CIS
Современные Информационные Системы
№ 3 (13) / 2020

Всегда приятно вернуться

Стр. 37

Юлия Жукова
USTA Management
«я-ИТ-ы»

Актуальное положение дел в ИТ-отрасли в момент экономического спада

Стр. 38

Сергей Груданов
TESSIS

ЭКСТРЕННАЯ ЦИФРОВИЗАЦИЯ

Какие подходы помогли компаниям во время пандемии

Стр. 46

Александр Старыгин
Hewlett Packard Enterprise

АУТЕНТИФИКАЦИЯ: прошлое, настоящее, будущее

Стр. 84

Владимир Безмалый
Kaspersky Certified Trainer

ПРЕДИСЛОВИЕ

РЕШЕНИЯ

ОПЫТ

ПРОДУКТЫ

МИСС CIS

ТЕХНОЛОГИИ

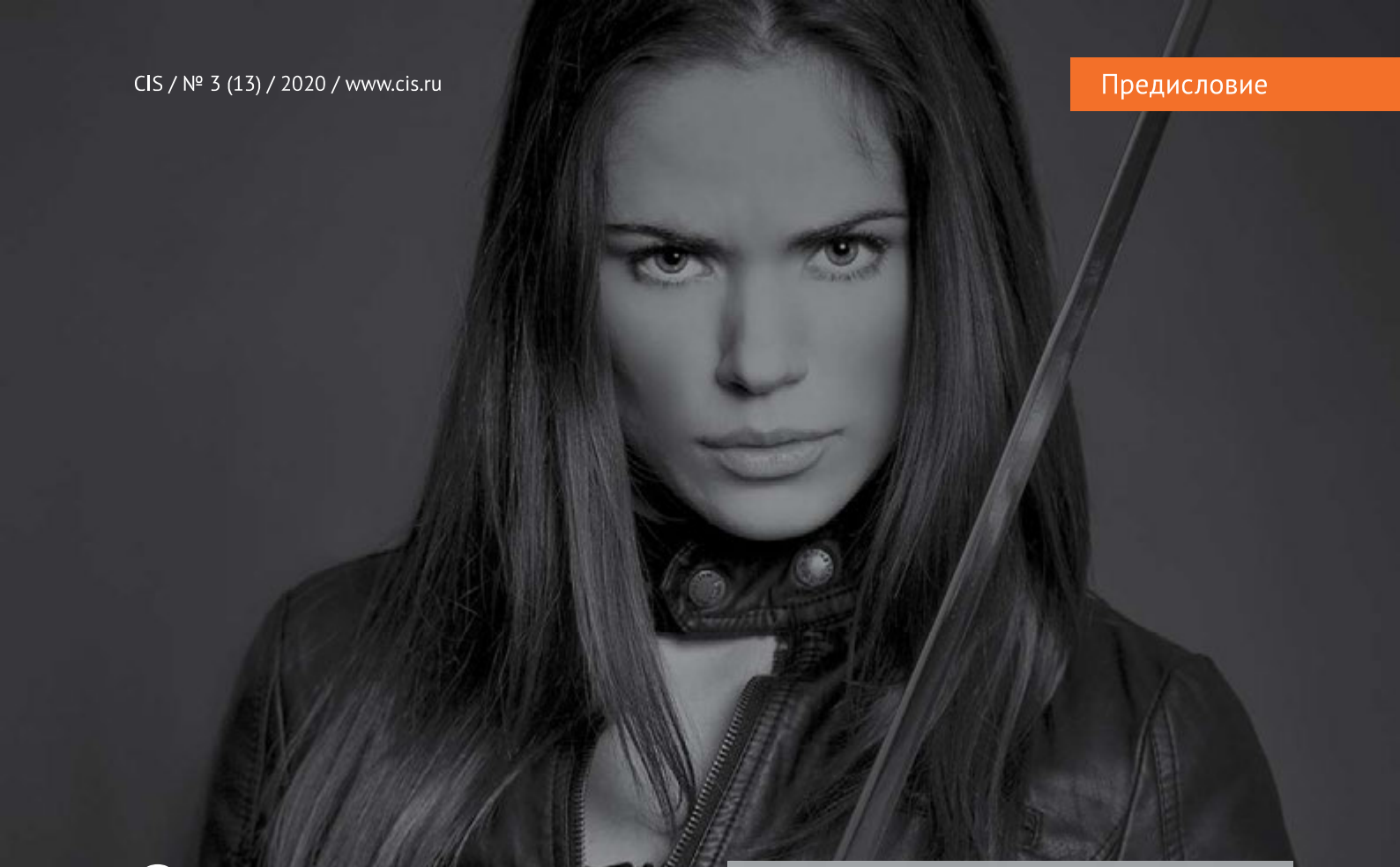
КУЛЬТУРА

АНАЛИТИКА

КРОССВОРД

КОМИКСЫ

КАЛЕНДАРЬ



От редактора

Дорогие читатели!

Эпидемия атипичной пневмонии, вызванная коронавирусом COVID-19, всколыхнула весь мир и оказала серьёзное влияние на ИТ-отрасль. Сегодня много компаний переживает сложный период: переход на удалённую работу, отказ инвесторов, потеря действующих клиентов, отсутствие финансирования, экономический кризис. Кажется, перспектив нет. Но это не так!

ИТ-индустрия – одна из немногих сфер, в которой грамотные действия в момент кризиса привели к росту бизнеса и отложенному выигрышу в перспективе.

В новом номере мы обсудим актуальное положение дел в ИТ-отрасли в момент экономического спада: что уже удалось достичь, над чем ещё предстоит работать и чего ожидать в скором будущем от последствий пандемии. Освещение этих важных тем мы доверили лидерам ИТ-отрасли: Елене Нагорной, Сергею Груданову, Владимиру Безмалому, Александру Старыгину.

На осень 2020 года наш журнал запланировал проведение конкурса красоты Beauty & DigITal. На страницах номера вы сможете ознакомиться со статьями участниц о компаниях, в которых они работают.

Но Beauty & DigITal не единственное мероприятие, намеченное на осень. 15 октября в Москве пройдёт благотворительная ИТ-конференция, организованная нашим журналом. Мы с радостью приглашаем вас принять в ней участие, предварительно зарегистрировавшись на сайте www.cisevent.ru.

С уважением,
редакция журнала CIS.

Главный редактор: Станислав Понарин.

Фотограф, руководитель интернет-маркетинга: 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: Юлия Жукова.

Тираж 5000 экз. (отпечатанный тираж).

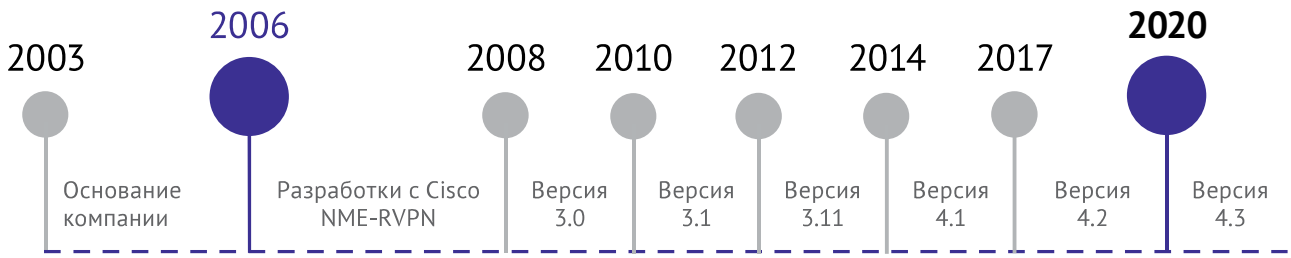
Журнал предназначен для лиц старше 16 лет.

Решения C-TERRA

Новинки 2020 года для защиты корпоративной сети

Мы разрабатываем и производим сертифицированные средства защиты информации. Основной профиль – криптографическая защита информации.

С-Терра СиЭсПи



От основания и идеи к актуальной версии 4.3

Партнёрство

Рос Интеграция

ГРУППА КОМПАНИЙ «РОСИНТЕГРАЦИЯ»

- инновационный мультивендорныйсистемный интегратор
- с 2012 года на российском рынке
- один из лидеров рынка системной интеграции Сибири
- сеть представительств в регионах РФ

CIS Современные Информационные Системы

ЖУРНАЛ CIS

- об информационных технологиях в России
- выходит ежеквартально
- портал www.cismag.news
- распространяется на всех крупных ИТ-выставках и мероприятиях в Москве и на мероприятиях партнёров

Регуляторы ИБ и их влияние

Законодательство

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- 152-ФЗ от 27.07.2006
- Приказ ФСТЭК России №21
- Приказ ФСБ России №378

ФИНАНСЫ

- ГОСТ Р 57580.1-2017
- ЦБ: 382-П, 672-П, 673-П
- Указ №4859-У/01/01/782-18 (ЕБС)

ОБЪЕКТЫ КИИ

- 187-ФЗ от 26.07.2017
- Приказ ФСТЭК России №239, №235
- Приказ ФСБ России о ГОССОПКА

С-ТЕРРА VPN

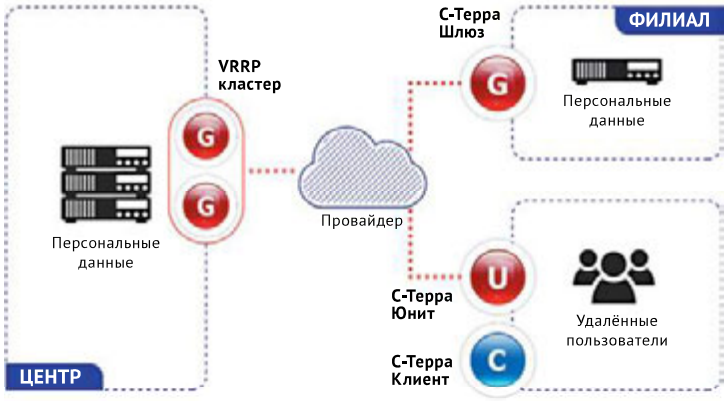
1 ПОНЯТНАЯ АРХИТЕКТУРА

Проверенные технологии
IPsec согласно RFC

Вендор СКЗИ

Проприетарные разработки
...

Site-to-site VPN & Remote access VPN



С-Терра Шлюз
- ФСБ России КС1, КС2, КС3
- ФСТЭК России МЭ А4, 4 ур. доверия

С-Терра Юнит
- ФСБ России КС1, КС2
- ФСТЭК России* МЭ А4, 4 ур. доверия

** в процессе сертификации*

НОВОЕ! Astra Linux 1.6
Поддержка OTP с Radius

Модельный ряд С-Терра Шлюз

С-Терра Шлюз	Артикул	Кастомизация АП	IMIX mono, Mbps	UDP1400 mono, Mbps	Максимальное количество туннелей
100	1701		45	80	10/200
1000	1723	vga	125	190	50/500
2000	1725	vga	250	380	500
3000ST	1727	vga	690	1000	1000
3000ST	1740	RED	900	1150	1000
3000HE	1742	4 оптических интерфейса, RED, RP, IPMI	1180	1550	1000
7000ST	1747	4 или 8 оптических интерфейсов, RED, RP, IPMI	2030	3080	Без ограничений
7000HE	1753	4 или 8 оптических интерфейсов, RED, RP, IPMI	**3400** (было 2200)	**5700** (было 3100)	Без ограничений

Замеры выполнены на автоматизированном шасси Spirent.

Промышленные исполнения

ПАК для использования в сложных условиях

С-Терра Шлюз (промышленный)

- ФСБ России КС1
- ФСТЭК России МЭ Б4, 4 ур. доверия

РАСШИРЕННЫЙ ДИАПАЗОН ТЕМПЕРАТУР
от -40 до +70°С

ПЫЛЕЗАЩИЩЁННЫЙ КОРПУС
металлический, компактный

КРЕПЛЕНИЕ
на DIN-рейку

ПИТАНИЕ
24 Вольт

Кастомизация АП и ПО

КОМБИНАЦИИ ПО

- VPN + МЭ на одной АП
- СОВ (IDS)
- VPN + МЭ + СОВ на одной АП

НАБОР ПОРТОВ

- для младших моделей – фиксированный
- для старших моделей – кастомизированный

ПОДДЕРЖКА ИНТЕРФЕЙСОВ
1/10 GbE(RJ45, SFP, SFP+)
*QDR 40 GbE–в версии 4.3

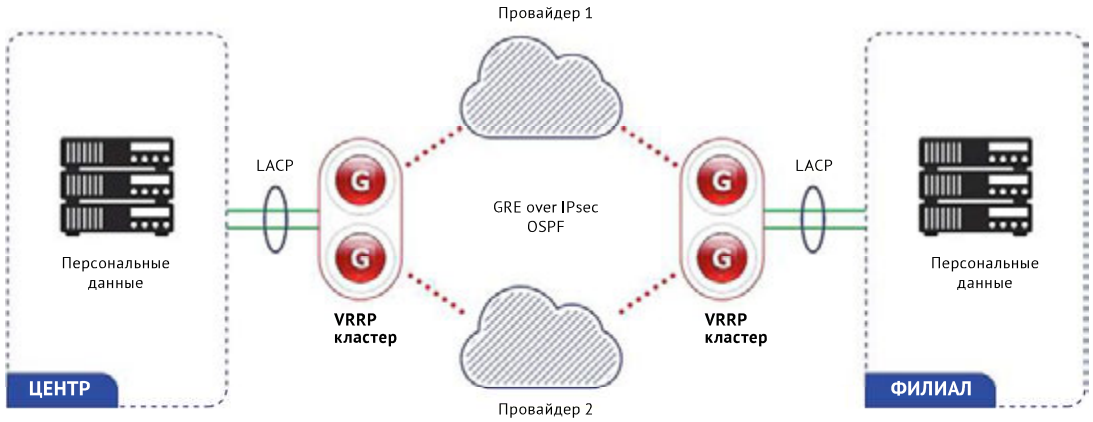
РЕЗЕРВИРОВАНИЕ

- блоки питания
- диски

ВЫДЕЛЕННЫЙ ИНТЕРФЕЙС УПРАВЛЕНИЯ (IPMI)
для исполнений КС1 и КС2

Отказоустойчивость в IPsec VPN

На всех уровнях: интерфейсы, устройства, провайдеры



НОВОЕ! Резервирование провайдеров с мониторингом доступности удалённого узла – changeroutesна КС3
Динамическая маршрутизация – FRR на КС3

Универсальные компактные устройства

IPsec VPN

С-Терра Юнит

- ФСБ России КС1, КС2
- ФСТЭК России МЭ А4, 4 ур. доверия

** в процессе сертификации*

ГАБАРИТЫ –80 х 45 х 22 мм

самый миниатюрный шлюз в России

ИМПОРТОЗАМЕЩЕНИЕ

- АП – производство в России
- ПО – С-Терра VPN

УНИВЕРСАЛЬНОСТЬ

- не зависит от операционной системы (ОС)
- мобильные устройства – Android, iOS

ГИБКОСТЬ

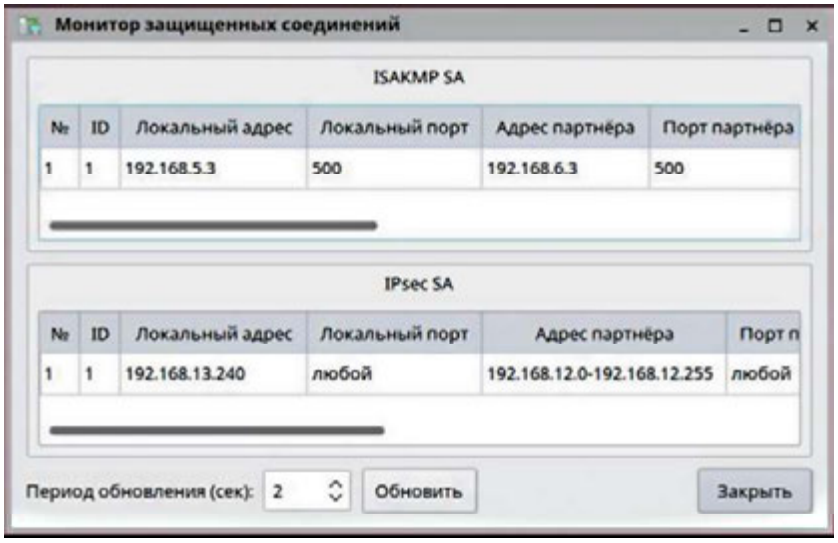
- 2 x FastEthernet
- WiFi, 3G, 4G

Что нового в версии 4.3

Улучшения/исправления в С-Терра Клиент

- Запись лог-файлов в локальную ФС
- Поддержка одноразовых паролей (OTP)
- Несколько IKECFG-интерфейсов
- Защита дистрибутивов паролем

Клиент для Астра Линукс



C-ТЕРРА VPN

2 НАСТРОЙКА И ОБСЛУЖИВАНИЕ

C-Терра Шлюз

НАСТРОЙКА и УПРАВЛЕНИЕ
- индивидуальное: SSH, Console
- централизованное: C-Терра КП

МОНИТОРИНГ
- SNMP v2, SNMP v3
- NetFlow, IPFIX, Zabbix-агент

НОВОЕ!

ЛОГИРОВАНИЕ
- система управления C-Терра КП
- syslog

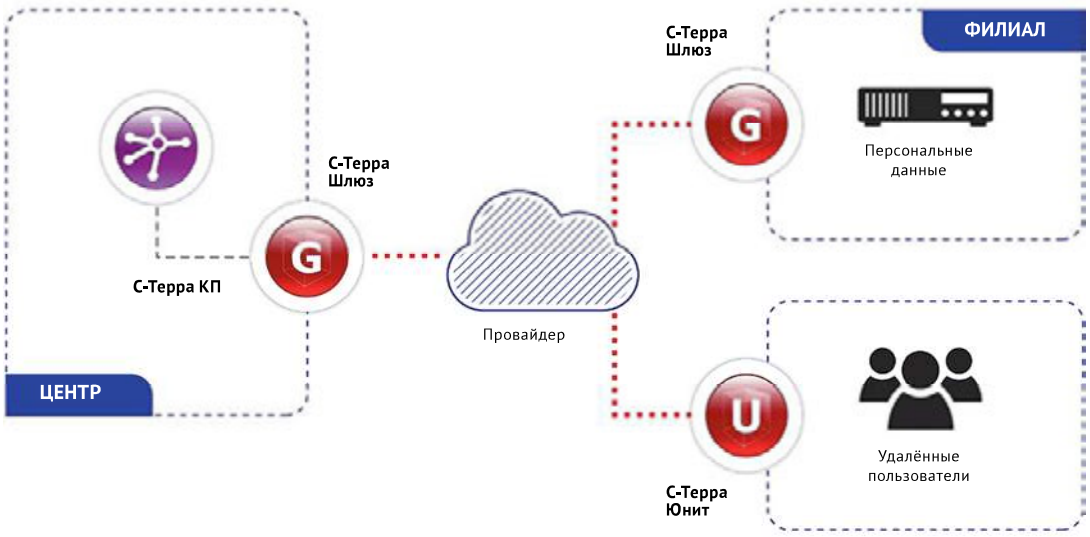
```
crypto isakmp policy 1
 encr gost
 hash gost
 authentication gost-sig
 group vko
!
crypto ipsec transform-set TSET esp-gost28147-4m-imit
!
ip access-list extented LIST
 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
!
crypto map CMAP 1 ipsec-isakmp
 match address LIST
 set transform-set TSET
 set pfs vko
 set peer 10.0.0.2
!
```

Пример настройки site-to-site VPN.

НОВОЕ! **Расширен перечень Cisco-likeкоманд, например: show interfaces, show vrrp**
Добавлены Object Group

Централизованное управление

Вариант размещения С-Терра КП



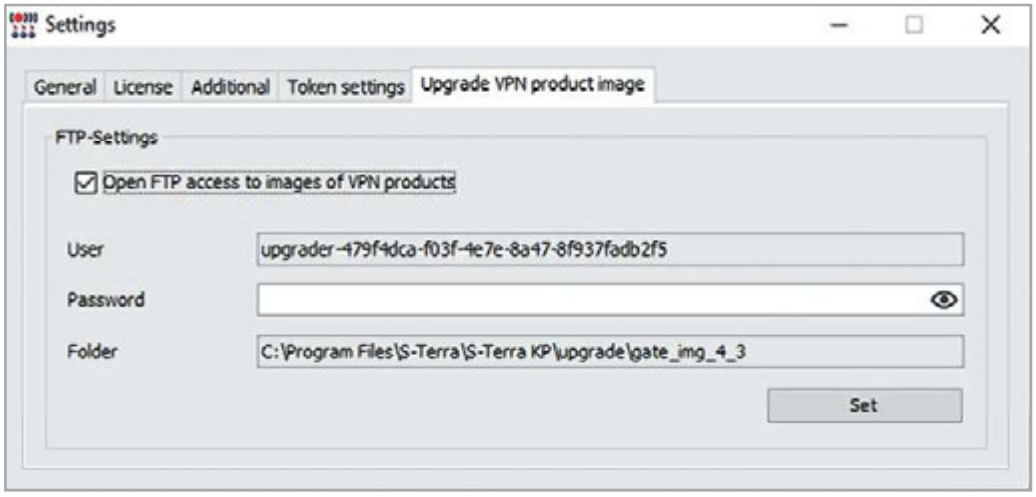
Функциональность С-Терра КП

НОВОЕ!

