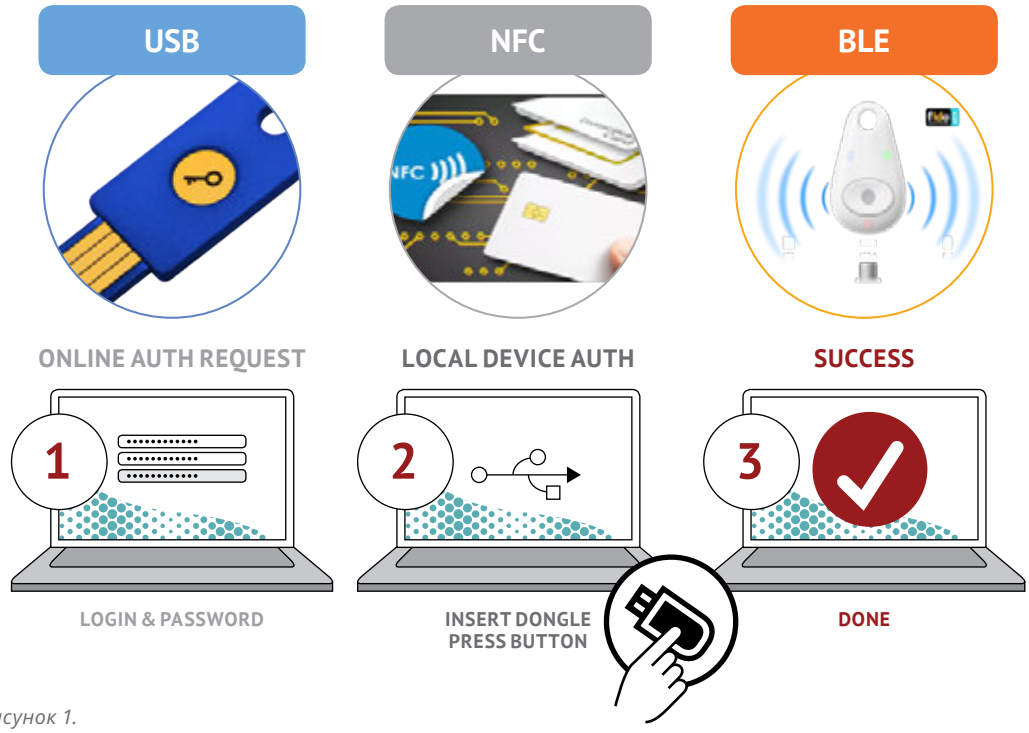


Рисунок 1.

Схема взаимодействия с браузером клиента может быть представлена следующим образом (рис. 2).

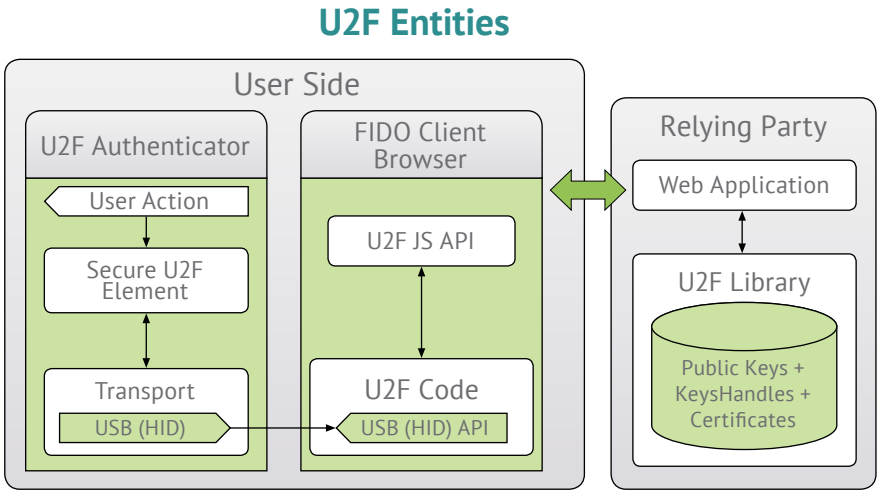


Рисунок 2.

Формальный протокол взаимодействия сторон при выполнении процедур строгой многофакторной аутентификации пользователей компьютерной системы по схеме FIDO Alliance можно представить следующим образом (рис. 3).

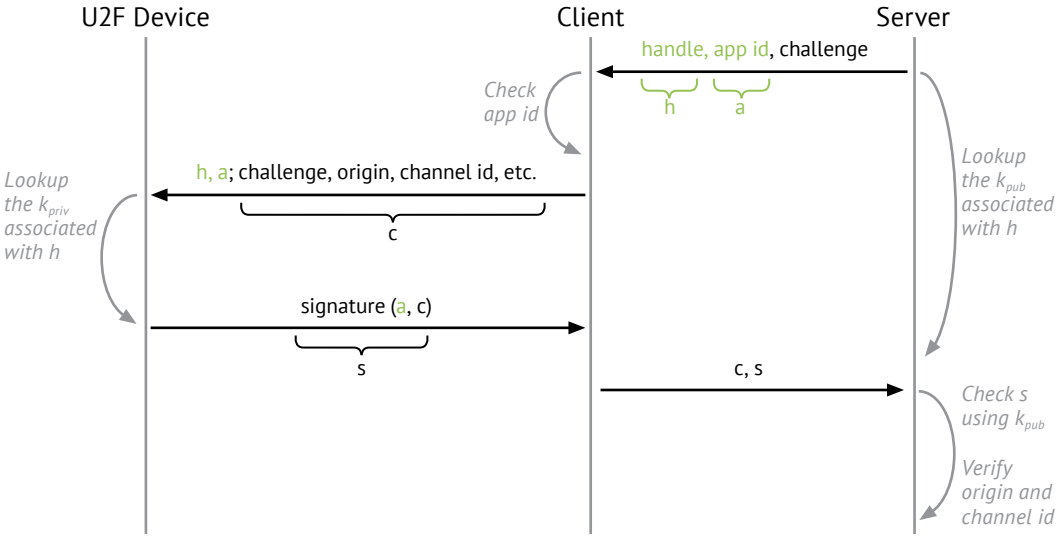


Рисунок 3.

Другой подход был предложен в проектах и развитии отечественных глобальных систем аутентификации, таких как Единая система идентификации и аутентификации (ЕСИА) и Единая биометрическая система (ЕБС). Основные этапы развития системы ЕСИА таковы:

- 2010 г. – запуск первой версии системы ЕСИА;
- 2011 г. – начальный этап развития системы ЕСИА: обеспечена возможность доступа пользователей к региональным порталам государственных услуг;
- 2012 г. – дальнейшее развитие системы ЕСИА: обеспечена возможность идентификации и аутентификации пользователей при доступе к информационным системам других участников взаимодействия с системой ЕСИА;
- 2014 г. – приказ Минкомсвязи РФ «О вводе в эксплуатацию модернизированной версии Единой системы идентификации и аутентификации...» (ЕСИА);
- С 2015 г. по настоящее время – последовательное расширение функционала системы ЕСИА, интеграция с ЕБС.

Процедура выполнения аутентификации клиента банка при посредстве системы ЕСИА, например для проведения банковской операции по оплате товара или услуги, может быть представлена следующим образом (рис. 4).

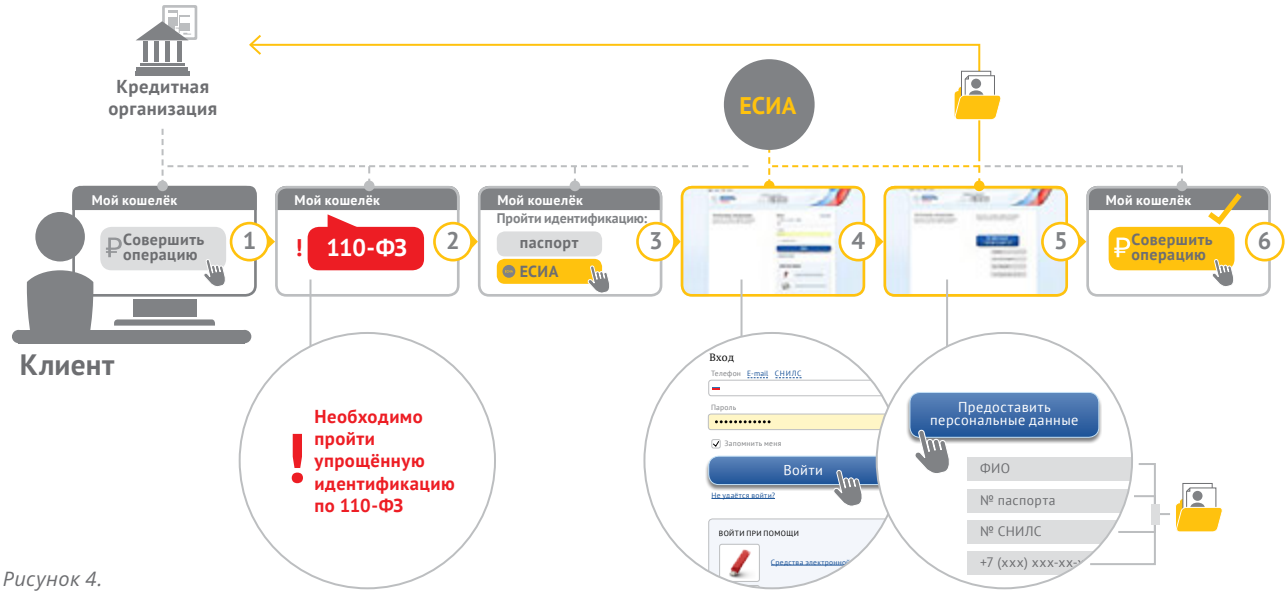


Рисунок 4.

Как видно из представленной схемы процедуры аутентификации, все необходимые для этого процесса персональные данные (ФИО, номер паспорта, номер СНИЛС, номер мобильного телефона +7 (XXX) XXX-XX-XX и т.д.) собираются в единой базе данных и служат как уникальный идентификатор пользователя системы ЕСИА.

В первоначальных версиях системы ЕСИА использовался протокол аутентификации SAML (Security Assertion Markup Language), который может быть представлен следующим образом (рис. 5).

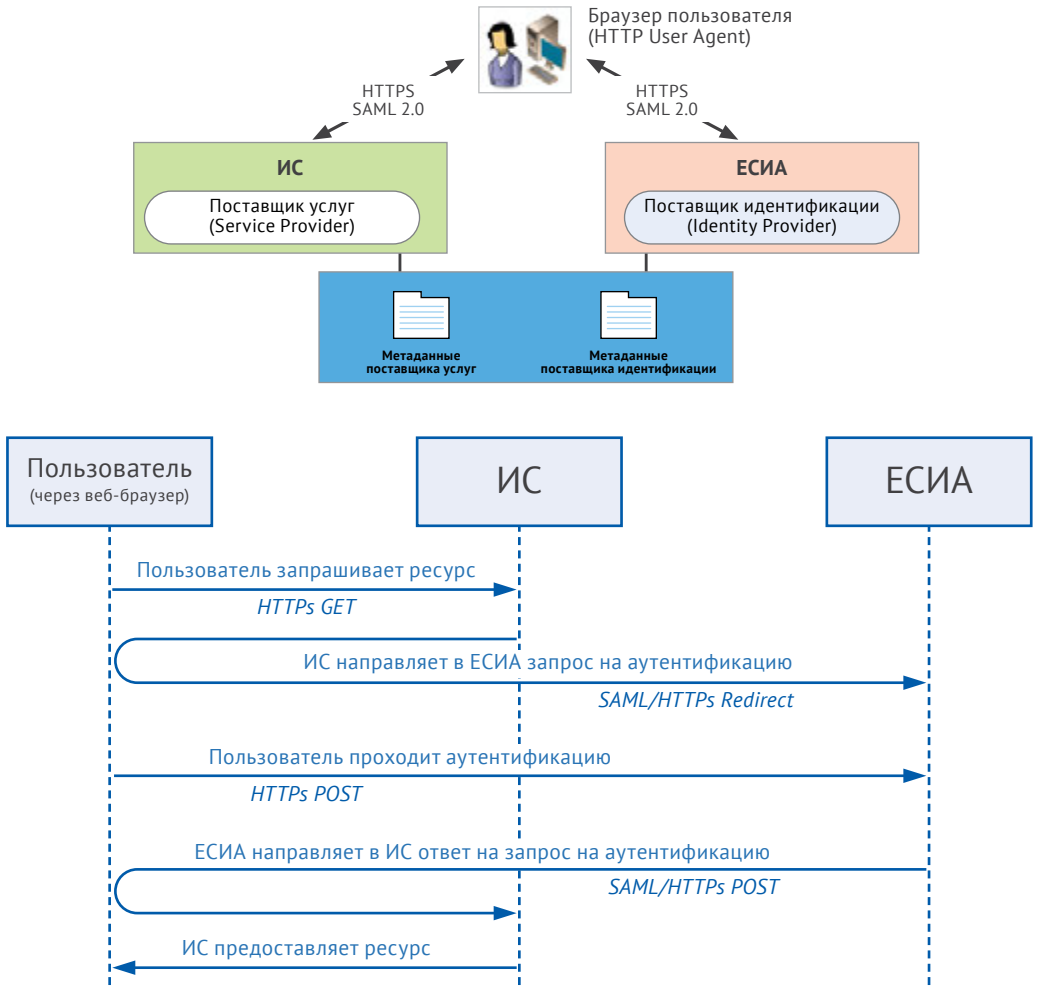


Рисунок 5.

Этот протокол считается устаревшим с 2018 года, поэтому в новых версиях системы он был заменён протоколом OpenID Connect 1.0, который можно представить следующим образом (рис. 6).

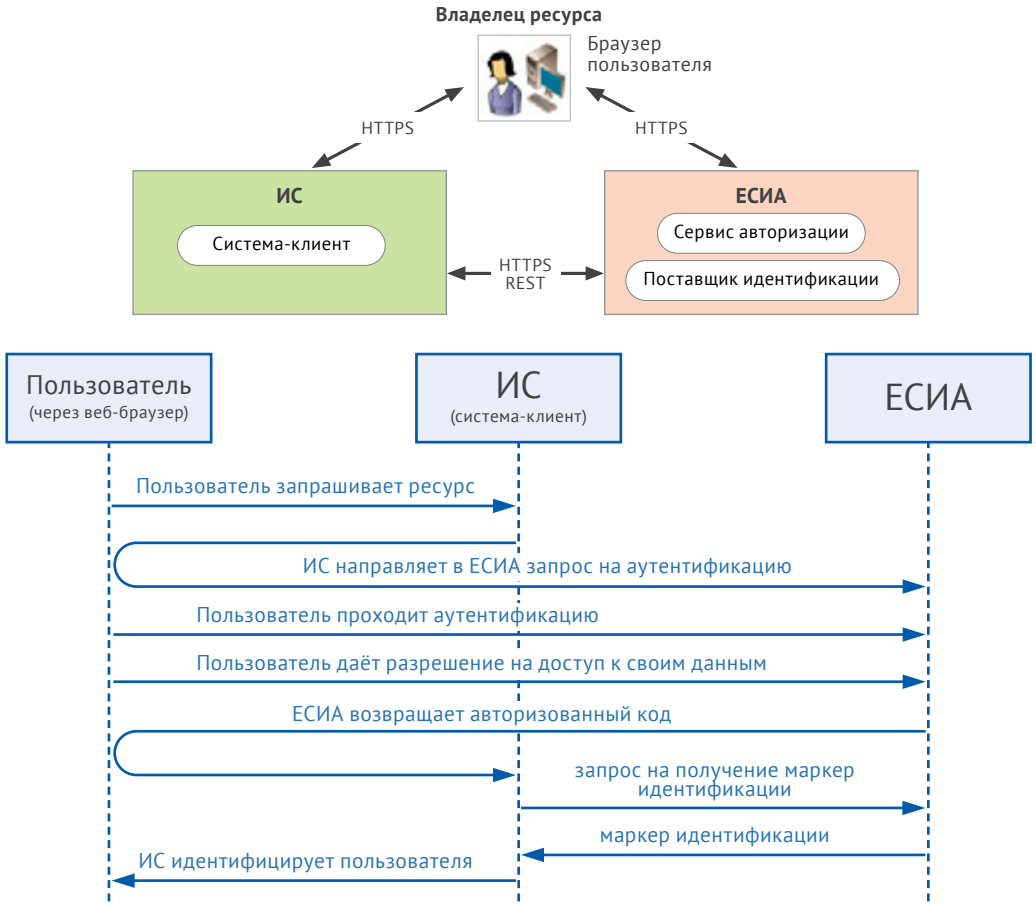


Рисунок 6.

Уже сам факт сбора в единой базе данных персональной информации обо всех пользователях системы ЕСИА, а также тот факт, что эти практически неизменные (одинаковые для конкретного пользователя в течение длительного периода времени) персональные данные пользователь вынужден предъявлять каждый раз в процессе аутентификации вызывает серьёзные сомнения в безопасности такой системы аутентификации.

При самом оптимистическом подходе к оценке надёжности системы защиты информации на серверах ЕСИА следует предполагать, что утечка персональных данных пользователей из единой централизованной базы данных будет происходить регулярно. А это касается такой персональной информации, которую пользователь не сможет оперативно изменить. Поэтому следует исходить из того, что такой подход к аутентификации пользователей информационных систем гораздо более подвержен атакам, чем описанный выше подход FIDO.

Более того, в Единой биометрической системе аутентификации (ЕБС) предполагается собирать и хранить в единой базе данных такие биометрические характеристики всех субъектов, как запись голоса и видео изображения лица. При этом предполагается, что и в ходе процесса аутентификации пользователь также передаёт свои биометрические характеристики по каналам общедоступных сетей (пусть даже с применением надёжных средств защиты) на серверы центральной базы данных систем ЕСИА и ЕБС.

Даже абстрагируясь от того факта, что персональные устройства для сбора биометрических данных пользователя (Web-камера и микрофон компьютера, планшета или смартфона) в ходе конкретного процесса аутентификации могут сильно отличаться по качеству от той профессиональной аппаратуры, с помощью которой они получались от этого пользователя при первичной регистрации в системе, а потому они будут вносить сильные искажения в измеряемые биометрические характеристики (снижая качество аутентификации), можно сказать, что и в этом случае сбор неизменяемых биометрических данных всех пользователей системы в единой базе приводит к увеличению опасности серьёзных утечек этих данных.

Таким образом, на основании объективного анализа базовых процедур, положенных в основу процесса аутентификации пользователей информационных систем на основе принципов FIDO и принципов ЕСИА-ЕБС, следует признать первый гораздо более надёжным, безопасным и эффективным, чем второй.

Анатолий Лебедев
доцент МГТУ им. Н.Э. Баумана

Краткая история Security Awareness

История преступности в Интернет началась вместе с его появлением. Как только всемирная сеть стала основным ресурсом, преступники начали использовать её в своих целях.

Владимир Безмалый
Microsoft Security Trusted Advisor
Microsoft MVP
Kaspersky Certified Trainer
Консультант ООН по информационной безопасности

Одним из самых первых примеров такого вида преступлений стал арест группы 414, названной так в честь кода города Милуоки. Данная группа была арестована за взлом примерно 60 различных компьютеров. К ним относились устройства, расположенные от Мемориального онкологического центра Слоуна-Кеттеринга, вплоть до устройств, расположенных в Национальной лаборатории Лос-Аламоса.

Правительство очень быстро отреагировало на новую угрозу. С целью предотвращения подобных преступлений был принят Закон о компьютерном мошенничестве и злоупотреблениях. Была сформирована группа реагирования на компьютерные чрезвычайные ситуации и в целях расследования растущего числа взломов и потенциальных методов защиты.

Десятилетие 80-х закончилось появлением первой признанной версии «червя». За атакой стоял хакер Роберт Моррис, и даже вначале его самораспространяющийся вирус был способен нанести огромный ущерб. Фактически, в то время он отключил почти всю всемирную паутину. Вирус Морриса также был первой версией широко распространённой атаки DoS (Denial of Service «отказ в обслуживании»). Подобная атака на вычислительную систему производится с целью довести её до отказа, то есть создать такие условия, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

Данная и последующие атаки интересны прежде всего потому, что именно они послужили толчком для создания большей части того, что сегодня принято называть кибербезопасностью. В результате атак появились CERT (компьютерные группы реагирования на чрезвычайные ситуации). Именно после этого компании начали понимать, насколько они действительно уязвимы. И в результате этого во многих компаниях стали осознавать, что профилактика куда лучше лечения.

На протяжении 1990-х преступники продолжали свои атаки, но большинство жертв в этот момент времени были либо правительственными организациями, либо транснациональными компаниями.

В 1998 году Бюро статистики труда стало жертвой одной из первых версий спама, когда оно получило сотни тысяч информационных запросов.

В 1999 году Джонатан Джеймс смог удалённо подключиться к одному из компьютеров Министерства обороны США и с помощью программы получил доступ к сообщениям, реальным именам сотрудников и их действующим паролям. Полученная Джеймсом информация, разумеется, была секретна и касалась в основном планов по защите Штатов от потенциальных угроз. Но, пожалуй, самое главное, в его руках оказался даже программный код системы жизнеобеспечения космонавтов на Международной космической станции. На момент первой атаки Джеймсу было 16 лет.

В результате этих и других кибератак Министерство юстиции США создало Национальный центр защиты инфраструктуры. Его миссия заключалась в защите телекоммуникационных, транспортных и технологических систем страны от хакеров.

Расцвет современного хакерства

Гораздо большее распространение проблема хакерства получила в начале 2000-х годов, когда оно превратилось в проблему, которую мы знаем сегодня. Вполне понятно, что она совпадает с увеличением числа пользователей Интернет.

В это время уже стало понятно, что выполнять такие атаки могут уже не только люди, обладающие техническими навыками, равные или даже превосходящие по своему уровню знаний ведущих специалистов мира.

Появлялось все больше статей на тему, как именно ломать. Широкое распространение получают как платные, так и бесплатные средства для взлома. В то же время огромное количество пользователей Интернет являются в своей массе низкоквалифицированными.

В результате даже те, кто никогда не пытался совершить кибератаку, смог стать реальной угрозой менее чем за месяц. В 2005 году хакер по имени Альберт Гонсалес использовал свои способности для создания преступной сети хакеров – цифровой организованной преступности, чтобы украсть информацию с более чем 45 миллионов платёжных карт, выпущенных TJX, розничным продавцом в США, владеющим TJ Maxx и версией для Великобритании – TK Maxx.

Прежде чем быть пойманными и приговорёнными к 20 годам тюремного заключения, группа Гонсалеса будет нести ответственность за ущерб в размере 265 миллионов долларов.

Помимо очевидных масштабов преступления, этот инцидент примечателен тем, что повлиял на бизнес. Характер украденных данных регулировался, поэтому каждый инцидент требовал уведомления властей. Кроме того, этим компаниям необходимо было выделить деньги для выплаты компенсации пострадавшим.

В результате деловой мир понял, что хакерство – это куда больше, чем просто лёгкая неприятность!

Осведомлённость о безопасности

Увы, как вы понимаете, кибератаки не замедлились. В 2013 году нарушение мер безопасности Target стало ещё одним шокирующим напоминанием миру о том, насколько уязвимы даже крупнейшие корпорации. Около 40 миллионов клиентов провели дни после Дня благодарения, проверяя свои счета, чтобы узнать, не украли ли у них деньги.

Другая причина, по которой здесь упоминается атака Target, заключается в том, что используемый уровень сложности стал очередной вехой в истории кибербезопасности. В отличие от прямого нападения на TJX, преступники, добившиеся успеха с Target, атаковали компанию-поставщика Target.

Они выбрали стороннюю компанию, которая поставляла Target решения для отопления и вентиляции. Хакеры воспользовались моментом и нанесли удар. Номера кредитных карт присутствовали в незашифрованном виде в памяти системы в течение короткого времени.