Удалённое обновление ПО СКЗИ

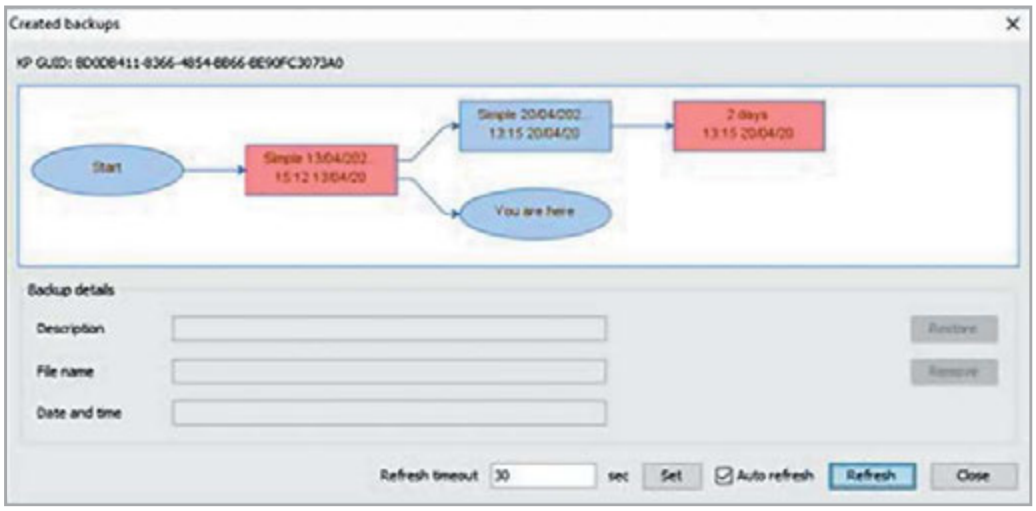
НОВОЕ!

Новая ролевая модель доступа с разграничением прав



НОВОЕ!

Новая BACKUP система

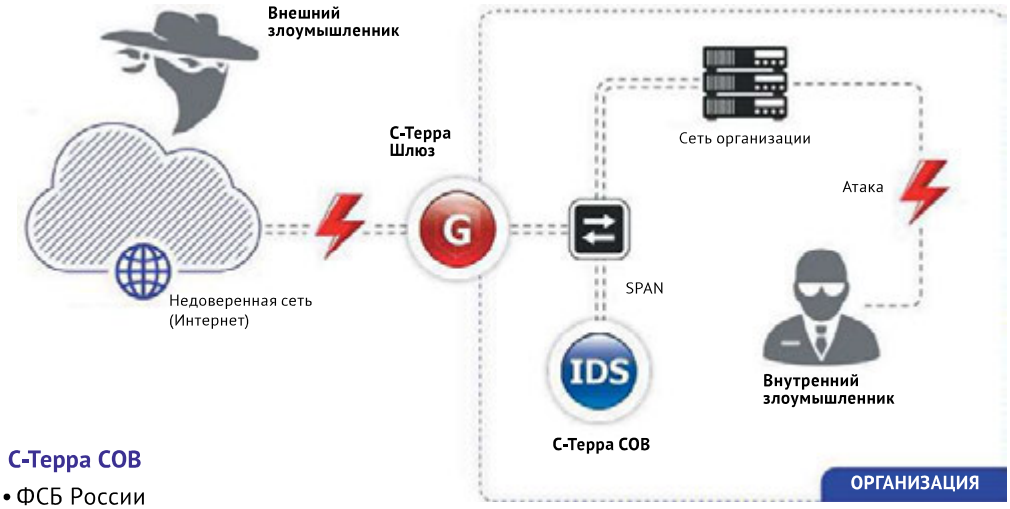


C-TERRA VPN

3 СПЕЦИАЛИЗИРОВАННЫЕ РЕШЕНИЯ

Обнаружение сетевых атак

Функциональные возможности С-Терра СОВ



С-Терра СОВ

- ФСБ России
  СОА класса В
- ФСТЭК России
  СОВ уровня сети 4 класса защиты

С-Терра СОВ. Преимущества

СЦУМ БЕСПЛАТНО
расширенные возможности аналитики

ГАРАНТИЯ 3 ГОДА
на аппаратную платформу

БЕСПЛАТНАЯ ТЕХПОДДЕРЖКА
- в течение первого года
- БРП входят в стандартный пакет

СОБСТВЕННЫЕ БРП
сертификат ФИПС от 23.10.2019

СЕРТИФИКТЫ ФСБ РОССИИ
- СОА класса В
- действительны по 2023 г. (2021+2)

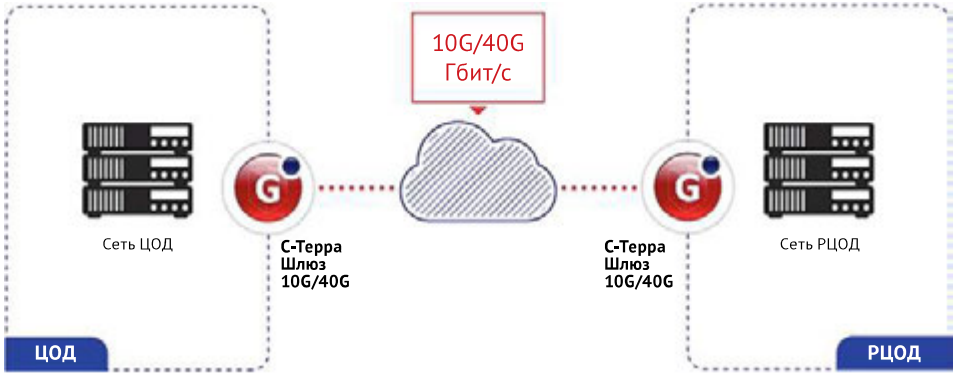
СЕРТИФИКАТЫ ФСТЭК РОССИИ
- СОВ уровня сети 4 класса защиты
- действительны по 2023 г.

СОВМЕЩЁННОЕ ИСПОЛНЕНИЕ С VPN
ФСБ России – СКЗИ КС1, КС2

ВИРТУАЛЬНОЕ ИСПОЛНЕНИЕ
KVM, Xen, Hyper-V, ESXi и т.д.

Выскопроизводительные решения

Защита канала взаимодействия ЦОД-РЦОД.
Решение на L2 OSI



С-Терра Шлюз 10G

- ФСБ России
  КС1, КС2, КС3
- ФСТЭК России
  МЭ А4, 4 ур. доверия

С-Терра Шлюз 40G

- ФСБ России
  КС1, КС2, КС3
- ФСТЭК России*
  МЭ А4, 4 ур. доверия

** в процессе сертификации*

Производительность

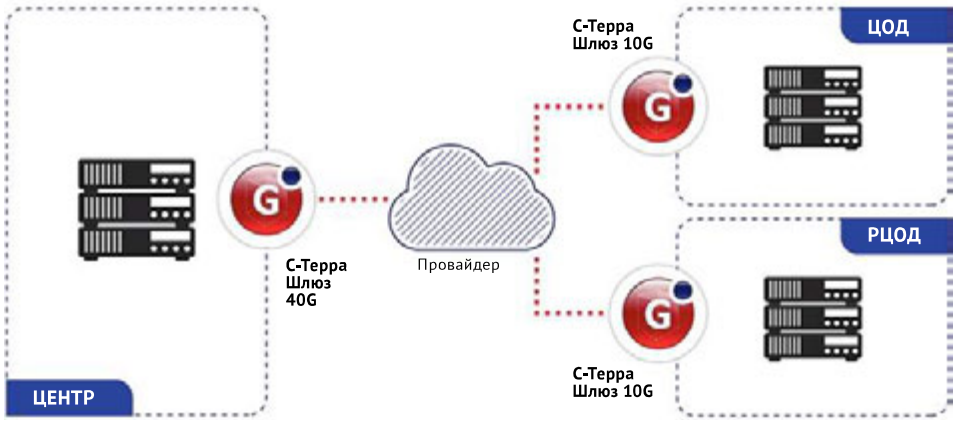
Frame size	НОВОЕ!	С-Терра Шлюз 40G Mbps	С-Терра Шлюз 10G Mbps
UDP 9000 Mono		40 000	9914
UDP 1446 Mono		38 137	9 505
UDP 512 Mono		33 355	8 748
UDP 110 Mono		11 222	4 452
UDP IMIX Mono		30 278	8 405
UDP 9000 Dual		68 961	(14 269) **19 609**
UDP 1446 Dual		60 172	(12 644) **18 843**
UDP 512 Dual		45 477	(10 433) **17 011**
UDP 110 Dual		14 961	(5 355) **6 190**
UDP IMIX Dual		40 950	(9 964) **15 194**

НОВОЕ!

Замеры выполнены на автоматизированном шасси Spirent.

Выскопроизводительная «звезда»

Защита канала взаимодействия ЦОД-РЦОД.
Решение на L2 OSI



Преимущества С-Терра VPN

ПОНЯТНАЯ АРХИТЕКТУРА
IKE / IPsec

НИЗКАЯ СТОИМОСТЬ ВЛАДЕНИЯ
- бесплатная поддержка 1 год
- гарантия на АП 3 года

СЕРТИФИКАЦИЯ
ФСБ России и ФСТЭК России
до 2023 года

КАСТОМИЗАЦИЯ и ОТКАЗОУСТОЙЧИВОСТЬ
на всех уровнях

Андрей Шпаков
Руководитель отдела технического консалтинга
ashpakov@s-terra.ru

s·terra®

+7 (499) 940 9061
www.s-terra.ru
sales@s-terra.ru

Рос Интеграция

8 (800) 333 9199
www.rosintegracija.it

Информационное партнёрство: журнал CIS www.cismag.news

CIS / № 3 (13) / 2020 / www.cis.ru

Цифровое рабочее место

– Елена, давайте начнём с определения. Что же такое цифровое рабочее место (ЦРМ)?

Чаще всего под ЦРМ понимается виртуальный эквивалент физического рабочего места. Видимые части ЦРМ – это способы и методы работы, которые позволяют людям объединиться, общаться и взаимодействовать, не находясь лицом к лицу. ЦРМ включает в себя технологии, которые можно использовать при выполнении своих профессиональных обязанностей на современном рабочем месте. Эти технологии варьируются от CRM-систем и бизнес-приложений до электронной почты, мгновенных сообщений, а также корпоративных социальных коммуникаций и виртуальных встреч.

– Почему современному бизнесу лучше сделать ставку на ЦРМ сегодня? И какой путь ведёт к успешным преобразованиям?

Крупным корпорациям, таким как мы, особенно важно внедрить легко интегрируемое ЦРМ, чтобы идти в ногу со временем в новой цифровой эпохе. Объём данных, разнообразные инструменты и множество уровней прозрачности процессов в разных подразделениях могут перегрузить рабочий процесс, нарушить его организацию и снизить эффективность. К сожалению, некоторые крупные компании не уделяют внимания правильному концепту и созданию единого рабочего места, пока оно не станет критически важным для ведения бизнеса. Те же, кто внедряет ЦРМ заранее, пользуются значительными преимуществами, которые отражаются на эффективности и скорости работы в организации. А если учитывать, что сотрудники территориально распределены по всему миру, то эффект от внедрения ЦРМ гораздо выше. Инвестируя в удобное взаимодействие на всех этапах проекта, мы предоставляем сотрудникам интерактивную платформу, которая улучшает важный баланс между работой и жизнью. Благодаря единому интерфейсу на всех используемых устройствах, будь то стационарное рабочее место, смартфон или ноутбук, ускоряются процессы, и пользователи не тратят время на поиски нужного инструмента для выполнения простой задачи.

– ЦРМ становится основой цифровизации компании. Каковы преимущества использования цифрового рабочего места?

На самом деле преимуществ от внедрения ЦРМ гораздо больше, чем недостатков. Помимо повышения производительности (по данным исследования «Битрикс24» и J»son & Partners Consulting по итогам проекта Beeline – BeeFREE), цифровое рабочее пространство также способствует профессиональному развитию. Применение цифровых технологий развивает новые навыки и повышает удобство коммуникаций между сотрудниками, создаёт рабочую среду с широкими возможностями для совместной деятельности ввиду наличия возможности работы из любой точки мира. Соответственно, развитие цифровых технологий в компании способствует увеличению автоматизированных процессов, что создаёт благоприятные условия для более успешного пользовательского опыта на рабочем месте в части интеллектуальной и эффективной рабочей среды. А это в свою очередь уже повышает имидж компании до передового.

Если мыслить более приземлённо, то для руководителей компаний самым важным преимуществом является повышение экономии на содержание рабочих мест и потенциальные доходы. ЦРМ таким преимуществом также обладает.

Подводя итог вышесказанному, организация удалённого доступа к цифровому рабочему месту и переход части сотрудников на работу из дома позволяет достичь следующих результатов для компании:

- существенная экономия и потенциальные доходы;
- повышение лояльности сотрудников;
- увеличение производительности;
- имидж передовой компании;
- повышение безопасности ИТ;
- возможность работы из любого места;
- не требуется специальных мероприятий для организации работы в командировке.

– Сколько времени Вам потребуется для реализации данного проекта?

С «нововведениями» в государственном секторе всё непросто. В 2018 году мы защитили реализацию проекта ЦРМ, в принципе, как и везде, не с первого раза. Первым этапом по подготовке перехода к ЦРМ можно считать внедрение защищённой мобильной почты. Далее мы перешли к этапу проектирования и выбора решений как для поддержания ИТ технологий, так и средств защиты информации. Несколько месяцев занял процесс проработки юридических вопросов. На сегодняшний день идёт активная стадия тестирования и наладки бесперебойной работы ЦРМ, а уже к концу 2019 года планируем тиражирование решения и перевод на удалённую работу порядка 30 сотрудников для активного пилотирования «объекта цифровизации». Этапы и сроки реализации проекта представлены на рисунке 1.

– При разработке проекта, какие сложности могут возникнуть на Ваш взгляд? Как планируете их предотвращать?

На удивление, сложности, которые могут возникнуть, не относятся к применению и вы-

Елена Нагорная
Начальник отдела информационной безопасности
АО «Техснабэкспорт»

Рисунок 1. Сроки и этапы реализации проекта

бору технических решений и выполнению требований регуляторов в области информационной безопасности. Как ни прозаично, эти сложности связаны с организационными мероприятиями. На сегодняшний день невооружённым взглядом видна неготовность государственной системы в части трудового законодательства переводить работников на удалённую работу с гибким графиком. При анализе Трудового кодекса мы столкнулись с такой проблемой, что работник может осуществлять свои функции исключительно либо находясь на рабочем месте в организации, либо работая дистанционно. Согласно ст. 312.1 Трудового кодекса РФ дистанционной признается работа, выполняемая вне места нахождения работодателя, его обособленных подразделений, территорий или объектов, прямо или косвенно находящихся под контролем работодателя, с использованием информационно-телекоммуникационных сетей общего пользования, в том числе сети Интернет. Местом постоянной работы дистанционного работника является место его нахождения, а поездка от места нахождения до места нахождения работодателя является служебной командировкой. При этом ст. 312.1 ТК РФ закреплено, что на дистанционных работников распространяется действие трудового законодательства, в том числе требование ст. 168 ТК РФ о возмещении работникам командировочных расходов при направлении их в служебные командировки. Получается, что в случае необходимости дистанционному работнику приехать в офис, даже если дислокация находится в рамках одного города, работодателю придётся оформлять командировку. А это в свою очередь увеличит нагрузку работы кадровым служ-

бам и расчётчикам заработной платы. На сегодняшний день выхода из сложившийся ситуации мы пока не нашли: существуют юридические риски в случае нелояльности сотрудников. Надеюсь, что с развитием государственной политики в области цифровизации будет совершенствоваться и наше законодательство.

– Как оценить экономический эффект от внедрения ЦРМ?

Экономический эффект от внедрения идеи состоит из нескольких частей. В первую очередь это экономия на аренде освобождаемых площадей, сюда же входит сокращение расходов на «коммунальные платежи». В зависимости от территориального нахождения организации и престижности арендуемого офиса сокращение расходов из расчёта на 100 человек ориентировочно может варьироваться от 15 до 80 млн рублей в год.

Также мы экономим на обслуживании рабочего места и расходах на печать. В случае ЦРМ меняется порядок лицензирования, приобретаются не «физические» лицензии на системное программное обеспечение и средства защиты информации, а одна лицензия для «виртуальной машины» с привязкой к пользователю, а не к количеству используемых им устройств. Расходы на печать, соответственно, минимизируются, так как большинство процессов автоматизировано, а документооборот ведётся исключительно в электронном виде.

– А как быть с безопасностью? Оборотная сторона цифровой трансформации – возрастание рисков информационной безопасности. Есть ли способы противостоять такому росту, особенно в тех областях, где это наиболее важно, например в атомной промышленности?

Наряду с большим числом преимуществ ЦРМ обеспечение информационной безопасности является серьёзным вызовом для компаний, решивших идти в ногу со временем в области цифровой трансформации. Как показывает практика, сотрудники, работающие с использованием ЦРМ высоко осведомлены в вопросах информационной безопасности, однако не всегда следуют правилам. Считаю, что к основным рискам информационной безопасности можно отнести человеческий фактор, если говорить о неумышленных действиях пользователей, например: передача паролей и устройств другим пользователям, использование одних и тех же паролей в нескольких приложениях и учётных записях, запись и хранение паролей рядом с мобильным устройством. Можно долго говорить о рисках, связанных с культурой кибербезопасности, но в этом случае утечка информации может возникнуть и на рабочем месте без учёта использования ЦРМ.

Если говорить о внешних злоумышленниках, то основными источниками угроз являются потенциально небезопасные открытые Wi-Fi-сети, кража устройств или же автоматическая передача данных с мобильного устройства в облако. Но современные средства защиты данных способны нивелировать указанные риски информационной безопасности. Если рассмотреть проблему с другой стороны, то имеются и неоспоримые преимущества ЦРМ с точки зрения обеспечения информационной безопасности: фактически, обрабатываемые в ЦРМ данные не покидают ЦОД компании и являются более защищёнными, чем в других мобильных решениях.

– Какие технические решения по информационной безопасности нужны для успешной реализации проекта? По каким критериям Вы их отбираете? (Решение каких вендоров Вы рассматриваете? Почему остановили свой выбор на конкретном решении? Что повлияло на Ваш выбор?)

Для реализации проекта ЦРМ необходимо обеспечить техническое решение для трёх основных задач:

1. Организация инфраструктуры ЦРМ.
2. Доставка ЦРМ до пользователя.
3. Комплекс мер информационной безопасности на стороне пользователя.

Практически вся информационно-телекоммуникационная инфраструктура нашей компании развёрнута в среде виртуализации VMware. Виртуализация вычислительных ресурсов и конвергентные решения VMware использованы для реализации серверной инфраструктуры. Учитывая положительный опыт эксплуатации решений VMware, вопрос по выбору средств для организации инфраструктуры, в которой будут развёрнуты виртуальные машины ЦРМ, не возник.

При выборе средств доставки ЦРМ были рассмотрены следующие лидирующие технологии, представленные на сегодняшнем ИТ-рынке:

- Citrix Virtual Apps and Desktops
- VMware Horizon.

Решения других производителей, таких как Microsoft, Dell или IBM, а также OpenSource мы не стали рассматривать из-за явной сложности интеграционной реализации с нашей инфраструктурой, хотя по каким-то критериям они даже лучше выбранных нами.

При сравнении двух основных игроков стало ясно, что Citrix обладает проверенными временем решениями, обеспечивая при этом стабильный доступ к ЦРМ по «плохим» каналам передачи данных. Учитывая, что у наших пользователей имеется возможность использовать современные высокоскоростные средства доступа к публичным сетям передачи данных, преимущество решения Citrix над предложением VMware нивелируется отсутствием необходимости обеспечивать интеграцию системы доставки ЦРМ и среды виртуализации разных производителей.

Также на практике оказалось, что решение VMware Horizon хорошо интегрируется с системами шифрования каналов по ГОСТ, что немаловажно при обеспечении защиты каналов связи по требованиям регуляторов.

Дополнительным аргументом для выбора VMware Horizon стало наличие в их продуктовой линейке защищённой мобильной почты – Boxer, обеспечивающей безопасное взаимодействие с корпоративными информационными системами с мобильных устройств пользователей. Отметила бы, что первым этапом в развитии ЦРМ для нас как раз стал проект по созданию службы защищённой мобильной почты и внедрение сервиса управления мобильными устройствами – решение Workspace ONE (MDM). В результате внедрения Workspace ONE нам удалось обеспечить следующее:

- повышение вовлечённости пользователей и эффективности их работы при использовании корпоративной мобильной электронной почты;
- сокращение времени реакции на возникающие инциденты и быстрое устранение проблем в части работы организованных мобильных ИТ-сервисов.

Применяемые политики безопасности защищённой мобильной почты позволяют осуществлять контроль действий пользователей в части их работы со вложениями, такими как: невозможность сделать «скриншот» экрана, сохранить вложения на мобильном устройстве и др. Политики безопасности MDM-системы позволяют чётко разграничить корпоративные и личные данные на мобильном устройстве сотрудников, а также позволяют ИТ-менеджеру удалённо управлять компонентами устройства, например блокировать его и полностью стирать корпоративную информацию в случае его потери или кражи. Указанные возможности позволяют обеспечить конфиденциальность информации ограниченного доступа.

Выбранное нами решение предназначено для защиты информации, обрабатываемой на ЦРМ, и реализовано в виде комплекса средств обеспечивающих:

- двухфакторную аутентификацию пользователя с использованием защищённых ключевых носителей;
- защиту данных на мобильном рабочем месте с использованием шифрования.

Реализованный комплекс средств защиты информации позволяет обеспечивать следующий функционал:

1. Выпуск ключевого носителя для пользователя.
2. Шифрование ЦРМ-пользователя с помощью системы Secret Disk Enterprise.
3. Запуск ЦРМ-пользователя и подключение зашифрованных дисков.
4. Аутентификация пользователя на АЦРМ с помощью ключевого носителя.
5. Аутентификация удалённого пользователя по ГОСТ сертификату в системе VDI через Привратник.

После проведения пилотного испытания решений доставки ЦРМ мы получили подтверждение первоначальных предположений: моновендорное решение ЦРМ имеет ряд преимуществ перед интегрированными системами многих производителей. Мы получили позитивный опыт при проведении интеграции среды виртуализации, средств доставки ЦРМ и средств информационной безопасности таким, как, например двухфакторная система аутентификации пользователей, когда взаимодействие с одним производителем значительно сокращало сроки решения вопросов, возникавших при внедрении.

Возможно, после проведения пилотных испытаний ЦРМ схема решения по обеспечению информационной безопасности немного изменится. На наш взгляд, такой алгоритм на сегодняшний день наиболее эффективен.

– Как планируете контролировать удалённых пользователей? Есть ли ограничения на обработку информации? И планируете ли устанавливать контроль за привилегированными пользователями, если они тоже задействованы в проекте, конечно?

Для контроля удалённых пользователей предполагается использовать тот же подход и те же средства, которые используются внутри ИТ-инфраструктуры, находящейся в пределах контролируемой зоны. Но будут внедряться и дополнительные средства, решающие новые задачи, такие как:

- использование мобильных устройств (BYOD) для доступа к корпоративным системам;
- решение задач безопасности, связанных с утратой мобильных устройств.

Тем не менее все пользователи ЦРМ контролируются точно так же, как и локальные пользователи, не использующие ЦРМ. Этот подход выбран изначально для единообразной организации процессов информационной безопасности. А это означает, что ограничений на обработку информации нет и пользователи не почувствуют «дискомфорта» при организации своей удалённой работы.

Привилегированные пользователи при возникновении потребности получают дополнительные вычислительные ресурсы, что позволяет организовать с помощью ЦРМ удобную и комфортную работу с большими объёмами данных, например для различного анализа.

– Изучали ли Вы кейсы других компаний, которые внедрили ЦРМ?

Нам в какой-то мере повезло. В рамках реструктуризации в периметр нашей компании была включена организация, успешно внедрившая ЦРМ в 2013 году и имеющая значительный позитивный опыт использования ЦРМ. Поэтому мы не только изучали кейсы в теории, а проводили пилотные испытания, сравнивая имеющееся в нашем распоряжении техническое решение с конкурентными.

При выборе технологий, используемых в ЦРМ, мы анализировали отраслевой опыт. И убедились, что при примерке других кейсов «на себя», в первую очередь, требуется оценить, в чём наш и исследуемый кейс различны. Как правило, минимальные отличия в требованиях к применению ЦРМ в каждом конкретном случае могут привести к выбору совершенно другого решения, и такой выбор будет полностью оправдан.

При выборе сложных современных технологий наибольшую пользу приносят пилотные внедрения и опытная эксплуатация предлагаемых решений, на основании которых можно скорректировать изначальные требования и получить именно то решение, которое требуется бизнесу.

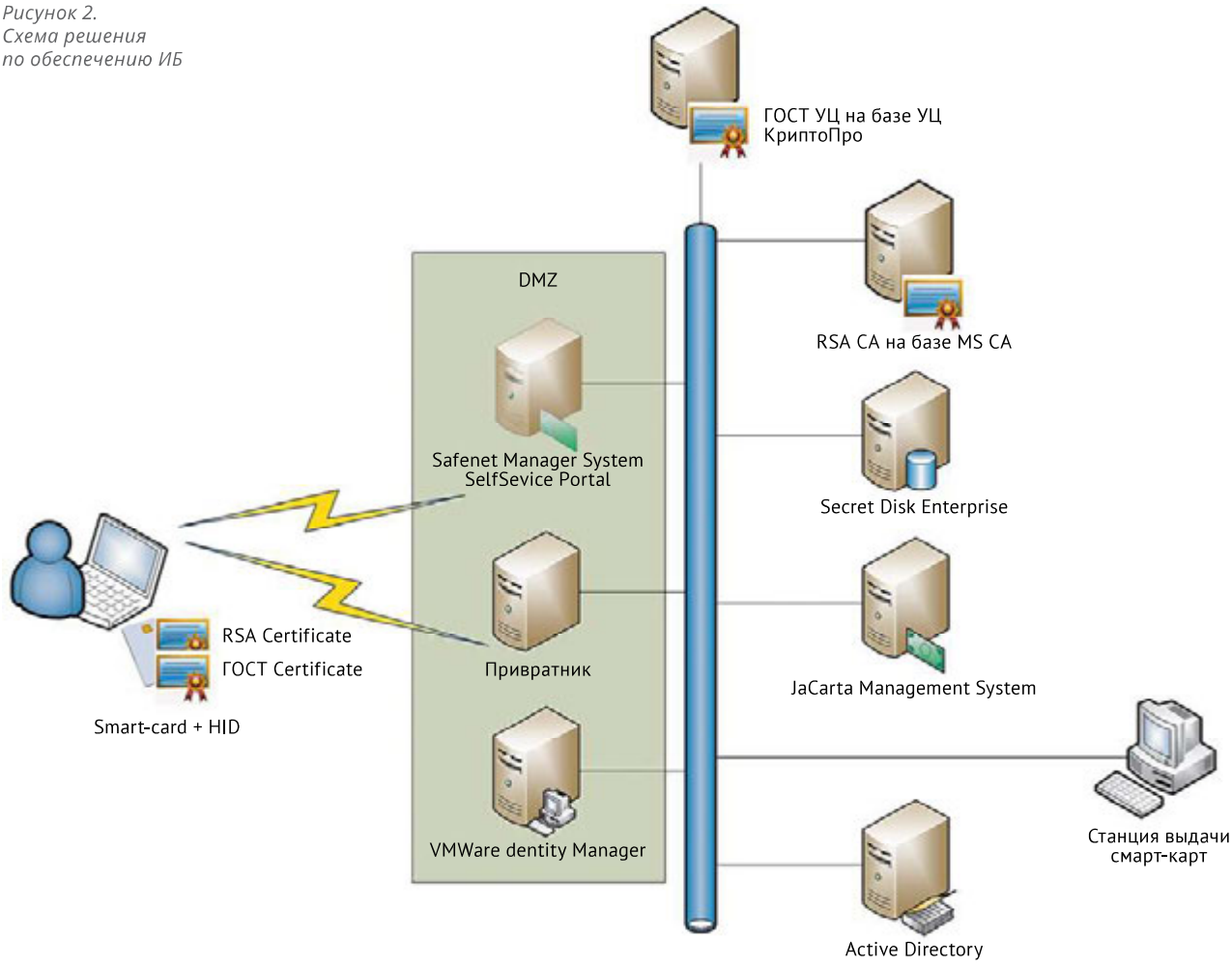
– Елена, подведём небольшой итог: компаниям необходимо адаптироваться, чтобы задействовать все преимущества новых технологий ЦРМ, при этом одновременно минимизируя риски безопасности. Какие рекомендации Вы можете дать представителям крупных компаний, которые тоже раздумывают о внедрении ЦРМ?

ЦРМ – это технология, позволяющая вести свой бизнес более гибко. Фактически, необходимо адаптироваться не компании, а её ИТ-подразделению, чтобы суметь наиболее эффективно и удобно для пользователей провести внедрение.

Я бы рекомендовала компаниям при внедрении ЦРМ принять следующие меры:

- определить план развития цифрового рабочего пространства в сотрудничестве с топ-менеджерами, конечными пользователями и другими заинтересованными участниками;
- планировать рабочую среду ЦРМ «без границ» и инвестировать в её развитие. Это означает, что организация удалённой ра-

Рисунок 2.
Схема решения
по обеспечению ИБ



боты должна распространяться не только на работников, находящихся в офисе, но и на удалённых сотрудников, а возможно, и на заказчиков;

- проектировать ЦРМ, принимая во внимание требования информационной безопасности. Это означает, что перед реализацией проекта необходимо учитывать все возможные угрозы со стороны злоумышленников, оценить существующие риски информационной безопасности и только потом, на основе оценки рисков, создавать оптимальную систему безопасности, способную адаптироваться к новым вызовам и угрозам.

– Какие ещё проекты по цифровой трансформации в атомной отрасли ждать в ближайшее время?

В целом политика проведения цифровой трансформации в атомной отрасли предполагает революционные изменения бизнес-моделей на основе использования цифровых платформ, которые приведут к радикальному росту объёмов рынка и конкурентоспособности компании.

Думаю, что приоритетными проектами в атомной отрасли до 2030 года станут следующие:

- создание и передача в эксплуатацию высококачественной цифровой модели АЭС;
- цифровое импортозамещение путём создания продуктов для собственных потребностей;
- создание инфраструктуры больших данных с подключением к ней их поставщиков и лабораторий отрасли;
- модернизация процессов, подлежащих автоматизации с помощью прорывных технологий с применением искусственного интеллекта;
- создание интеллектуальной системы управления ресурсами ИБ и ИТ.

TENEX

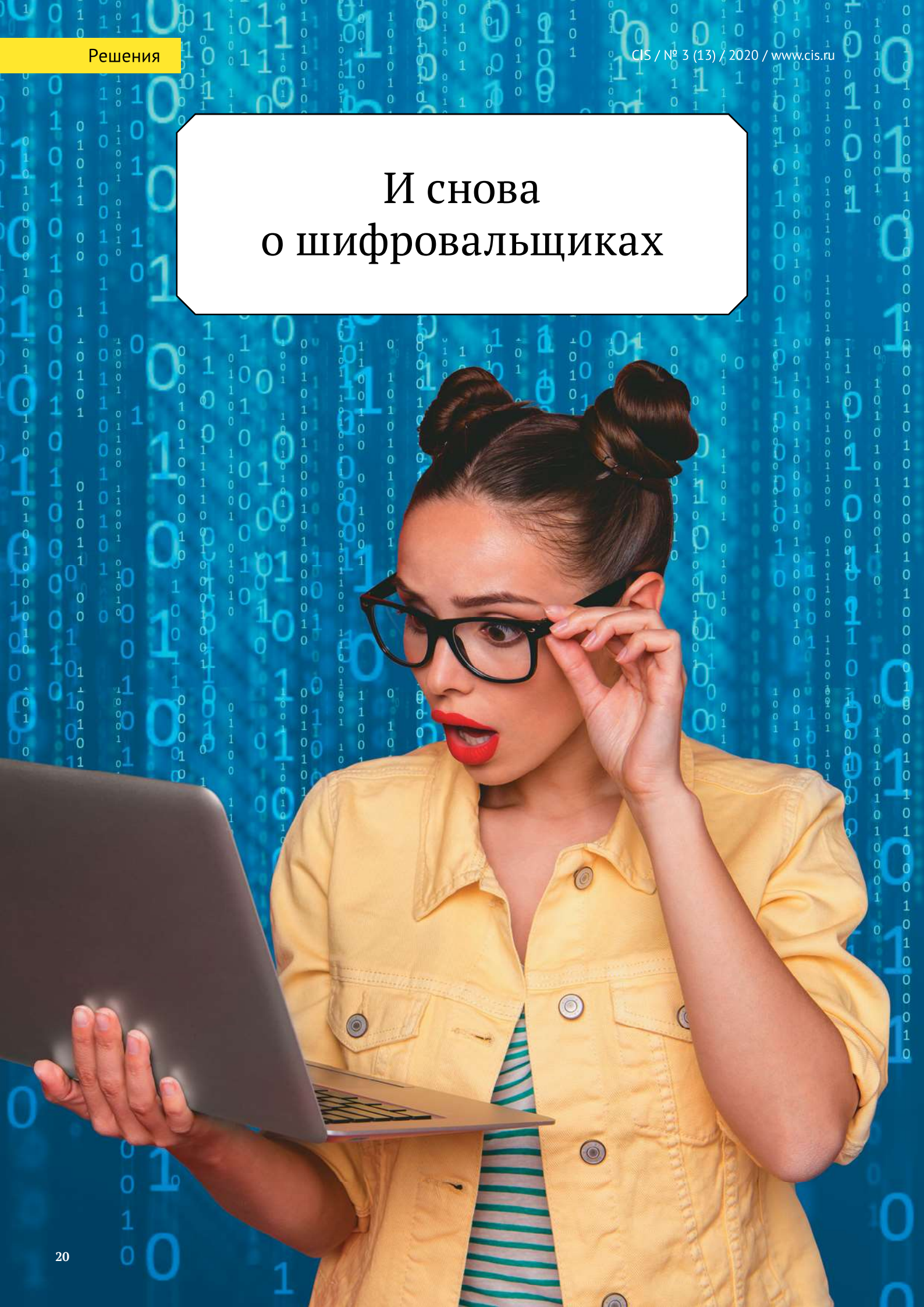
АКЦИОНЕРНОЕ ОБЩЕСТВО «ТЕХСНАБЭКСПОРТ»

АО «Техснабэкспорт» (торговая марка TENEX) – один из крупнейших мировых поставщиков продукции ядерного топливного цикла (ЯТЦ), обеспечивающий значительную часть потребностей реакторов зарубежного дизайна в услугах по обогащению урана.

www.tenex.ru

CIS / № 3 (13) / 2020 / www.cis.ru

И снова о шифровальщиках



О проблемах шифровальщиков, наверное, не слышал только тот, кто вообще никогда не работает с компьютером. На самом деле подобное вредоносное ПО распространяется уже много лет. И тем не менее для тех счастливчиков, которые никогда не сталкивались с ним, стоит всё же повторить, а что же такое «шифровальщик».

Что такое Ransomware?

Ransomware или трояны-вымогатели – это разновидность зловредных программ, которая в последнее время получила огромное распространение. По вредоносному поведению их можно разделить на два основных типа:

- Шифровальщики (cryptoransomware)
- Блокировщики (blockers, блокеры)

При этом шифровальщики, попадая на ваше устройство, шифруют ценные файлы (документы, фото, сохранённые игры, базы данных и т.д.). Файлы шифруются таким образом, чтобы вы не могли их открыть. То есть ими просто нельзя воспользоваться. А за расшифровку с вас потребуют денег. Мало того, сейчас, если вы не хотите платить, то возможны два варианта:

- Ваши данные будут проданы конкурентам или просто выставлены в Интернет
- Через небольшой промежуток времени ключи шифрования будут уничтожены, а, следовательно, расшифровывание файлов будет невозможно

Но стоит учесть, что очень часто оплата, которую получат злоумышленники, не гарантирует, что вы получите возможность расшифровки файлов.

Блокировщики получили своё имя за то, что просто блокируют доступ к устройству. То есть не получится воспользоваться не только файлами, но и всем компьютером. Они тоже требуют «выкуп», но обычно не такой большой, как шифровальщики.

Стоит учесть, что на сегодня вымогателей уж очень много и встречаются они довольно часто. Кроме того, они есть для всех операционных систем: Windows, Mac OS X, Linux и Android. То есть трояны-вымогатели встречаются не только для компьютеров, но и для смартфонов и планшетов. Больше всего их для Windows и Android.

Нужно понимать, что существуют различные пути заражения.

Пути заражения

Троян-шифровальщик проникает к пользователю через почту (как вложение в письмо). Дальше, постепенно усложняясь, идут различные техники уклонения, но в каждом случае работает своя система защиты.

Пользователь получает вирус в письме в виде исполняемого файла, который уже использовался в других атаках. Вопрос: знают ли ваши пользователи типичные расширения исполнимых файлов?

Уверен, что даже системные администраторы не знают их все.

Напомним их.

Самыми распространёнными расширениями считаются .EXE, .APP, .VB, .SCR и .MSI.

Полный список исполняемых файлов приведён в таблице 1.

Что посоветовать? Прежде всего, если это касается корпоративной электронной почты, то администратор должен запретить все вложения в виде исполняемых файлов. Вместе с тем необходимо крайне внимательно отнестись ко вложениям, содержащим архивы и файлы, которые могут содержать макросы.

Таблица 1

Расширение	Описание	Популярность
.apk	Пакет приложения Android	Очень часто используется
.bat	Пакетный файл MS-DOS	Очень часто используется
.bin	Исполняемый файл Unix	Средне используется
.bin	Двоичный исполняемый файл	Средне используется
.cgi	Общий интерфейс шлюза	Очень часто используется
.cmd	Пакетный файл Windows	Часто используется
.cmd	Программа dBASE	Очень редко используется
.cmd	Пакетный файл OS/2 REXX	Редко используется
.com	Исполняемый файл MS-DOS	Очень часто используется
.cpp	Файл Apple Xcode Core C	Редко используется
.js	Исполняемый файл JScript	Средне используется
.jse	Зашифрованный файл JScript	Средне используется
.exe	Исполняемый файл	Очень часто используется
.exe	Приложение PortableApps.com	Часто используется
.gadget	Гаджет Windows	Очень часто используется
.gtp	Исполняемый файл Atari ST	Очень редко используется
.hta	Исполняемый HTML-документ	Часто используется
.jar	Файл архива Java	Очень часто используется
.msi	Установочный файл (инсталлятор) Windows	Очень часто используется
.msu	Пакет обновлений Windows	Средне используется
.paf.exe	Файл PortableApps.com	Часто используется
.pif	Информация о приложении Windows	Очень часто используется
.ps1	Скрипт Windows PowerShell	Часто используется
.pwz	Файл мастера создания Microsoft PowerPoint	Редко используется
.scr	Файл скрипта	Часто используется
.thm	Макро файл Thermwood	Редко используется
.vb	Скрипт VBScript	Очень часто используется
.vbe	Зашифрованный скрипт VBScript	Часто используется
.vbs	Скрипт VBScript	Часто используется
.wsf	Файл сценария Windows	Очень часто используется

Стоит учесть, что есть и другие пути: спам, эксплоит-киты, фейковые инсталлеры, значительную долю шифровальщиков сейчас распространяют вручную через подбор паролей к RDP (этот вектор касается и b^2b, и b^2c). А на крупные организации проводятся таргетированные атаки с проникновением в корпоративную сеть, ручным продвижением по сети и централизованным запуском малвары. Также известный и до сих пор актуальный вектор распространения шифровальщиков через ботнеты.

Если этот вирус уже известен облачному сервису или установленному антивирусу и содержится в его локальных базах, то у антивируса уже есть его идентификатор. Такой вирус будет сразу же детектирован **классическим сигнатурным методом:** идентификатор файла сравнивается с записями из базы.

Но чаще вирус будет использовать **метод для изменения своей сигнатуры (полиморфизм)** таким образом, чтобы она не совпадала с сигнатурой оригинального, ранее уже обнаруженного зловреда. Естественно, в этом случае, сигнатурный метод не сработает. Тогда к обнаружению будет подключён искусственный интеллект (система детектирования на основе машинного обучения), которая собирает много разных параметров вредоносных файлов, обучается на них, а после может выявлять целые семейства сходных вирусов.

Вирус использует более серьёзную маскировку (**обфускация кода**), что не позволяет детектировать его только по коду без исполнения. В этом случае, его детектируют с помощью эмуляции (песочницы): файл запускают в изолированной среде, которую вирус считает реальной. А на самом деле, это имитация, где «все ходы записаны», таким образом выявляются вредоносные действия.