Это также показало деловому миру, что последствия такой атаки вызовут волну во всех направлениях. Кибербезопасность теперь является проблемой на уровне совета директоров, поскольку после кражи генеральный директор Target фактически ушёл в отставку.

Это привело к осознанию необходимости совершенно иначе относиться к вопросам безопасности. Безусловно, в компании нужна своя служба безопасности и профессионалы, которые смогут её настроить, запустить и сопроводить.

Но стоит учесть, что и злоумышленники поняли, что гораздо проще атаковать не компьютерную сеть компании, а людей, которые работают в этой компании. Ведь сегодня более 80% всех успешных атак осуществляются атаками на сотрудников.

Подход сверху вниз

Самая важная особенность осведомлённости о безопасности заключается в том, что сотрудники не могут просто изучать меры, которые им придётся применять. Необходимо применять подход сверху вниз. Ведь руководство компании становится первой и причём лёгкой мишенью, если они сами не знают о том, каким атакам могут быть подвергнуты. Более того, если руководство не подчиняется принятым в компании мерам безопасности, то вскоре они становятся пустышкой и их не соблюдает уже весь персонал.

Составление бюджета на осведомлённость о безопасности

Как узнать, насколько серьёзно компания относится к вопросам безопасности? На самом деле всё просто. Нужно оценить бюджет, который выделяется на эти вопросы.

Если всё, что вы делаете в области осведомлённости о безопасности состоит в том, чтобы время от времени рассылать электронные письма, напоминающие людям о возможности атаки, вы должны ожидать, что вскоре станете жертвой.

Чтобы быть ясным, осведомлённость о безопасности – это лишь часть жизнеспособного плана защиты. Другие части будут включать следующее:

- создание политики безопасности;
- оценка уязвимостей вашей компании;
- инвестиции в технологии безопасности.

Однако нет ничего важнее осведомлённости о безопасности. Компании должны инвестировать в это столько же, сколько на программное обеспечение и другие виды технологий безопасности. Ничего из этого не принесёт пользы, если ваши люди являются лёгкой мишенью для фишинговых атак.

Организационная структура, посвящённая осведомлённости о безопасности

Этот тип осведомлённости о безопасности жизненно важен, потому что он затрагивает всех в компании. Как и при подходе сверху вниз, наличие организационной структуры, построенной вокруг безопасности, упростит работу каждому.

Если есть возможность, то у вас должна быть группа людей, ответственных за реализацию вашей программы повышения осведомлённости о безопасности. По крайней мере, эту работу должен взять на себя хотя бы один человек в организации.

В противном случае осведомлённость о безопасности превращается в рутинную работу, которую никто не воспринимает всерьёз.

Создание плана и сопутствующей документации

План для каждой компании будет немного отличаться, но это важный тип осведомлённости о безопасности, который заслуживает внимания. Характеристики плана должны включать следующее:

- описание команды по обеспечению безопасности и задействованных ролей;
- заявление о миссии программы повышения осведомлённости о безопасности, объясняющее её необходимость;
- календарь мероприятий на год, который включает в себя регулярные действия, а не только электронные письма с напоминаниями, предназначенный для того, чтобы сотрудники понимали общие угрозы и свою роль в их предотвращении;
- положение для новых сотрудников, объясняющее программу повышения осведомлённости о безопасности и их роли;
- ссылки на процедуры и политики безопасности компании.

Обратитесь за помощью к профессионалам

Если в настоящий момент у вас нет абсолютно никаких мер по обеспечению безопасности, стоит подумать о том, чтобы воспользоваться услугами профессионалов. Они помогут вам начать работу и быстро наверстают упущенное.

Даже если вы вложили средства в политику осведомлённости о безопасности и другие меры, неплохо было бы время от времени привлекать независимого консультанта, чтобы проверять, есть ли области, в которых вы можете что-то улучшить.

CIS / № 1 (15) / 2021 / www.cis.ru

Искусственный интеллект: проблемы и надежды

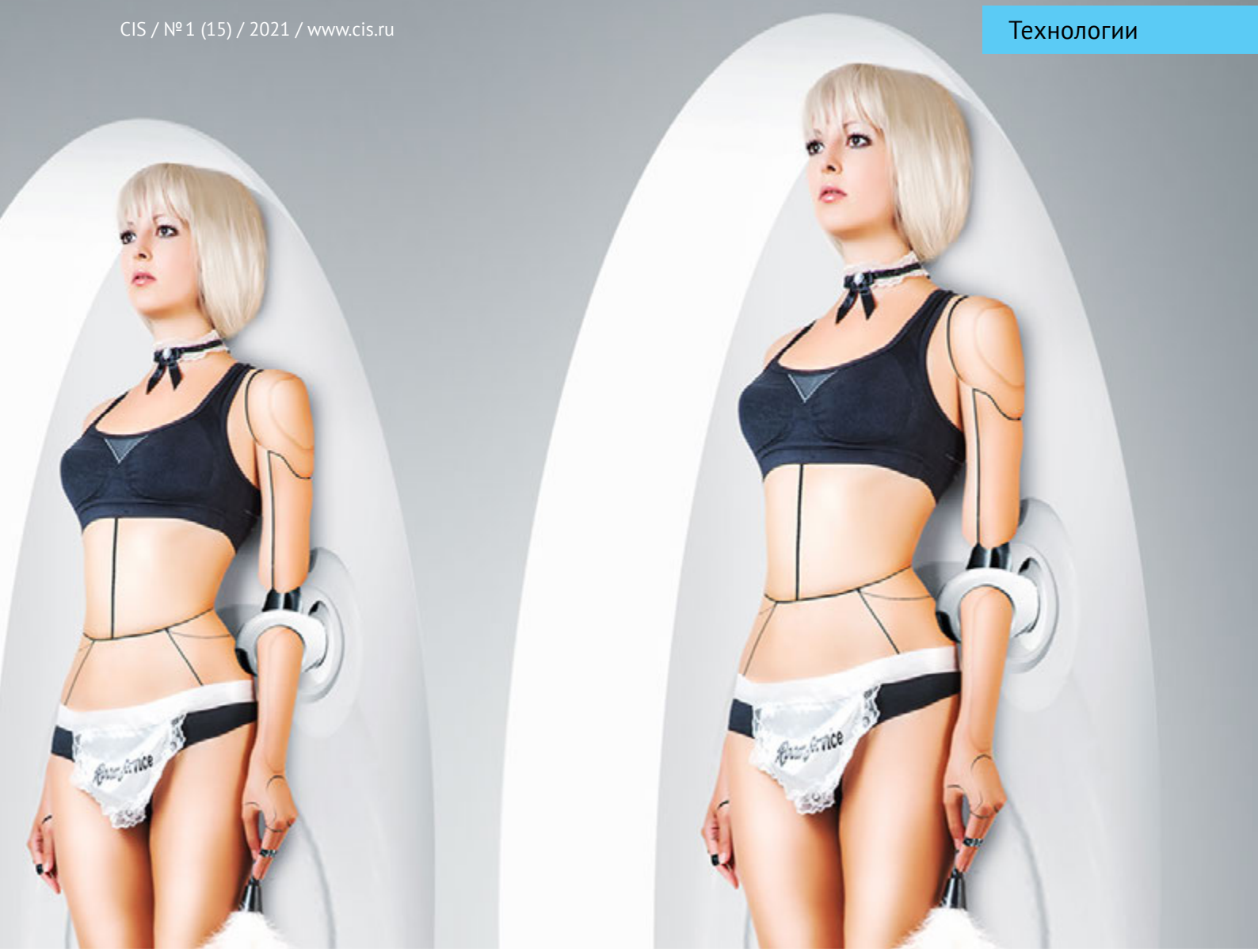
Ранее мы уже писали (см. журнал CIS № 4 (10)), какое влияние оказывают информационные технологии (ИТ) и искусственный интеллект (ИИ) на экономику и в целом на жизнь общества. ИТ и ИИ создают предпосылки для построения разумной экономики, свободной от кризисов и социального неравенства, разорительного воздействия на окружающую среду.

Сегодняшний уровень развития позволяет уйти от старых экономических догматов: погоня за прибылью, абсолютизация рынка и т. п. Он выдвигает или порождает новые идеи, растёт роль знаний, необходимость охраны природы и социальной справедливости. ИТ и ИИ, как и научно-технический прогресс, создают потенциальную возможность ликвидации разительной дифференциации доходов за счёт роста объёма создаваемых материальных благ.

Обостряющиеся противоречия между уровнем развития производительных сил и производственных отношений современного общества должны привести к переходу на новую социально-экономическую модель. Но каков механизм реализации предпосылок для такого перехода и как это будет происходить во времени? Каков путь от теоретических ожиданий к практике? И что сегодня происходит, в частности на примере внедрения ИИ?

Да, он широко используется в интеллектуальной деятельности человека, и трудно найти такую область или сферу, где бы ИИ не использовался: юристы, экономисты, финансисты, инженеры и многие другие прибегают к услугам интеллектуальных помощников, которые разрабатываются на основе нейронных сетей, когнитивных вычислений и других решений. Широко применяется ИИ и в области здравоохранения. Подчеркнём неоправданно слабое применение в фундаментальной науке, что, по-видимому, связано с недостаточностью финансирования.

Правда, оппоненты утверждают, что в системах машинного обучения на основе нейронных сетей пока нет понимания, как именно взаимодействуют структуры внутри системы – это чёрный ящик, всё зависит не от разработчика, а от входных данных. Это иногда приводит к неповторяемости или неоднозначности. Всё это не делает нейросеть самостоятельной, но придаёт оттенок непредсказуемости и тенденциозности её заключениям. Тем не менее ИИ способен решать многие задачи, в некотором смысле может выступать как альтернатива некоторым элементам рынка.



В общем, говоря о предпосылках, порождаемых ИИ, можно сказать, что прикладной ИИ даст возможность проводить анализ исторических альтернатив, а это позволит превратить стратегическое планирование в экономике из искусства в науку, оценить тот или иной выбор. В целом оно станет одним из инструментов повышения адаптивности производственных отношений, такое планирование, как и планирование вообще, основывается на принципах детерминизма. Наличие данного оптимального плана позволит прежде всего добиться существенного повышения производительности общественного труда. Но вопрос в том, как общество распорядится этим благом: то ли ещё больше усугубится дифференциация доходов и ужесточится эксплуатация человека, то ли это пойдёт на благо всего общества. То есть, с одной стороны, позитивное концептуальное видение роли ИИ, выражающееся в создании общих предпосылок совершенствования общества и мощный фактор повышения производительности труда. А с другой – как будет применён ИИ, в чьих интересах. Очевидно, это зависит от того, кто будет владеть этим инструментом. Какие выводы можно сделать на основе полученного опыта и наблюдений? Какие проблемы имеются и что нужно делать?

Уже первые этапы применения ИИ вызывают опасения в связи с занятостью людей. Если смотреть на вопрос шире, то, с одной стороны, растёт численность населения на планете, а с другой – из-за автоматизации труда число рабочих мест сокращается. Трудно себе представить современное общество без машин и механизмов, человеку не надо двигаться, за него всё делает техника. Хорошо ли это? Да, если на пользу здоровью, но здесь скрыто противоречие: человек не знает, куда девать свою энергию, а машины требуют от природы энергию, что неестественно. Такое противоречие может привести автоматизацию к своей противоположности или по меньшей мере отказе от всеобщей автоматизации. Но что тут нового?

Если ранее шла речь об автоматизации физического труда и высвободившихся людей можно было переориентировать на умственный труд, рабочий становился инженером, то сегодня и умственная сфера автоматизируется, то есть человеку не надо думать, его лишают такой возможности. Ранее он из-за механизации ручного труда становился физически не полноценным, и общество несло двойные потери: сначала тратило энергию на машины для замены физического труда, а затем потери на лечение людей свободных от него. Теперь, в случае автоматизации умственного труда, это уже серьёзнее, тут фитнес не поможет. И если человеку остаётся думать только о еде и развлечениях, он деградирует, что является одной из причин деинтеллектуализации людей.

Теперь труд человека не востребован ни в каком виде.

Возникает вопрос: а надо ли так стремительно внедрять ИИ в хозяйственную деятельность и какова готовность общества? Сегодняшний хозяйственный механизм стимулирует минимизацию занятости на производстве: всякие начисления на фонд оплаты труда, социальные льготы и др. Почему так происходит и всегда ли это оправдано?

Рассмотрим простой условный пример. Допустим, хозяин предприятия увольняет 100 человек, и его годовая прибыль составит 30 млн (без учёта начислений на фонд оплаты труда), от которой в бюджет он направит в виде налога на прибыль 6 млн. Государству для содержания этих людей нужно минимум 100 х 120000-12 млн. Где брать остальные? Да, хозяину это выгодно, но обществу нет. Налицо конфликт общегосударственных и корпоративных интересов, вот пример, где не состоятелен тезис: что выгодно бизнесу, то выгодно и государству. И, разумеется, вопрос, какое государство рассматривается? Которое стоит на страже только бизнеса, или речь идёт о построении социального государства?

В связи с коронавирусом наиболее отчётливо проявился конфликт: банки, фармацевтические и ИТ-компании имеют небывалый рост прибыли, а в то же время общество несёт колоссальные потери. Даже при существующей социально-экономической модели можно добиться смягчения противоречия: найти баланс интересов – работник – предприятие – государство. Но здесь есть политическая подоплёка: хозяину выгодно, он действует по ситуации, а какова роль государства? Оно тоже заинтересовано в том, чтобы выдвинуть человека из производительной сферы, превратить его в деградирующего послушного субъекта?

По-видимому так рассматривает миссию ИИ мировая элита. Они понимают, что высокий уровень производительных сил, в том числе и наличие ИИ, неизбежно приведёт к изменению системы. Это следует из закона соответствия. Не желая этого, они хотят убрать с арены человека как движущую силу неминуемых преобразований. Как это сделать? Правда, кроме ИИ, есть много других подходов: евгеника, трансгуманизм и т. п. Здесь и «новый», и «усовершенствованный» человек из пробирки. Но ведь человек должен развиваться естественным путём, в том числе и за счёт взаимодействия с ИИ, но не насильственно вмешиваясь в его природу.

Человечество всегда мечтало о построении идеального общества на основе высокоразвитых производительных сил и соответствующей производительности труда. Вот такое время приходит, нужна только новая полит-экономическая система, когда ИИ будет служить не только кучке богатых, а всему обществу. Общество, где материальные блага будут распределяться не только по трудовому вкладу, а скорее на основе человеческих склонностей и призвания.

Возвращаясь к нашему примеру, 100 работников не будут уволены, они будут переучены и станут работать сообща с ИИ с целью получения максимального эффекта и дальнейшего взаимного совершенствования.

Существует мнение, что проблема занятости переоценена, трудно с этим согласиться. В настоящее и ближайшее время вопрос стоит не остро, но в перспективе ситуация изменится. Кроме занятости, первый опыт показывает, что ИИ как инструмент в руках правящей элиты в целом может усугубить существующие противоречия, что неминуемо приведёт в конечном счёте к социальной катастрофе, то есть ИИ может быть не только благом, но и таит в себе угрозу.

Находясь на стадии прикладного ИИ, надо готовиться к повсеместному вхождению его в нашу жизнь. Такая подготовка – длительный процесс, который включает в себя прежде всего радикальные социально-экономические преобразования, при этом необходимо учитывать существующую структуру производственных отношений и уровень производительных сил. Исходя из готовности общества, необходимо планировать внедрение ИИ и не стараться форсировать этот процесс. Хотя существует дилемма: не тратить ресурсы на бесперспективные проекты и в то же время не отстать. Наука, в том числе ИИ должны помочь государству найти этот оптимум. В рамках такой подготовки надо актуализировать вопрос применения ИИ в школьном образовании – важнейший элемент всей подготовительной работы. При этом не предполагается замена учителя, так как повышение качества образования неисчерпаемая тема и оно во многом определяет наше будущее.

Кроме социальных проблем, существуют и другие – технологического характера. Прежде всего качество и адекватность ИИ. Сегодня одним из преимуществ его может быть отсутствие эмоций, объективность и неподкупность. В таком случае его целесообразно было бы использовать, как носителя общегосударственных интересов (можно параллельно с соответствующим чиновником) или при решении задачи распределения ресурсов по регионам, помощь государственным деятелям в изучении общественного мнения. Но, к сожалению, нельзя сказать, что существующие решения позволяют утвердительно ответить на такое предложение. Практика показывает, что ИИ бывает и тенденциозен, и не объективен.

Вместе с тем поборники ИИ полагают, что он будет меньше допускать ошибок, чем человек. Пока это не так, и очень важен анализ природы их возникновения. Ошибки связаны прежде всего с тем, что ИИ, как и любое другое программное обеспечение, требует сопровождения, которое заключается в постоянном обновлении и совершенствовании алгоритмов, обязательном их тестировании. Зачастую это недооценивается, в то время как сопровождение не менее важный и трудоёмкий вопрос, чем собственно разработка. В некоторых фирмах назначается директор по контролю за корректной работой ИИ. Другой вопрос касается данных, которых не всегда достаточно, они не всегда точны и репрезентативны, ведь именно наличие таких данных является главным условием работоспособности алгоритмов машинного обучения.

В связи с массовым внедрением ИИ обостряется вопрос кибербез-

опасности. Потребность в большом объёме пользовательских данных вынуждает компании-разработчиков в погоне за ними иногда выходить за границы конфиденциальности. Данные, используемые ИИ, могут попасть к мошенникам. Защитить от этого и возможных последствий ИИ пока не может, так как последние опережают его своими изощрёнными схемами. Более того, мошенники активно развивают ИИ для его злонамеренного использования, что представляет большую опасность и подрывает доверие у людей.

Компании, занимающиеся ИИ, должны принимать меры по анонизации и защите персональных данных. Не прорабатывается пока вопрос о коммуникациях между различными функционирующими системами ИИ в свете проблем информационной безопасности и опережения злоумышленников. Все эти вопросы свидетельствуют о том, что не стоит задача, как можно быстрее заменить, вытолкнуть человека, скорее наоборот, нужно привлечение квалифицированных работников. Опыт показывает, что основным критерием успеха от внедрения ИИ является готовность взаимно учиться в сочетании различных вариантов взаимодействия и обратной связи, что в конечном счёте повышает эффективность от ИИ в разы.

Особые надежды связаны с ИИ в улучшении взаимоотношений человека и природы. Сейчас степень воздействия его на природу в значительной степени превосходит уровень знаний о ней. Не сбылись пророчества В.И. Ленина о том, что человеческий ум уже открыл много диковинного в природе и откроет ещё больше, тем самым увеличив свою власть над ней.

Властвование, которое мы сегодня наблюдаем, оборачивается многими бедами. И, с одной стороны, ИИ должен помочь людям в познании природы посредством сбора и обработки данных об окружающей среде с выявлением тех негативных факторов, зачастую скрытых, которые ведут к её разрушению. Надо использовать ИИ для изучения влияния количества населения планеты на окружающую среду с привлечением международных институтов для выработки глобальной демографической политики. Наконец настало время сконцентрировать усилия разработчиков на создании узкоспециализированного ИИ, который поможет учёным продвинуться в фундаментальных науках: физике, химии, биологии. Может быть, ИИ поможет защитить и спасти человечество от вирусов и т.п. С другой стороны, надо помнить, что ИИ может оказывать и негативное влияние на среду, что связано с большим расходованием электрической энергии современными компьютерами, а также широком использовании в них редкоземельных элементов.

Большое препятствие на пути продвижения ИИ – отсутствие регулирующих юридических нормативов, начиная от определения статуса и заканчивая ответственностью. Но это общая проблема, что прослеживается на примере законодательства об интеллектуальной собственности. Сколько бы не корректировались законы и другие нормативные акты, это никак не стимулирует использование инноваций на благо всего общества. Экономическая выгода от исследований и разработок может быть получена полностью только в том случае, если никто не лишён возможности применять их с того момента, как они получены, но из-за противоречия государственных и корпоративных интересов такой доступности нет. Патентное право, например, может тормозить использование открытий и изобретений. Государство должно взять на себя этот вопрос и решить его путём максимизации финансирования исследований и разработок. Такое решение способствовало бы также созданию общедоступных библиотек программного обеспечения типовых решений на базе ИИ.

Многие авторы говорят об опасности победы ИИ над человеком, о наличии противоречия между ними. Да, интеллектуальное соревнование мы будем наблюдать, но противоречия носят не антагонистический характер. В будущем это соревнование закончится тем, что человеческий интеллект и ИИ сблизятся, возможно, сольются на последующем витке развития, но человек всегда будет доминировать в этом процессе, и в конечном счёте возможные проблемы могут возникнуть только по его вине из-за игнорирования и отказа от сотрудничества, что чревато выходом ситуации из-под контроля.

Поэтому все перечисленные трудности и призывы к взвешенному подходу в деле освоения ИИ не означают ослабления внимания к нему, в том числе со стороны государства. Наоборот, отсюда следует, что общество, в первую очередь государственные органы, должно увеличивать финансирование работ по ИИ и в поисках оптимальной точки, о чём выше упоминалось, учитывать и военный аспект. Здесь недопустимо отставание, о чём учит история. Хотя могут вызывать сомнения попытки разработки сильного или человекоподобного ИИ с целью его широкого применения на практике по этическим и энергетическим соображениям. Разумеется, в научных целях работы должны вестись в обязательном порядке.

В заключение подчеркнём, что ИИ поможет создать более совершённую экономическую модель, максимально увеличить производительность общественного труда и будет способствовать достижению полной гармонии человека и природы как условия выживания человечества. Но для этого мы должны лучше изучить природу, что происходит сегодня, она нам мстит за потребительское отношения к ней или пока только предупреждает. Все людские ресурсы, которые высвобождаются, в том числе от применения ИИ, должны быть направлены на исследования природы. В конечном счёте это основная цель в жизни человека, но не только исследования, а и активные действия по её охране в соответствии с полученными знаниями.

Таким образом, благодаря ИИ, человечество выйдет на путь устойчивого развития и достигнет высот в совершенствовании мира при условии успешной подготовке к его внедрению. Конечно, нельзя всецело предсказать будущее, но мы должны делать всё возможное, чтобы быть к нему максимально готовыми.

Анатолий Орлюк
доцент МИИТа, к.э.н

8 985 215 18 36
an.orlyuk@yandex.ru

Женщины в ИТ

Женщины, достигшие немалых успехов в бизнесе, в том числе и в ИТ-сфере, говорят: «Очень важно быть готовым совершать ошибки и не бояться. Провал – это не конечный результат, а недостаток усилий...»

«В бизнесе работает «принцип велосипеда» – чтобы не упасть, нужно постоянно находиться в движении».

Мы с интересом наблюдаем, что в последние годы в сферах ИТ и ИБ становится всё больше и больше женщин. И это несмотря на результаты исследования 2020 года, проведённого для Women In Tech, в котором говорится, что «девушки продолжают сталкиваться с трудностями, вызванными на почве стереотипов о женщинах в ИТ». Так, 56% респондентов хотя бы раз получали в свой адрес утверждение, что «технологии не для девушек». Мы решили узнать, как женщинам, работающим в сфере ИТ-технологий, удаётся добиться успеха.

Ольга Попова
директор по развитию бизнеса, компания «Индид»

В сфере ИТ я начала работать 15 лет назад, когда по простой случайности попала в компанию ИТ-интегратора. Через полгода скучной обработки трудозатрат я начала постигать тонкости работы в должности помощника менеджера проектов, а через год я стала самостоятельно «рулить» ими. Управление проектами – это сложно, но интересно! За годы работы я приобрела очень полезные навыки, которые применяю и в повседневной жизни, и в управлении командой на текущем месте работы.

Конечно, в начале карьеры я не раз слышала стереотипные мнения о женщине и технологиях. Поначалу меня это очень возмущало, и я рвалась в бой, доказывая, что я – эксперт. Но со временем поняла, что такое утверждение – это, в какой-то степени, благо. Оно автоматически делает беседу более лёгкой, и можно «расслабиться», так как не будет «трудных» вопросов. Сейчас уже не сталкиваюсь с такими утверждениями в свой адрес. По какой-то причине во мне сразу видят эксперта. Может, потому что у меня на визитке написано «директор»?

Сейчас, занимая руководящую должность, могу сказать, что важными составляющими своего успеха считаю мотивацию, уверенность в себе и самообразование! Чтобы работалось легко и карьера шла в гору, тебе должно нравиться то, что ты делаешь. Скажу больше: тебя должно «драйвить» от этого! Ты не должен бояться трудностей, которые точно возникнут на пути! Да, ты будешь уставать, и иногда какие-то проблемы будут казаться неразрешимыми, но... Если ты уверен в себе, то сможешь решить все задачи. Ещё очень важно стремление к саморазвитию, которому я уделяю отдельное внимание, так как каждый лидер должен быть в курсе быстро меняющихся технологий, направлений, тенденций. Вместе всё это помогает найти новые идеи, силы для их реализации и достичь успеха.

Любите своё дело, тогда работа будет приносить не только деньги, но и удовольствие! А «довольные люди генерируют лучшие идеи!», как написано в книге Л. Бок «Работа рулит!». Я очень люблю свою работу, свою команду. Мне безумно нравится делиться с ней опытом, рассказывать, как решались те или иные проблемы. Получаю истинное удовлетворение от того, в каком энергичном темпе развивается наша компания. Считаю, что такой быстрый рост связан не только с грамотным управлением, но и с умением команды адаптироваться к меняющимся условиям, работать в режиме многозадачности и со стремлением каждого её члена к самосовершенствованию. В этом секрет успеха!

Сложнее всего адаптацию к моей работе в ИТ и ИБ переносила семья. Но сейчас мы научились планировать время работы и отдыха, выделили «неприкасаемое время для общения с детьми». Дети при такой занятой маме становятся крайне самостоятельными. Тут всё, как в управлении проектами: мама всем делегирует задачи и контролирует их результат. Муж понимает и поддерживает меня, он знает, что такое работа в ИБ, так как сам является руководителем ИТ в одной из компаний ритейла.

Анна Глухова
ведущий менеджер по работе с заказчиками, Научно-технический центр ЕВРААС

Я пришла в информационную безопасность случайно: после института друзья предложили поработать в небольшом ИТ-интеграторе в Санкт-Петербурге. Мне сразу понравилась атмосфера: адекватная молодая команда и увлекательные задачи. Вроде бы участвуешь в процессах, которые на слуху, но с необычной стороны: нужно придумать, как обеспечить их цифровизацию, сделать жизнь чуть лучше с применением новейших технологий. При этом работа с людьми составляла 90% моего времени, отодвигая технические вопросы на второй план. Потом я устроилась на работу в компанию, основной специализацией которой являлась информационная безопасность.

Рынок ИБ повторяет рост ИТ в целом, привлекая ярких людей и ставя необычные задачи. Здесь трудятся люди, не зацикленные только на работе: разносторонние увлечения, интерес к жизни, внутренняя энергия – всё это объединяет коллектив. Среди знакомых ИБ-тусовки можно набрать команду на дайв-сафари, съездить в горы с лыжами, сходить в поход на катере или парусной яхте. А какие таланты раскрываются в караоке! Из-за того, что рынок не очень большой, я постоянно встречаю знакомых вне зависимости от решаемого вопроса и региона России, в котором нахожусь. Всегда радуюсь, когда вижу коллег из других компаний на офлайн мероприятиях. Кстати, акцент на отечественных решениях и обилие таких конференций предопределяют один из самых приятных бонусов работы в ИТ-компании – доступ к безбарьерному общению с производителями! Очень часто я получаю быстрый эффект от такого «общения напрямую». Например, если высказать пожелания к продукту, то можно получить их оперативную реализацию.

Несмотря на то, что коллектив преимущественно мужской, работать мне комфортно и интересно. Меня с детства окружали настоящие мужчины, общение и само нахождение в кругу которых доставляло удовольствие. Именно тогда я приобрела навыки общения с сильным полом. С тех пор я легко вливаюсь в любой мужской коллектив, зачастую работая переводчиком между «женским» и «мужским» языками.

Открою свой секрет успешной работы в ИТ-компании. Всегда нужно быть одновременно и женщиной, и равным партнёром. Но всегда можно «прикинуться девочкой», и тебе любой мужчина с удовольствием будет объяснять, сколь угодно сложные вещи самым простым языком.

Известно, что женское начало призвано гармонизировать реальность. Это применимо и в мужских коллективах. Когда в компании появляется девушка, резко меняется тематика обсуждаемых в коллективе вопросов и манера общения. Возникает атмосфера галантности и внимательности.

Одно из преимуществ быть «девочкой» в брутальном коллективе – основное неформальное общение проходит за тортиками. Мужчины – настоящие сладкоежки, но не могут признаться в этом друг другу. Вовремя выставленный на деловой встрече тортик способен мгновенно собрать компанию нужных специалистов, даже если они очень заняты. Сразу вспоминаются интересные случаи, увлечения, появляется гитара. Бывали случаи, когда на переговорах секретари предлагают чай, а серьёзные люди, оглядываясь и немного смущаясь, достают из сейфа шоколад. Бесконечно приятно наблюдать за подобными изменениями даже в таких «серьёзных и не женских» сферах, как ИТ и ИБ.

Анна Исакова
ведущий маркетолог, компания «Астерит»

Пандемия оказала влияние на все сферы жизни, в том числе и на отношение к сотрудникам женского пола в технических отраслях. Стираются границы социальных рамок, и предрассудки становятся всё менее значимыми. Думаю, что сейчас выбор женщиной профессии в ИБ или в ИТ связан прежде всего с перспективностью сферы, с интересными задачами и высокой оплатой труда, с гибкостью графика и возможностью удалённой работы. Как пока-

зал опыт прошлого года, важно, чтобы сотрудник был самоорганизован настолько, что сможет продуктивно работать даже в атмосфере семейного окружения. Многие задачи должны были эффективно решаться даже при удалённой работе. А кто, как ни женщина, способен на это? Женщинам, работающим в тестировании, проектировании, разработке, продажах и прочих профессиональных областях в удалённом режиме легко удавалось скоординировать и работу вне офиса, и справляться с отвлекающими домашними делами. Поэтому девушка в ИТ или ИБ – настоящая находка для любой компании. И это подтверждает мой опыт.

Когда я выбирала направление самореализации, сразу остановилась на компании из сферы информационной безопасности, и ни на минуту не пожалела о своём выборе! Наш коллектив преимущественно мужской. Здесь есть то, чего не встретишь нигде: мужчины готовы делиться своими знаниями и сверкать эрудицией, попутно обучая меня тонкостям технического мира. Это очень помогло в построении карьеры, потому что в начале пути мой опыт в ИБ сводился только к пониманию одной фразы: «Антивирус Касперский», причём именно в таком произношении!

Мне очень нравится моя работа. Считаю, что эта сфера менее всего подвержена кризисным падениям, т.к. безопасность всегда будет приоритетной, а информационная безопасность – это основа и защита стабильного бизнеса! Моя профессиональная страсть – это все бизнес-мероприятия нашей компании! Я всегда хотела работать в прогрессивном, амбициозном коллективе. Последние четыре года я «горю» своим делом в компании ИТ-интеграторе! Как организатор, я присутствую на каждом своём мероприятии. Меня окружают умные и успешные люди. Работать с ними – сплошное удовольствие! Как всегда, приходится много общаться при организации конференций: подрядчики, вендоры, спикеры, участники, арендодатели, ведущие и многие другие – на 90% это мужчины. Со всеми удаётся найти общий язык: для подрядчиков я всегда строга и требовательна, а для партнёров и гостей мероприятия – заботлива и внимательна! Совершенно точно я ощущаю себя настоящей душой всех наших мероприятий!

Отлично помню свою первую конференцию. Тогда со мной заговорил седовласый мужчина на тему защиты персональных данных, сертифицированных СЗИ и т.д. Из всей речи мне были понятны только предлоги, но я активно слушала, кивала, отвечая только: «Конечно!», «Согласна с Вами!», «Непременно, Вы правы». В тот момент для меня наградой была его финальная фраза: «Как приятно поговорить с компетентным человеком!». И тут я себя почувствовала всемогущей! Сейчас, конечно, я свободно веду беседы на любые темы! Каждый день я много читала, разбиралась в решениях и направлениях, донимала коллег вопросами.

Лично мне работать с мужчинами проще: всё чётко и по делу. Никаких секретов и тайн о достижении успеха в мужском коллективе у меня нет. Просто нужно качественно делать своё дело и продолжать оставаться женщиной. Часто бывает, что хочется стать «своей» в мужском коллективе, и девушки начинают грубо выражаться, пить крепкий алкоголь и перенимать другие мужские качества. В итоге, девчонки теряют себя! Я за то, что нужно оставаться собой. А иногда даже использовать женскую хитрость.

Оксана Степенко

директор Axoft Azerbaijan

Моё знакомство с ИТ произошло более 23-х лет назад, а если быть точнее, ещё раньше: когда я училась в школе. На открытии первого компьютерного класса я пожелала работать в IBM. Этот мир захватил меня, вдохновил, и сегодня, являясь руководителем Axoft — Service IT distributor, я могу сказать, что он и многому научил. Информационные войны, партизанские бизнес-игры, жестокая реальность, схватки — я испытала многое, немало потерь, поражений и обид, много взлётов, а также падений, побед и наград. И хотя я многое осознавала, но всё больше задавалась вопросом: для чего мне это и чего хочу на самом деле?

Жизненный путь у каждого свой, он многообразен и учит понимать, для чего происходят те или иные события в твоей жизни, учит мудрости, принятию, прощению и умению отпускать ситуации с любовью и благодарностью. В моей жизни были люди — учителя, которые многому научили через обман, предательства, измены. Порой казалось, что всё это — твой последний день и вопросы, за что и почему одним достаётся счастье, а другим — уныние, слёзы и разочарование, не закончатся никогда...

Вселенная предоставила мне много возможностей: ДАО, цигун, ароматерапию, которые позволяют идти, улыбаться, наслаждаться жизнью и миром ИТ. И только сейчас я могу сказать, что все трудности и сложности — это мой путь к саморазвитию и пониманию себя.

Я очень люблю зону комфорта, и сколько себя помню, всегда стремилась её создать. Но при каждой такой попытке натыкалась на преграду, препятствие, сложную ситуацию, болезнь. ДАО — мой путь познания себя, именно здесь я научилась принимать жизнь такой, какая она есть, благодарить, любить и улыбаться. Я приняла тот факт, что жизнь состоит из белого и чёрного и каждый может найти баланс и равновесие.

Реакции на происходящее, сильные эмоции — гнев, злость, обида, разочарование, печаль, тоска, депрессия разрушают наше здоровье, вредят внутренним органам, жизненный ресурс расходуется и истощается. Трансформация возможна, и я делюсь этим с удовольствием и радостью.

Успех — это отражение внутреннего мира человека, его намерений, желаний, ценностей и жизненной позиции! Возможности настоящего изобильны — улыбайтесь себе, и мир улыбнётся вам в ответ!

Виктория Варичева

руководитель отдела по работе с ключевыми партнёрами, Axoft

Сама судьба повлияла на мой выбор профильного образования: я окончила факультет защиты информации. После окончания вуза погрузилась в изучение зарождающегося направления и оказалась в очень интересном, динамично развивающемся, активном мире ИБ. Я несказанно рада такой возможности!

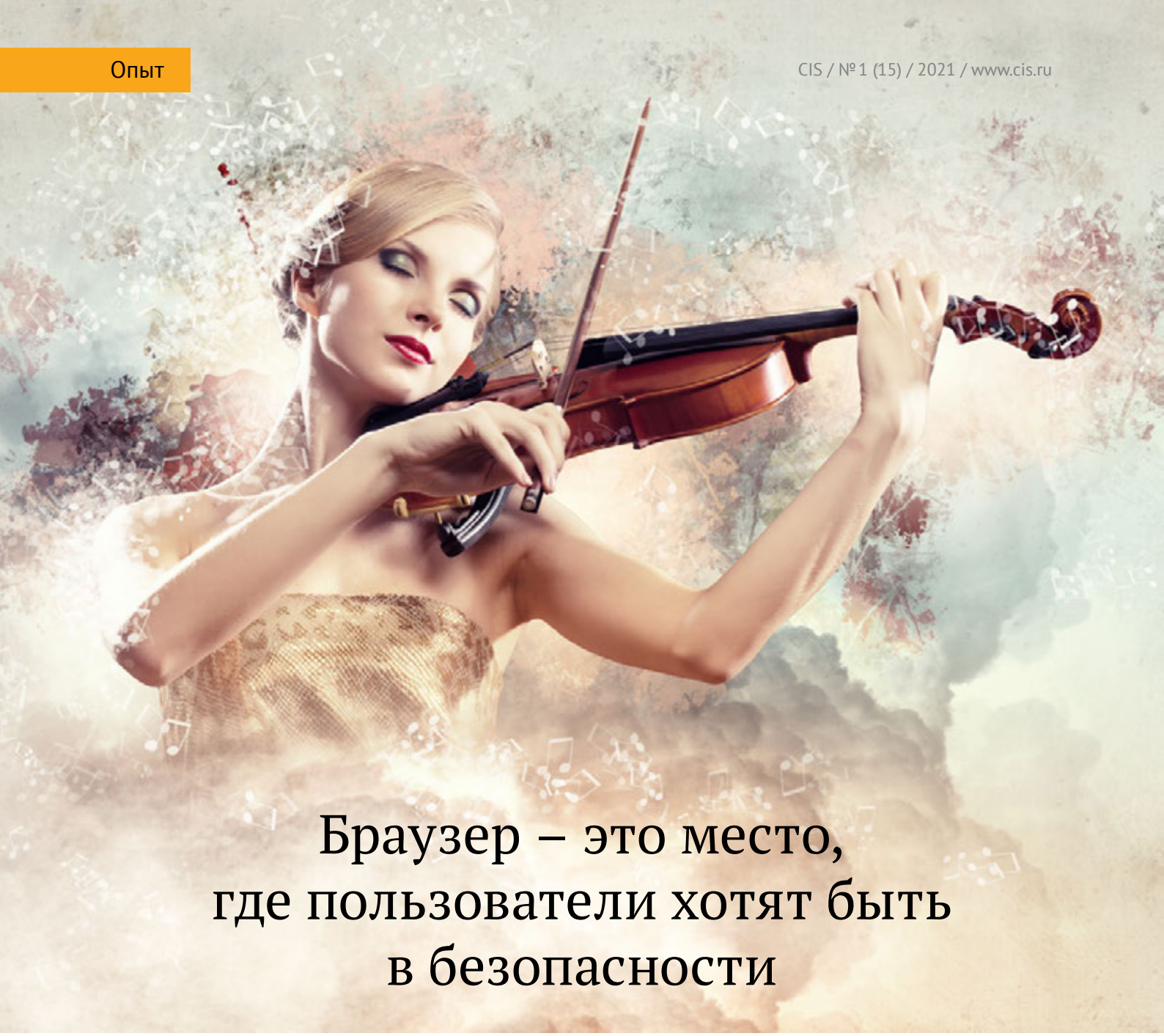
ИБ – это очень активная среда обитания, жизни. Всегда происходит что-то новое, ты всегда в движении. Достижение одних целей знаменуется постановкой новых, цели могут корректироваться в процессе работы, если меняются, например, обстоятельства рынка. Каждая новая цель отличается от ранее поставленной и достигнутой, поэтому всегда есть понимание того, что перед тобой огромное поле для деятельности, роста, развития, интересных проектов, где ты можешь себя реализовать и заниматься своим любимым делом. А люди, которые меня окружают – уникальны и неповторимы.

Для меня мужской коллектив – это очень сильный драйвер, это неисчерпаемый океан положительной энергии, это люди, которые готовы всегда помочь, поделиться опытом, подставить своё мужское плечо в трудной ситуации. В первую очередь это соратники по общему делу, умные, неординарные, у которых многому можно научиться. Как в такой среде не добиться успеха? Было бы желание и здоровье, всё остальное будет непременно!

И если говорить о мужском и женском, то мужчин я считаю земными волшебниками, которые помогают воплощать мечты. Поэтому мне очень легко работать рядом с сильными, умными людьми, даже когда мы спорим и каждый доказывает свою точку зрения, всегда это происходит с пониманием того, что мы стремимся к одному и тому же: сделать лучше, эффективнее, найти оптимальные варианты решения задач. И при этом мужчины не дают спуска или послаблений, но всё равно за общением стоит их забота, даже если это общение происходит в формате жёстких переговоров (и такое иногда бывает). Так что работа в мужском коллективе – это своего рода небольшая «фора» для женщины. Это неуловимое преимущество и доверие со стороны коллег даёт возможность реализовать возлагаемые на женские плечи зачастую непростые и нетривиальные задачи. Огромное спасибо моим коллегам по цеху за их доверие и поддержку!

Мой первый и единственный секрет успеха в «мужской» отрасли: быть собой! У нас потрясающие мужчины! Иногда они дают возможность передохнуть, отпустить ситуацию, собраться с мыслями. Работая в таком коллективе, понимаешь, что ты можешь опереться на крепкое мужское плечо, коллег профессионалов, и они не подведут тебя на своём участке работы. Очень приятно слышать во время обсуждения проекта и распределения ролей в нём: «Этот вопрос я беру на себя». И ты понимаешь, что человек не только возьмёт в реализацию, но успешно всё сделает и доведёт до конца, а это означает, что нам по плечу самые смелые, амбициозные проекты. Я очень ценю то, что работаю в таком коллективе! Спасибо вам дорогие мужчины за то, что вы есть!

Очень люблю одну историю, когда, казалось бы, обычное обсуждение промежуточных результатов проекта переросло в изложение ситуации в форме сказки. У нас получилось что-то вроде «Красная Шапочка на просторах ИБ-рынка». Там появился и «волк», и «бабушка», и «дровосеки», и самый главный персонаж – отважная «Красная Шапочка», попадающая в разные ситуации, которые хорошо вписывались в повествование сказки и находили в ней своё отображение. Главная героиня справлялась со всеми перипетиями и с честью из них выходила. В общем, в жизни, как в сказке, только ещё интереснее!



Браузер – это место, где пользователи хотят быть в безопасности

Йон Стефенсон фон Течнер
бывший генеральный директор Opera Software и основатель Vivaldi

Господин Фон Течнер, со времени продажи первого браузера, разработанного Вами, прошло почти 25 лет. Как изменились с тех пор приоритеты в разработке, сами решения, рынок веб-браузеров?

С 1994 года многое изменилось. Тогда ведущим браузером был NCSA Mosaic. Год спустя это был Netscape. В то время было много крупных компаний, делающих браузеры, в том числе IBM, Oracle, Sun, Apple и многие другие. Большинство браузеров были главным образом основаны на NCSA Mosaic.

Было довольно легко создать браузер, так как он в то время был, скорее, средством просмотра документов. Теперь же браузеры внедряют дополнения. С самого начала большой проблемой была совместимость, так как стандарты были довольно размытыми и крупные компании рассматривали это как преимущество в плане контроля над рынком. Вскоре после этого Microsoft вышла на рынок и использовала свою власть, чтобы вытеснить Netscape и другие компании.

Разработку Opera мы начинали вдвоём в Норвегии. Мы решили собрать браузер с нуля, и нам удалось сделать действительно конкурентоспособное решение. Команда росла, как и наша способность расширять доступность браузера на большем количестве устройств.

С 1994 года многое изменилось, но многое и осталось прежним. Роль лидера на рынке браузеров переходила от Mosaic к Netscape, затем к Internet Explorer и теперь к Chrome, и мы наблюдаем везде одну и ту же динамику: лидером становится тот, кто имеет сильные позиции на других рынках. Конкуренция сложная, но, к счастью, многие люди хотят получить лучший

браузер и готовы попробовать новые продукты.

Сейчас вопросам кибербезопасности уделяется всё больше внимания. Однако повышение уровня безопасности может привести к потерям в удобстве работы в интернете. Вы согласны? Если да, то где, по Вашему мнению, находится золотая середина?

Кибербезопасность каждый понимает по-своему. Можно разделить её на четыре компонента: базовая безопасность браузера, конфиденциальность, защита от фишинга и вирусов и VPN.

Базовая безопасность браузера. Здесь мы имеем в виду такие вещи, как шифрование соединения, безопасная обработка паролей и т. д. Браузер – это место, где пользователи хотят быть в безопасности, и большинство браузеров это обеспечивают. Часто это больше вопрос безопасности разных сервисов, банковских платежей например.

Конфиденциальность. Сегодня ей уделяется большое внимание. Сбор данных в Интернете огромен и используется для создания профилей пользователей. Мы не собираем данные и не создаём рекламные профили. Как и многие другие коллеги, мы внедрили блокировщики слежки и рекламы. Они усложняют сбор информации о пользователях, но иногда могут и нарушить работу сайтов, поскольку отслеживание может быть неотъемлемой частью работы сервиса. Найти баланс здесь может быть сложно. В Vivaldi мы предлагаем пользователю возможность самому осуществлять контроль, позволяем выбирать уровень блокировки даже на отдельных сайтах.

Защита от фишинга и вирусов. Большинство браузеров имеют определённый уровень проверок известных фишинговых и вирусных сайтов.

VPN и Tor. В качестве дополнительной безопасности вы можете использовать VPN или Tor. Иногда сложно найти программу, которой можно доверять и которая не замедлит работу сайтов.

Я считаю, что всегда следует оценивать бизнес-модель используемых сервисов и дополнительные возможности компании. Например, выглядит немного странно, если компания, предоставляющая одну определённую услугу, также создаёт профили пользователей и предлагает рекламную платформу.

Мы фокусируемся на безопасности браузера в целом, его конфиденциальности и защите от вирусов. Я полагаю, что большинство браузеров относительно хорошо справляются с этими пунктами. Когда дело доходит до конфиденциальности, есть большие различия. Занимается ли разработчик браузера созданием рекламных профилей? Есть ли у браузера рекламная площадка? Предоставляет ли браузер опции отслеживания и блокировки рекламы? Мы не создаём профили для наших пользователей, и наши сервисы, такие как почта, форумы и блоги, не содержат рекламы.

Веб-браузер Vivaldi был анонсирован в 2015 году. Каких успехов Ваша команда добилась за 5 лет?

Много произошло за эти 5 лет. В 2015 году Vivaldi был лишь сырой тестовой сборкой. Теперь мы предоставляем многофункциональный браузер, который стал намного быстрее и мощнее. Мы также запустили мобильный браузер для Android. Vivaldi теперь работает на Windows, Mac, Linux и Android. Мы поддерживаем множество дистрибутивов Linux, и Vivaldi даже будет работать на Raspberry Pi. На самом деле он работает довольно хорошо на Pi, хотя рекомендуется Pi3 или даже Pi4 и максимально возможное количество памяти.

Мы внедрили много уникальных функций. Вот некоторые примеры: хотя большинство браузеров по умолчанию запускаются с одной вкладкой, Vivaldi запускается по умолчанию с того места, где вы остановились. Вы также можете легко сохранять и загружать сессии.

У Vivaldi очень гибкий пользовательский интерфейс. Пользователи очень ценят, например, группировку вкладок. Мы продолжаем делать браузер настраиваемым, понимая, что у всех нас есть свои предпочтения. У нас вы найдёте встроенные инструменты для снимка выделенной области, заметки, блокировщики рекламы и слежки.

Функция синхронизации в Vivaldi позволяет синхронизировать данные между Vivaldi на нескольких компьютерах и мобильных телефонах. Это включает историю, закладки, пароли, заметки и многое другое. Данные зашифрованы с помощью пароля, который вы задаёте на своём компьютере и который не передаётся Vivaldi.

Конечно, большинство пользователей не будут использовать всю функциональность, но мы стараемся сделать так, чтобы каждый нашёл в Vivaldi то, что ему нужно.