Анти-эмуляция. Вирус умеет выявлять эмуляцию и избегает вредоносных действий (то есть не выдаёт себя). Например, вирус проверяет, может ли он выйти в Интернет. Если не может, тогда он «понимает», что попал в эмуляцию, и не делает ничего подозрительного.

Как работает защита: сам пользователь, будучи сознательным, может отказаться от запуска файла, потому что это неизвестный исполняемый файл (exe). Правда, в этом случае остаётся вопрос: а что, если он всё-таки запустит? Это мы узнаем на следующем шаге.

Вирусописатель маскирует вирус: теперь он посылает не исполняемый файл, а некий «привлекательный» документ со встроенным в него вызовом «заразы». Это может быть документ Word с названием «бухгалтерский отчёт» или поздравительная открытка с днём рождения с красивыми картинками. Такой файл, который пользователь точно откроет и запустит «заразу». В таком случае срабатывает модуль защиты от эксплуатации (AEP), который фиксирует обращение к «запрещённой» области памяти и блокирует вредонос.

Вирус хорошо маскируется под некое полезное приложение, например под игру. Приложение успешно запускается, но его блокирует система поведенческого анализа и откатывает вредоносные действия (восстанавливает зашифрованные файлы).

Вместе с тем необходимо помнить ещё об одной защите от атаки через Интернет – служба репутаций. О работе службы репутаций написаны горы статей. Суть её в том, что если на одном из компьютеров, использующих антивирус, выявится вирус, то у всех интернет-страниц, на которых обнаружится данный файл, будет снижена репутация (равно как и у самого файла), а также и у соответствующих сайтов, на которых расположатся данные страницы. Вместе с тем репутация снизится и у всех файлов, которые можно загрузить с этих страниц. Это повлияет на возможные права в системе и приведёт к тому, что вероятность успешного запуска потенциально заражённого файла будет снижена.

Атака через внешний носитель типа заразного USB, который найден на улице и вставлен в компьютер. Защита – модуль контроля внешних носителей, запрет на автозапуск.

Защита от программ-вымогателей на этапах доставки и выполнения

Программа-вымогатель (шифровальщик) – это троянец, изменяющий данные на компьютере таким образом, что жертва лишается возможности использовать их или вообще работать на компьютере. Когда данные превращаются в «заложника» (блокируются или шифруются), пользователь получает требование выкупа. Чтобы восстановить данные или вернуть компьютер в рабочее состояние, жертве предлагается отправить злоумышленнику деньги.

В настоящее время программы-вымогатели входят в число наиболее распространённых угроз кибербезопасности. Причины в следующем:

- эта угроза имеет чёткую модель получения прибыли
- такие вредоносные программы легко применять

Программы-вымогатели могут быть сложными или простыми, в зависимости от предполагаемых жертв.

- Обычные программы-вымогатели широко распространяются посредством кампаний рассылки вредоносного спама, наборов эксплойтов и т.д.
- Сложные программы-вымогатели используются для целевых атак

Атака с помощью программы-вымогателя включает несколько этапов:

Ransomware delivery	Доставка программы-вымогателя
Ransomware execution	Выполнение программы-вымогателя
File location	Расположение файлов
File encryption	Шифрование файлов
Demand of ransom $ 1000	Требование выкупа 1000 $
Payment	Оплата
File decryption (maybe)	Дешифровка файлов (возможно)
Ransomware: stages	Программа-вымогатель: этапы действия

- доставка на компьютер жертвы: вредоносное вложение в письме со спамом, использование уязвимости, проникновение в случае целевой атаки
- выполнение: шифрование важных пользовательских файлов
- требование выкупа
- дешифровка данных (необязательно)

Чтобы обезопасить себя от программ-вымогателей, необходимо использовать решение безопасности с многоуровневой моделью защиты. Многоуровневая защита нового поколения, разработанная «Лабораторией Касперского», позволяет обнаруживать программы-вымогатели на этапе доставки и выполнения атаки. Давайте рассмотрим эти этапы подробнее.

Этап доставки: вредоносное вложение в письме со спамом

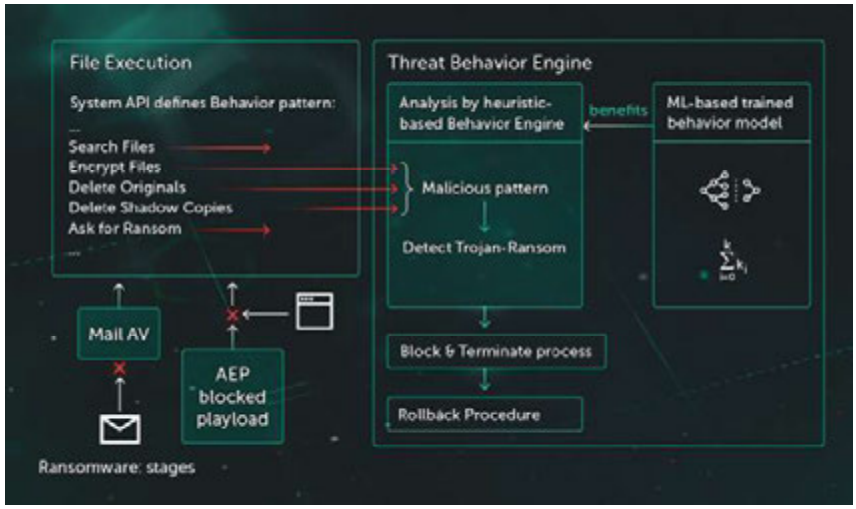
В настоящее время одним из наиболее популярных методов распространения программ-вымогателей является отправка архивов с исполняемыми скриптами по электронной почте (спам). Альтернативный способ – использование в качестве вложений документов Microsoft Office с вредоносными макросами.

Компонент «Почтовый антивирус», входящий в состав продуктов «Лаборатории Касперского», анализирует весь контекст сообщения (включая вложения) и применяет строгий эвристический анализ содержимого.

Этап доставки: использование уязвимости

Автоматическая защита от эксплойтов (AEP) <ссылка на AEP> – это специальный компонент, который препятствует проникновению вредоносных программ (включая программы-вымогатели) через уязвимости ПО. К числу наиболее важных приложений, защищаемых AEP, относятся браузеры, офисные приложения, программы для чтения PDF-файлов и др. Для каждого подозрительного действия упомянутого ПО, такого как запуск дочернего процесса, этот компонент выполняет дополнительный анализ поведения по вредоносным шаблонам.

AEP помогает блокировать программы-вымогатели, включая CryptXXX и множество других.



File Execution	Выполнение файла
System API defines Behavior pattern:	Системный API определяет поведенческий шаблон:
Search Files	Поиск файлов
Encrypt Files	Шифрование файлов
Delete Originals	Удаление оригиналов
Delete Shadow Copies	Удаление теневых копий
Ask for Ransom	Требование выкупа
Mail AV	Почтовый антивирус
AEP blocked playload	Автоматическая защита от эксплойтов (AEP) блокирует атакующий код
Threat Behavior Engine	Ядро для анализа поведения
Analysis by heuristic-based Behavior Engine	Анализ поведения приложений с применением эвристического ядра
Malicious pattern	Шаблон поведения вредоносной программы
Detect Trojan-Ransom	Обнаружение троянской программы-вымогателя
ML-based trained behavior model	Модель поведения, усвоенная на основе машинного обучения
Benefits	Преимущества
Block & Terminate process	Блокирование и завершение процесса
Rollback Procedure	Процедура отката действий вредоносной программы
Ransomware: stages	Программа-вымогатель: этапы действия

В 2017 году мир узнал об использовании сетевых уязвимостей для распространения вредоносного ПО. Программа-вымогатель WannaCry распространялась через уязвимость, характерную для компаний малого и среднего бизнеса. Такой эксплойт можно остановить только на уровне сети. Продукты «Лаборатории Касперского» содержат специальный компонент для анализа сетевого трафика – систему предотвращения вторжений (IDS). Этот компонент анализирует сетевые пакеты на низком уровне и применяет шаблоны эвристического анализа для обнаружения вредоносной сетевой активности. Он успешно обнаруживает эксплойты EternalBlue/EternalRomance, помогая предотвратить заражение программой-вымогателем WannaCry.

Этап выполнения

Злоумышленники пытаются использовать различные способы обхода статических методов обнаружения. В таких ситуациях «Поведенческий анализ» <ссылка на поведение> становится последней, но самой мощной линией обороны. Анализ активности каждого процесса помогает выявлять вредоносные шаблоны. После этого продукт останавливает процесс и выполняет откат вызванных им изменений. Технология выявления на основе поведения эффективно работает даже для ранее неизвестных угроз, включая программы-вымогатели. Основной шаблон действия такой программы состоит из нескольких шагов.

1. Поиск важных файлов на компьютере жертвы
2. Чтение содержимого каждого файла
3. Шифрование содержимого и сохранение изменений на диск

При обнаружении соответствия такому вредоносному шаблону поведения «Модуль анализа поведения» <ссылка на поведение> блокирует процесс и выполняет откат изменений. В качестве примеров успешного выявления программ-вымогателей с помощью такого шаблона можно привести Polyglot, WannaCry (часть вредоносной программы, выполняющая шифрование) и др.

Помимо упомянутого шаблона, для выявления программ-вымогателей может использоваться множество других эффективных против этого типа угроз шаблонов.

Действенность данного подхода была подтверждена в июле 2017 года во время атаки программы-вымогателя ExPetr. Злоумышленники использовали часть вредоносной программы Petya низкого уровня для шифрования основной таблицы файлов (MFT, содержит все файлы, каталоги и метаданные файлов файловой системы NTFS). Для этого запускался компонент верхнего уровня, перезаписывающий основную загрузочную запись (MBR) жёсткого диска. Ядро для анализа поведения отмечает такое поведение как вредоносное и останавливает процесс. Даже если другие злоумышленники создадут подобную программу-вымогатель, она не будет работать, независимо от используемых типов технологий обфускации/препятствования эмуляции.

Программы-вымогатели в целевых атаках

В 2017 году «Лаборатория Касперского» выявила несколько групп злоумышленников, которые атаковали организации с одной главной целью – зашифровать их данные.

Во множестве случаев целевых атак использовались разрешённые утилиты шифрования дисков/файлов. Например, утилита DiskCryptor для шифрования и PSExec для массированной установки через корпоративную сеть. Статические и базовые поведенческие методы выявления будут неэффективны из-за ложных срабатываний при разрешённом использовании этих утилит. В этом случае возникает необходимость сбора и анализа полного **контекста использования утилиты**. В приведённом примере подозрительным может являться шаблон установки разрешённой утилиты для шифрования посредством утилиты PSExec, и соответствующее усиление защиты с помощью продукта позволит предотвратить повреждение данных без излишних ложных срабатываний для других пользователей.

Но вполне возможно, что вы всё же заразились и ваши данные были зашифрованы. Можно ли восстановить файлы без выкупа?

Ответить на этот вопрос чрезвычайно сложно. Потому что это не всегда удаётся. Большинство современных шифровальщиков используют стойкие криптоалгоритмы. Это значит, что расшифровкой можно безуспешно заниматься долгие годы.

Порой злоумышленники допускают ошибки в реализации шифрования или же правоохранительным органам удаётся изъять серверы преступников с криптографическими ключами. В этом случае у экспертов получается создать утилиту для расшифровки.

Если же вы всё же захотите оплатить выкуп, то это придётся делать с помощью криптовалюты – биткойнов. Это такая хитрая электронная наличность, которую невозможно подделать. История транзакций видна всем, а вот отследить, кто хозяин кошелька, очень сложно. Именно из-за этого злоумышленники и предпочитают биткойны. Меньше шансов, что застукает полиция.

Некоторые вымогатели используют анонимные интернет-кошельки или даже вовсе платежи на номер мобильного телефона. Самый экстравагантный способ, когда злоумышленники принимали выкуп исключительно карточками iTunes номиналом $ 50.

Иногда пользователи задают вопрос: «Если не кликать по чему попало и не лазить по интернет-помойкам, то не заразишься?»

К сожалению, шанс «подцепить» вымогателя есть даже у самых разумных пользователей. Например, в процессе чтения новостей на сайте крупного «белого и пушистого» СМИ.

Конечно, само издание вирусы распространять не станет. Как правило, такие заражения происходят через систему обмена рекламными баннерами, к которой удалось подключиться злоумышленникам. И если вы окажетесь на сайте именно в этот момент, а на компьютере есть незакрытая программная уязвимость, но нет хорошего антивируса, считайте, что вам не повезло.

Пользователям Mac

Не стоит считать, что пользователи этой операционной системы заранее защищены. Увы, это не так. Например, пользователей Mac успешно атаковал троянец-вымогатель KeRanger, сумевший вклиниться в официальную сборку популярного торрент-клиента Transmission.

Наши эксперты считают, что со временем вымогателей для устройств Apple будет всё больше и больше. Более того, поскольку сами устройства дорогие, то злоумышленники не постесняются требовать с их владельцев более солидные суммы выкупа.

Есть вымогатели и для Linux. В общем, ни одна из популярных систем от этой «заразы» не избавлена.

Как расшифровать файлы?

Если шифровальщик проник в систему и успел «натворить дел», то просто так файлы вы не расшифруете. Вариантов, по сути, два. Можно, конечно, заплатить выкуп злоумышленникам, но мы этого делать не советуем по вышеуказанным причинам.

Ransomware: data encrypted	Программа-вымогатель: данные зашифрованы

Второй вариант – зайти на сайт noransom.kaspersky.com и www.nomoreransom.org, чтобы посмотреть, нет ли там декриптора, который помог бы расшифровать файлы. Все декрипторы абсолютно бесплатны, но, к сожалению, далеко не от всех шифровальщиков получается создать такое лекарство. Поэтому лучше не доводить до крайностей и защищаться от них заранее.

Контролируемый доступ к папкам в Windows 10

Стоит отметить, что существует функция безопасности в Windows 10 «Контролируемый доступ к папкам», которая также может использоваться как защита от шифровальщиков.

Системные администраторы и обычные пользователи могут управлять функцией «Контролируемый доступ к папкам» с помощью групповых политик, PowerShell или приложения Центр безопасности Защитника Windows.

Эта функция – часть Exploit Guard Защитника Windows.

Функция безопасности защищает файлы от несанкционированного доступа со стороны вредоносных программ. Microsoft позиционирует новую функцию как механизм защиты от троянов-шифровальщиков. Для её работы необходим Защитник Windows и активная защита реального времени. Впервые «Контролируемый доступ к папкам» представлен в Windows 10 версии 1709 (Fall Creators Update) и не является частью более старых версий операционной системы.

Как работает эта функция безопасности?

Все приложения (фактически под приложением в данном случае имеется в виду любой исполняемый файл: .exe, .scr, .dll и другие) проверяются программой Защитник Windows. Если приложение признаётся вредоносным или подозрительным, ему будет запрещено вносить изменения в любые файлы во всех защищённых папках.

Принцип работы данной функции отличается от других инструментов для защиты от программ-вымогателей, антивирусы используют более глубокий проактивный подход при защите важных файлов и папок.

Центр безопасности Защитника Windows

Пользователи Windows 10 могут включать и управлять «Контролируемым доступом к папкам» с помощью приложения **Центр безопасности Защитника Windows**.

1. Для запуска приложения «Параметры» можно использовать сочетание клавиш Win+I.
2. Перейдите в «Обновление и безопасность», затем выберите пункт «Защитник Windows» и нажмите кнопку **Открыть Центр безопасности Защитника Windows**.
3. Выберите панель **Защита от вирусов и угроз**.
4. На открывшейся странице выберите ссылку **Параметры защиты от вирусов и других угроз**.
5. Убедитесь, что «Защита в режиме реального времени» включена.
6. Активируйте переключатель **Контролируемый доступ к папкам**.

После активации функции станут доступны две новые ссылки: «Защищённые папки» и «Разрешить работу приложения через контролируемый доступ к файлам». Если у вас уже установлен сторонний антивирус, то вы не сможете активировать переключатель «Контролируемый доступ к папкам».

Защищённые папки

Список защищённых папок отображается, когда вы нажмёте по одноимённой ссылке. По умолчанию Защитник Windows защищает некоторые папки:

- Пользователь (User): Документы, Изображения, Видео, Музыка, Рабочий стол и Избранное
- Общие (Public): Документы, Изображения, Видео, Музыка, Рабочий стол

Удалить стандартные папки нельзя, но пользователь может добавить любые другие папки для защиты.

Нажмите кнопку «Добавить защищённую папку», затем выберите папку на локальной машине и добавьте её в список защищённых папок.

Разрешить работу приложения через контролируемый доступ к файлам

Всё же иногда возможны ложные срабатывания. В таком случае вы можете добавить приложение, которому хотите разрешить взаимодействовать с защищёнными папками и файлами. Для этого необходимо нажать кнопку «Добавление разрешённого приложения» на странице и выбирать исполняемый файл из локальной системы, чтобы разрешить доступ к защищённым файлам и папкам.

Групповые политики

Вы можете настроить функцию «Контролируемый доступ к папкам» с помощью групповых политик.

Учтите, что данный способ подходит для пользователей Windows 10 Pro. Пользователи Windows 10 Home не могут использовать групповые политики напрямую.

1. В строке поиска введите **gpedit. msc**.
2. Перейдите в Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Антивирусная программа «Защитник Windows» > Exploit Guard в Защитнике Windows > Контролируемый доступ к папкам.
3. Выберите политику «Настройка контролируемого доступа к папкам» и щёлкните по ней дважды.
4. Выберите опцию «Включено».

При этом вам доступны следующие значения параметра:

1. **Выкл (по умолчанию)** – аналогично отключению. Контролируемый доступ к папкам будет неактивен.
2. **Блокировать** – «Контролируемый доступ к папкам» будет активен и защитит объекты от несанкционированного доступа.
3. **Проверять** – доступ будет разрешён, но каждое событие будет записано в журнал событий Windows.

Кроме того, вы можете настроить данную функцию с помощью дополнительных политик:

- **Настроить разрешённые приложения** – включите данную политику, чтобы добавить приложения в список исключений.
- **Настройка защищённых папок** – включите данную политику, чтобы добавить папки для защиты.

PowerShell

- В строке поиска введите **PowerShell** и, удерживая клавиши Ctrl+Shift, выберите объект PowerShell, предлагаемый службой поиска Windows. В результате будет запущена командная строка PowerShell с правами администратора.
- Чтобы изменить статус функции, запустите команду

```
Set-MpPreference
-EnableControlledFolderAccess
Enabled
```

  Можно устанавливать три различных статуса: `enabled`, `disabled` или `AuditMode`.
- Чтобы добавить папки в список защищённых папок, запустите команду

```
Add-MpPreference
-ControlledFolderAccessProtect
edFolders «<папка, которая бу-
дет защищена>»
```

- Чтобы добавить приложение в список исключений, запустите команду

```
Add-MpPreference
-ControlledFolderAccessAllowed
Applications «<приложение,
которое должно быть включено
в список, включая путь>»
```

События функции «Контролируемый доступ к папкам»

Загрузите **Exploit Guard Evaluation Package** с сайта Microsoft (https://aka.ms/mp7z2w) и извлеките его в локальную систему.

1. Нажмите на клавишу Win, введите **Просмотр событий** и выберите одноимённый объект, предлагаемый службой поиска Windows.
2. Выберите Действие > Импорт настраиваемого представления.
3. Выберите извлечённый файл **cfa-events-xml**, чтобы добавить его как пользовательское представление.
4. Нажмите OK в следующем экране.

В пользовательском представлении отображаются следующие события:

1. Event 1123 – события режима «Блокировать».
2. Event 1124 – события режима «Проверить».
3. Event 5007 – изменение настроек.

Самым надёжным способом защиты от шифровальщиков на сегодня является регулярное резервное копирование. Но помните о том, что резервная копия должна осуществляться на внешний жёсткий диск (в облако). При этом хранилище, на которое вы осуществляете копирование, может подключаться как внешний жёсткий диск только на период осуществления резервной копии.

Однако необходимо подчеркнуть, что существует ещё один бесплатный продукт, направленный на защиту от ransomware – Acronis Ransomware Protection. Следует заметить, что для домашних пользователей это бесплатный продукт, основанный на технологии Acronis Active Protection.

Как работает Acronis Active Protection

Acronis Active Protection – это передовая технология защиты от вымогателей. Она полностью совместима с наиболее распространёнными решениями по защите от вредоносных программ, активно защищает все данные в системах, включая документы, файлы мультимедиа, программы и многое другое, даже файлы резервного копирования Acronis.