Разработка Vivaldi ведётся при активной помощи сообщества. Как Вы обеспечиваете построение цикла безопасной разработки ПО (Secure Software Development lifecycle)?

В команде Vivaldi есть несколько экспертов по безопасности. Работа программистов проверяется как на качество кода, так и на безопасность. Новые функции и обновления анализируются сотрудниками на соответствие принципам безопасности и конфиденциальности. Это в дополнение ко всем тестированиям команды и Sopranos (добровольные бета-тестеры).

У нас уникальные отношения с нашим сообществом. Пользователи помогают нам тестировать, переводить и рассказывать о Vivaldi. Sopranos тестируют новые функции браузера первыми и дают обратную связь. Почти каждую неделю мы рассылаем новую тестовую сборку нашему сообществу.

Отзывы, которые мы от них получаем, позволяют нам создавать лучшее программное обеспечение для наших пользователей. Вместо сбора данных об использовании браузера мы прислушиваемся к пользователям и их отзывам. Мы считаем, что это позволяет создавать лучшее, более безопасное программное обеспечение, поскольку мы не оптимизируем его для одного типа пользователей, а видим, что у всех разные пожелания.

Как Вы оцениваете перспективы Vivaldi в России? Есть ли особенности работы в нашей стране?

Мы с самого начала много внимания уделяем России. Многие россияне готовы попробовать новое и интересное программное обеспечение. В России у нас довольно большое сообщество.

---

*Интервьюируемый: **Йон Стефенсон фон Течнер,** бывший генеральный директор Opera Software и основатель Vivaldi.*

Автор: ***Игуменшева Татьяна,*** BISA.

Источник: www.bis-expert.ru

CIS / № 1 (15) / 2021 / www.cis.ru

Непрерывность бизнеса в эпоху пандемии

Сегодня мы говорим о непрерывности бизнеса. Как думаете, для каких рынков или, может быть, ниш этот вопрос стоит особенно остро? Можете назвать ТОП-3?

Честно говоря, это необходимо любому бизнесу без исключений. Например, для большинства западных компаний разработка комплекса мер по обеспечению непрерывности бизнеса – это обязательная и рутинная процедура. И это понятно, ведь согласно Veeam 2020 Data Protection Trends Report, в среднем по миру только один час простоя, когда организация не может использовать электронную почту, платёжные инструменты, веб-сайты или мобильные приложения, приводит к ущербу суммой в $67 тыс. По мере того, как всё больше компаний стремится вести бизнес в режиме 24/7, восстановление должно происходить максимально быстро. Но если уже говорить о тех сферах, где это критически важно – финансовый сектор (банки, кредитные и страховые организации и т.п.), телеком и ритейл – вполне ожидаемо.

Насколько коронавирус и последовавший за ним переход большинства компаний на удалённый формат работы усложнил задачу обеспечения непрерывности бизнеса в России?

Всё зависит от компании и специфики бизнеса. Многие и до пандемии работали в удалённом или гибридном формате, и для них ничего существенно не изменилось. Крупные предприятия из консервативных отраслей, конечно, столкнулись с определёнными сложностями. Но перевести несколько сотен или даже тысяч сотрудников на работу из дома и при этом обеспечить бесперебойную работу ИТ-инфраструктуры и защиту корпоративных данных в один день невозможно. Именно поэтому большинство современных компаний, для которых критичен даже один час простоя в результате технического сбоя или, например, потери доступа к данным, имеют так называемый Business Continuity Plan (BCP). Это документ включает в себя целый комплекс мер не только в отношении ИТ-инфраструктуры, но и службы безопасности, юридического департамента, службы персонала и т. п.

Есть ли какие-то общие требования к такому документу, рекомендации, с чего начать?

Универсального шаблона BCP не существует. Всё опять-таки зависит от специфики бизнеса и его масштаба. Но если говорить о пошаговой схеме, то в любом случае начинать надо с анализа данных: компания должна определить для себя, какие данные для неё стратегически важны, а какие не очень, кто может иметь к ним доступ, а кто нет. И на основании этого анализа начать разрабатывать комплекс мер по обеспечению непрерывности бизнеса. Важно понимать, что разработка и внедрение BCP – это очень сложный и дорогостоящий процесс. Более того, он требует постоянной актуализации. Мир стремительно меняется, угроз как физических, так и виртуальных становится больше. Как правило, большинство BCP успевают устаревать к моменту внедрения, поэтому этот процесс в принципе не может считаться завершённым. Компаниям необходимо постоянно проверять свой BCP на соответствие текущей ситуации на рынке, масштабу компании, формату её работы и т. п.

Есть ли какие-то инструменты, позволяющие оптимизировать этот процесс?

Дело в том, что ключевое условие разработки эффективного BCP – это досконально понимание специфики бизнеса. И, конечно, комплексный подход, который позволит предусмотреть весь спектр угроз для компании. Безусловно, существуют целые методики и решения. Например, та же самая Information Technology Infrastructure Library (ITIL), которая представляет собой набор взаимосвязанных «рекомендованных практик», основополагающих принципов и процедур, образующих вместе полное руководство по достижению надёжности ИТ-решений и услуг, но, как вы понимаете, ITIL не даёт никаких универсальных ответов…

Вы не раз упомянули разнообразие угроз для бизнеса. Одна из них – киберпреступность, в частности ransomware атаки, которые способны остановить деятельность целых больниц, энергостанций и т. п. Как предприятию защитить себя?

Ransomware – очень прибыльный бизнес. Недаром в последнее время мы всё чаще слышим новости о том, что тот или иной эксплоит начал продаваться в даркнете по модели Software as a Service (SaaS). И это на самом деле тревожный знак, ведь соглашаясь на выкуп, компании в реальности спонсируют этот преступный бизнес и способствуют его развитию. Один из вариантов защиты от последствий ransomware-атак – резервное копирование. Но важно понимать, что бэкап не спасает от заражения ransomware. Восстановление здесь имеет решающее значение, так как вам необходимо получить доступ к резервной копии, чтобы откатить все системы и восстановить данные без потерь (в зависимости от RPO). Если говорить о превентивных мерах, то у Veeam, например, в состав Veeam Availability Suite входит решение по мониторингу Veeam ONE. С его помощью можно с лёгкостью отследить подозрительную активность в инфраструктуре, например: повышение нагрузки или запуск каких-то новых процессов (как вариант, неизвестное приложение начало собирать слишком много информации), а после обнаружить конкретную угрозу и на основе этого принять дальнейшие меры.

А может произойти такая ситуация, что резервная копия тоже будет заражена ransomware?

Конечно, и её тоже следует учитывать при разработке BCP и стратегии управления данными. Выбирая решения для резервного копирования,

Виталий Савченко
руководитель группы системных инженеров Veeam Software

я рекомендую отдавать предпочтение тем, которые обеспечивают безопасность резервных копий. Этого можно достигнуть разными способами, в том числе и проверенными. Например, WORM (Write Once Read Many) для лент LTO (Linear Tape-Open) и такими новыми и эффективными, как хранение резервных копий в хранилищах объектов, поддерживающих функцию S3 Object Lock. Речь идёт о т. н. immutable, или «незыблемом» бэкапе, давайте назовём его так. При записи точки восстановления её можно прочитать, но ничего нельзя записать в неё, соответственно, ни один ransomware-вирус не сможет нанести ущерб данным.

Насколько становится понятно из Вашего рассказа, внедрение BCP, бэкап – это всё довольно дорого. Насколько такие серьёзные вложения в защиту данных сопоставимы с потенциальными потерями малого или среднего бизнеса? Стоит ли расходовать на это и без того скромные бюджеты?

На самом деле, для небольших компаний никакого отличия нет. Конечно, в денежном выражении их риски меньше. Если я крупный ритейлер и у меня 5 тысяч магазинов, то у меня, условно, 5 тысяч рисков и ещё гигантская логистика. Если у меня маленький бизнес, тоже есть риски, но их существенно меньше и от них легче защититься. Но это не значит, что защита от таких рисков мне не нужна. Как раз-таки наоборот, небольшой бизнес должен думать о защите данных в первую очередь, так как если крупная корпорация, скорее всего, сможет покрыть убытки в случае простоя или потери данных, то малый бизнес может этого и не пережить. Поэтому, небольшим компаниям тоже необходим свой BCP. Вопрос только в требованиях.

Я бы провёл аналогию с рынком мобильных телефонов, которая сложилась в середине нулевых. Смартфоны или КПК могли позволить себе только очень обеспеченные пользователи, у большинства были кнопочные телефоны. Но времена изменились, и сейчас смартфон может позволить себе практически каждый. Так же и с решениями для резервного копирования и защиты данных: чем больше компания готова вложить, тем меньше времени и сил займёт восстановление. Простой пример: поставщик ПО для резервного копирования обещает вам, что допустимое время восстановления данных (RTO) составит 20 минут. Но клиента не устраивает, он хотел бы сократить это время до минуты. И поставщик говорит: конечно, я могу это сделать, но будет стоить дороже. И клиент, исходя из специфики своего бизнеса, уже сам должен решить, что для него критичнее: 20 минут простоя или дополнительные расходы на бэкап и сокращение RTO и RPO. Но я думаю, что постепенно стоимость таких решений станет снижаться, и они будут становиться всё более доступными для бизнеса безотносительно его формата.

Можете ли Вы сказать как один из ключевых игроков рынка, что за время пандемии COVID-19 востребованность бэкапа выросла?

Конечно! Защита информации сейчас приобрела особое значение. Например, мы видим значительный рост решений для резервного копирования Office 365. Переход на удалённую работу привёл также и к взрывному росту использования Microsoft Teams. За прошедший год число ежедневных активных пользователей составило 115 млн, что на 475% больше, чем годом ранее. А наш Veeam Backup для Microsoft Office 365 скачали свыше 133.000 раз в десятках тысяч организаций.

Как Вы думаете, какое мы увидим обеспечение непрерывности бизнеса в будущем? Если сейчас уже возможно обеспечить бесперебойную работу сервисов или их восстановление за несколько минут, то чего нам ожидать в ближайшие годы? Мгновенное восстановление?

Конечно, до мгновенного восстановления данных ещё очень далеко. Хотя я не исключаю, что в перспективе отсчёт пойдёт и вовсе на наносекунды. Технически многое возможно уже сейчас. Но скорость восстановления не единственное, что можно усовершенствовать. Большое значение имеет также тонкость настройки и кастомизация под конкретные запросы пользователей.

Так, например, если вы пользуетесь Microsoft Teams, вам важна возможность быстро и легко находить и восстанавливать нужные данные именно в Teams, в том числе отдельные каналы, настройки или группы целиком. Ключевую роль здесь играет конкретная конфигурация Teams.

Мы в Veeam стремимся упростить для компаний эту непростую задачу и создаём решения, которые обеспечивают возможности тонкой настройки восстановления данных. Примером тому может служить наш новый Veeam Explorer для Microsoft Teams, созданный с нуля специально для Microsoft Teams. Он позволяет чётко структурировать данные и может служить надёжным инструментом для поддержания непрерывности бизнеса.

Стремление усовершенствовать существующие и успешно работающие средства, обеспечивающие непрерывность бизнеса, и есть одна из главных задач на ближайшую перспективу. И компания Veeam будет продолжать двигаться вперёд и быть лидером.

VEEAM

www.veeam.com

Учебный Центр

Курсы с сфере иформационных технологий

CIS
Учебный Центр

Образование в ИТ-сфере

Курсы предназначены для специалистов и компаний, служб безопасности, работающих в сфере защиты информации.

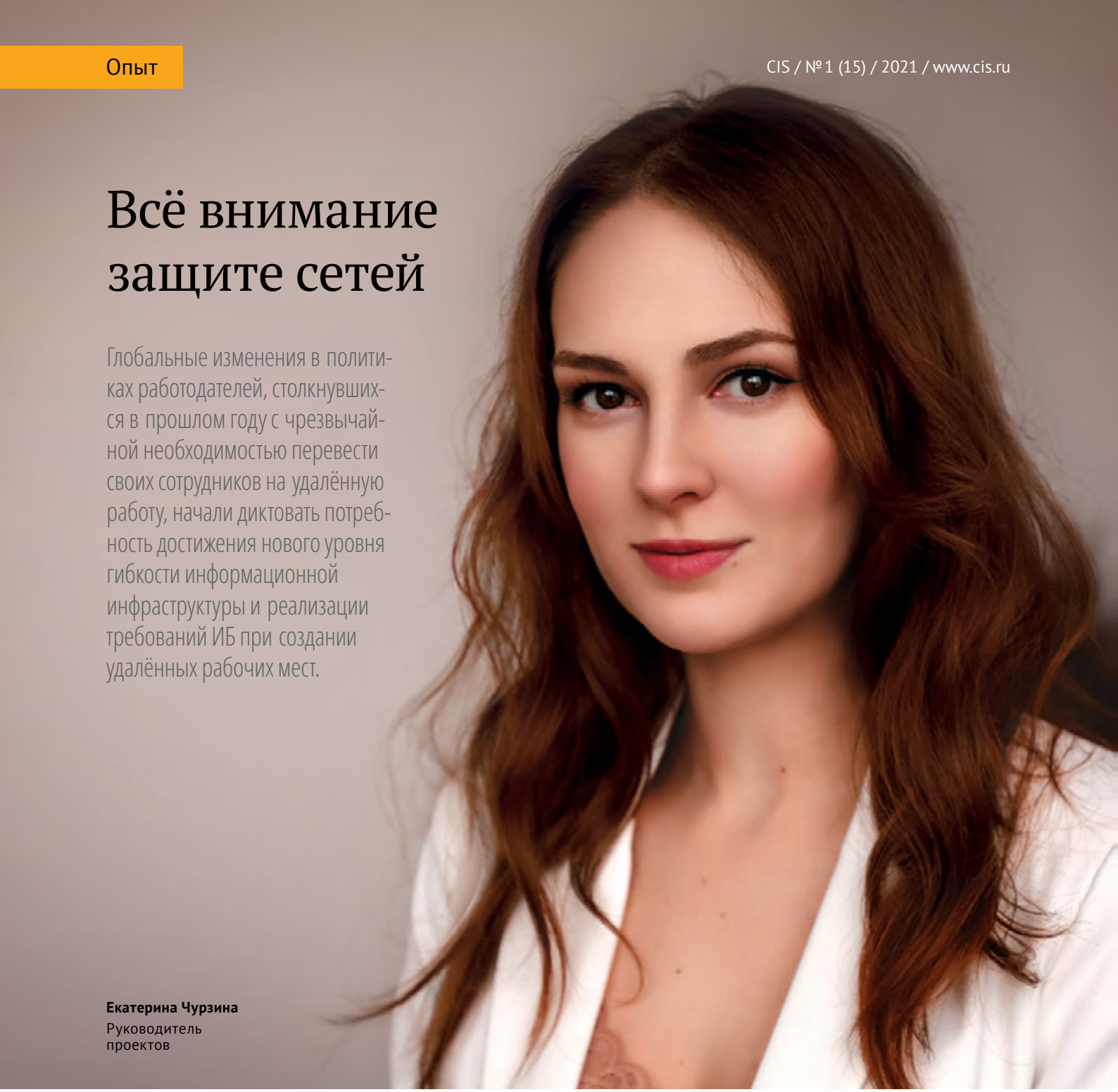
В процессе обучения Вы получите не только теоретические знания, но и комплексные практические навыки по созданию надёжного центра информационной безопасности в своей компании.

education@cis.ru

CIS / № 1 (15) / 2021 / www.cis.ru

Всё внимание защите сетей

Глобальные изменения в политиках работодателей, столкнувшихся в прошлом году с чрезвычайной необходимостью перевести своих сотрудников на удалённую работу, начали диктовать потребность достижения нового уровня гибкости информационной инфраструктуры и реализации требований ИБ при создании удалённых рабочих мест.



Екатерина Чурзина
Руководитель проектов

Бизнес был вынужден либо вырабатывать с нуля, или оперативно и существенно изменять подходы к интеграции таких рабочих мест, усилить методы аутентификации и защиту каналов связи. Зачастую это было сделано в «пожарном режиме», в результате чего компании самых разных масштабов столкнулись с целым спектром проблем:

- рабочая среда плохо организована, сотрудникам неудобно выполнять свои обязанности, и в результате падает производительность;
- доступ во внутренние системы пользователи получили как с корпоративных устройств, на которых есть все необходимые настройки, так и с личных устройств, которые не соответствуют корпоративным политикам ИТ и ИБ;
- отсутствует полноценный контроль подключений пользователей и используемых ими устройств.

Как следствие этого, в ИТ/ИБ-подразделениях отсутствует полноценная картина происходящего, что ставит под серьёзную угрозу конфиденциальные данные бизнеса, чревато репутационными потерями и значительными финансовыми издержками. В 2020 году было отмечено рекордное количество атак на средний и крупный бизнес. Основными факторами, привлекающими внимание хакеров к пользовательским устройствам, стали: операционная система, приложения и сетевой трафик. Как правило, главную угрозу представляют собой вредоносные программы, фишинг, уязвимости в приложениях, атаки типа Man-in-the-Middle, эксплойты для операционных систем, не эффективные профили настроек пользовательского устройства.

Бизнесу необходимо использовать комплексную защиту мобильных устройств, которая позволит предотвращать продвинутые кибератаки, ведущие к утрате конфиденциальных данных. Также требуется обеспечить доступ в корпоративную

сеть только с проверенных безопасных устройств. Решить подобную задачу можно несколькими путями.

Один из них – использование Cisco Duo – решения адаптивной многофакторной аутентификации пользователей и устройств. Аутентификация осуществляется перед предоставлением доступа для работы с различными корпоративными и облачными приложениями. Двухфакторная аутентификация всех пользователей поможет определить и подтвердить истинность их личностей, а работодателю предоставляется возможность вводить наиболее гранулированную политику в отношении доступности данных для каждого работника. Ещё одна особенность Duo – это проверка устройств пользователей на наличие неактуальных версий программного обеспечения и недостающих протоколов защиты.

Другой вариант обеспечения безопасного доступа в корпоративную сеть с пользовательских устройств – VMware Workspace ONE – аналитическая платформа цифровой рабочей области, обеспечивающая удобное и безопасное предоставление и администрирование любых приложений на всех устройствах. На этой платформе объединены возможности контроля доступа и управления приложениями и конечными устройствами на базе различных операционных систем, а использовать её можно в формате облачной услуги или локального решения. Workspace One предоставляет пользователям упрощённый удалённый доступ к корпоративным ресурсам и обеспечивает ИТ/ИБ-специалистам возможность более целостного управления информационной инфраструктурой, предоставляя в их распоряжение комбинированный комплекс устройств управления, аутентификации и безопасного хранения приложений предприятия.

Обеспечив контроль за устройствами, с которых осуществляется удалённый доступ в корпоративную сеть, необходимо не забыть и о беспроводных сетях Wi-Fi, ставшими де-факто основным каналом передачи данных. Для предотвращения и минимизации данных угроз необходимо регулярно проводить аудит безопасности Wi-Fi сетей и использовать современные средства и методы защиты, в том числе системы предотвращения вторжений IPS (Intrusion Prevention System), которые позволяют существенно повысить уровень защищённости и снизить риски компрометации устройств пользователей.

Эксперты CTI обращают внимание на то, что сейчас наиболее используемые виды атак на сети и Wi-Fi – это атаки на сами устройства (брутфорс, атаки на прошивку и т. д.), атаки на авторизацию (брутфорс, DDoS и т. д.), на пользователя (перехват данных, фишинг и т. д.), а также на устройства пользователей (подмена загружаемых файлов на вирусы, компрометация устройства и т. д.).

Антон Афанасьев, руководитель направления информационной безопасности CTI, рекомендует регулярно контролировать настройки устройств: обеспечивать обновление прошивок, проверять пароли, актуализировать сетевые доступы и связи с элементами корпоративной сети, контролировать правила авторизации пользователей при подключении к Wi-Fi. Важное значение приобретает регулярный аудит Wi-Fi (в том числе использовать специализированные WIDS/WIPS), а также переход на современные методы аутентификации, включая сертификаты.

Эксперты CTI рекомендуют настроить интеграцию со средствами мониторинга и обеспечения ИБ, регулярно обучать сотрудников безопасному использованию Wi-Fi, а также постоянно проводить радиоразведку для выявления слепых зон, проверки систем качества настройки точек доступов и высокочувствительной технологии по перераспределению трафика с перегруженных участков без потери качества подключения.

В случае наличия у организации сети филиалов развёртывание распределённых корпоративных сетей на основе технологии Cisco SD-WAN может стать хорошим решением для организации централизованного управления и автоматизации распределённой корпоративной сети. Владимир Ярославский, менеджер по развитию бизнеса, Cisco отмечает, что особенностью этой технологии является разделение уровней транспорта и контроля, что позволяет удалённым филиалам централизованно управлять транспортными сетями. Ключевая характеристика Cisco SD-WAN – высочайший уровень защищённости от киберугроз, который обеспечивается встроенными сегментацией, шифрованием, поддержкой логических топологий, сервисных точек, а также внешними средствами ИБ.

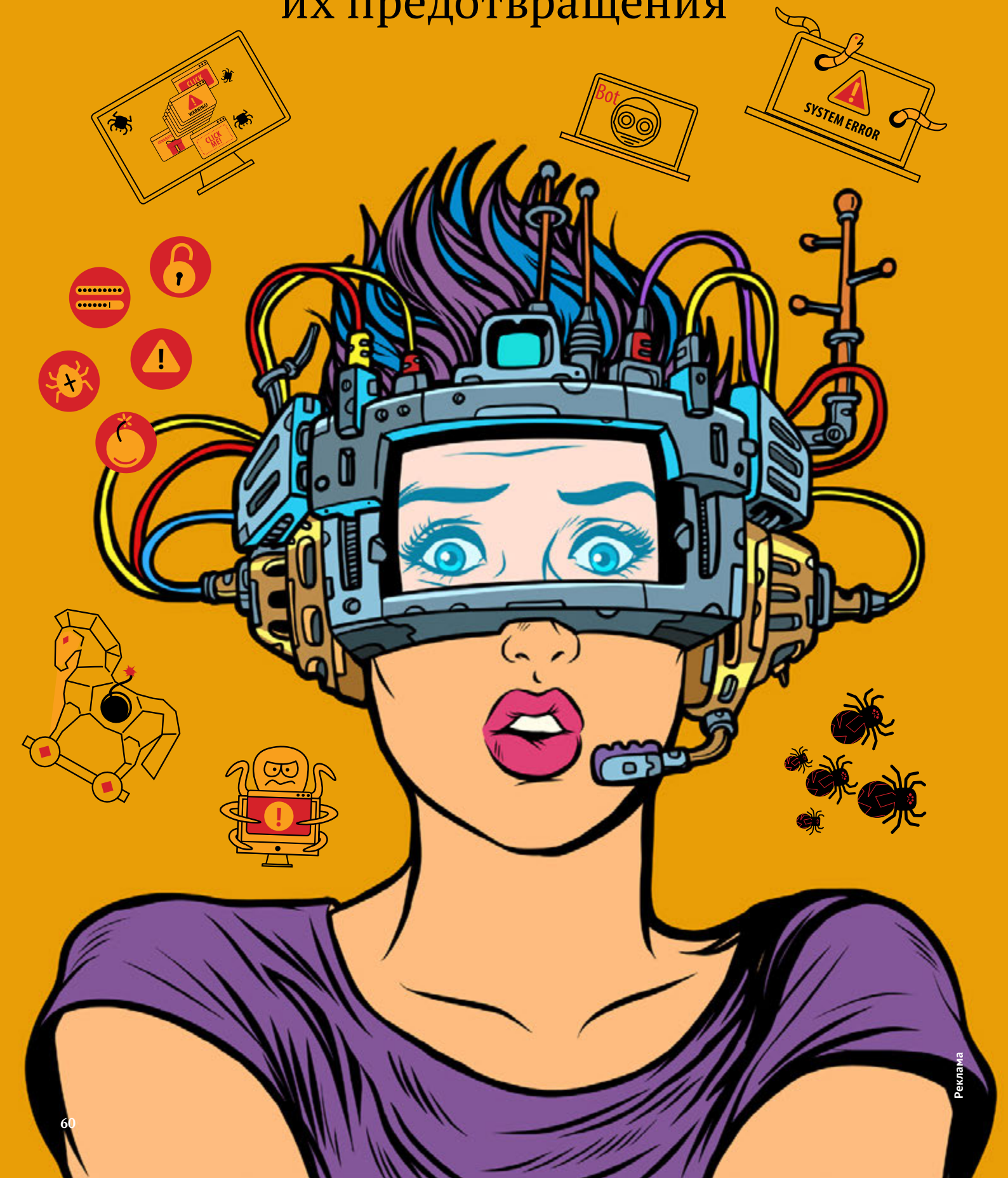
Выгоды внедрения SD-WAN можно обобщить следующим списком:

- обеспечение безопасности;
- использование всех доступных каналов связи;
- экономия пропускной способности каналов связи;
- ускорение подключения новых точек;
- автоматизация рутины, снижение ошибок.