Распознавание паттернов

Acronis Active Protection постоянно наблюдает за изменениями файлов данных в системе. Один набор поведений может быть типичным и ожидаемым. Другой набор поведений может сигнализировать подозрительному процессу о принятии враждебных действий против файлов. Подход Acronis анализирует эти действия и сравнивает их со схемами вредоносного поведения. Этот подход может быть исключительно мощным в выявлении атак вымогателей, даже тех, о которых пока не сообщают антивирусные компании.

Белый и чёрный списки

С помощью данного подхода программа способна обнаруживать новые угрозы на основе уже определённых и изученных шаблонов. Результаты должны быть скорректированы, чтобы уменьшить вероятность ложного обнаружения тех продуктов, которые на самом деле не являются вымогателями. Acronis Active Protection поддерживает белый список – программы, которым разрешено и ожидается выполнение определённых действий – для предотвращения ложной пометки авторизованных действий как несанкционированных.

Самозащита файлов резервных копий

Один из способов, с помощью которого злоумышленники могут пойти на компрометацию файлов, – это атаковать само программное обеспечение резервного копирования, чтобы испортить созданные им файлы. Для защиты от этого в Acronis реализован надёжный механизм самозащиты, который не позволит преступникам нарушать работу приложения Acronis или резервное копирование содержимого файлов.

Кроме того, Acronis Active Protection отслеживает основную загрузочную запись компьютеров под управлением Windows. Это не позволит внести какие-либо незаконные изменения, чтобы помешать правильно загрузить компьютер.

Актуальное восстановление атакованных файлов

Если вымогатель начинает шифровать файлы, Acronis быстро обнаруживает и останавливает этот процесс. Поскольку Acronis является решением для резервного копирования, любые данные, которые были раскрыты и зашифрованы до остановки процесса, могут быть восстановлены из различных источников резервного копирования. Мало того, что альтернативные решения для защиты от вымогателей обычно не только заканчивают атаку после её начала, но и не имеют возможности восстановить любые зашифрованные файлы. Acronis Active Protection обнаруживает и отклоняет атаки, а также восстанавливает файлы любого размера.

Запомните, лучшая защита от ransomware – это вовремя созданные резервные копии. Не забывайте их регулярно создавать!

Владимир Безмалый
Kaspersky Certified Trainer

Автоматизация бизнеса как средство повышения качества обслуживания клиентов

Business Automation (также известная как Business Process Automation или BPA) – это, по сути, замена всех бизнес-процессов интеллектуальными автоматизированными системами. Встроенные инструменты аналитики позволяют максимально эффективно и точно в срок преобразовать всё то, что вы бы делали «вручную».

Автоматизируйте свой бизнес с помощью интеллектуального программного обеспечения.

С его помощью вы сможете получить ряд значительных преимуществ:

- большая производительность;
- повышение эффективности;
- возможность отслеживания всех бизнес-процессов;
- интеллектуальная автоматизация на основе алгоритмов;
- снижение нагрузки;
- экономия времени и сил персонала;
- сокращение времени рабочего цикла;
- минимизация человеческой ошибки;
- возможность более эффективно документировать результаты;
- повышение качества и согласованности услуг;
- более прозрачный и эффективный процесс аудита;
- сокращение времени выполнения заказов;
- увеличение лояльности клиентов.

Важно помнить, что даже самые автоматизированные бизнес-процессы требуют участия человека и их совместной работы. Когда люди вовлечены в процесс, им нужны инструменты, которые позволяют сотрудничать и отвечать на вопросы. Включение таких инструментов, как обсуждение, позволяет заинтересованным сторонам общаться напрямую, будь то до, во время или в конце процесса. Необходимым аспектом оптимизации бизнес-процессов является интеллектуальная автоматизация на основе выработанных правил – это приложение, которое работает с системой автоматизации бизнеса и автоматически принимает решения на основе заданных алгоритмов. Решения обычно включают в себя переход к конкретной задаче и назначение её исполнителя или действию в определении рабочего процесса.

Интеллектуальные инструменты могут помочь повысить эффективность бизнес-процессов, но полностью автоматизированное функционирование может в конечном итоге привести к неожиданным результатам. Необходимо соблюсти баланс автоматизации и непосредственной работы сотрудников.

Автоматизация бизнес-процессов позволяет анализировать их показатели. Функция аналитики необходима как для оценки существующего положения компании, так и для выработки стратегии её развития. Бизнес-показатели, связанные с автоматизированными процессами, хранятся в базе данных. Отчёты и необходимая информация отображаются в режиме реального времени. Также можно составить план распространения данных в срок, когда они необходимы. Очень удобны в использовании визуальные отчёты и информационные панели. С помощью панелей инструментов можно отслеживать общий прогресс всей команды и эффективность бизнес-процессов для обеспечения их улучшения.

Если вы сомневаетесь в возможностях автоматизации бизнес-процессов, подумайте о том, к каким результатам приведёт её внедрение.

- Улучшение качества выполняемых работ

Когда вы автоматизируете свой бизнес, нагрузка на сотрудников уменьшится, и они смогут направить силы на реализацию других бизнес-процессов.

- Повышение удовлетворённости сотрудников

Некоторые бизнес-процессы чрезвычайно сложны, и если вы оставите их на усмотрение сотрудников, это может лишить мотивации. С автоматизацией ситуация станет обратной.

- Минимизация ошибки из-за человеческого фактора

Когда все бизнес-процессы лежат на плечах сотрудников, ошибки неизбежны. Автоматизация бизнеса поможет устранить их, обеспечивая достижение поставленных задач и получение необходимого результата.

Бизнес постоянно сталкивается с внешним давлением, которое нужно преодолевать, чтобы быть успешным. Это давление становится более очевидным в нынешнее экономически нестабильное время. Моделируя и оптимизируя бизнес-процессы, компании оставляют больше времени для выполнения ряда важных задач. Автоматизация бизнес-процессов помогает устранить потери времени и других ресурсов, затрачиваемых на обдумывание процедур, которые могли бы быть выполнены более эффективно. Она приносит пользу не только сотрудникам (уменьшение рабочей нагрузки), но и компании (увеличение итоговых показателей).

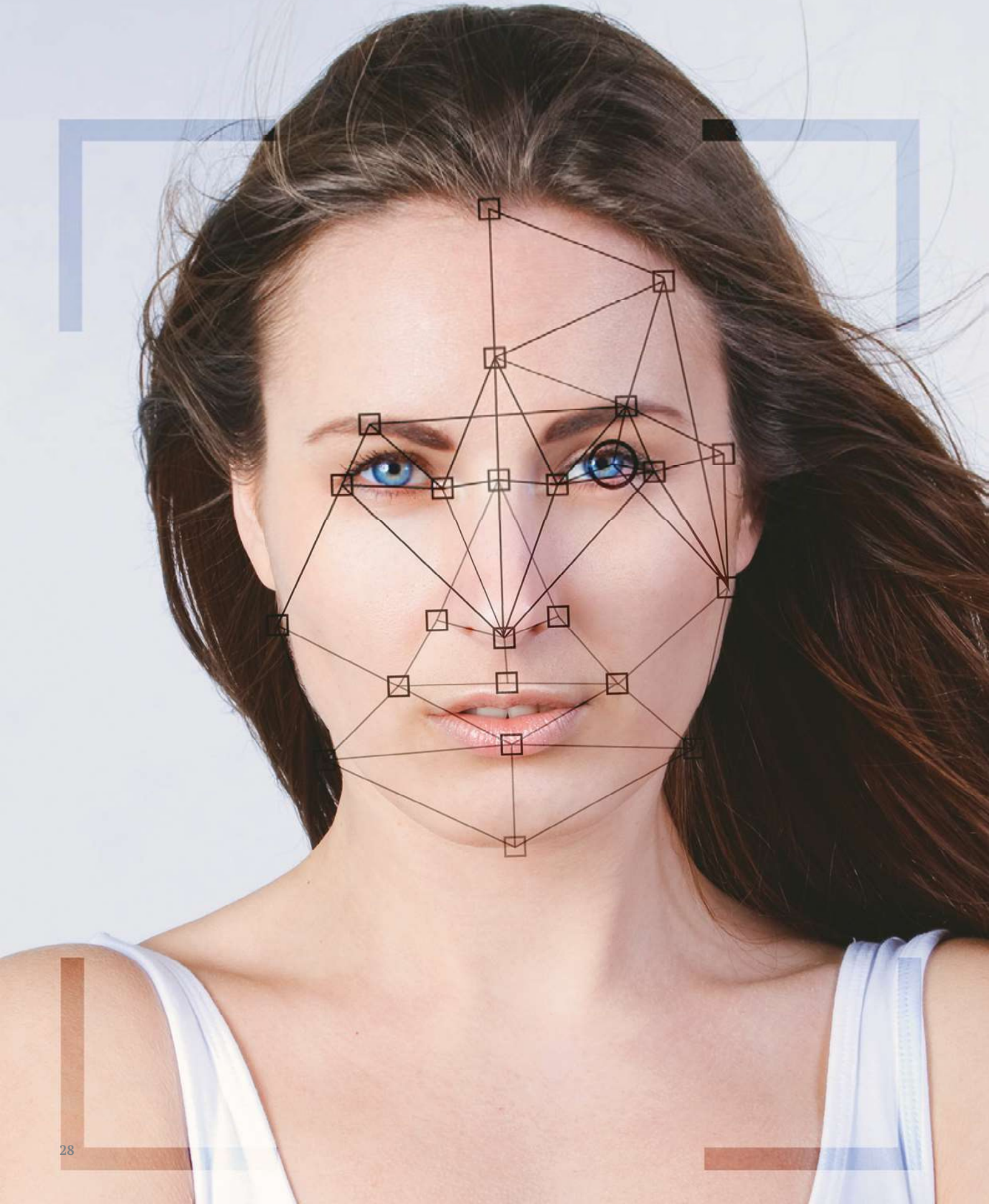
Специалисты компании «АСТР» помогут проанализировать ваш бизнес и предложат пути автоматизации, исходя из принципов бизнес-обоснованности.

АСТР IT

info@astr-it.ru

www.astr-it.ru

Технология распознавания лиц



Распознавание лиц — наиболее проверенный способ защитить устройство от посторонних. Этот метод обеспечивает надёжность и точность проверки человека. В некотором роде это современная наука о личности.

Универсальность и удобство – основные факторы, которые делают распознавание лица ключевым элементом в системе защиты вашего устройства. С этим способом телефону обеспечена безопасность на любой сезон. Лицо считается самым гибким инструментом для аутентификации. Его можно использовать всегда, в разных условиях и без датчиков. Современные технологии постоянно совершенствуются, а сочетание высокого уровня безопасности, гибкость и мобильность способствуют популярности и распространению данного способа защиты.

Несмотря на то, что технологию распознавания лиц дополняют другие меры безопасности (логин и пароль, контрольные точки безопасности), этот метод имеет свои недостатки. В криминальном триллере «Без лица» Джона Траволты и Николаса Кейджа разыгрывается сценарий смены лица. Это, конечно, вымысел, но опасения по поводу того, что ваше лицо может быть украдено, ненадуманные. Подобные ситуации уже осуществлялись в прошлом. Разберёмся с некоторыми проблемами технологий более низкого уровня, связанными с безопасностью. Также разберём поэтапно развитие противостояния этим угрозам.

Торговые места

Имея более ранние интеграции распознавания лиц и воспользовавшись фотографиями, видео и 3D-масками, мошенники смогли бы провести даже камеры. В боевике «Без лица» показан идеальный сценарий по смене лица. Такой план позволил Траволте стать персонажем Кейджа. Это было настолько убедительно, что поверили даже родные. С возникновением распознавания лиц этот план с лёгкостью подделал бы базовые последовательности ранней технологии.

В наше время система по распознаванию лиц – биометрия – очень быстро развивается. По данным распознавания находят и проверяют человека. Для этого нужна уникальная личная информация. Как правило, она специфична для каждого человека. В отличие от привычных для нас методов удостоверения личности – предъявления паспорта, водительских прав, пенсионного удостоверения – её подделать крайне сложно. Система проверяет и ищет совпадения среди набора биометрических идентификаторов: расстояние между глазами, их форма и цвет, переносица, контур губ.

Также существует метод обнаружения «живучести». Он занимается поиском индикаторов неживого изображения (например, несовместимость переднего плана и фона). Если возникают сомнения в идентификации, человека, его просят моргнуть или перейти в другое место. Эти методы нужны для того, чтобы преступники не смогли обмануть систему распознавания лиц с помощью маски или фотографии.

Спящая угроза

После принятия Face ID одной из распространённых проблем производителей телефонов стала возможность разблокировки мобильного устройства, наведя его на лицо человека, который спит. С этого момента появились опасения о принудительной аутентификации. Человека можно заставить пройти её, держа устройство у его лица.

Этот фактор может стать существенным недостатком в системе безопасности. Но многие производители телефонов предугадали такую ситуацию. Например, IPhone можно разблокировать, только если у пользователя открыты глаза. Это помешает взломать телефон во время сна его владельца. В связи с постоянным прогрессом в технологиях, разрабатываются новые способы противостояния биометрическим мошенникам. Также должна подстраховать система обнаружения «живучести», проверяющая мигание и движения лица.

Существует ещё один способ избежать принудительной аутентификации. Нужно использовать распознавание лица как один из элементов процесса идентификации. Для низкого уровня безопасности может подойти только распознавание. Но для высокого – можно установить многофакторную аутентификацию. Например, добавить пароль и отпечаток пальца. Для увеличения степени защиты можно заблокировать как всё устройство, так и отдельные его приложения.

Преимущества технологии распознавания лица

Благодаря развитию технологий камер, картографирования и скорости обработки, распознавание лица стало одним из основных методов в процессе аутентификации для мобильных устройств. За последнее время эта новая разработка полюбилась многими пользователями.

Для выполнения и поддержки распознавания лица компания Thales предлагает проверенный набор аппаратных и программных инструментов мирового уровня. Система работает на основе биометрических показателей и анализа отпечатков пальцев.

С помощью новых технологических решений идёт борьба с мошенниками и расхитителями личных данных. Биометрия быстро стала наиболее подходящей системой для аутентификации. У Thales в наличии полный набор для сбора, управления и проверки биометрических данных. В наше время инструменты распознают лица класса: 1-к-1,1-к-N. Вместе с анализом отпечатка пальцев поддерживают технологии биометрического сравнения.

Производители смартфонов сделали возможным разблокировку телефона с помощью распознавания лица. Преимущества этого решения очевидны: уменьшение случаев мошенничества с гаджетами и увеличение комфорта пользователей. Технология распознавания лица как эффективный и популярный метод аутентификации обладает возможностью продвигать другие не менее действенные и неожиданные способы. Рассмотрим некоторые из них.

Консервация

В рамках борьбы с незаконной торговлей шимпанзе и другими животными индустрия консервации недавно ввела в пользование новое программное обеспечение. Оно идентично с тем, что распознаёт лица людей на фотографиях в социальных сетях. В этом случае морду шимпанзе, живущего в дикой природе, фотографируют с разных ракурсов. После этого его «лицо» вносят в базу данных с помощью прямоугольника вокруг группы изображений, которые потом объединяются. Затем в соци-

альных сетях происходит поиск «лица» обезьяны из составленной базы. В случае если технология распознаёт жертву торговли, владельцы страниц, на которых изображён шимпанзе, могут преследоваться законом. На чёрном рынке такую обезьяну продают за 12500 долларов. Соответственно, можно предположить, что подобных преступников велико. По результатам исследований, ежегодно в результате торговли пропадает 2000 шимпанзе.

Этот способ использовался и в отношении других животных, находящихся под угрозой вымирания. Например, это красно-пузатый лемур. Программное обеспечение под названием LemurFaceID распознавало образ животного. Таким образом облегчалась жизнь исследователей, которые изучали жизнь и популяцию особей лемуров. С помощью этой технологии они определяли, насколько долго может прожить животное в условиях дикой природы, как часто они размножаются, рост и уменьшение их численности. Проверено, что данное программное обеспечение определяет лемуров с точностью до 97%. Многие защитники природы надеются, что с развитием и усовершенствованием технологий, люди смогут использовать их во благо и с целью защиты животных.

Лояльность клиентов

Для розничных продавцов отличным шансом превратить нерегулярных покупателей в постоянных является технология распознавания лица. Для того чтобы человека сразу же узнавали в его любимых магазинах, необходимо быстро расставить приоритеты. Например, при входе в кофейню бариста предлагает заказ, основанный на истории посещений постоянного клиента. Таким принципом руководствуются ритейлеры.

Также одним из способов повышения благосклонности клиента будет предложение VIP-услуг, как только он входит в магазин. Например, покупатель, который пришёл за изделием только из натуральных материалов понятия не имеет, где они располагаются. Однако специалист по обслуживанию клиентов при наличии разрешения на мгновенное распознавание лица, может получить предупреждение заранее и вовремя дать полезную консультантацию. Таким образом, увеличивается вероятность осуществления покупки.

Ещё одним вариантом для завоевания благосклонности и доверия покупателей станет полученная ими возможность пропускать очередь, используя своё лицо. Это сделает процесс осуществления покупок значительно легче, быстрее и комфортнее. Одним из наглядных примеров, показывающих, как работает эта технология, стал магазин Amazon Go. Здесь автоматически определяется, когда товар взяли или вернули на полку. Покупки отслеживаются в виртуальной корзине. Закончив совершать покупки, человек может спокойно возвращаться домой. Позже ему придёт квитанция по заказу. Оплата происходит с помощью личного аккаунта в Amazon.

Здравоохранение

Технология распознавания лиц также активно применяется в сфере здравоохранения. С помощью этой системы можно помочь как диагностике, так и лечению. AiCure создала приложение, в котором, благодаря распознаванию лиц, люди могут принимать препараты в соответствии с предписаниями врача. Приложение находит пациента и определяет назначенный медикамент. После этого необходимо снять, как пациент принимает препарат. Приложение визуально подтверждает, что лекарство было принято. Таким образом, врач может отслеживать и изучать отметки по времени, делать выводы о добросовестности пациента и целесообразности назначенного лечения.

Исследователи из Национального института исследования генома человека в Америке также нашли успешное применение программному обеспечению технологии распознавания лица. Они используют его для диагностики синдрома ДиДжорджа. Эта болезнь, начиная с рождения, может вызвать множество проблем на протяжении всей жизни человека. Возможны физиологические и интеллектуальные дефекты. При осуществлении правильной диагностики в 96,6% случаев было выявлено 126 индивидуальных особенностей.

Listerine – бренд для полоскания рта – изобрёл мобильное приложение в помощь слепым людям. Благодаря технологии распознаванию лиц, люди с ограниченными возможностями могут узнать, кто им улыбается. Приложение проводит сканирование лица и подаёт звуковой сигнал и вибрацию, обозначающие улыбку находящегося рядом человека.

В мире биометрии распознавание лица набирает свою популярность. Технология получает хвалебные отзывы и критику, связанные с этикой, стоящей за её использованием. Она может упростить и улучшить жизнь не только людей, но и других существ во всём мире.

Live Face Identification System

LFIS – это новое биометрическое решение для распознавания лиц. Его изобрела компания Thales. В основе алгоритма LFIS лежат глубокие нейронные сети. Они обеспечивают точность обнаружения, отслеживание и распознание лиц. Система имеет возможность обрабатывать видео в режиме воспроизведения и реального времени без оператора.

LFIS предлагает свои разработки для разных областей использования. Технология распознавания лица может быть легко включена в системы контроля допуска на границе, контроля внутренних передвижений и поездок, проверки идентификаторов безопасности и видеонаблюдения.