Сетевая инфраструктура – основополагающий элемент любого бизнеса, независимо от размеров и отрасли. Конкурентоспособность, возможности масштабирования бизнеса и, конечно, неуязвимость от внешнего воздействия зависят от того, на каком функциональном и техническом уровне построена корпоративная сеть. Бизнес, столкнувшийся с возросшими требованиями к качеству и надёжности сетевой инфраструктуры, имеет в своём распоряжении комплексные информационные системы, обеспечивающие сбор данных, их анализ, передачу и защиту. Дело за малым – грамотно расставить приоритеты и внедрить правильные решения, обеспечивающие необходимый уровень безопасности сетей.

---

10 различных типов вредоносных атак и способы их предотвращения



Ежегодно к существующей армии ИТ-специалистов добавляются новые люди. К сожалению, стоит отметить, что уровень знаний этих специалистов с каждым днём падает.

Всё чаще и чаще они относятся к своим обязанностям как просто к работе оператора. Они знают, на какие кнопки нажимать, но не имеют ни представления, ни желания понять, зачем это нужно делать. Увы, то же самое относится и к специалистам по информационной безопасности, а уж тем более к обычным пользователям, роль которых в обеспечении безопасности в связи с распространением удалённого формата работы чрезвычайно выросла.

Именно поэтому специалисты из компании «Совинтегра» решили написать статью, посвящённую типам вредоносных атак и способам их предотвращения. Безусловно, полезнее было бы прочитать об этом на сайтах антивирусных компаний. Но если серьёзно, много ли пользователей читает такие статьи? Ответ очевиден: нет, конечно! Итак, мы практически ежедневно сталкиваемся с вредоносными программами. Но что это такое? Как классифицировать их по типам? Как правильно с ними бороться?

Типы вредоносных программ

Вредоносное программное обеспечение, как правило, предназначено для повреждения, нарушения работы или использования компьютеров или компьютерных систем в целях злоумышленника. Все боятся, что «хакнут» именно их, или, наоборот, считают, что «до меня никому дела нет». Но в действительности злоумышленникам нет никакого дела до пострадавших, им нужен масштаб.

Следовательно, вредоносное ПО может угрожать вашей компании как с коммерческой точки зрения, так и в плане производительности.

Именно поэтому крайне важно иметь надёжный анализ вредоносного ПО, так как понимание того, как распространяются различные типы программ, имеет жизненно важное значение для их распознавания и удаления последствий.

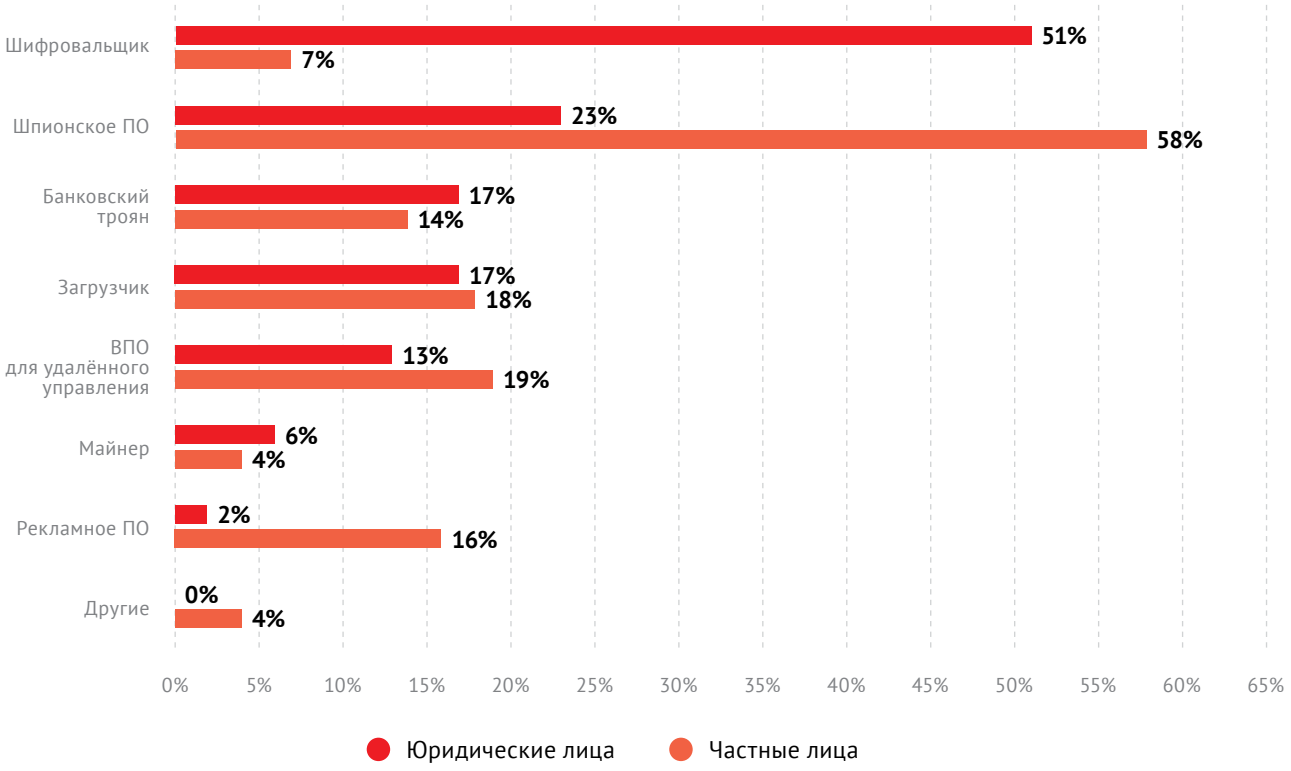
10 различных типов вредоносного ПО

1. Trojan Horses (трояны).
2. Worms (черви).
3. Adware (рекламное ПО).
4. Cryptojacking («чёрные криптовалютчики» – злонамеренный майнинг криптовалюты).
5. Spyware (шпионское ПО).
6. Ransomware (программы-шифровальщики, программы-вымогатели).
7. Malvertising (вредоносная реклама).
8. Backdoor.
9. Rootkits (руткиты).
10. Botnets (ботнеты).

Вся статистика приведена по данным Positive Technologies.

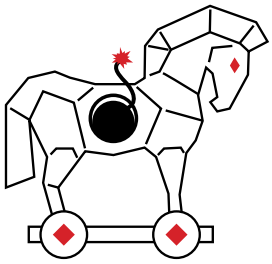
Типы украденных данных (в атаках на юридические лица).

Типы украденных данных (в атаках на частных лиц).



Типы вредоносного ПО (доля атак с использованием вредоносного ПО).

1. Trojan Horses



На первом месте сегодня среди вредоносных программ выделяются троянские. При этом для проникновения в компьютерную систему злоумышленники притворяются, что это вредоносное ПО является чем-то полезным, например конкретным предложением или подарком.

Основные цели троянов – кража конфиденциальных данных, сбой устройства, кража личной информации, например данных платёжных карт.

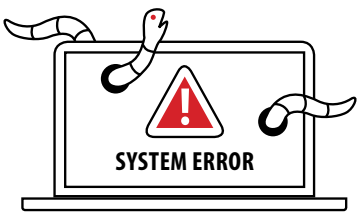
При этом блокируется антивирусное ПО, замедляется работа вашей системы: она не работает должным образом. Именно поэтому крайне важно защитить вашу систему от данного вида вредителя.

Профилактика

Троян может проникнуть в систему только с разрешения пользователя или при эксплуатации уязвимости в сетевой подсистеме. Именно поэтому для проникновения часто применяются приёмы социальной инженерии (обман пользователя).

В первую очередь обратите серьёзное внимание на ссылки в письмах и вложениях, которые при открытии начнут самостоятельно скачивать вредоносные программы. Особенностью такого механизма распространения является то, что именно пользователь инициирует скачивание.

2. Worms (черви)



Распространение червей не требует вмешательства пользователя.

Компьютерный червь – это разновидность программ, которые распространяют свои копии с компьютера на компьютер. Червь может копировать себя без какого-либо вмешательства человека, и ему не нужно прикрепляться к программе, чтобы нанести ущерб.

Как работают компьютерные черви

Стоит помнить, что червь – это более продвинутый троян, который помимо захвата машины жертвы старается захватить другие устройства в сети за счёт наличия в них уязвимостей.

Компьютерные черви могут передаваться через уязвимости ПО или могут приходить в виде вложений в спам-сообщениях или мгновенных сообщениях (IM). После открытия эти файлы могут содержать ссылку на вредоносный веб-сайт или автоматически загружать компьютерного червя. После установки червь незаметно начинает работу и заражает машину без ведома пользователя.

Черви могут изменять и удалять файлы, даже внедрять на компьютер дополнительные вредоносные программы. Иногда целью компьютерного червя является лишь многократное копирование самого себя, тем самым перегружая общую сеть, истощая системные ресурсы: место на жёстком диске или пропускную способность. Помимо того, что черви наносят ущерб ресурсам компьютера, они могут также украсть данные, установить бэкдор и позволить хакеру получить контроль над компьютером и его системными настройками.

Как узнать, есть ли на вашем компьютере червь

Если есть подозрения, что ваши устройства заражены компьютерным червём, немедленно выполните проверку на вирусы. Даже если результат сканирования отрицательный, продолжайте проявлять активность, выполнив следующие действия:

- **Следите за свободным местом на жёстком диске.** Когда черви многократно воспроизводятся, они начинают использовать свободное место на компьютере.
- **Следите за скоростью и производительностью.** Ваш компьютер в последнее время тормозит? Некоторые из программ дают сбой или работают неправильно? Это может быть признаком того, что червь съедает вычислительную мощность.
- **Следите за отсутствующими или новыми файлами.** Одна из функций компьютерного червя – удалять и заменять файлы на компьютере.

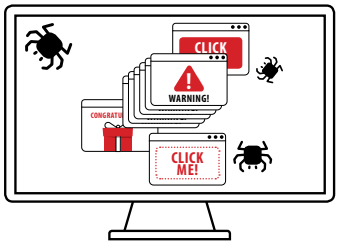
Профилактика

Предотвращение подобных атак довольно сложно, но факт в том, что вы можете обезопасить свой компьютер, просто активировав брандмауэр, поскольку он ограничит или уменьшит сетевой трафик.

Ещё один способ профилактики – периодическое сканирование (червь может спать до определённого времени), а также контроль сетевого взаимодействия (внутрисетевого и внешнего) – многие средства защиты уже знают поведение червя (сигнатуры сетевого пакета), IP-адрес, куда обращается червь наружу (для скачивания дополнительного ПО).

Не забудьте о необходимости применять и регулярно обновлять антивирусное ПО.

3. Adware (рекламное ПО)



По определению, рекламные программы – это любое программное обеспечение, вредоносное или нет, которое отображает рекламу на компьютере. Однако чаще всего люди используют понятие «рекламные программы» для обозначения вредоносного ПО, которое показывает обманчивую рекламу, всплывающие окна, большие баннеры и полноэкранные рекламные ролики с автоматическим воспроизведением в веб-браузере.

Всё рекламное ПО предназначено для получения дохода для своего разработчика каждый раз, когда пользователь нажимает на показываемую им рекламу. Некоторые типы рекламного ПО могут затруднять просмотр веб-сайтов, перенаправляя вас на вредоносные сайты с контентом для взрослых. Существуют также типы, которые собирают данные о ваших просмотрах без разрешения и используют их для показа рекламы, которая больше соответствует вашим вкусам и на которую вы с большей вероятностью нажмёте.

Кроме того, подчеркну, что в случае мобильных устройств рекламное ПО осуществляет подписку на платные сервисы.

Таким образом, эти вредоносные программы нарушают функциональность и эффективность вашей работы.

Симптомы заражения рекламным ПО

Если подозреваете, что ваш компьютер может быть заражён рекламным ПО, обратите внимание на один или несколько из следующих признаков:

- Ваш браузер внезапно стал работать медленнее, чем раньше, и/или очень часто некорректно завершает свою работу.
- Баннеры и реклама появляются на сайтах, на которых их раньше не было.
- Ваша домашняя страница каким-то образом изменилась, и вы не можете вернуть её обратно.
- Каждый раз, когда хотите посетить сайт, вы перенаправляетесь на другую страницу.
- Вы замечаете в своём браузере новые панели инструментов, плагины или расширения.
- Щелчок в любом месте страницы открывает одно или несколько всплывающих окон.
- Ваш компьютер начинает установку нежелательных приложений без вашего разрешения.

Как удалить рекламное ПО

Универсального рецепта удаления рекламного ПО с компьютера не существует. Для удаления некоторых типов такого ПО достаточно просто удалить расширение и перезапустить браузер, с другими типами могут потребоваться специальные инструменты для успешного обнаружения и удаления рекламного ПО.

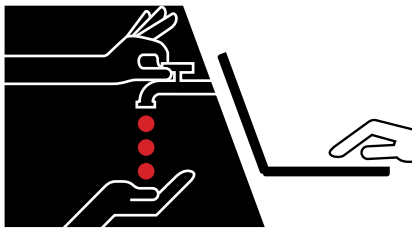
Другие типы ПО могут быть настолько серьёзными, что даже самое лучшее антивирусное ПО не сможет их удалить. В таких редких случаях переустановка операционной системы может быть единственным решением.

Несмотря на то, что наиболее распространённые типы рекламного ПО не так опасны, вы не должны ничего оставлять на волю случая в Интернете. Если вы это сделаете, то не только рискуете потерять файлы на своём компьютере, но и ваша личная информация может быть скомпрометирована.

Общая рекомендация. Есть сервисы DNS, которые уже категоризируют адрес, куда вы хотите перейти – www.dns.yandex.ru/advanced

В этом случае переход на вредоносный сайт будет просто блокироваться.

4. Cryptojacking («чёрные криптовалютчики»)



Атака Cryptojacking, это, по сути, тип вредоносных программ, которые используют вычислительные возможности для добычи криптовалюты.

Cryptojacking – это несанкционированное использование чужого компьютера для добычи криптовалюты. Хакеры делают это, заставляя жертву щёлкнуть вредоносную ссылку в электронном письме, которая загружает код криптомайнинга на компьютер, либо заражая веб-сайт

или онлайн-рекламу кодом JavaScript, который автоматически запускается после загрузки в браузере.

В любом случае код криптомайнинга работает в фоновом режиме, а ничего не подозревающие пользователи используют свои компьютеры. Единственный признак, который они могут заметить, – это более низкая производительность или задержки в выполнении команд.

Как работает Cryptojacking

У хакеров есть два основных способа заставить компьютер жертвы тайно майнить криптовалюту. Один из них – обманом заставить пользователей загрузить код криптомайнинга на свои компьютеры, например с помощью тактики, похожей на фишинг: жертвы получают законное письмо, которое побуждает их перейти по ссылке. Ссылка запускает код, который размещает скрипт майнинга на компьютере. Затем сценарий запускается в фоновом режиме, пока жертва работает.

Другой метод – внедрить сценарий на веб-сайт или объявление, которое доставляется на несколько веб-сайтов. Как только жертвы посещают веб-сайт или заражённое объявление появляется в их браузерах, скрипт запускается автоматически. На компьютерах пользователей код не хранится. Какой бы метод ни использовался, код выполняет сложные математические задачи на компьютерах жертв и отправляет результаты на сервер, который контролируется хакером.

Хакеры часто используют оба метода, чтобы получить максимальную отдачу. Атаки используют старые уловки вредоносного ПО для доставки более надёжного и устойчивого программного обеспечения на компьютеры жертв в качестве альтернативы.

Некоторые скрипты майнинга криптовалют имеют возможности заражения, которые позволяют им заражать другие устройства и серверы в сети. Это также затрудняет их поиск и удаление, поддержание постоянства в сети в лучших финансовых интересах крипто Cryptojacking.

Чтобы увеличить их способность распространяться по сети, код криптомайнера может включать несколько версий для учёта различных архитектур в сети. В одном примере, описанном в блоге AT&T Alien Labs, код криптомайнинга просто загружает имплантаты для каждой архитектуры до тех пор, пока один из них не заработает.

Сценарии также могут проверять, не заражено ли устройство конкурирующими вредоносными программами, занимающимися крипто-добычей. Если обнаружен другой криптомайнер, скрипт отключает его. Как отмечается в сообщении AT&T Alien Lab, у криптомайнера может быть механизм предотвращения отключения, который запускается каждые несколько минут.

В отличие от большинства других типов вредоносных программ, скрипты Cryptojacking не наносят вреда компьютерам или данным жертв. Они лишь крадут ресурсы процессора. Для отдельных пользователей более низкая производительность компьютера может быть просто раздражением. Организация со множеством систем с Cryptojacking может нести реальные затраты с точки зрения службы поддержки и времени ИТ, затрачиваемого на отслеживание проблем с производительностью и замену компонентов или систем в надежде решить проблему.

Почему Cryptojacking популярен

Никто точно не знает, сколько криптовалюты добывается с помощью Cryptojacking, но нет никаких сомнений в том, что эта практика широко распространена. Cryptojacking на основе браузера сначала быстро рос, но, похоже, постепенно сокращается, вероятно, из-за нестабильности криптовалюты и закрытия Coinhive – самого популярного майнера JavaScript, который также использовался для законной деятельности по майнингу криптовалюты в марте 2019 года. Объём атак с использованием криптоджекинга упал на 78% во второй половине 2019 года в результате закрытия Coinhive.

Однако спад начался раньше. Отчёт Positive Technology по угрозам кибербезопасности за первый квартал 2019 года показывает, что на долю криптомайнинга сейчас приходится только 7% всех атак по сравнению с 23% в начале 2018 года. В отчёте говорится, что киберпреступники переключились на программы-вымогатели, которые считаются более прибыльными.

В январе 2018 года исследователи обнаружили ботнет Smominru, который заразил более полумиллиона машин, в основном в России, Индии и Тайване. Ботнет был нацелен на серверы Windows для майнинга Monero, и, по оценкам компании Proofpoint, занимающейся кибербезопасностью, на конец января он заработал 3,6 миллиона долларов.

Cryptojacking даже не требует значительных технических навыков, ведь комплекты для cryptojacking доступны в DarkNet всего за $ 30.

При этом риск быть пойманным и идентифицированным также намного меньше, чем при использовании программ-вымогателей. Код криптомайнинга запускается тайно и может долгое время оставаться незамеченным. После обнаружения очень сложно отследить источник, а у жертв мало стимулов для этого, поскольку ничего не было украдено или зашифровано.

Cryptojacking: как выглядит атака

У хакеров есть два основных способа атаковать компьютер:

- Загрузить код криптомайнера на ваш компьютер. Это может быть сделано методом фишинга, то есть ссылкой на странице или в электронном письме. При нажатии на него загружается скрипт cryptominer на компьютер, который запускает его беззвучную работу. Это может быть сделано путём инсталляции легитимного платного ПО с «таблеткой внутри». «Таблетка» не только активирует ПО, но и устанавливает своё собственное, которое начинает «майнить».
- Внедрить вредоносный скрипт в код страницы. Когда пользователь заходит на такой сайт, появляется заражённое объявление и скрипт запускается автоматически. Код не хранится на заражённой машине: когда компьютер подключён к Интернету, тот подключается к серверу, контролируемому хакером, который использует вычислительные мощности заражённого ПК для майнинга криптовалюты.

Хакеры часто используют оба метода, чтобы увеличить шансы на успешную атаку и максимизировать прибыль.

Cryptojacking: как этого избежать

Как ни странно, но лучшим способом профилактики является обучение ваших сотрудников. Ведь, как правило, заражение происходит с помощью фишинга. Гораздо проще предупредить заражение, чем искать вредоносные программы позднее.

Установите дополнительные расширения против криптомайнеров и блокировщиков рекламы в браузере. Очень часто скрипты майнеров предоставляются рекламой, поэтому блокировка рекламы в данном случае может помочь.

Используйте антивирусные решения. Многие производители антивирусов добавили обнаружение майнеров.

Постоянно проверяйте обновления плагинов и расширений вашего браузера.

К сожалению, ни одна из вышеперечисленных практик не эффективна на 100%, но это единственное, что вы можете сделать.

5. Spyware (шпионские программы)

Эти вредоносные программы предназначены для слежки и сбора информации о пользователе.

Есть два основных типа spyware:

- **Трекер.** Отслеживает поведение пользователя на локальном устройстве, в интернете, его физическое перемещение (с помощью гео-данных). Сюда же входят некоторые виды adware, которые показывают пользователю рекламу с учётом истории его поисковых запросов.
- **Кейлогер.** Изначально кейлогеры регистрировали нажатия клавиш клавиатуры и клики мыши. Постепенно функционал расширялся: теперь они умеют делать скриншоты, перехватывать информацию из буфера памяти, аудиозаписи микрофона, сканировать email-трафик и многое другое. Вводимые логины, пароли и прочие личные данные – излюбленные цели создателей данного типа spyware, и в этом аспекте кейлогеры родственны с троянскими программами.

Существуют и легальные виды spyware, например сервисы Google. Они следят за местоположением пользователя, его предпочтениями в выборе контента, поисковой историей и т.д. Всё это преподносится как средство «повышения уровня обслуживания». Многие, впрочем, расценивают подобные действия как вмешательство в личную жизнь. Однако, в отличие от вредоносного spyware, большинство шпионских сервисов Google можно отключить самостоятельно.

Источниками могут стать заражённые веб-сайты, можно получить программу по почте, скачать «в нагрузку» с непроверенными бесплатными программами.

Stalkerware

Подвидом программ-шпионов является stalkerware – коммерческое шпионское ПО для слежки за супругами или интимными партнёрами.

Многие эксперты по информационной безопасности применяют этот термин для любого вредоносного ПО, которое может быть даже потенциально использовано в целях соответствующего слежения. При этом выделяются следующие характерные черты:

- наличие мощных функций мониторинга (кейлогер, снятие скриншотов экрана, мониторинг интернет активности, периодическая фиксация местоположения, возможность записи видео и звука);
- работа в скрытом режиме (мониторинг осуществляется без оповещения об этом пользователя, приложение отсутствует в списке установленных программ, маскировка работающего приложения под системные процессы и утилиты);
- требование отключения антивирусной или встроенной в ОС защиты для корректной установки и/или работы приложения;
- в случае с мобильными приложениями – установка в обход официальных магазинов приложений;
- прямое позиционирование производителем ПО своего продукта как средства слежения за интимным партнёром.

Методы распространения

Из-за своей агрессивной природы коммерческие программы-шпионы не попадают в App Store и Google Play. Тем не менее страницы таких программ со ссылками на скачивание можно без проблем найти в интернете. Естественно, эти программы вынуждают пользователей разрешить установку приложений из сторонних источников, вне официального магазина Google Play, что зачастую подвергает устройства риску. Это разрешение делает Android-устройство уязвимым к вредоносным программам и нарушает политики безопасности Google.