Задачи LFIS

Уровень безопасности повышается за счёт:

- обработки всех камер параллельно
- мгновенного получения оповещений
- быстрого и безопасного доступа
- использования метода «живучести»
- быстрого автоматического анализа видео
- возможности локального распознавания лиц

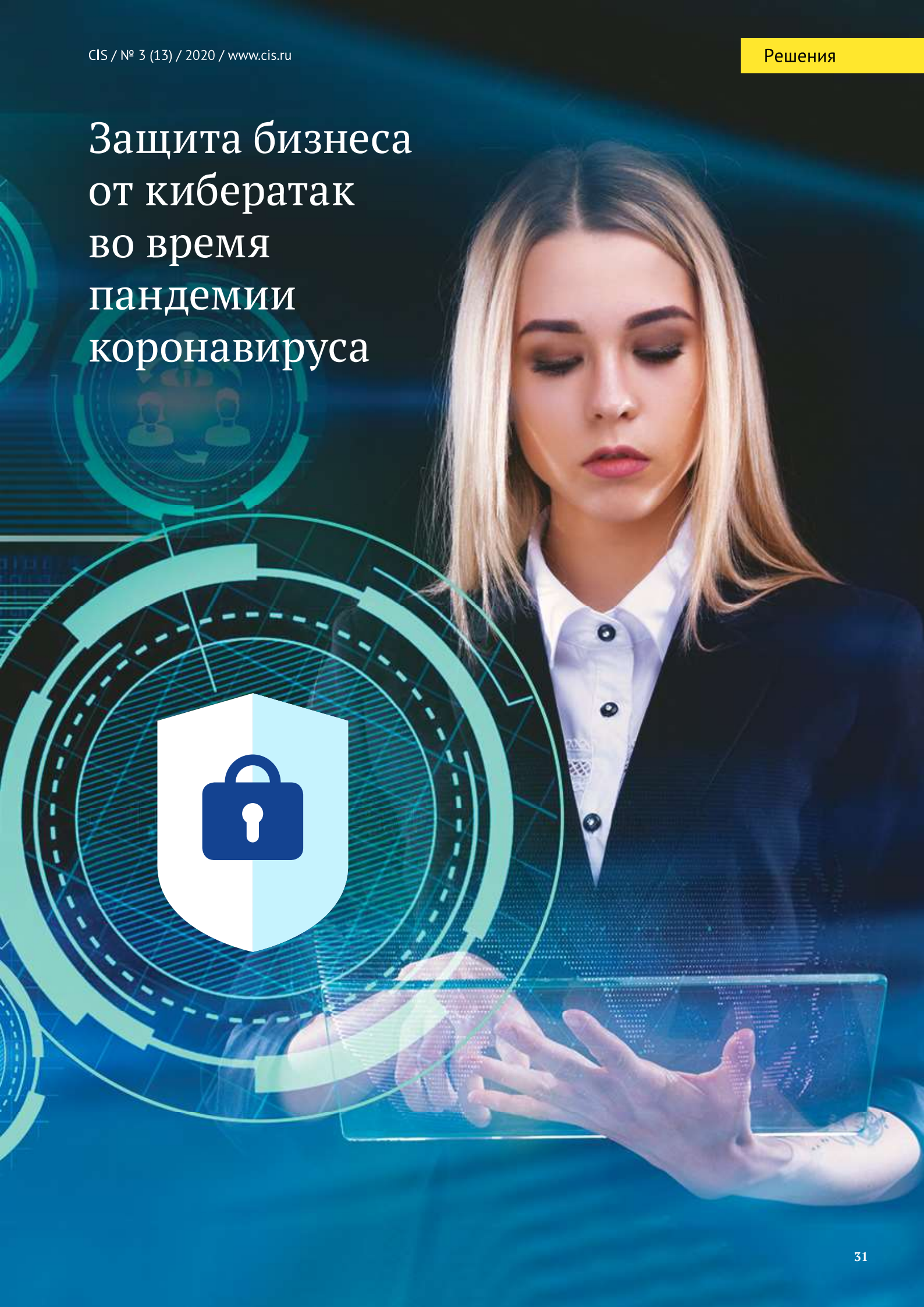
Покупатели и партнёры могут с лёгкостью создавать приложения на основе LFIS. Данное программное обеспечение работает на нескольких платформах: локально, в облаке, гаджетах и других типах встроенной среды.

TESSIS
TECHNOLOGIES SYSTEMS AND SOLUTIONS FOR INFORMATION SECURITY

TESSIS – официальный дистрибьютор в России.

www.tessis.ru

Защита бизнеса от кибератак во время пандемии коронавируса



Во время распространения коронавирусной инфекции хакеры пытаются найти способы взломать ИТ-системы крупных и средних компаний, тем самым получив доступ к их данным. Они используют COVID-19 как идеальную возможность совершать кибератаки, особенно для компаний, чья деятельность частично или временно приостановлена. Поэтому владельцы предприятий должны крайне внимательно относиться к существующим рискам и принимать все необходимые меры, которые помогут защитить себя от хакеров.

Сейчас многие предприниматели больше заинтересованы поддержкой работы своего бизнеса. Главная их цель – любыми способами продолжить работу после отмены режима повышенной готовности, самоизоляции и не понести финансовых убытков. Большинство забывает о кибербезопасности, ставя под угрозу свой бизнес и работу сотрудников. Это можно понять, ведь удалённая работа непривычна для индивидуальных предпринимателей и крупных компаний. Но, если вовремя не уделить особое внимание кибербезопасности, можно стать ловушкой для хакеров и понести значительные убытки.

Во время распространения коронавируса работа через интернет становится на первом месте. По большому счёту это единственный способ держать бизнес на плаву и не уйти в минус. Владельцы предприятий всё чаще переносят данные в облачное хранение для быстрого доступа с любого персонального компьютера. Именно поэтому обеспечение безопасности удалённой информации является важным этапом.

Чтобы бороться с хакерами, «наживающимися» на пандемии, была создана международная организация COVID-19 CTI League. В неё вошло более 400 добровольцев, которые имеют теоретические и практические знания в сфере кибербезопасности. В основном специалисты будут защищать медицинские учреждения и объединения, которые непосредственно борятся с COVID-19. Также организация активно работает с компаниями, специализирующимися на предоставлении услуг связи, поскольку именно такие предприятия обеспечивают бесперебойную работу всех остальных.

Международная группа добровольцев COVID-19 CTI League изучает новые тактики, которыми пользуются хакеры в разгар пандемии. Основные из них – это социальная инженерия и фишинговые атаки. Разберёмся более детально, как можно защитить свой бизнес от мошенников, и что представляют собой эти атаки.

Фишинг

Специалисты организации рассказали о «никогда не замеченном» распространении фишинговых сообщений. Они предназначаются для распознавания логинов и паролей для входа на сайты. Если пользователь «повёлся» на такой «развод», у мошенников появляется доступ к учётным записям, почте, банковским данным и другим личным аккаунтам. Это позволяет им контролировать конфиденциальную информацию, действия с нею и совершать операции без ведома владельца. Пользователь может понести крупные финансовые убытки и не только.

Каждый, кто не желает стать жертвой кибератаки, не должен отвечать на такие сообщения, особенно, если в них запрашивают личные данные, пароли из СМС-сообщений, которые приходят на телефон. Необходимо сравнить номер, с которого послано сообщение, с официальным номером банка. Если замечены расхождения, ни в коем случае нельзя отвечать или перезванивать. Также рекомендуется проверить наличие антишпионских или антивирусных программ у компании для защиты личных данных и другой информации во всемирной сети.

Социальная инженерия

Под этим термином подразумевается психологическое воздействие на человека при помощи определённых манипуляций, которые помогают мошенникам получить личную информацию о пользователях интернета. Чаще это мелочи, на которые мы не обращаем внимания в повседневной жизни. Ситуация, которая происходит в настоящее время, может негативно обернуться для большинства предпринимателей.

Приведём пример. Не так давно глобальная кибератака отразилась на людях, которые искали данные о распространении коронавирусной инфекции на просторах интернета. Программа мошенников скрывалась в картах, которые показывали статистику о количестве заражённых по всему миру, в том числе и в Российской Федерации. Более того, эти карты скачивались из официальных источников, которые, как казалось, вызывают минимум подозрений даже у продвинутых «юзеров». Пользователям сайта предлагалось скачать приложение с вредоносным программным обеспечением. Именно это скомпрометировало гаджеты и предоставило хакерам доступ к скрытой информации и сохранённым паролям.

Каждый интернет-пользователь должен внимательно относиться к защите своей конфиденциальности: не нажимать на ссылки, которые присутствуют в электронных сообщениях, если неизвестно их происхождение, а URL-адрес незнаком; не заходить на подозрительные сайты, особенно, если о вирусах напоминает антивирус, установленный на персональном компьютере или другом устройстве (планшет, телефон). Необходимо помнить, что виртуальные, цифровые вирусы распространяются быстро и несут негативные последствия.

Как сохранить данные, работая удалённо

Пандемия коронавируса обязала большинство владельцев предприятий перевести своих сотрудников на удалённую работу. Теперь деятельность компаний проходит в интернет-пространстве и зависит от него: сообщения, видеозвонки, распространение рекламы. Именно поэтому сейчас атаки хакеров, получив доступ к данным компании, могут иметь самые ужасные последствия.

Существует несколько рекомендаций, как защитить себя от мошенников, работая на дому:

- поставить на Wi-Fi сложный пароль, состоящий из букв и цифр, проверить, корректно ли работает антивирус

- не указывать в качестве пароля одинаковые комбинации для всех посещаемых сайтов: именно так мошенникам будет проще попасть в личные кабинеты и завладеть данными
- пользоваться только надёжным VPN для входа во всемирную сеть
- если в доме присутствуют интеллектуальные устройства (термостаты, динамики или другая техника), обязательно сменить заводские пароли на новые, более сложные и практичные
- если нужно сделать телефон раздатчиком Wi-Fi, очень важно придумать сложный пароль с использованием цифр и букв верхнего и нижнего регистра, чтобы предотвратить взлом хакеров и доступ посторонних лиц к интернету.

Также можно воспользоваться уже готовым решением **SafeNet Authentication Service** от компании Tessis. Оно создано для организации двухфакторной (многофакторной) аутентификации на базе одноразовых паролей. Одноразовые пароли могут использоваться самостоятельно как замена статическим паролям, так и совместно с ними для усиления функции аутентификации. Решение SafeNet Authentication Service представлено в двух редакциях: локальная, устанавливаемая непосредственно внутри компании, и облачная – предоставляемая заказчику как сервис по информационной безопасности.

Решение позволяет выполнять интеграцию с внешними сервисами и приложениями, используя готовые агенты, стандартные протоколы RADIUS и SAML. Основными преимуществами решения SafeNet Authentication Service являются:

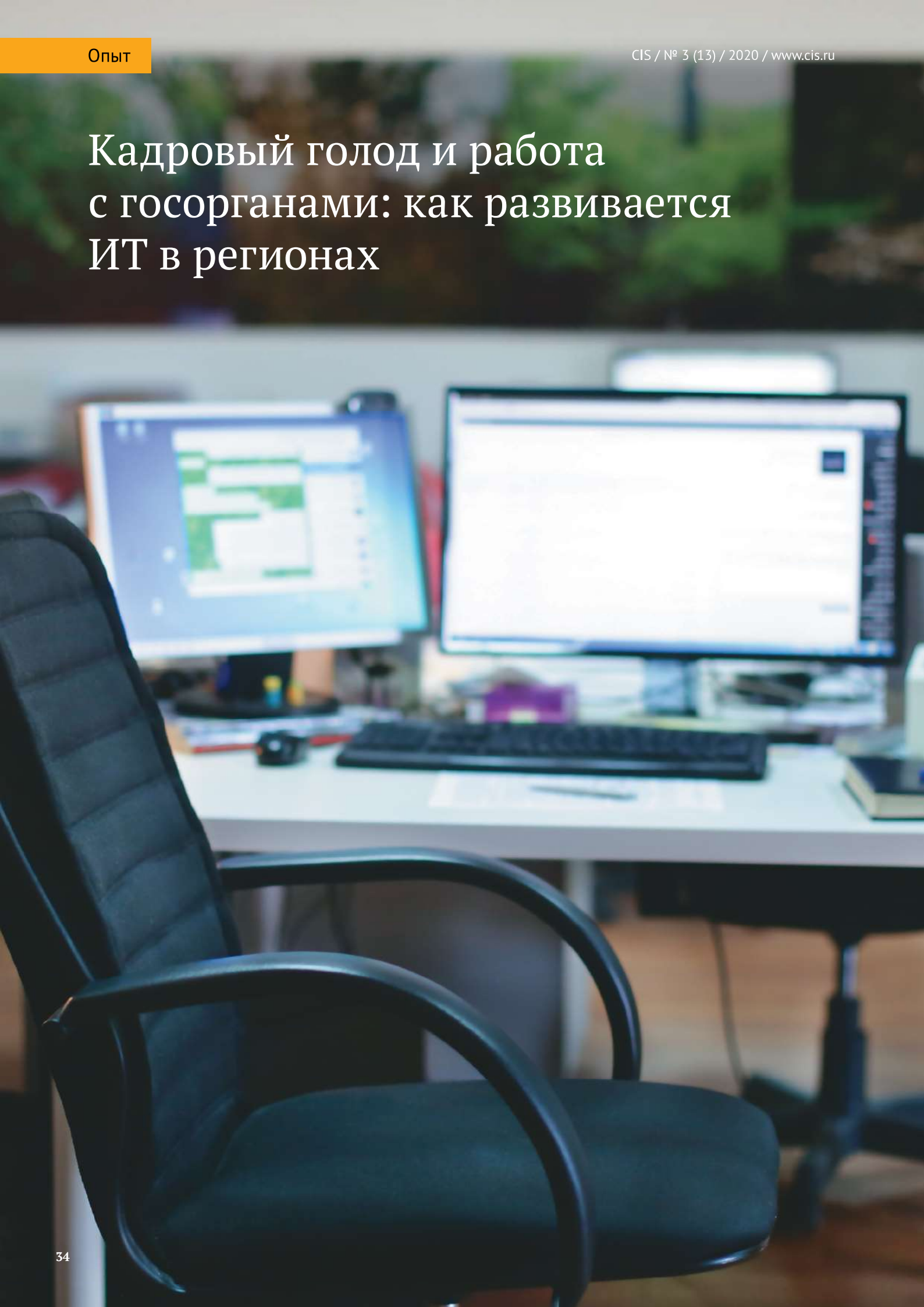
- широкая линейка аутентификаторов (аппаратных, программных с поддержкой технологии PUSH OTP, доставка в виде SMS или на почту, графического GridSure)
- архитектура Multi-tier multi-tenant, позволяющая на одной инсталляции SafeNet Authentication Service создавать независимые серверы аутентификации. Это сохраняет логическую структуру предприятия, определив требования по безопасности в части аутентификации для различных подразделений компании
- автоматизация процессов. SafeNet Authentication Service позволяет автоматизировать процесс назначения и отзыв аутентификатора пользователям в зависимости от выполнения условий принадлежности той или иной группе. Также решение может автоматизировать процесс аудита, обеспечивая плановую доставку отчётов как в решение SafeNet Authentication Service или на почту, так и во внешние системы – журнал регистрации событий Microsoft, текстовый файл или систему syslog.

Характеристики

Кибербезопасность – это важный и, пожалуй, основной аспект в сохранении бизнеса, тем более, когда речь идёт о пандемии коронавируса в больших масштабах. Знать о возможных способах мошенничества и уметь их предвидеть – это главное решение проблемы. Обеспечив кибербезопасность удалённой работы, владелец компании помогает своему бизнесу процветать, независимо от сложившихся мировых обстоятельств.

Поддерживаемые ОС	Windows Server 2008 R2 SP1 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 (64-bit)
Поддерживаемые базы данных	PostgreSQL 9.6 (PostgreSQL 9.6.4) MS SQL 2008, MS SQL 2012, MS SQL 2014, MS SQL 2016
Поддерживаемые LDAP директории	Active Directory Novell eDirectory 8. x SunOne 5.3
Поддерживаемая архитектура	64-бит
Поддерживаемые RADIUS протоколы	PAP MSCHAPv2
Дополнительные программные компоненты	Internet Information Services (IIS) 8.5 .NET 4.6.2 .NET Framework 3.5 Features
Компоненты MySQL	MySQL Connector 6.9.9
Процессоры	2.6 ГГц или выше
Память	16 Гб оперативной памяти или выше
Дисковое пространство	300 Мб

Кадровый голод и работа с госорганами: как развивается ИТ в регионах



Вячеслав Кислицын
Коммерческий директор компании Reactive

Сергей Калагин
Руководитель проектов компании Reactive

С какими вызовами имеют дело региональные ИТ-компании в России, как они выходят на федеральный и международный рынок и что изменилось на фоне пандемии? Об этом рассказали Вячеслав Кислицын и Сергей Калагин – эксперты пермской компании Reactive.

Поиск и сохранение кадров

На российском рынке дефицит специалистов, компаниям приходится буквально охотиться за ними. В Пермском крае около 1700 ИТ-компаний, а свободных профессионалов не хватает. По данным «Обзора рынка ИТ-вакансий» 2019 года от «Яндекс», спрос на ИТ-специалистов в Перми растёт быстрее всего в России. Москва – лишь вторая по темпам роста.

Именно в Пермском крае появились некоторые успешные ИТ-продукты. Например, виртуальная доска Miro. Ею пользуются как международные компании вроде Netflix, Twitter, Spotify, так и обычные учителя, репетиторы.

В Reactive сейчас два типа специалистов: штатные и на аутстаффинге. Общая численность колеблется от 50 до 70 человек, в зависимости от количества и масштаба проектов. Штатные сотрудники – основа команды. Это около 30 человек: разработчики, бэкенд-специалисты, фронтенд-специалисты, аналитики, дизайнеры, менеджеры. Компании всегда необходимо иметь возможность реализовывать большой проект своими силами.

Конкуренция за кадры не ограничивается пределами региона: часть специалистов переходит во «ВКонтакте», «Яндекс» или зарубежные компании. Местным игрокам приходится изобретать свои способы сохранения сотрудников. Зарплаты, хоть и выше средних по региону, но всё же не могут соревноваться со столичными доходами и возможными заработками за границей. Психологический комфорт, атмосфера взаимного доверия, гибкий график, полное покрытие расходов на профессиональное обучение – вот возможные инструменты укрепления корпоративной среды.

Сотрудничество со специалистами на аутстаффинге – это подушка безопасности на случай кризиса и дополнительный ресурс для компании. За их работу необходимо платить больше, потому что есть посредник. Кроме того, договорённость может быть об оплате «фулл-тайм», вне зависимости от простоев и наличия рабочих задач. В такой ситуации компания заработает меньше, однако в случае кризиса может просто не брать внешние команды на проект.

Взаимодействие с клиентами

ИТ-компании имеют дело с несколькими категориями клиентов, а именно: с сектором B2B, малым бизнесом, государственными структурами и крупными ИТ-компаниями, которые разрабатывают свой продукт.

Политика взаимодействия может быть разной. Есть региональные игроки, которые ориентированы на сотрудничество с малым и средним бизнесом, создание корпоративных сайтов и реализацию небольших проектов. Но перспективы роста более реальны в другом направлении: в работе с крупными компаниями и государством.

В сотрудничестве с госструктурами есть определённые риски, среди которых жёсткие сроки и сверхурочные работы, демотивация сотрудников, штрафы до 30% от общей стоимости проекта, попадание в реестр недобросовестных предпринимателей, отсутствие предоплат. Компания должна иметь возможности, достаточные для продолжительной реализации проекта на собственные деньги. Но далеко не всем подходит такой формат. Среда низкоконкурентна, но имеет свою специфику, в основе которой – тендерная система.

Reactive сотрудничает в основном с местными структурами: Правительством Пермского края, Администрацией Перми. Кроме того, работает с Московской областью и Камчаткой. Но найти заказы за пределами своего региона непросто: всё завязано на тендерах, а технические задания к ним могут быть специфичны. В каждом регионе уже есть свои компании, которые заточены под эти госзаказы.

Крупные компании, которые занимаются собственным web-продуктом (такие как «Яндекс»), интересны в качестве партнёров. Но работа на условиях подряда имеет свой недостаток: невозможность использовать результат в портфолио. Поэтому для некоторых региональных web-студий в приоритете работа над проектами, в которых всё – от аналитики до дизайна – будет сделано своими силами.

Как происходит поиск клиентов? Многое зависит от личного подхода менеджеров и руководителей компании. Часть клиентов приходит по знакомству. Работает и так называемое «сарафанное радио», когда клиенты идут, увидев успешную реализацию другого проекта. Дополнительно подключаются инструменты SMM, бренд-маркетинг, контент-маркетинг, холодные продажи. Ещё один вариант – форумы, на них бывает организована биржа деловых контактов. Отдельный поток заказчиков приходит с сайтов профильных рейтингов. Например, театры предпочтут обратиться к тем, кто уже зарекомендовал себя в области культуры и искусства. Одним из самых эффективных рейтингов в этом смысле считается «Тэглайн». Клиенты часто ориентируются на середину списка, чтобы соотношение между ценой и качеством было оптимальным.

Как повлияла пандемия коронавируса и что будет дальше?

Сфера ИТ оказалась самой подготовленной к переходу на дистанционный режим: часть специалистов работали удалённо и раньше.

Небольшие компании проявили гибкость и достаточную адаптацию, в то время как крупные порой испытывают затруднения в коммуникации и контроле процессов.

Студии, работающие по Agile (это гибкие методологии разработки программного обеспечения), перенесли их на виртуальную коммуникацию: ежедневные утренние созвоны, интернет-планёрки, закрытые созвоны для менеджеров. Всё это способствует эффективной организации труда небольших творческих групп.

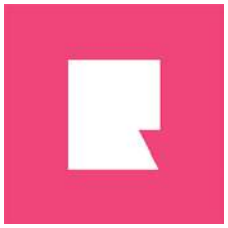
На Reactive пандемия, конечно, тоже повлияла. От компании ушли несколько крупных клиентов, потому что их индустрия сильно пострадала. Это была сфера общественного транспорта и грузоперевозок.