Коммерческие программы-шпионы завоевали определённую популярность, некоторые из них даже стали частью различных схем распространения. Они могут называться по-разному и распространяться с разных веб-сайтов, но при этом фактически быть одной и той же программой. Это важный момент, который относится ко многим представителям stalkerware. Существуют даже специальные предложения, позволяющие третьим лицам покупать франшизы и распространять продукты под собственными брендами.

Нет необходимости доказывать, что приложения stalkerware несут отрицательные последствия: их исходная концепция уже абсолютно неэтична. Однако есть много других угроз, которым подвергается пользователь, устанавливающий их. Такие приложения нарушают правила магазинов приложений, вредят безопасности устройства и подвергают данные, собранные у жертв, риску утечки в результате взлома. Впоследствии украденные данные могут использоваться для всех видов вредоносных действий от вымогательства денег до кражи цифровой идентичности. Кроме того, можно с уверенностью сказать, что есть люди, которые извлекают выгоду из таких программ и могут получить доступ к данным о жертвах при том, что про тех самих ничего неизвестно.

Несмотря на все вышеперечисленные находки, большинство производителей защитных решений не детектируют коммерческие приложения-шпионы

как угрозу из-за неопределённости их юридического статуса.

6. Ransomware (программы-шифровальщики, программы-вымогатели)

Это тип вредоносного ПО, которое может мешать пользователям входить в систему или данные, а также удалять или распространять данные, если платёж не оплачен.

Большинство программ-вымогателей сегодня делятся на две категории:

- Locker ransomware – сокращает доступ к компьютеру или заражённому устройству.
- Программа-шифровальщик – просто ограничивает доступ к файлам и сбор данных.

Ransomware (от ransom – выкуп и software – программное обеспечение) – тип зловредного ПО, предназначенного для вымогательства. Оно блокирует доступ к компьютерной системе или предотвращает считывание записанных в нём данных (часто с помощью методов шифрования), а затем требует от жертвы выкуп для восстановления исходного состояния.

Жертвами атак с применением вымогателей становятся как отдельные пользователи, так и организации. Программы-вымогатели могут попадать на компьютеры через вложения или ссылки в фишинговых электронных сообщениях, через заражённые веб-сайты с помощью drive-by-загрузок или в результате использования заражённых USB-накопителей.

Если компьютер или сеть подверглись заражению трояном-вымогателем, вредоносная программа блокирует доступ к системе или зашифровывает данные в ней. Киберпреступники требуют от жертвы уплаты выкупа за восстановление доступа к своему компьютеру или данным.

Профилактика

Вы получили электронное письмо, содержащее вирус-вымогатель. Что вы должны сделать, чтобы не быть жертвой атаки?

- Лучший способ распознать сообщение от шантажиста – проверить отправителя. Он вам известен? Если нет, будьте начеку.
- Не нажимайте ссылки и не открывайте вложения в сообщениях электронной почты от отправителей, которых не знаете.
- Будьте особенно осторожны, если во вложении вас попросят включить макросы. Это стандартный способ распространения вирусов-вымогателей.

Если вы стали жертвой атаки вымогателей, не платите выкуп.

Уплата выкупа не гарантирует, что киберпреступники вернут ваши данные, – в конце концов, это воры. И кроме того, таким образом вы способствуете укреплению их бизнеса, а значит, атаки будут продолжаться.

Если у вас есть резервные копии данных, которые хранятся на внешнем носителе или в удалённом хранилище, вы сможете восстановить их без всякого выкупа. А если нет, то рекомендую связаться с вашим поставщиком интернет-безопасности и узнать, есть ли у него инструмент для расшифровки данных, зашифрованных конкретным вымогателем. Вы также можете зайти на сайт No More Ransom (www.nomoreransom.org), общеотраслевой инициативы, призванной помочь всем жертвам программ-шантажистов.

7. Malvertising (вредоносная реклама)

Malvertising (вредоносная реклама) – это кибератака, в рамках которой используются рекламные объявления для распространения вредоносных программ. Этот тип угрозы активно развивается, поэтому следует обратить на неё внимание.

Само понятие состоит из двух английских слов advertising – реклама и malware – вредоносная программа. Как следует из названия, malvertising – это тип онлайн-рекламы, в которой рекламное объявление используется для распространения вредоносных программ. Киберпреступники встраивают вредоносную программу в рекламное объявление, которое размещают на хорошо известном сайте. Интернет-пользователи доверяют этому ресурсу, а потому спокойно загружают страницу этого сайта или могут даже нажимать на размещённые на нём рекламные объявления, в результате чего на их устройство скачивается вредоносная программа.

Как работает Malvertising

Как правило, malvertising возникает в том случае, когда киберпреступники покупают размещение рекламы на известном сайте и показывают внешне вполне нормальные рекламные объявления, но внутри них скрыт вредоносный код. Такое может случиться в силу того, что крупные веб-сайты используют стороннее ПО и/или внешних поставщиков для показа рекламных объявлений. Конечно, эти внешние поставщики пытаются отсеять вредоносную рекламу, однако злоумышленники постоянно находят обходные лазейки, которые позволяют им показывать свои рекламные объявления со встроенным вредоносным кодом.

Таким образом, реклама – отличный способ распространения вредоносного ПО, поскольку к ней прилагаются значительные усилия, чтобы сделать её привлекательной для пользователей с точки зрения продаж или рекламы товаров и услуг.

Типы вредоносной рекламы (malvertising)

С автоматической загрузкой (Drive-by Download)

Вредоносная реклама с автоматической загрузкой – вредоносное ПО загружается на компьютер жертвы без его взаимодействия с веб-страницей. Пользователю достаточно просто зайти на страницу сайта, где размещено мошенническое объявление, и его устройство будет заражено при загрузке страницы.

С загрузкой по клику (Click to Download)
Эти рекламные объявления имитируют обычные объявления и сделаны таким образом, чтобы обмануть попавшего на страницу сайта человека и побудить его нажать на такую вредоносную рекламу.

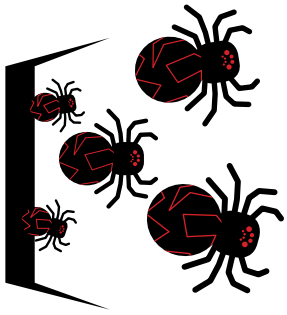
Профилактика

Проверяйте следующее:

- Выглядит ли рекламное объявление законным/легитимным? Посмотрите, кажется ли информация в нём разумной и точной.
- Используйте блокировщик рекламы для блокировки показа всех рекламных объявлений при просмотре любых сайтов. В результате этого, вы не будете видеть онлайн-рекламу, побуждающую вас нажать на неё.
- Если вас заинтересовало то, что рекламируется в объявлении, то лучше выполните отдельный поиск рекламируемой компании или продукта и посетите их сайт. Если всё законно, то такое же предложение должно быть на их сайте.
- Лучше всего не нажимать на рекламные объявления, независимо от того, насколько надёжным выглядит посещаемый сайт.
- Чтобы обеспечить безопасность вашего устройства, установите на него антивирус.

Размещение рекламы приносит сайтам неплохой доход, а потому использование рекламных объявлений для распространения с их помощью вредоносных программ будет процветать. Знания о том, что такое вредоносная реклама (malvertising) и как она может влиять на вас, помогут защитить себя от этих распространённых кибератак.

8. Backdoor



Backdoor – это секретный метод обхода стандартной аутентификации или шифрования в компьютерной системе, встроенном устройстве или других частях компьютера.

Backdoor обычно используются для получения уделённого доступа к компьютеру или получения доступа к зашифрованным файлам.

Можно использовать для получения доступа, мошенничества, удаления или предоставления конфиденциальных данных.

Бэкдоры могут принимать форму трояна, отдельной программы или кода во встроенном ПО и рабочих системах, поэтому бэкдоры широко известны.

Профилактика

Для предотвращения этого вредоносного ПО необходимо установить эффективный антивирус.

Не забудьте, что нужно установить все актуальные обновления по безопасности, что исключит вероятность создания бэкдора (с возможностью запуска так называемого «шел» или «реверс-шелла» – оболочка для удалённого управления системой атакующим).

9. Rootkit

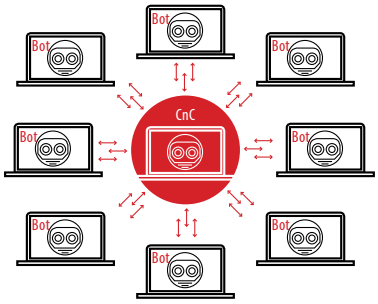
Rootkit – комбинация вредоносных программ, которые предназначены для предоставления незаконного доступа к компьютеру. Обычно скрывают своё существование или появление другого программного обеспечения.

Более того, установка rootkit может быть автоматизирована.

Удаление rootkit может быть сложной или почти невозможной, особенно когда rootkit остаются в ядре, поэтому микропрограммным rootkit может потребоваться замена оборудования.

Rootkit подменяют своим кодом системные функции и за счёт этого трудно обнаруживаются. Для их выявления необходимо записать загрузочный диск с антивирусом (Rescue Disk) и проверять ПК, загрузившись с него. Виртуализация файловой системы и виртуализация приложений, по сути, используют технологии rootkit, поэтому их функционал можно принять за работу rootkit по ошибке.

10. Botnets (боты и ботнеты)



Бот – компьютер, заражённый вредоносным ПО, что позволяет злоумышленнику удалённо управлять им.

Бота можно использовать для запуска дополнительных кибератак или преобразования в ботнет, который представляет собой набор ботов.

Таким образом, ботнеты – это традиционный метод рассредоточенного отказа в обслуживании, то есть DDoS-атаки, рост числа программ-вымогателей, кейлоггеров и других типов вредоносных программ. Вместе с тем стоит вспомнить прекрасный пример, когда на eBay продавали накрутку просмотров YouTube роликов. Понятное дело, что за деньги покупателя ролики «отсматривали» устройства ничего не знающих пользователей, угодивших в ботнет.

Профилактика

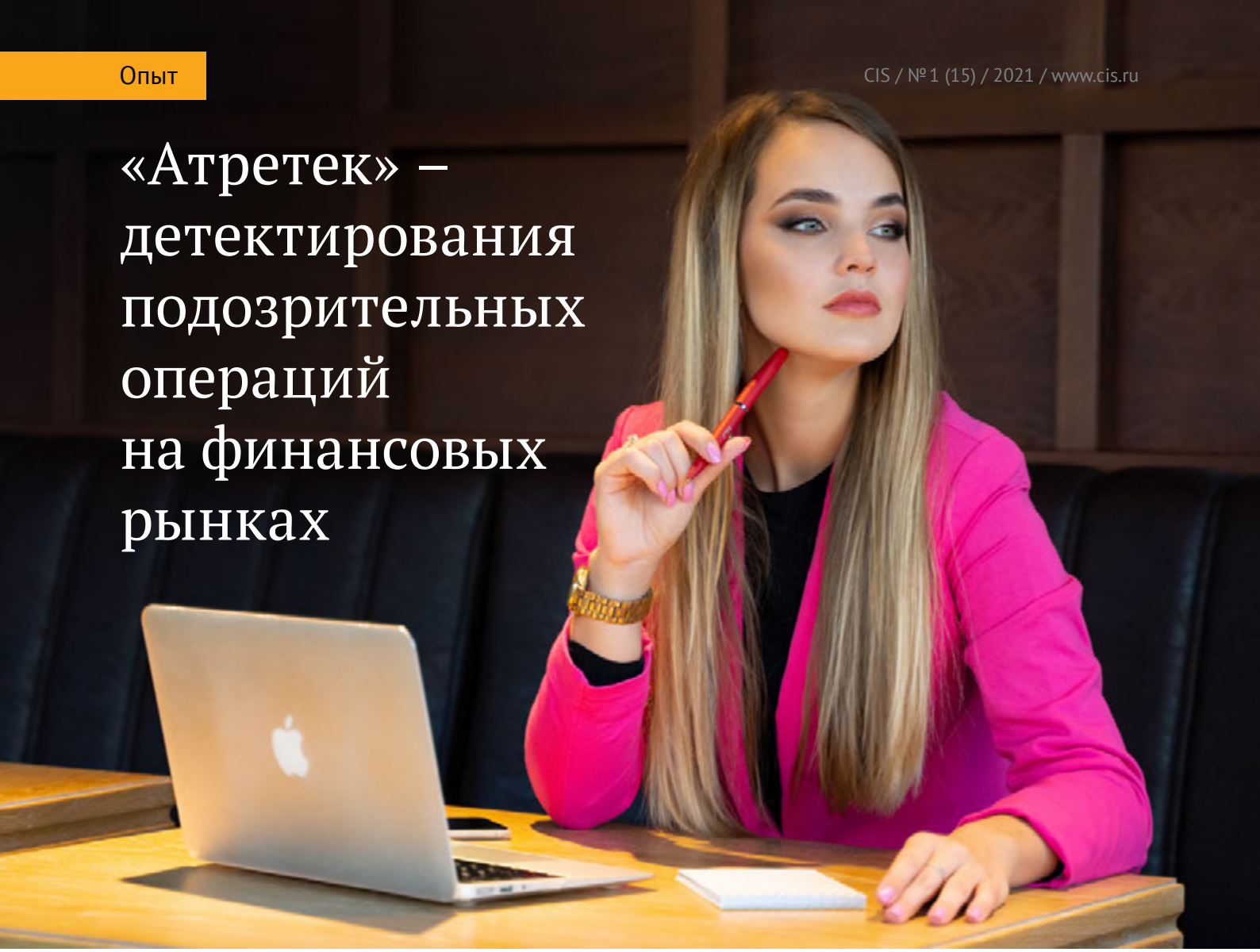
Следует использовать некоторые средства защиты, такие как инструменты защиты от ботнетов, программные исправления, мониторинг сети и осведомлённость пользователей.

Заключение

Надеемся, данная статья будет вам полезна и подтолкнёт к чтению статей на специализированных ресурсах.

CIS / № 1 (15) / 2021 / www.cis.ru

«Атретек» – детектирования подозрительных операций на финансовых рынках



Геннадий, добрый день! Мы публиковали интервью с Вами примерно 1 год назад. Как развивается система ТАФС и проект «Атретек»? Был ли негативный эффект от пандемии?

Добрый день. Спасибо, что снова пригласили пообщаться. Да, мы не стоим на месте. Пандемия заставляет всех меняться в сторону повышения эффективности. Поэтому, в целом, мы оцениваем эффект пандемии на индустрию цифровых технологий скорее как положительный. Нас это вынудило перейти полностью на «удалёнку», и в нашей команде это привело к сокращению затрат времени на транспорт и расходов на содержание офиса.

Напомню, что проект «Атретек» – это инновационный проект, который направлен на развитие цифровых технологий для комплексного автоматизированного детектирования профучастниками подозрительных операций на финансовых рынках.

В предыдущей статье мы рассказали о том, что наша команда занимается разработкой программного обеспечения, которое решает для своих пользователей две основных задачи: снижение вероятности санкций (штрафы, отзывы лицензий, уголовное преследование) со стороны Регуляторов за несанкционированную активность на финансовых рынках и предотвращение на ранней стадии мошенничества трейдеров, которые в сговоре с клиентами могут реализовывать схемы хищений денег у работодателей.

Что-нибудь с тех пор изменилось? Или Вы идёте вперёд по тем же рельсам? Появились ли у Вас в рамках проекта инновационные разработки или новые направления для инновационных исследований?

Сказать, что ничего не изменилось нельзя, хотя в целом наш проект развивается в рамках первоначальной концепции и изначально принятой стратегии. Но по ходу развития мы обнаружили много направлений внутри проекта, которые изначально казались незначительными.

Например, когда только начинали проект «Атретек» в 2018 году, мы наивно полагали, что самое главное, чтобы система умела автоматизированным образом находить «инцидент». Мы бросили все силы команды на разработку нескольких узкоспециализированных библиотек алгоритмов, которые умеют находить «инциденты». И не просто «инциденты», а «подлинные». К слову, инциденты бывают «ложные» и «подлинные». Ложные инциденты происходят от ложных срабатываний алгоритмов. И это отдельная интересная тема.

С общепринятой точки зрения «инцидентом» принято считать просто недоразумение, неприятное происшествие, даже некое «столкновение». А что такое инцидент по Вашей терминологии?

В терминологии инструкции пользователя нашей системой инцидент – это активность клиента (комбинация заявок/сделок в привязке ко времени, рыночным данным, новостному фону), которая может быть трактуема судом как «противоправное действие» либо трактуема руководством финансового института как «нежелательная активность» со стороны рыночных, репутационных и иных рисков.

Вы называете инцидентом «активность». Но ведь «активность» – это процесс, а при слове «инцидент» скорее приходит на ум результат, а не процесс. Разве не так?

Вы абсолютно правы, в общепринятом смысле это так и есть. Но если детально и глубоко посмотреть на то, что выявляет наша система, это будет похоже и на процесс, и на результат, как бы парадоксально это не звучало.

В терминологии «Общебанковское противодействие мошенничеству» (например, ДБО, пластиковые карты и т.п.) – инцидент – это, скорее, некое событие, которое происходит одномоментно. Например, перевод денежных средств со «спящих счётов» пенсионеров в пользу третьих лиц. На финансовых рынках инциденты – это не одномоментные события, а схемы, которые реализуются мошенниками в течение некоторого периода или иначе «интервала времени». Иногда это несколько секунд, а иногда это схемы, длящиеся несколько месяцев. Но практически никогда инцидент не бывает представлен разовой одномоментной транзакцией.

Приведите примеры. Что это за схемы, которые длятся то секунды, то несколько месяцев. О чём речь?

Самые одиозные примеры имели место не в текущем году. Но зато они были наиболее масштабные с точки зрения количества транзакций. Один из первых в современной истории резонансных случаев по данной теме был связан с трейдинговой активностью японского Daiwa Bank в США. Главный трейдер этого банка однажды вдруг раскаялся (интересно, что для него стало катализатором?) и написал «покаянное письмо» президенту Daiwa Bank о том, что в течение 12 лет скрывал мошеннические схемы и около 30000 фиктивных сделок на финансовых рынках. Все его транзакции проверяла специальная комиссия FED США и специальная комиссия Министерства Финансов Японии, не говоря уже о том, что до этого его торговую активность несколько лет подряд проверяла группа Больших аудиторов. И ни одна проверка не смогла обнаружить ничего подозрительного. В итоге оказалось, что убыток банка от активности Toshihide Iguchi (имя трейдера) превысил 1 млрд $. О чём это может говорить? О том, что любая отдельно взятая транзакция сама по себе может представлять инцидент в очень редких случаях. Поэтому её невозможно выявить «вне схемы» и тем более невозможно остановить на уровне «до нажатия кнопки трейдером».

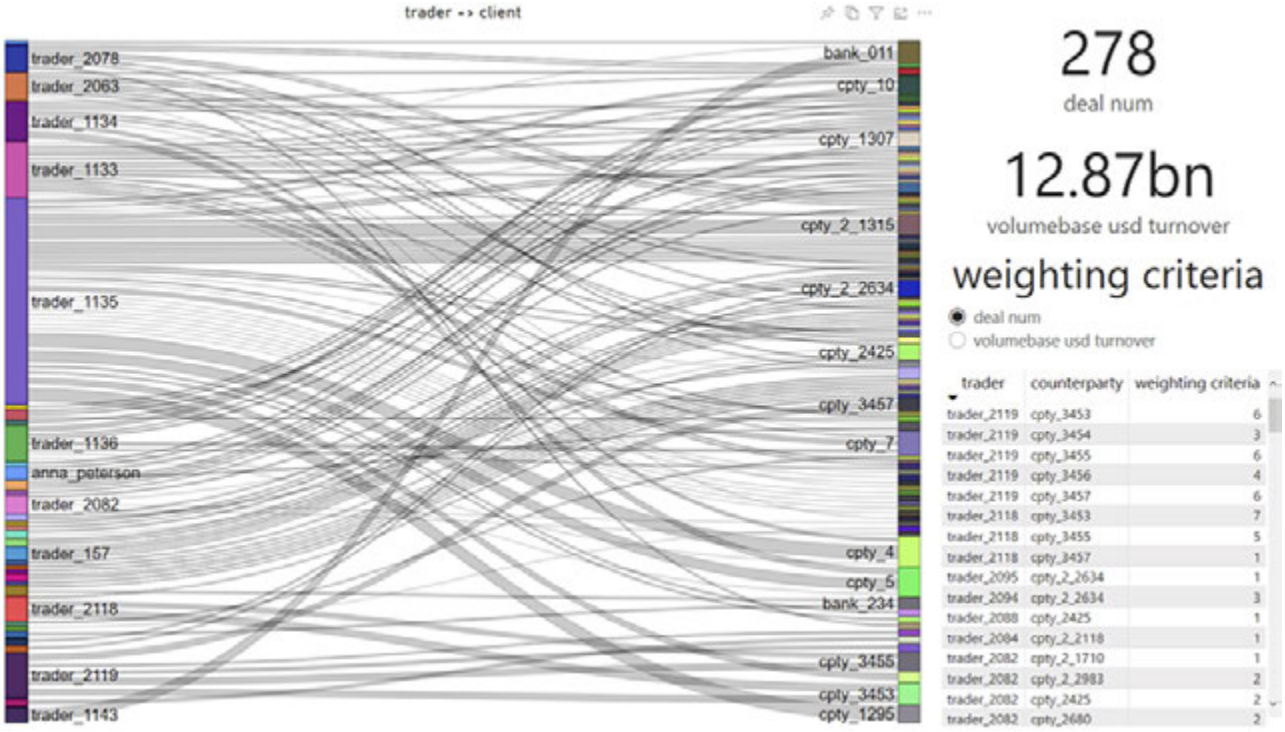
Да, в предыдущем интервью Вы ещё упоминали случай с Жеромом Кервелем из Societe Generale с убытком от его активности более чем на 7 млрд $, а также пример хищения российских трейдеров на 150 млн $ в банке «Открытие».

Поучается что один инцидент – это всегда серия сделок, которая может быть растянута по времени на несколько месяцев?

Вы абсолютно правы. Инцидент – это почти всегда серия сделок и заявок, которая растянута по времени и может быть выявлена только как цельный сценарий через реконструкцию мышления мошенника. В международной профессиональной литературе это называется «pattern recognition». Поэтому, при общении со службой безопасности того или иного профучастника в России или за рубежом нас не сразу понимают, когда мы говорим, что в большинстве ситуаций система выявляет то, что невозможно «перехватить на этапе нажатия кнопки». То есть подобную активность, конечно, можно выявить на ранней стадии и остановить. Но это не «перехват» отдельной транзакции, а выявление на ранней стадии серии сделок и заявок, которые распределены по времени и совокупно формируют подозрительный сценарий. Мы это называем «распознавание сценария», но не претендуем на корректность перевода.

Вы упомянули «мы наивно полагали, что самое главное, чтобы система умела находить «инцидент». В чём была наивность?

При разработке системы ТАФС наша команда старалась чётко фокусировать усилия на том, что называется её «ценность для пользователя» (в нашем контексте «added value»). Наивность заключалась в том, что несколько лет назад мы полагали, что вся ценность заключается в том, чтобы уметь не пропускать подлинные (не ложные) инциденты и эффективно отсеивать лож-



ные, чтобы приобретатель лицензии мог минимизировать ресурсы, выделяемые на анализ выявленных системой инцидентов.

Звучит логично. И что здесь не верно?

Здесь нет ошибки. Но оказалось, что этот функционал лишь минимально необходимый ингредиент в приготовлении блюда под названием «ценность» для пользователя. Необходимый ингредиент, но недостаточный.

Другие ингредиенты включают в себя в первую очередь способность системы автоматизированным образом формировать отчёты. Как оказалось, этот функционал имеет наиболее высокую ценность. Это должен быть не просто отчёт со списком номеров подозрительных сделок или заявок, совсем нет. Ценный для пользователя отчёт должен обладать несколькими критично важными качествами:

1) формироваться системой по заданному расписанию, в режиме близком к реальному времени;
2) удовлетворять требованиям регулятора;
3) может быть использован в качестве улики для суда.

А в чём сложность формировать отчёт, удовлетворяющий требованиям регулятора? Это же, скорее всего, какие-то всем известные формы для заполнения. Разве сложно автоматизировать их заполнение из данных о сделках и заявках, вошедших в инцидент?

Для того чтобы удовлетворить требования регулятора, необходимо своевременно отправлять ему отчёты по заранее известной форме. В Европе этот формат называется STOR («Suspicious Transaction and Order» template report to Regulator). В России это указание Банка России от 14.09.2020 г. № 5549-У «О требованиях к содержанию уведомлений, предусмотренных 224-ФЗ, а также о порядке и сроках представления в Банк России указанных уведомлений».

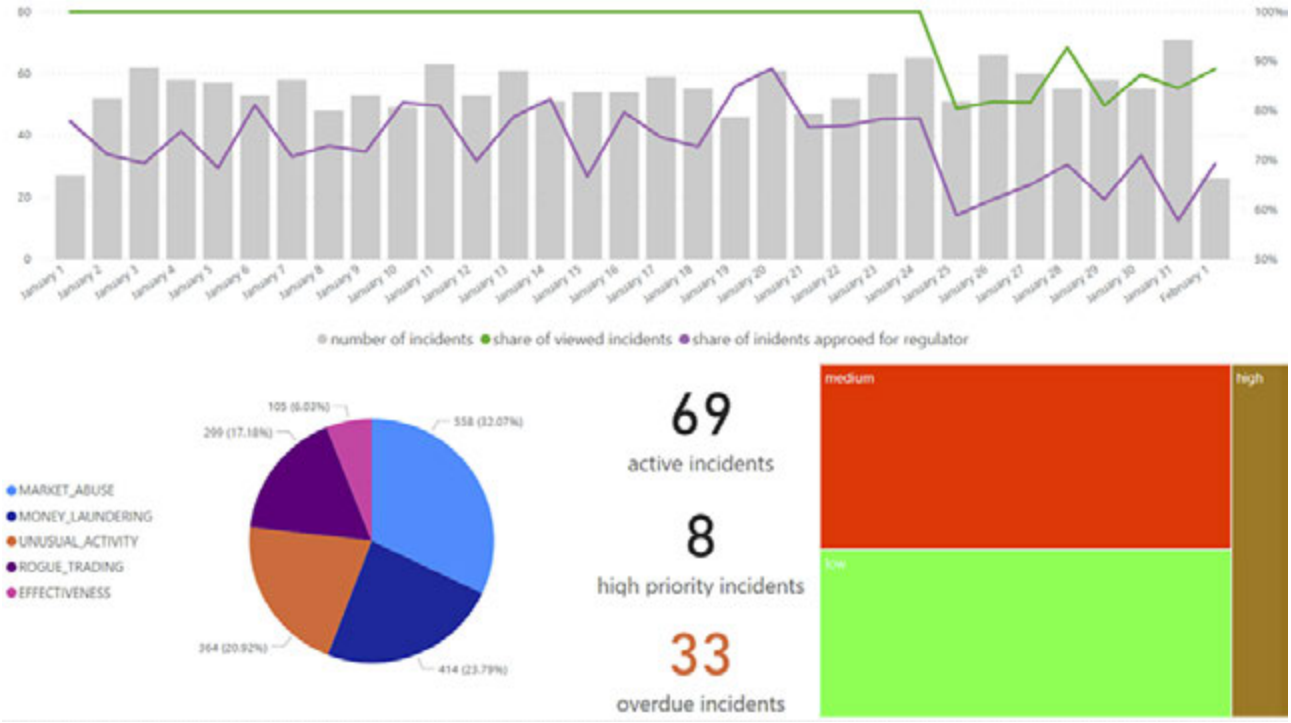
Основная сложность автоматизированного заполнения полей по форме STOR заключается в поле Reasons for the suspicion. В этом поле должно быть чётко и недвусмысленно изложены основания для подозрений.

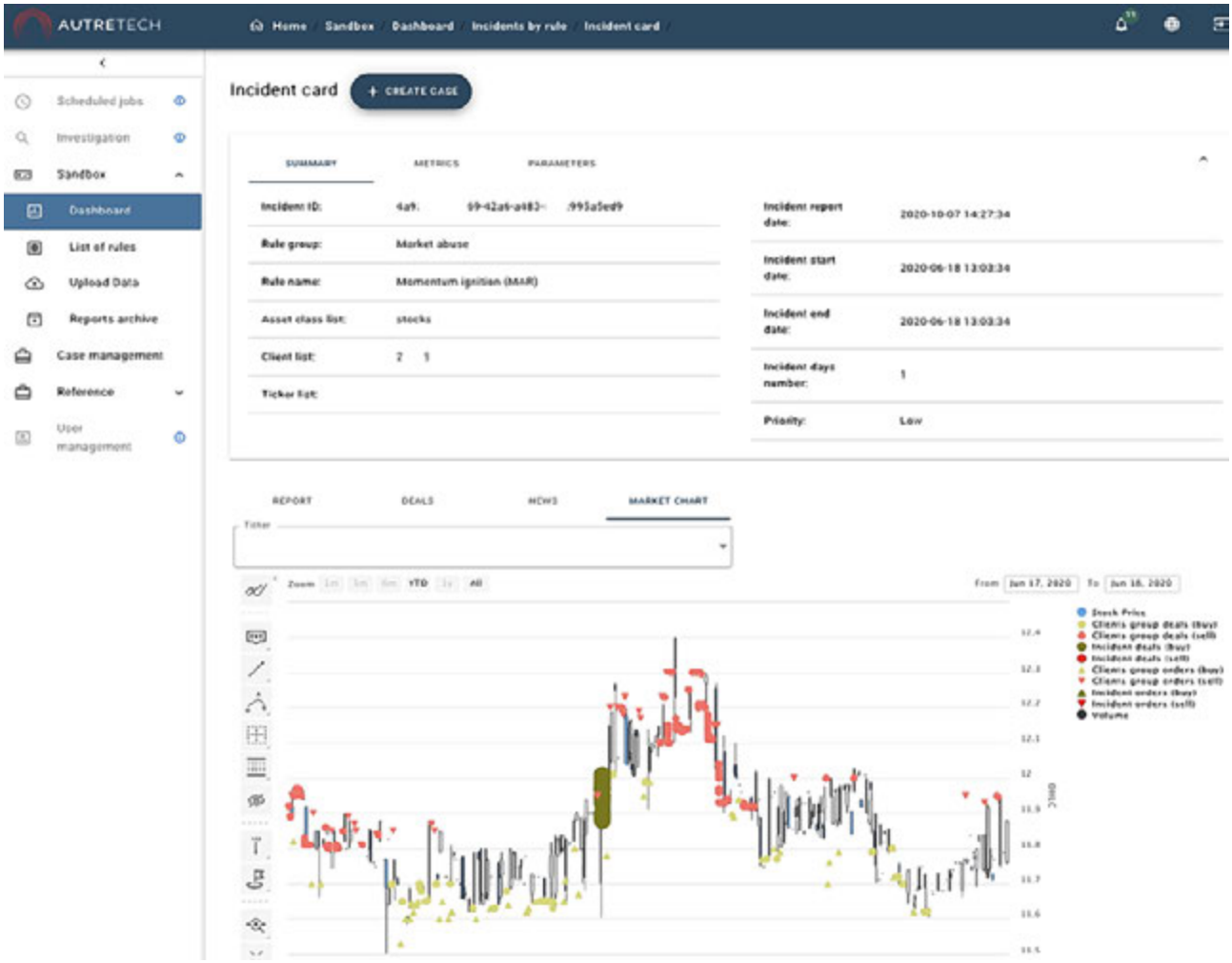
Аналогичное поле есть и в требованиях к отчёту российского регулятора: «Описание признаков неправомерного использования инсайдерской информации и (или) манипулирования рынком потенциально нестандартной операции» и «Вывод, сделанный участником организованных торгов по результатам проведённого им анализа каждой потенциально нестандартной операции».

Эти поля требуют аналитической обработки с участием специалиста, который хорошо ориентируется не только в том, как на практике работают трейдеры и клиенты и как они принимают свои решения о выставлении заявок. Такой специалист должен дополнительно иметь представление о многочисленных практических способах манипулирования и иного мошенничества на финансовых рынках. Он должен уметь реконструировать логику мошенника, уметь обрабатывать данные по сделкам и заявкам при помощи методов математической статистики и теории вероятности. Специалистов, которые имеют в своём арсенале полный набор таких компетенций на рынке, прямо скажем, не много.

Хорошо, допустим, подготовка отчёта для регулятора требует наличие специалиста с таким редким набором компетенций. Но ведь банк или брокер могут себе позволить найм таких сотрудников или воспитание собственных кадров из выпускников, например мехмата МГУ. В чём проблема?

Основная проблема заключается в том, что у крупного брокера может по формальным признакам формироваться несколько десятков и даже несколько сотен инцидентов ежедневно. Специалист с требуемым набором уникальных компетенций должен по каждому подозрительному инциденту скрупулёзно провести анализ «вручную» (с использованием современных систем бизнес-аналитики) и «вручную» изложить своё мнение в полях Reasons for the suspicion для MAR, в полях «описание признаков» и «вывод по результатам анализа».





Да, это действительно звучит как не простая задача даже для подготовленного специалиста. Что Вы можете посоветовать в такой ситуации?

Мы не берёмся давать совет. На наш взгляд, эта задача не может быть решена «вручную» через увеличение штата аналитиков с редким набором компетенций. Внутри нашей команды мы провели целую серию брейнстормингов, и в результате разработали собственную методику автоматизированного заполнения этих полей.

В самом деле? А это не будет выглядеть для Регулятора как формальная отписка, если он будет видеть типовое повторяющееся клише в поле «причина для подозрений», которое Ваша система заполняет автоматизированным образом?

Нет, мы научили систему готовить отчёты так, что повторений практически не будет, если речь не идёт о действительно полностью повторяющихся сценариях. Если говорить точнее, то в нашу систему встроен движок генерации многовариантных ответов, основанных именно на реконструкции логики мошенника. Ответы выстроены по понятной, хотя и многовариантной логике. Всё что остаётся сделать сотруднику Комплаенс – это проверить предложенную системой формулировку и выбрать из всего списка инцидентов те, которые, по его мнению, предназначены для отправки Регулятору, то есть не являются ложными срабатываниями.

К слову говоря, мы научили систему минимизировать число ложных срабатываний, но свести это число к нулю практически невозможно по многим причинам. Анализ этих причин в применении к финансовым рынкам – отдельная тема, которую мы с удовольствием можем обсудить позже.

По Вашим словам, Вы научили систему готовить логически понятные ответы. Но, Вы упомянули, что хороший отчёт должен не только удовлетворять требованиям Регулятора, но и может быть использован в качестве улики для суда. Этому Вы тоже сумели «научить» Вашу систему?

Вы задаёте очень актуальный вопрос. Пока у нас есть только многочисленные наработки по этой теме. И они ещё не объединены в единое стройное автоматизированное решение, имеющее в качестве основы математические теоремы или критерии, на которые можно опираться в суде. Такой критерий Колмогорова-Смирнова например, используется для проверки простых гипотез о принадлежности анализируемой выборки некоторому полностью известному закону распределения. Мы привлекаем для обсуждений этих вопросов специалистов из академических кругов. Но всё же полагаем, что это скорее относится к области «разработки завтрашнего дня». Формирование улик для суда на основе срабатываний алгоритмов в области финансовых рынков – суперинтересная задача. Над решением этой задачи сейчас трудимся не только мы, но и профильные команды специалистов во всём мире.

Геннадий Белов
Генеральный директор, ООО «Атретек»

www.tafs.pro

На что важно обратить внимание при получении КЭП в 2021 году

Предыстория

С целью оздоровления рынка электронной подписи несколько лет назад был принят пакет масштабных законодательных изменений (Закон № 476-ФЗ*), которые уже два года последовательно вступают в силу. Так, одна из главных норм указанного закона повысила требования к аккредитации удостоверяющих центров (УЦ), установив высокие финансовую и репутационную планки. Благодаря этому «раздутое» количество участников рынка сократится с более чем 400 компаний, выпускающих квалифицированные электронные подписи (КЭП), до нескольких организаций.

2021 год можно однозначно назвать активной фазой переходного периода: часть изменений уже вступила в силу, и рынок – в одном шаге от фундаментальной трансформации. Подробнее об этом можно прочитать в прошлых номерах журнала CIS или на Едином портале Электронной подписи в разделе «Статьи».

На что следует обращать внимание при получении электронной подписи, чтобы не остаться без этого цифрового инструмента?

С 1 июля 2021 года не все удостоверяющие центры смогут выдавать КЭП

Закон № 476-ФЗ повысил требования **к аккредитации** удостоверяющих центров. С 1 июля 2020 года попасть в эту категорию могут только компании, удовлетворяющие следующим **повышенным требованиям:**

- минимальный размер собственных средств (капитала) не менее 1 млрд рублей либо 500 млн рублей при наличии не менее чем в трёх четвёртых субъектов РФ одного или более филиала или представительства УЦ;
- наличие финансового обеспечения ответственности в сумме не менее чем 100 млн и 500 тысяч рублей за каждое место осуществления

* Федеральный закон от 27.12.2019 №476-ФЗ (ред. от 23.06.2020) «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля».

лицензируемого вида деятельности (всего на сумму не более 200 млн рублей);

- соответствие требованиям к деловой репутации руководителя и учредителей (участников) УЦ;
- в отношении УЦ, претендующего на получение аккредитации, не была досрочно прекращена его аккредитация в течение трёх лет до подачи заявления (аналогично – в отношении единоличного исполнительного органа УЦ-претендента на аккредитацию).

По истечении года с момента ввода процедуры аккредитации в соответствии с новыми правилами или, другими словами, **с 1 июля 2021 года выдавать КЭП смогут только те удостоверяющие центры, которые соответствуют указанным требованиям.**

В каких УЦ можно получать электронные подписи в 2021 году

На официальном портале Минкомсвязи России **в разделе «Список аккредитованных удостоверяющих центров»** представлен перечень действующих УЦ. Отличить компании, соответствующие повышенным требованиям, можно по дате приказа об аккредитации (начиная с 1 июля 2020 года и далее).

С начала 2022 года произойдёт массовое прекращение действия квалифицированных сертификатов

Часть 4 статьи 3 Закона № 476-ФЗ регламентирует с 1 января 2022 года **прекращение действия квалифицированных электронных подписей,** выпущенных УЦ, которые **не смогли пройти аккредитацию в соответствии с повышенными требованиями.** Таким образом, если до 1 июля 2021 года получать КЭП в удостоверяющих центрах, у которых отсутствует аккредитация по новым правилам, то срок действия выданных ими подписей будет менее 1 года – до начала 2022-го.

Важно: Недобросовестные УЦ могут продавать КЭП за полную стоимость, не информируя об ограниченности срока её действия. В связи с этим пользователям следует сохранять бдительность.

Резюме

Перед получением в 2021 году квалифицированной электронной подписи – аналога собственноручной подписи, проверяйте у удостоверяющего центра **наличие аккредитации по новым правилам.**

УЦ как новый бизнес-партнёр

Удостоверяющий центр «Основание» (АО «Аналитический Центр») **подтвердил финансовую устойчивость и тождественность современным запросам регуляторов и рынка:** УЦ аккредитован в соответствии с повышенными требованиями (Приказ Минкомсвязи России № 668 от 4 декабря 2020 года).

Удостоверяющий центр «Основание» – сплав опыта и активов компаний, каждая из которых внесла свой вклад в формирование УЦ нового поколения.

АО «Аналитический Центр» – компания, сотрудники которой имеют более чем 20-летний опыт работы на рынке электронной подписи. До вступления в силу законодательных изменений организация выступала центром авторизации удостоверяющих центров при Ассоциации Электронных Торговых Площадок, формировавшей в стране единое интерактивное пространство в сфере электронных торгов.

Компания «РТ-Проектные Технологии» госкорпорации Ростех – один из ключевых игроков по внедрению в России новых цифровых сервисов в рамках нацпроекта «Цифровая экономика».

Группа компаний «Селдон» – разработчик ИТ-решений в сфере электронных торгов и создания информационных систем. Обладает широким спектром компетенций в сфере работы с данными, а также новейшими технологиями искусственного интеллекта собственной разработки.

Московский кредитный банк (МКБ) – универсальный коммерческий частный банк, предоставляющий весь спектр банковских услуг для корпоративных и частных клиентов, а также для финансово-кредитных организаций. МКБ входит в список системно значимых банков, утверждённый ЦБ РФ.

Обращаясь в удостоверяющий центр «Основание», клиент получает не просто сертификат электронной подписи, но и нового делового партнёра. Для удобства заявителей УЦ формирует широкую филиальную сеть федерального масштаба из надёжных участников рынка. Воспользовавшись любым из представленных ниже способов связи, можно подробнее узнать о возможностях партнёрства.

Основание
Удостоверяющий центр

uc-osnovanie.ru
info@uc-osnovanie.ru
8 800 1001 500

Гороскоп для ИТ-компаний на весну 2021 года

Зная, под каким знаком зодиака была основана ваша компания, и руководствуясь нашим гороскопом, вы будете в курсе того, что её ожидает и к чему надо готовиться для роста и развития вашей компании.

Овен (21 марта – 20 апреля)

Компании-Овны должны проявить предприимчивость. Нужно показать партнёрам и конкурентам, чего вы стоите. Возможно, неуверенность заслоняла успех, но пора отбросить стереотипы и начать работать по-новому. Компания сразу же обзаведётся верными наставниками и партнёрами. Контролирующие органы станут более лояльными. Не бойтесь выйти из зоны комфорта.

Индивидуальные предприниматели должны быть особенно осторожны в делах. Сейчас есть риск потерять много денег или ввязаться в неприятную историю с органами власти. Вас могут подставить близкие партнёры. Чтобы не допустить подобных казусов, нужно заранее проработать бизнес-план и не быть чересчур доверчивым. Прислушивайтесь к советам, но двигайтесь по намеченному пути.

Телец (21 апреля – 21 мая)

Компании-Тельцы смогут улучшить репутацию на рынке. Вы с лёгкостью справитесь даже с тяжёлыми заказами и преодолеете все барьеры, которые устроили конкуренты. Возможно, к вам обратятся за серьёзной помощью – это будет шансом на успех в будущем. Сейчас важно наладить контакт со всеми важными компаньонами и клиентами, показать свои преимущества. Деятельность компании будет высоко оценена, возможна достойная прибыль.

В финансовой сфере возможны потери. Это могут быть проигрыши в аукционах, потеря клиентов или некачественные услуги партнёров. Пусть это вас не расстраивает, такой период встречается у всех. Сейчас нужно постараться быть максимально осторожными, не разбрасываться финансами и не совершать крупных сделок. Лучше все финансовые вопросы отложить до мая. Если есть возможность, сохраните часть прибыли на свежие летние проекты.

Близнецы (22 мая – 21 июня)

Организации-Близнецы помешаны на своём деле, они во всём видят азарт и деньги. Это, конечно, неплохо, но можете столкнуться с проблемами в смежных сферах деятельности, если будете зацикливаться на чём-то одном. Распределите бизнес-задачи между структурными подразделениями или привлеките партнёров к решению того или иного вопроса, и тогда у компании появится свободное время для новых проектов.

Не стоит зацикливаться на росте. Он и так вас ждёт в ближайшем будущем, а своим напором вы можете испортить отношения с выгодными партнёрами и клиентами и подвести репутацию компании. Сейчас нужно расслабиться и позволить делам разрешаться самим. Если есть возможность, то лучше уйти в решение спокойных приятных вопросов.

Берегите финансы. Вы рискуете совершить необдуманные сделки, которые не представляют особой выгоды. Лучше доверьтесь проверенным способам прибыли или примите решение коллегиально.

Рак (22 июня – 22 июля)

Компании-Раки привыкли плыть по течению, и в апреле не собираются отклоняться от курса. Вы будете выполнять обычный план, и делать это хорошо. Только вам не интересна материальная сторона вопроса. Вам нравится получать удовольствие от процесса и воплощения в жизнь собственных проектов. Особенно хорош этот период для изобретений и исследований, которые приблизят компанию к давним проектам – мечтам.

Возможно, компания разбавит старый коллектив новыми полезными сотрудниками. При перестановке кадров важно правильно настроить персонал к таким переменам. Холодная голова руководителя позволит принимать взвешенные решения. Только не стоит брать в компанию знакомых или родственников, если не хотите испортить дело.

Лев (23 июля – 22 августа)

Компании-Львы способны на большее, чем обычно. Вам легко даются сложные цели, трудные переговоры и затяжные проекты. Не нужно показывать своё превосходство и хвастать. Клиенты и так видят ваши преимущества, а хвастовство примут за наглость. Вам сейчас не нужны стычки и конфликты, обходите стороной тех, кто недружелюбен, сейчас вам с большой вероятностью устроят козни и будут выживать с рынка.

Нелегко придётся маленьким предприятиям. Вы рискуете столкнуться с жестокими конкурентами, которые будут добиваться превосходства любыми путями, выживая вас. Это значительно ударит по бюджету компании, придётся сократить штат и искать способы экономии. Гибкость и хитрость поможет быть всегда на шаг впереди.

Дева (23 августа – 22 сентября)

Компании-Девы смогут реализовать много творческих проектов. У вас прекрасный потенциал и ресурсы. Самое время начинать что-то новое, пробовать, экспериментировать и не бояться получать удовольствие от нового процесса. Кого-то очень заинтересуют новые проекты, будет много предложений о сотрудничестве.

Сотрудники, которые привыкли к рутине, будут справляться с задачами лучше, чем обычно. Конечно, будут раздражать недоделанные проекты, потому что компания стремится к порядку. Кто-то из партнёров будет подводить. Но сейчас можно показать весь свой потенциал и стать на уровень выше.

Пусть не огорчают финансовые потери, которые ждут в апреле. Компания не будет остро нуждаться в прибыли, но и сэкономить не получится. То и дело будут возникать новые неожиданные траты. В конце месяца ждёт прибыль, но и она будет меньше, чем ожидалось.

Весы (23 сентября – 22 октября)

Весов ожидает сложный период. Придётся вкладывать много сил, осваивать новые технологии, методы. Но такой период придаст стимул и поможет больше заработать на давние планы. Радуйтесь такому шансу получить прибыль, ведь впереди спокойная пора, и вам очень понадобятся средства.

Следует проявить бдительность тем компаниям, которые работают с финансами и ценными бумагами. Велика вероятность потерь, особенно во второй половине месяца. Всегда перепроверяйте выполненные задачи и контролируйте результат. При подписании важных договоров принимайте коллегиальной решение с мудрыми партнёрами. Наивность и доверчивость может помешать.

Скорпион (23 октября – 22 ноября)

Организации-Скорпионы могут быть удручены неудачами. Такие трудности временны и даны для переосмысления планов на будущее. Готовьтесь к проверкам на прочность, к сложным заказам. Вы не должны сломаться, покажите всё, на что способна компания, ведь есть перспектива занять лидирующую позицию в вашей области, а вместе с ней наступит и финансовое благополучие.

Менее доходные компании должны попробовать себя в новой сфере. Звёзды говорят о том, что перед вами открыто много дорог, которые приведут к успеху. Например, сейчас самое время учиться чему-то новому, развивать дополнительные услуги, менять стиль работы.

Стрелец (23 ноября – 21 декабря)

Компании-Стрельцы готовы к бою, однако на рынке затишье. Сейчас лучше уйти в подполье и полноценно набраться новых сил. Вскоре появится шанс, чтобы доказать своё превосходство и претендовать на лидерство. Берегитесь коварных и завистливых конкурентов. Вероятно, вокруг бродят слухи, которые портят репутацию компании.