Если говорить о перспективах развития регионального ИТ-сектора в будущем и о том, что будет после пандемии, то лучшим решением станет ориентация на сотрудничество с государством и крупными компаниями. Есть ощущение, что это единственно верный курс, после того как остальной бизнес практически вымер, а тот, что жив, пользуется готовыми конструкторами сайтов. Кроме того, в Reactive стараются отдавать предпочтение технически сложным проектам и параллельно разрабатывать свой продукт.

По мнению эксперта, между московской ИТ-студией и пермской нет глобальных принципиальных различий. Многие компании-разработчики, которые запускались в начале нулевых и выжили, находятся в ТОП-20 России в своей категории. Основатели некоторых веб-студий не пошли на федеральный рынок: в регионе было достаточно клиентов, и они сидели спокойно. В результате это отразилось на узнаваемости. Они менее известны. А процессы, технологии, специалисты – на том же уровне, что и в московских студиях. Далеко не все профессионалы имеют желание переезжать: есть те, кому нравится дома.

ИТ-компании в российских регионах оказывают влияние и на рынок труда, и на экономические процессы, и на проекты госструктур. На фоне общего дефицита рабочих мест индустрия ИТ наоборот испытывает недостаточность сотрудников и готова вкладывать в них большие средства: тем самым создаётся тренд на образование и компетенции именно в этой сфере.

Проекты ИТ-компаний кросс-граничны: в итоге деньги и другие ресурсы притягиваются из других регионов и стран. Гиганты сферы готовы делегировать проекты региональным командам, у которых хорошо настроены процессы удалённой работы. И наконец, государственные структуры признают пользу и высокий престиж ИТ, учатся взаимодействовать с компаниями, использовать технологии и платформы в своей работе. Такие тренды вселяют надежду на развитие не только российских ИТ-технологий, исследований и бизнеса, но и местного производства высокотехнологичного оборудования и гаджетов. Отрасль ИТ может стать локомотивом экономического развития для регионов, где будут созданы соответствующие условия.



www.rktv.ru

«Всегда приятно вернуться» – Usta Management

Расскажите подробнее о компании Usta Management

Управляющая компания USTA Management входит в состав группы компаний USTA group (крупнейшая в Уральском федеральном округе диверсифицированная компания, объединяющая предприятия сферы гостеприимства, основана в 2000 году).

В управлении USTA Management находятся:

- Сеть отелей USTA Hotels (в управлении 530 номеров в 7 отелях в г. Екатеринбурге и Свердловской области)
- Скандинавский парк-отель Еловое (60 номеров и 4 точки питания в Челябинской области)
- Кафе и рестораны USTA Rest (700 посадочных мест в 4х городских ресторанах и 7 точек питания при отелях)
- Продажи апарт-комплексов (4 апарт-комплекса, более 300 апартаментов).

Как Usta Management отреагировал на пандемию коронавируса?

Мы, как и все представители отрасли HoReCa, ещё в начале марта с отменой первых крупных мероприятий в городе одними из первых ощутили последствия кризиса, вызванного пандемией. Уже к апрелю были закрыты все наши рестораны, и загрузка в отелях составляла не больше 10% – 15%. Пришлось закрыть часть отелей, а всех гостей разместить в оставшихся.

Несмотря ни на что это время было продуктивным для нашей команды: мы принимали медицинский персонал на самоизоляцию, создали обсерватор для туристов, прилетевших из других стран, достигли плановых показателей в загородном сегменте.

И в то же время мы активно развивали единую службу доставки из ресторанов и занимались подготовкой к открытию нового объекта – Скандинавский парк-отель ELOVOE, который успешно запустили 1 июля.

На текущий день все отели вернулись в обычный режим работы. Рестораны остаются закрытыми, работают только летние веранды и служба доставки.

Как был организован процесс удалённой работы и насколько сложно было его наладить?

Мы и до пандемии имели опыт удалённой работы: доступы к информационным ресурсам уже были у большинства руководителей компании. Поэтому технически мы были готовы к переходу на дистанционный график работы. Оставалось только масштабировать этот опыт на линейных сотрудников, раздать соответствующие доступы и помочь с настройками. Небольшие сложности возникли при настройке коммуникаций между сотрудниками и подразделениями, но все достаточно быстро освоили формат видеоконференций.

Внесла ли пандемия изменения в ИТ-стратегию компании?

Глобальных изменений нет, ИТ-процессы остались те же. Но в связи со значительной потерей дохода пришлось кардинально пересмотреть расходную часть бюджета компании и ИТ-бюджета соответственно. На этот год планировалась замена серверного и сетевого оборудования в ряде отелей, компьютерной техники в офисе. Сейчас понимаем, что часть запланированного откладывается на длительное время, а от части планов, возможно, мы откажемся совсем.

Появились ли у Вас новые проекты вследствие пандемии? Планируете ли Вы внести изменения в переподготовку сотрудников? На что акцентируете внимание?

Во-первых, сейчас в работе проект по внедрению в рестораны электронного меню с возможностью бесконтактного приёма и оплаты заказов.

Во-вторых, активно прорабатываем вопрос смены PMS (Property Management System) в наших отелях, и смотрим мы теперь именно в сторону облачных решений и решений с бесплатным открытым API.

Со сменой ПО, думаю, нас ждут новые возможности: это и интеграции с CRM-системой, с бонусной программой, возможность электронной регистрации гостей и более глубокая проработка аналитики по ним, новые маркетинговые «фишки» и другие полезные для бизнеса открытия.

Подготовка специалистов напрямую связана с изменениями в операционной деятельности компании и планами по развитию, поэтому «прокачиваемся», когда это необходимо для бизнеса и вместе с бизнесом.

Девиз нашей компании «Всегда приятно вернуться», и если сейчас для наших гостей и сотрудников важно создать безопасное с точки зрения санэпидблагополучия пространство, сократить социальные контакты, то мы сделаем всё зависящее от нас, в том числе через автоматизацию процессов.

Юлия Жукова
директор департамента ИТ USTA Management
Член клуба ИТ и Digital директоров «я-ИТ-ы»

www.ustagroup.ru
www.ciocdo.ru

Клуб IT& Digital директоров «я-ИТ-ы» – крупнейшее сообщество цифровых управленцев России, насчитывающее более 450 директоров.

Наша миссия – рост конкурентоспособности экономики России и производительности труда за счёт повышения уровня зрелости цифрового управленческого сообщества страны.

Мы создаём доверительную атмосферу профессионального общения, повышаем управленческие и профессиональные компетенции, помогаем нашим членам создать сеть деловых контактов.

CIS / № 3 (13) / 2020 / www.cis.ru

Актуальное положение дел в ИТ-отрасли в момент экономического спада

Интервью Сергея Груданова, генерального директора TESSIS (ЗАО «СИС»)

Сергей Борисович Груданов
генеральный директор TESSIS (ЗАО «СИС»)

Журнал CIS: ***Добрый день, Сергей Борисович! Спасибо, что уделили время для интервью. Давайте поговорим об актуальном положении дел в ИТ-отрасли в момент экономического спада, что происходит сейчас и что мы можем ожидать в ближайшем будущем от последствий пандемии?***

Сергей Борисович: Правда заключается в том, что сейчас наблюдается спад не только в ИТ-отрасли, но и в экономике. На самом деле, что уж там говорить, кому война, а кому мать родная. У всех по-разному, всё зависит от заказчика. Кто-то сохранил свои проекты, может быть, с какими-то сложностями – ограничениями доступа на объект, с задержками финансирования – это одна ситуация. Если мы говорим о компаниях разработчиках, у которых большой штат специалистов, а основные издержки находятся в фонде заработной платы и, соответственно, некоторые проекты зависли или вообще остались без финансирования, безусловно, им тяжелее. А у других, занимающихся организацией удалённого доступа, наоборот, конъюнктура сложилась таким образом, что у них сейчас работы много, а в обозримом будущем станет ещё больше. В любом случае ИТ себя показала на переднем крае, и совершенно не напрасно то, что сейчас происходит – это признание компаний из сферы ИТ как системообразующих.

И последняя новость – выступление президента, который озвучил некоторые меры по поддержке отрасли, направленные на развитие: ослабление налогового режима и ряд других преференций – очень радует. Неизвестно, в каком виде эти меры мы увидим в ближайшем будущем, но факт остаётся фактом: выступление президента было посвящено именно ИТ-индустрии, а не какой-нибудь другой отрасли.

Мы понимаем, что многие отрасли народного хозяйства пострадали достаточно сильно от пандемии. Какой новый опыт у нас появился? Безусловно, это то, что сейчас называется уже общепринятым словом «удалёнка». Мне на память пришли некоторые сюжеты из области киноискусства – уже появился ни один сериал на эту тему, носящие в основном комедийный характер. А почему бы и нет?! Тем не менее это некий тренд, новый энергетический уровень, о котором мы, безусловно, знали как работу на дому. Практиковалась эта работа не очень широко, потому что всем понятно, что для эффективных результатов нужны зрелость бизнес-процессов, компетентность персонала, умеющего работать удалённо. Поэтому решиться на внедрение такого формата в компании сложно.

Сейчас термин «на удалёнке» вошёл в повседневность, и такой формат работы принимается, но, наверное, в ближайшее время будут приняты поправки в трудовом кодексе, которые легитимизируют удалённую работу, и такой формат станет стандартом. В любом случае, мы должны это принять, хотим этого или нет. Мы вынуждены были это опробовать. Результаты скорее позитивные.

Какой ещё есть результат? Я вижу развитие цифровизации всего процесса: цифровые пропуска, контроль за их исполнением, выставление постановлений за нарушение пропускного режима и пр. В любом случае это было сделано быстро, масштабно, речь идёт буквально о миллионах инсталляций, миллионах пропусков. В такие короткие сроки это, конечно, большое достижение, значительный опыт для всей инфраструктуры.

Теперь давайте обратим внимание непосредственно на технологии и решения, которые реализовывали видеоконференцсвязь (известны эти компании и их продукты – облачные решения, ставшие незаменимыми).

На самом деле тема «облаков» – это уже тренд, отошедший на второй план. Несколько лет назад все только и говорили: «облака, облака». Если мы говорим о паблик-облаках, это было всё-таки предубеждением. Сейчас деваться стало некуда: то преимущество, которое дают облака, например ТОП-масштабируемость и готовность мгновенно решать масштабные задачи, сейчас на пике.

Учебный год в России закончился с использованием видеоконференцсвязи. Я не готов говорить о цифрах, но сильно подозреваю, что они просто огромные. Сервис, предоставлявший такую возможность, стал востребованным. Конечно, у него снизилась скорость, появились сбои, но стратегически он выстоял.

Мы, например, внутри компании **не пользовались** системой, которой **пользовались** школьники, исключительно чтобы им не мешать. У меня в семье у самого два дошкольника. Я видел, как была загружена сеть, которая находилась не в Москве, а на некотором удалении, когда надо было всем одновременно провести уроки. Тем не менее они проведены, учебный год закончился, оценки и аттестаты получены. Поэтому вывод простой: за облаками – будущее.

Вся инфраструктура, весь прогресс постепенно переходит в облака. Передовые продукты для этой инфраструктуры разрабатываются. Все они сначала выходят в облачной версии. Но, понимая некоторое предубеждение – отсутствие доверия к облакам как к технологии для повседневной жизни и работы, компании выпускают и версии продуктов, предназначенные для развёртывания в закрытой инфраструктуре, так называемый on-premise-технологии. То есть я могу со своим частным облаком жить внутри замкнутого периода. Таким образом, это даст мне возможность, во-первых, держать серверы физически у себя, а не у каких-то провайдеров. Так легче исполнить те стандарты, которые адресовал мне регулятор для реализации безопасности.

В связи с этим я позволю себе упомянуть о том, что наше предприятие является дистрибьютором французской компании «Талис», у которой очень много облачных решений, которые находятся в сфере ИТ и в ИБ. Если мы говорим об информационной безопасности, то, безусловно, от защиты данных нам никуда не деться. У нас есть зрелые промышленные технологии, готовые шифровать любые форматы. Я имею в виду файлы, системы хранения данных, виртуальные машины, сетевые протоколы – всё это делается прозрачно, совершенно незаметно для потребителя, позволяя ему сохранить свои данные, сделать их более труднодоступными или полностью недоступными для злоумышленника.

Также у нас есть решение, которое позволяет обеспечивать двухфакторную аутентификацию десятков тысяч пользователей. Это очень эффективное промышленное решение. И мы как раз относимся к тем компаниям, которые ощутили большой интерес, с точки зрения продаж в период пандемии. Причина в том, что наша компания представляет технологии, которые во-первых, позволяют реализовать эффективный удалённый доступ, а во-вторых, сделать его максимально безопасным.

У нас есть ещё один повод для гордости: в нашем портфеле есть разработка отечественного производителя под названием палиндром – это высокоскоростной шифратор, который работает на ростовых библиотеках шифрования. Хотя решение новое, но у нас уже есть достаточно крупные пилоты и большой интерес к этому. Эту разработку мы и пытаемся реализовать для наших клиентов.

Журнал CIS: ***Спасибо за развёрнутый ответ. У меня к Вам следующий вопрос: какие есть положительные и отрицательные моменты в сложившейся ситуации?***

Сергей Борисович: Позвольте мне перефразировать ваш вопрос. Когда на одной чаше весов жизни людей, говорить о плюсах достаточно тяжело. Есть один большой минус – много жертв в результате пандемии. Поэтому в этом отношении я бы не говорил о плюсах и минусах, а рассказал бы об уроках, которые мы можем вынести из этой ситуации. И эти уроки я вижу в том, что необходимо «переформатировать» свою профессиональную и рабочую жизнь с точки зрения ограничения передвижений, нахождения в замкнутом пространстве или где-то на удалённых точках. При всём при этом не выпасть из рабочего процесса и из коммьюнити. Мы должны с готовностью принять технологии, которые сейчас даёт индустрия. Это технологии удалённого доступа и всё, что с ними связано: шифрование каналов, защита удалённого доступа, аутентификация и пр., чтобы мы понимали, кто подключается к нам с той стороны, и это было проверено и надёжно. Может быть, к условным плюсам стоит отнести то, что в такой экстраординарной ситуации (к которой я отношу пандемию), могло быть и хуже, но несмотря на то, что количество жертв велико, инфраструктура жизнеобеспечения не рухнула, электричество не отключили, связь функционировала, продукты были доступны для покупки. Каких-то обширных катастрофических последствий нам удалось избежать. Спасибо и правительствам, и народам,

и жителям разных стран, которые поддержали порядок: особо не противодействовали, уходили на самоизоляцию, соблюдали дистанцию. И мы с вами ведём себя корректно – соблюдаем социальную дистанцию.

Журнал CIS: ***Спасибо за дополнительные комментарии к вопросам! Давайте затронем тему антикризисных мер: что нужно делать управленцам, чтобы компании могли встать на ноги после COVID-19 и набрать обороты как можно быстрее. То есть какие стратегии управления наиболее эффективны в условиях изменения среды?***

Сергей Борисович: Давайте уточним, что сейчас произошло. В период пандемии произошла некая деформация, слом привычной модели существования в бизнесе. Я сейчас не говорю слова «ведение бизнеса», просто – существование: люди, офис… Вот ты, вот логистика, привычные обязанности – никаких ограничений. Или ограничения есть, но все уже выработали методику их преодоления. Сейчас появились некие новые вызовы, поэтому, с моей точки зрения, необходимо исключить риски нарушения непрерывности бизнеса: отсутствие возможности нахождения в офисе, отсутствие доступа к информационной системе и пр. Всё это или по отдельности ограничивает нашу привычную возможность ведения бизнеса. Мы должны быть готовы работать с нашими поставщиками и заказчиками удалённо – из дома. Пусть это понятие – «на удалёнке», которое уже вошло в обиход, обязательно появится в словарях, если ещё не появилось.

Журнал CIS: ***Прокомментируете ли Вы анонсированные руководством страны меры поддержки ИТ-компаний или опустим этот вопрос?***

Сергей Борисович: Не отпустим, зачем? Это на самом деле вещи в достаточной степени принципиальные для ИТ. Во-первых, обратили внимание; во-вторых, сказали, что надо разработать эти меры; в-третьих, уже какие-то меры анонсировали. Но остаётся в-четвёртых: как это будет в конце концов реализовано, какими мерами и на каких условиях компании смогут воспользоваться. Это будет мера, которая коснётся разработчиков или которая затронет компании, занимающиеся системной интеграцией? Эту меру применят только к разработкам продуктов или, например, к продажам продуктов собственной разработки? Я вижу большую пользу оттого, что сейчас эта тема поднята, обсуждается и в правительстве.

Я не думаю, что завтра российское ИТ перевернёт весь мир. Но потенциал у российских компаний, которые работают в этой сфере, большой, и в любом случае помощь государства нужна. С моей точки зрения, если вести речь об импортозамещении, то эта помощь должна была быть оказана давно, и оно шло бы значительно эффективнее.

Журнал CIS: ***Какое место занимает информационная безопасность в условиях кризиса? То есть можно ли экономить на безопасности? Если да, то как?***

Сергей Борисович: Вопрос, конечно, философский. Дальше можно говорить о чём угодно. Да, мы с вами можем экономить на еде, но мы будем есть, можем экономить на одежде, но мы будем одеваться. Понятно, что защититься от всего нельзя. Мне трудно однозначно ответить на вопрос. Могу дать взаимоисключающие ответы.

Все мы, по большому счёту, устроены одинаково. Никто не хочет тратить лишних денег даже на то, что ему необходимо. Мы всегда что-то выбираем, не зная, где та самая золотая середина. Конечно, есть исключения, когда хочется побаловать себя и просто «выкинуть» деньги на красивое украшение для любимой девушки. Но опять же, будут ли это выкинутые деньги, я не вполне уверен. Наверное, они пойдут на упрочение отношений и улучшение настроения.

А если мы будем говорить об ИБ, то от всего защититься нельзя. Злоумышленник впереди планеты всей, и зачастую борьба происходит именно в реактивном режиме, поэтому, я считаю, надо выбрать конкретные направления, которые мы хотим защищать, и сконцентрироваться на этом. В любом случае это та же самая рисковая модель.

Компания, которая в зависимости от требований регулятора, а иногда из собственной зрелости принимает для себя решения.

Какие есть риски? Во-первых, компания должна находиться в правовом поле работы с информационной системой – это требование регулятора. Компания должна защищать собственный бизнес – это то, что я назвал бы зрелостью. Но люди относятся к этому по-разному. Кому-то всё равно: ничего не украдут или мы никому не нужны.

Но нет компании, где бы ни поработал злоумышленник, есть только компании, которые не обнаружили свои уязвимости. Индустрия, которая работает по ту сторону баррикад, не дремлет: она ищет уязвимость и просто хочет заработать. Денег и ресурсов у неё много, и тратит она достаточно для того, чтобы свою цель реализовать. Поэтому от всего защититься невозможно. Враг не дремлет в широком смысле, и он будет искать уязвимости.

Мы должны сами определить те направления безопасности, которые хотим защитить и начать действовать. Надо так построить процесс шифрования данных, защиту каналов передачи и средств обработки данных, что даже если злоумышленник получил бы к ним доступ, то не смог бы ими воспользоваться, сразу продать или модифицировать. Резюме: от всего защититься я не умею, если кто умеет, пусть скажет как. Поэтому выбираем направления, которые для нас наиболее критичны, и защищаем их.

Журнал CIS: ***На этой положительной ноте наше интервью подошло к концу. Это был последний вопрос. Благодарю Вас за уделённое время!***

Сергей Борисович: Большое спасибо Вам!

COVID-19: перезагрузка безопасности

2020 год диктует ИТ и всему миру новые правила: безопасность людей и бизнеса — это главное. Первая волна пандемии закончилась, но ситуация остаётся нестабильной. Разбираемся, как защитить бизнес в новой реальности.

Безопасность 2.0

На фоне прогнозов, что вирус пришёл к нам надолго, СИНТО и партнёры разрабатывают комплексные решения для текущих условий работы компаний. Наша задача – предупредить опасность, связанную с распространением инфекционных заболеваний, снизить риски заказчика, минимизировать ущерб (человеческий и финансовый) для предприятий. Мы хотим сделать общее будущее безопасным. И у нас есть на это ресурс и возможности.

Совместно с производителями ИТ-технологий мы создаём, перерабатываем, тестируем и выбираем максимально эффективные решения для наших клиентов. Мы не ограничиваемся стандартными рамками: ИТ-сфера находится в постоянном движении и развитии, и непозволительно стоять на месте, использовать устаревшие алгоритмы. Мы собираем полный антивирусный пакет для защиты бизнеса: соединяем «железные» решения с технологиями нейронных сетей в проектах, в помощь заказчику разрабатываем инструкции и регламенты действий при обнаружении инфицированных сотрудников, обучаем работе с оборудованием, консультируем и поддерживаем в тестовый период. При таком подходе наш клиент защищён со всех сторон и уверен, что система безопасности обеспечит стабильность работы компании при любых, даже самых негативных сценариях.