Будьте готовы к финансовым потерям. Скорее всего, придётся потратиться, в итоге компания может остаться ни с чем, зато поможете партнёрам. Также не совершайте крупных сделок. Есть вероятность небольших выигрышей в сделках. Испытывайте судьбу после 20 апреля, тогда удача будет максимально на стороне компании.

Козерог (22 декабря – 20 января)

Предприятия-Козероги находятся на взлётной полосе и готовы лететь навстречу к новым высотам. Партнёры выделят ваши услуги и предложат выгодные условия сотрудничества. Звёзды гордятся вашей настойчивостью и трудолюбием, вы действительно заслужили высокий статус. Не теряйте уверенности.

Компания сможет найти новые способы дохода. Возможно, именно сейчас пришло время для её расширения. Для того чтобы всё складывалось в пользу компании, нужно не скупиться и нанять грамотных сотрудников.

Финансовые проблемы будут возникать время от времени. И если всё же придётся брать какие-то обязательства, то вы эффективно с ними справитесь. Скорее всего, у компании не будет больших долгов или затяжных кредитов. Умение экономить поможет держать материальный баланс.

Водолей (21 января – 19 февраля)

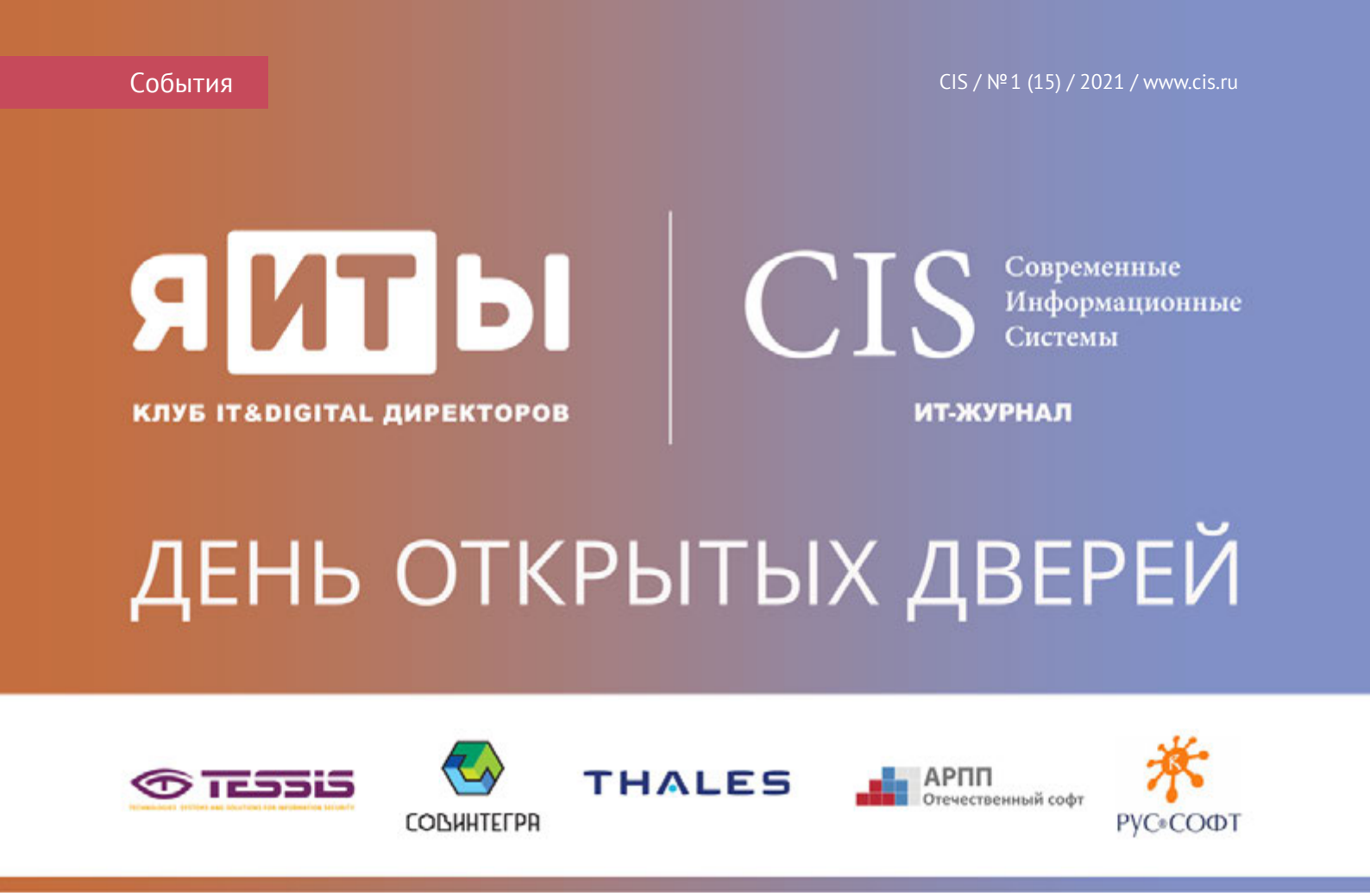
Финансы компаний-Водолеев в критическом состоянии. Не стоит обвинять других в своём безденежье, лучше направить энергию на развитие бизнеса. У компании есть направление, которое в перспективе принесёт неплохой доход. Задумайтесь, может не откладывать на потом то, что можно начать сегодня.

Лучше составить чёткий бизнес-план и придерживаться его. В принципе, любые проекты будут даваться легко, но безучастие партнёров или клиентов будет напрягать. Это не должно огорчать, а стимулировать к ещё более стремительным целям.

Рыбы (20 февраля – 20 марта)

Творческие компании-Рыбы перенесут кризис. Будет не хватать вдохновения и пространства. И то, и другое можно получить, сменив офис. Состояние стабилизируется к концу месяца. Именно тогда компания сможет показать новые разработки и получить за свои проекты неплохую прибыль.

В бизнесе будут активно вестись дела и переговоры. Любые сделки будут удачными, если заключать их не на «скорую руку». Тщательно просматривайте бумаги, которые подписываете и не доверяйте финансовые операции ненадёжным сотрудникам. В апреле придётся пересмотреть штат подчинённых и сделать несколько перестановок. После этого дела пойдут в гору.



ИТ-журнал CIS «Современные Инфосистемы» и клуб ИТ-директоров «я-ИТ-ы» 18 февраля 2021 года провели День открытых дверей.

Основной целью мероприятия было в неформальной обстановке продемонстрировать возможности совместного сотрудничества и рассказать о планах на будущее. Гостей пригласили на одну из лучших площадок Москва-сити. Среди присутствующих были представители крупных компаний, мировых лидеров индустрии – Кузнецов Сергей из компании Thales, а также Макаров Иван из TESSIS.

Выступления представителей журнала CIS и клуба «я-ИТ-ы»

ИТ-журнал CIS «Современные Инфосистемы» представляла маркетолог Валерия Рябинина. Основные положения её выступления:

- Журнал поддерживает масштабные ИТ-конференции в России.
- Издание открыто для предложений и различных проектов от своих клиентов и партнёров.
- В планах журнала организация очередного ИТ-конкурса красоты, где ИТ-красавица, занявшая первое место, станет не только обладательницей ИТ-короны, но и символом информационной безопасности России.
- Создание Учебного Центра CIS и образовательных программ в ИТ-сфере.
- Работа в области производства обучающих видео, мастер-классов, видеоотчётов, видеоконференций и т.д.
- Команда журнала CIS будет организовывать и проводить ИТ-мероприятия, целью которых станет обсуждение насущных вопросов настоящего и будущего информационных технологий, информационной безопасности и смежных с ней сфер.

Валерия Рябинина подчеркнула, что журнал CIS тесно сотрудничает с фондом Константина Хабенского – CISummIT Digital Hearts, помогая в сборе средств для помощи детям с заболеваниями головного мозга.

Клуб «я-ИТ-ы» представлял Павел Клепинин. Он рассказал о довольно нескромных амбициях своего общества, о формах сотрудничества с журналом CIS и о конкретных планах на 2021 год.

Интеллектуально-развлекательная часть мероприятия

Для создания тёплой и дружеской атмосферы гостям было предложено поучаствовать в интеллектуально-развлекательной игре «Квиз».

Играющие разделились на команды и смогли проявить свои находчивость, эрудицию, логику, сообразительность и нестандартное мышление. Формально первенство одержала команда «Молодые Креативные», но фактически победила дружба. Во время соревнования гости знакомились друг с другом, вели непринуждённую беседу, а иногда и просто встречали своих старых знакомых. Игра «Квиз» подвела собравшихся к более серьёзной части мероприятия.

Был фуршет, неформальная дружеская обстановка и много всего интересного. Посмотреть, как проходил этот вечер, можно на страницах журнала в разделе «Фотоотчёт».

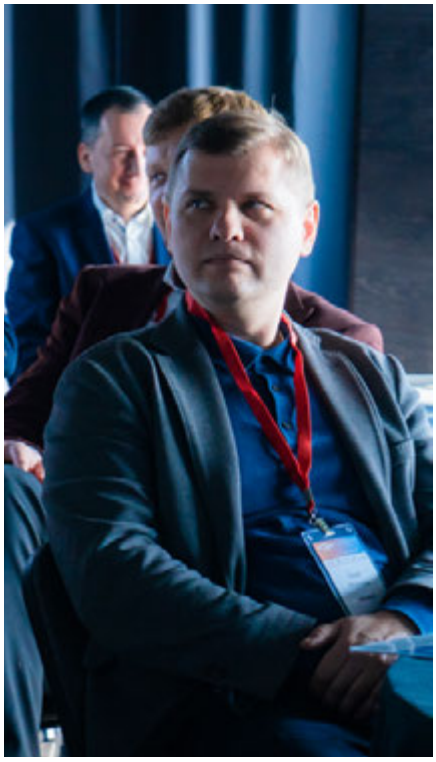
CIS Современные Информационные Системы

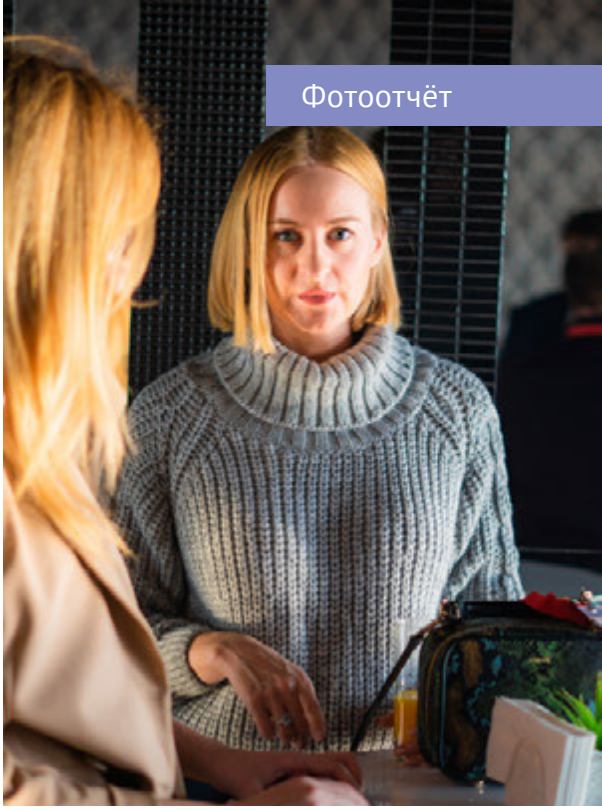
ИТ-журнал CIS (Современные Инфосистемы)

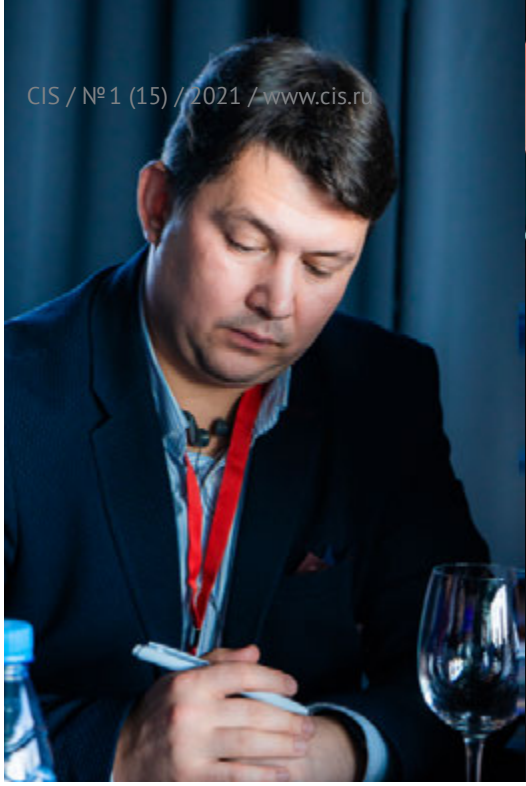
www.cis.ru


CIS


CIS








CIS


2 МЕСТО
ЯИТЫ


1 МЕСТО

CIS / № 1 (15) / 2021 / www.cis.ru

Выставка «Постспекулятивный дизайн. Деколонизация будущего»

Алина Золотых. Second Skin You Are In

Noate Atkociunas.
Gasp

Юлия Вергазова.
Flora.Onion 2.0

Changkun Lin.
Hungerism

Анастасия
Алехина.
The Criticism
Of Violence

Nonhuman Nonsense.
Pink Chicken Project

5 февраля в галерее «Электромузей в Ростокино» Объединения «Выставочные залы Москвы» открылась выставка «Постспекулятивный дизайн. Деколонизация будущего», рассматривающая дизайн и его инструментарий как попытку выхода из существующей политической и экономической системы.

Спекулятивный, иначе критический, дизайн как дискурсивная практика был описан сравнительно недавно и быстро вошёл в инструментарий современных художников и концептуальных дизайнеров. Спекулятивный дизайн предложил пространство, радикально отличающееся от преобладающей парадигмы дизайна модернистского, утилитарного, ставящего своей задачей решение «Проблемы». Спекулятивный дизайн, конструируя вымышленный нарратив, фокусируется на создании идеи, способной проникнуть в культурную среду и инициировать дискуссию о будущем, задавая тем самым его вектор.

Отсутствие необходимости создавать функциональный артефакт, который удовлетворил бы спрос пользователя, освобождает дизайнеров и художников от экономических ограничений коммерческой практики, присущих утилитарному дизайну. Однако в такой свободе от открытого рынка кроется одна из главных проблем спекулятивного дизайна, который становится инкубатором для венчурных инвестиций в идеи и потенциальные технологические разработки, предложенные художниками и дизайнерами. Задавая вектор развития и получая необходимый приток капитала, спекулятивный дизайн становится важным звеном в процессе колонизации будущего.

Вводя понятие постспекулятивного дизайна, гиперонима по отношению к ксенодизайну, нон-хьюман дизайну, дизайну антиутопий и др., куратор выставки и художники делают попытку артикулировать вышеописанную ситуацию и найти другой подход к использованию инструментов дизайна для того, чтобы деколонизировать наши представления о будущем. Работы, представленные на выставке, сохраняют формальные признаки спекулятивного дизайна, но в каждой из них кроется концептуальная и визуальная странность, обеспечивающая дистанцию по отношению к спекулятивному дизайну и делающая эти работы чем-то принципиально другим, создавая совершенно новые типологии взаимодействий.

Департамент культуры города Москвы

ВЫСТАВОЧНЫЕ ЗАЛЫ МОСКВЫ
ОБЪЕДИНЕНИЕ
ЭЛЕКТРО МУЗЕЙ

Участники выставки: *Анастасия Королёва, Юлия Вергазова, Nonhuman Nonsense, Changkun Lin, Аристарх Чернышёв, Noatė Atkočiūnas, Алина Золотых, Анастасия Алехина, Thomas Thwaites*

Куратор выставки: *Алиса Смородина*

«Постспекулятивный дизайн и деколонизация будущего»*, 6+*

Даты проведения: *5 февраля – 28 марта, 2021*

Вернисаж: *4 февраля в 19:00, вход свободный по сеансам.*

Место проведения:
«Электромузей в Ростокино»
(Ростокинская ул., 1, м. ВДНХ, МЦК «Ростокино»)

Тел: 8 (499) 187-10-45
electromuseum@vzmoscow.ru
www.vzmoscow.ru
www.facebook.com/electromuseum
vk.com/electromuseum
electromuseum.ru

CIS / № 1 (15) / 2021 / www.cis.ru

ИБЭШНИКИ: ПОХИЩЕНИЕ

ИТАК, ГОСПОДА, У НАС ЧРЕЗВЫЧАЙНОЕ ПРОИСШЕСТВИЕ! У НАШЕГО СОТРУДНИКА, ГОСПОДИНА МАННА ПОХИЩЕНЫ СЕГОДНЯ НОЧЬЮ ЖЕНА И ДОЧЬ. КАК ВЫ ЗНАЕТЕ, МАНН СЕЙЧАС В КОМАНДИРОВКЕ, Я УЖЕ ВЫЗВАЛ ЕГО. СЕЙЧАС ОН УЖЕ ДОЛЖЕН ПРИЗЕМЛИТЬСЯ В АЭРОПОРТУ, ОТКУДА ЕГО ДОСТАВЯТ К НАМ ВЕРТОЛЕТОМ. ФАКТИЧЕСКИ ЭТО ВЫЗОВ ВСЕМ НАМ!

ДА. ТРЕБОВАНИЕ - ОСВОБОДИТЬ РУКОВОДИТЕЛЯ ТЕРРОРИСТИЧЕСКОЙ ЯЧЕЙКИ. ДА, ОНИ ПРИСЛАЛИ ВИДЕО, НА КОТОРОМ ПОКАЗАНО, ЧТО ЖЕНУ И РЕБЕНКА СОДЕРЖАТ ГДЕ-ТО ЗА ГОРОДОМ. ВИДЕО, СУДЯ ПО ВСЕМУ, СНЯТО НА СМАРТФОН. НЕДАЛЕКО, СКОРЕЕ ВСЕГО, РАСПОЛОЖЕНА АВТОТРАССА, СЛЫШЕН ГУЛ АВТОМОБИЛЕЙ. БОЛЬШЕ НИЧЕГО МЫ СКАЗАТЬ НЕ МОЖЕМ.

Сегодня координаты в фотографии и видео добавляют все устройства, которые имеют в своём составе датчики GPS. Так что, если вы заботитесь о конфиденциальности, найдите программное обеспечение, которое позволит вам удалить эти координаты. *Автор: Владимир Безмалый*

Календарь мероприятий

12 - 13 марта

Санкт-Петербург • Курс

IT продукт. Продвижение и продажа ИТ продуктов, ИТ решений, ИТ сервисов, информационных систем, прикладных программ

12 марта

Москва • Онлайн-трансляция • Соревнование

CDO Award 2021

13 марта

Онлайн-трансляция • Мастер-класс

Workshop Day 2021

13 марта

Минск • Конференция

START-IT 2021

15 марта - 10 мая

Онлайн-трансляция • Вебинар

Школа DevOps приглашает на обновленный курс «DevOps Инженер 2021»

25 марта

Москва • Онлайн-трансляция • Форум

BIG DATA 2021

25 марта

Онлайн-трансляция • Вебинар

Управление результативностью сотрудников в новых условиях. Автоматизация OKR и KPI-Управления

6 - 9 апреля

Онлайн-трансляция • Конференция

Heisenbug 2021 Piter: техническая конференция для тестировщиков и не только

8 апреля

Онлайн-трансляция • Вебинар

Корпоративный университет онлайн. Реализация «Управления талантами» на 1С

8 апреля

Москва • Онлайн-трансляция • Конференция

VII ЕЖЕГОДНАЯ КОНФЕРЕНЦИЯ ПО НАГРУЗОЧНОМУ ТЕСТИРОВАНИЮ

13 - 16 апреля

Онлайн-трансляция • Конференция

Mobius 2021 Piter: Конференция по мобильной разработке

13 - 16 апреля

Онлайн-трансляция • Конференция

JPoint 2021: международная конференция для опытных Java-разработчиков

20 - 23 апреля

Онлайн-трансляция • Конференция

DotNext 2021 Piter: конференция для .NET-разработчиков

20 - 23 апреля

Онлайн-трансляция • Конференция

HolyJS 2021 Piter: Конференция для JavaScript-разработчиков

27 апреля

Москва • Конференция

Russian Gaming Week 2021

11 - 13 мая

Москва • Онлайн-трансляция • Конференция

DevOps Pro Moscow 2021 Hybrid Edition

18 мая

Онлайн-трансляция • Вебинар

Управление подбором и адаптацией в новой CRM-системе на базе 1С:Предприятие

8 - 10 июня

Москва • Онлайн-трансляция • Конференция

DevDays Moscow 2021 HYBRID EDITION

24 июня

Онлайн-трансляция • Вебинар

«Корпоративный университет онлайн. Реализация «Управления талантами» на 1С

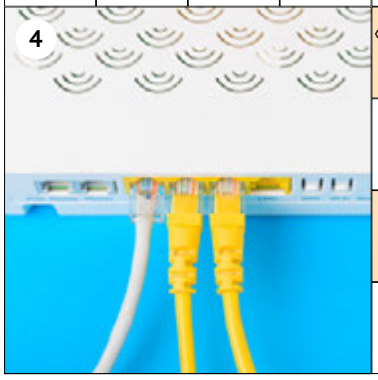
9 июля

Санкт-Петербург • Конференция

PG Day Russia 2021

Сканворд

Пришлите разгаданный сканворд на почту info@sovinfosystems.ru
и получите приз от редакции журнала «CIS».



1. Акустический усилитель
2. Противотанковая траншея
3. Красный командир из анекдотов
4. Компьютерная жертва Касперского
5. Мужское имя (благочестивый)
6. «Важнейшее из искусств»
7. Бог, который всегда навеселе
8. Столица Судана
9. Определяется по штемпелю письма
10. Право на въезд в страну
11. Сумчатый яйцекладущий «ёж»
12. Жираф из «Красной книги»
13. Имя путешественника Хейердала
14. Республика близ Суринама
15. Кормовая культура, медонос
16. Диван без спинки
17. Написал о трёх толстяках
18. Бахчевой сахарный гигант
19. Открывают от изумления
20. Английский «гектар»
21. Деревянная кадка, кадушка для теста
22. Шпионка ... Хари
23. Случай, достойный хохота
24. Кинорежиссёр-сказочник
25. Абориген Белграда
26. Коловорот для зимней рыбалки
27. Методичное «метание» пулями
28. Райская любительница яблок
29. Автор романа «Богач и бедняк»
30. Годовая смета страны
31. Выкуп за невесту на Руси
32. Волосок на колоске
33. Крупный пёстрый попугай
34. «Орлиная» сторона монеты
35. «Укороченный» автомобиль
36. Компьютерный шифр
37. Слово, на которое не найти суда

Thales CipherTrust Data Security Platform

Thales CipherTrust Data Security Platform объединяет функции обнаружения, классификации и защиты данных с инструментами детального контроля доступа и централизованного управлением ключами. Она упрощает управление защитой данных, помогает быстрее адаптироваться к нормативным требованиям и обеспечивает безопасность миграции в облако. Это позволяет обеспечить защиту данных меньшими ресурсами, полностью контролировать соблюдение нормативных требований и существенно снизить риски для бизнеса.

Основанная в 2007 году компания **TESSIS** (ЗАО «СИС») — специализированный дистрибьютор решений для информационной безопасности. Компания занимается их импортом, производством, сертификацией, продажей, интеграцией и технической поддержкой в России.

TESSIS — авторизованный дистрибьютор компании **Thales** и центр компетенции по ее решениям для управления доступом и защиты данных, включая средства для усиленной аутентификации, ЭЦП, шифрования данных и управления ключами шифрования, а также шифраторы для сетей Ethernet.

Thales Accelerate Partner Network
DISTRIBUTOR

+7 (495) 228-02-08
info@tessis.ru
tessis.ru