Кейс

Один из наших последних проектов по безопасности в условиях сложной эпидемиологической ситуации – установка тепловизионного комплекса на предприятии крупного ритейлера (ЦФО). Задача – автоматизировать входной контроль и предупредить допуск на территорию инфицированных сотрудников. На объекте 5 проходных, входящий трафик ~15 человек в минуту на каждой. Численность сотрудников – 7500 человек. Мы установили 10 тепловизионных камер, по две на каждой проходной, с дальностью определения температурного фона до 9 метров. Измерение температуры тела входящих лиц происходит с точностью до 0.3 °C. Камеры подключены на автоматизированное рабочее место оператора и интегрированы с системой контроля и управления доступом предприятия. Для максимального результата мы предложили соединить программное обеспечение тепловизионных камер с технологией машинного зрения. В итоге, законченное решение не только выявляет сотрудников с повышенной температурой тела и оповещает отдел безопасности голосовым сигналом, но и фиксирует нарушителей без масок, осуществляя детектирование масочного режима.

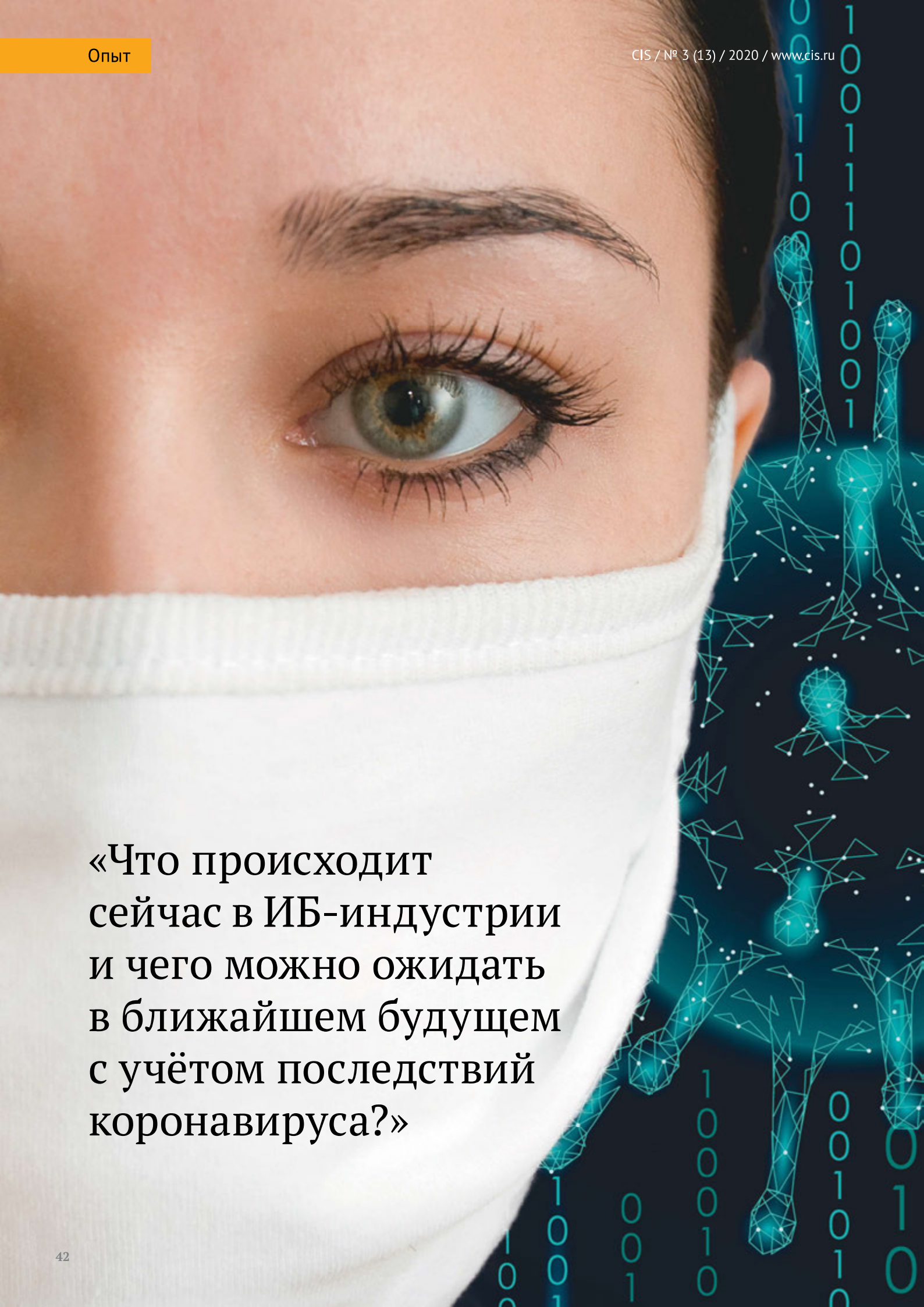
Решение показало высокую работоспособность при плотном входящем потоке. Лица с повышенной температурой тела выявляются автоматически и не допускаются на рабочее место, служба безопасности применяет разработанные нами регламенты. Система внедрена в общую ИТ-инфраструктуру предприятия, видео-аналитика хранится на серверах, создаются отчёты, архив данных доступен 24/7.

Удалённая работа

Многие компании сейчас перешли в режим дистанционного взаимодействия. Бизнес-процессы при таких условиях не могут выстраиваться без решений для удалённой работы, которые мы включаем в проекты по безопасности. Мы сотрудничаем со 150 российскими и мировыми производителями ИТ-продуктов и ПО: устанавливаем антивирусные программы, платформы для совместной удалённой работы, оборудуем дистанционные рабочие места ПК и печатной техникой, выполняем настройку, осуществляем техподдержку.

Наш комплекс мер безопасности для бизнеса и госпредприятий применим в любых отраслях. Он обеспечивает бесперебойную работу в условиях пандемии и помогает снизить риски распространения вируса COVID-19 и иных инфекционных заболеваний.

Илья Шинкарь
Управляющий компании «СИНТО»



«Что происходит сейчас в ИБ-индустрии и чего можно ожидать в ближайшем будущем с учётом последствий коронавируса?»

Журнал CIS: ***Следует ли ожидать массовых сокращений сотрудников в подразделениях ИБ? Может ли это вызвать серьёзные последствия, ведь такие люди хорошо осведомлены о внутренней организации, используемых технологиях и многом другом?***

Михаил Стюгин: Проблемы с кибербезопасностью, несмотря на пандемию, только усугубились. Кратно вырос объём фишинговых рассылок, переход на удалённый режим работы привёл к тому, что «наружу открылись» многие сервисы, которые ранее работали в периметре организации. Плюс к этому быстрая трансформация бизнес-процессов также не сопровождалась столь же быстрой адаптацией и корректной настройкой систем безопасности. Всё это приводит к мысли, что возможное сокращение специалистов в ИБ будет ниже, чем в других отраслях ИТ. Однако исключать этого нельзя. В зону риска здесь в первую очередь попадают вендоры и интеграторы, на другой стороне которых находится потребитель. А любой потребитель в этом году стремится к оптимизации расходов.

Журнал CIS: ***Скорее всего, кризис очень сильно повлияет на формирование бюджета следующего года. По-Вашему, это хорошая возможность сконцентрироваться на реально необходимых действиях по обеспечению безопасности или большая угроза компаниям?***

Михаил Стюгин: Внутренние службы ИБ-компаний не отвечают за развитие бизнеса, поэтому любое сокращение бюджетов для них не может нести полезных возможностей. То есть это не тот случай, когда кризис – это возможность. Возможностью это может быть для вендоров, которые смогут правильно сконцентрировать свои усилия в игре по новым правилам.

Журнал CIS: ***Есть мнение, что кризис положительно скажется на конкурентоспособности организаций, ведь он заставляет оптимизировать процессы, рационально перераспределять ресурсы. Согласны ли Вы с этим?***

Михаил Стюгин: Наблюдения последних лет показывают, что кризис всегда убивает слабых, а сильных делает ещё сильнее. Кризис – это время, когда растёт разрыв между бедными и богатыми. Это работает не только с людьми, но и с целыми государствами. Мне не очень верится, что кризис благотворно повлияет на экономику нашей стороны, в том числе и по рынку решений кибербезопасности. Скорее всего, и без того незначительная доля наших вендоров на международном рынке ещё больше сократится, а на внутреннем – будет поддерживаться протекционистскими мерами. Не уверен, что компетентен говорить за весь рынок ИТ, но, скорее всего, это общая тенденция.

Журнал CIS: ***Как Вы относитесь к передаче всех функций ИБ (или хотя бы части наименее критичных) специалистам на аутсорсинг? Может показаться, что это хорошая возможность доверить ИБ квалифицированному специалисту за умеренную плату. Как Вы считаете?***

Михаил Стюгин: Всё верно, аутсорсинг – это хороший способ для компаний малого и среднего бизнеса сделать эффективное разделение труда вместо того, чтобы вешать всю работу по ИБ на одного человека и ожидать качественный результат. По отдельной компании всегда можно сделать простую аналитику между ФОТ сотрудников, необходимых для поддержания всех процессов ИБ, и стоимостью покупки отдельных сервисов по аутсорсингу. В зависимости от исходных данных эти графики будут пересекаться в определённой точке. Вот эта точка и есть разделительная линия между принятием решения перехода на аутсорсинг и наймом достаточного количества собственных специалистов.

Журнал CIS: ***Может ли введение неких критериев оценки показателей безопасности повысить эффективность ИБ-отдела? Или же это приведёт к тому, что сотрудники будут улучшать эти самые критерии, а не действительно защищать информацию?***

Михаил Стюгин: Когда я писал кандидатскую, а потом и докторскую диссертацию по информационной безопасности, то всегда упирался в проблему оценки эффективности любых систем защиты. Нет такого прибора, который может измерить уровень защищённости системы или сервиса и сказать, насколько он уменьшился или вырос с принятием определённых мер. О безопасности всегда судят либо субъективно, либо по факту наличия инцидентов. Инциденты обнажают уязвимости информационной системы. Однако всё это сложно конвертируется в обоснование бюджетов ИБ. Чтобы решить эту проблему, можно придумывать критерии эффективности ИБ-отдела, но они никогда не будут напрямую измерять уровень ИБ в компании, это всегда косвенные критерии, а косвенными критериями всегда можно манипулировать. Повышать эффективность ИБ-отдела надо не формальными критериями, а повышением уровня персональной ответственности и заинтересованности сотрудников в результатах своей работы.

Журнал CIS: ***Насколько позитивно вы оцениваете перспективы развития ИБ в России?***

Михаил Стюгин: В целом оптимистично. Несмотря на санкции и рыночную изоляцию, Россия до сих пор считается родиной «хакеров». Многие с большим интересом смотрят на решения кибербезопасности из России. Плюс к этому мы законодательно стимулируем внутренний рынок ИБ. Есть некоторые объективные сложности, о которых я уже говорил выше, но относительно многих других секторов ИТ, ИБ выглядит достаточно позитивно.

Михаил Стюгин
Руководитель направления «Информационная безопасность»

Константин Анатольевич Алексеев
Senior Software Engineer at EPAM Systems Poland

Главное – начать: история успеха нашего соотечественника

Успех – это не судьба и не благосклонность Вселенной, это упорный труд как моральный, так и физический.

Поэтому, если вам кажется, что жизнь несправедлива, а все начинания заканчиваются оглушительным провалом, не спешите опускать руки. Сложные жизненные обстоятельства, неудачи могут стать настоящим трамплином на пути к успеху. Выбор всегда за вами! Читайте историю успеха топового backend разработчика и не сомневайтесь, что и вы так сможете!

Алексеев Константин Анатольевич родился и вырос в Пятигорске, провинциальном городе, который славится не только атмосферными памятниками архитектуры и потрясающей природой, но и сложной криминальной обстановкой. До 8 класса мальчик Костя демонстрировал незаурядные успехи в учёбе, был круглым отличником и гордостью школы, но с наступлением подросткового возраста всё встало с ног на голову. Пришлось играть по правилам окружающего мира. Не быть «своим» стало опасно.

К счастью, Константину хватило мужества и силы воли не сбиться с верного пути, и после окончания школы он поступил в Пятигорский филиал Санкт-Петербургского государственного университета аэрокосмического приборостроения на факультет «Программное обеспечение вычислительной техники». Здесь ему удалось в полной мере проявить свои таланты и способности, зарекомендовав себя как ответственного и подающего большие надежды студента. На 4 курсе Константин перевёлся в головной ВУЗ в Санкт-Петербурге. Выпускной экзамен сдал на отлично, диплом защитил на твёрдую «4». После получения ди-

плома принял решение вернуться на малую родину, в Пятигорск. К тому моменту он уже был в браке и воспитывал дочь.

Сфера программирования не стала золотой мечтой Константина. Он устроился на работу системным администратором в местное издательство «Из рук в руки», а уже через полтора года был переведён на пост редактора. Новая должность стала отправной точкой в его дальнейшем профессиональном становлении. Будучи редактором, Константин влюбился в рекламу и твёрдо решил развиваться в этом направлении: открыл ИП, купил несколько рекламных скроллеров сити-формата и устанавливал их в городе, параллельно продолжая трудиться в газете. Но надолго в издательстве Константин не задержался и через некоторое время оставил должность редактора. К тому моменту он окончательно понял, что не готов связывать свою жизнь с программированием.

Рекламный бизнес не приносил достаточного дохода, поэтому встал вопрос дополнительной занятости. А когда возникает твёрдое желание и чёткое намерение, возможности сами идут к нам в руки. Знакомая Константина предложила поработать графическим дизайнером на крупнейшем предприятии Северного Кавказа по изготовлению и продаже окон из ПВХ. «Отличное предложение!» – решил Константин и согласился, тем более опыт дизайнерской деятельности у него был.

Однажды, ещё во время его работы в оконной компании, перед ним поставили задачу сделать дизайн нового сайта компании, а впоследствии и сверстать его. Начинающему дизайнеру предоставили пару книг по HTML, CSS и JS и заверили, что он со всем обязательно справится. Готовый результат впечатлил не только генерального директора компании, но и самого Константина. Именно тогда он понял, что работа с кодом – это всё-таки то, что у него отлично получается, а главное, приносит огромное удовольствие.

Константин быстро сориентировался, добавил к своему ИП соответствующий вид деятельности и начал оказывать услуги по разработке сайтов, параллельно развиваясь и повышая навыки в этой сфере. Уже через время, подучив Java, предприниматель добавил в перечень услуг бэкэнд (backend). Как это часто бывает, местный рынок не способствовал должному развитию предприятия и высокой прибыльности проекта. Хотя попадались действительно сложные и достаточно интересные заказы.

В поисках новых возможностей Константин приобрёл печатное оборудование и добавил в кейс услуг небольшую типографию и сувенирку. Однако спустя несколько лет доходы от ИП упёрлись в потолок ввиду специфики местного рынка и экономики, чего нельзя было сказать о стремлении Константина достичь большего, расти, развиваться и повышать доход.

Онлайн-курсы по java-разработке стали следующим шагом на пути к успеху. В процессе обучения пришло окончательное понимание, что реклама и полиграфия исчерпали себя и срочно нужно выходить на новый уровень, двигаться в направлении корпоративной энтерпрайз-разработки.

Константин сразу приступил к действию: составил резюме на hh.ru и благополучно провалил первые собеседования, в том числе очные встречи с работодателями в Москве. Опустил ли он руки? Конечно, нет! И вскоре получил должность программиста в Альфа-Банке. Показав себя при выполнении мелких задач, он получил серьёзное задание по оптимизации кода старого внутреннего банковского приложения, которое очень медленно работало. Задание было выполнено на отлично! Константин стал одним из ключевых разработчиков важного проекта Альфа-Банка.

Как признался сам Константин, он до сих пор с любовью вспоминает Альфа-Банк и безмерно благодарен своим бывшим коллегам, которых считает настоящими друзьями.

Примерно через год Константин получил предложение работать в компании МТС в роли ведущего бэкэнд-разработчика одного из популярных мобильных приложений. Высокая зарплата, мобильная разработка, IoT – в МТС знали, как завербовать «классного» специалиста. Собеседование прошло на ура, и Константин попал в штат престижной компании.

Во время работы в МТС поступали предложения релокации в Сингапур, Китай, ОАЭ, но душа не лежала. И только когда с ним связался рекрутер из Епам, предложив переехать в Европу, а конкретно в Польшу, он дал положительный ответ. Ведь желание уехать, сменить локацию, попутешествовать работая, не отпускало его уже давно.

Сегодня Константин работает в Епам старшим разработчиком на очень интересном проекте для крупнейшего американского инвестиционного банка. Он частый гость на польских и международных хакатонах, где выступает в качестве ментора и судьи, является спикером на топовых ИТ-форумах.

Константин уже получил предложение перевода в США, но по причине временного бана рабочих виз пока остаётся в Польше. Возможно, когда-нибудь он вернётся в Россию, но точно не сейчас. Впереди новые горизонты, новые победы и достижения! Нам остаётся лишь пожелать ему удачи!

---

alxkonstantin@gmail.com
www.linkedin.com/in/konstantinaleks

CIS / № 3 (13) / 2020 / www.cis.ru

Экстренная цифровизация

Какие подходы помогли компаниям во время пандемии

Из-за пандемии коронавируса все трансформационные активности, которые компании планировали развивать в течение нескольких лет, потребовали практически мгновенного внедрения.

Результатов ждали даже не через месяцы и недели, а через считанные дни. От этого зависел не только коммерческий успех в конкретной точке времени, но и выживание бизнеса в принципе. О том, за счёт чего российский рынок без больших потерь прошёл через ускоренную цифровизацию, в статье для CNews поразмышлял Александр Старыгин, директор департамента подготовки технических решений, Hewlett Packard Enterprise в России.

Что помогло бизнесу быстро перестроиться

Александр Старыгин: Стремительная смена бизнес-модели и ИТ-приоритетов зачастую упирается в ограничения используемой в организации ИТ-инфраструктуры.

Массовая цифровизация стала основным последствием пандемии, связанным с ИТ. Это выразилось, в первую очередь, в переносе существенной части бизнес-функций и бизнес-процессов в информационные системы, виртуализации рабочих мест и существенном расширении онлайн-взаимодействия с потребителями. Другими ускорившимися в десятки раз процессами стали массовый переход на электронный документооборот, перевод в онлайн производственных совещаний, переговоров и встреч, выстраивание интерфейсов с информационными системами партнёров, а также рост объёмов и повышение уровня безопасности коммерческих и персональных данных.

Однако такая стремительная смена бизнес-модели и ИТ-приоритетов зачастую упирается в ограничения используемой в организации ИТ-инфраструктуры.

Первые результаты анализа, проведённого Hewlett Packard Enterprise на основе своего опыта общения с заказчиками в этот сложный период, позволяют выделить ряд особенностей корпоративных ИТ различных компаний и отраслей. Именно эти отличия помогли организациям оказаться наиболее устойчивыми и гибкими, а также перестроиться в самые сжатые сроки с минимальными потерями для бизнеса.

Александр Старыгин: Понятно, что трехлетняя заводская гарантия на оборудование не является панацеей, подобный расчёт можно назвать опрометчивым и несущим прямую угрозу непрерывности бизнеса.

1. **Высокий уровень автоматизации управления ИТ**

Этот пункт предполагает мониторинг всех используемых приложений и платформ, конфигурацию и настройку систем удалённо в полуавтоматическом (а лучше – в автоматическом) режиме на основе шаблонов, сценариев, лучших мировых практик, выявление потенциальных проблем и опасных тенденций в функционировании ИТ и их предотвращение на ранних стадиях и т.д.

2. **Широкое использование сервисов технической поддержки**

За них могут отвечать как профильные службы самой компании, так и различные игроки ИТ-рынка, авторизованные и прошедшие сертификацию производителей программного и аппаратного обеспечения. Этот уровень должен включать техподдержку 24/7, профилактические процедуры, позволяющие снизить до минимума риск возникновения отказов оборудования и ПО, а также фиксированное время восстановления работоспособности с момента регистрации заявки. Понятно, что трехлетняя заводская гарантия на оборудование не является панацеей, подобный расчёт можно назвать опрометчивым и несущим прямую угрозу непрерывности бизнеса.

В условия пандемии особенно важно снабжение персонала подразделений и компаний, специализирующихся на техподдержке, индивидуальными средствами защиты. Также необходимо провести тренинги и инструктаж по работе в условиях карантина, а также проверку состояния здоровья перед визитом к заказчику.

3. **Построение ИТ-инфраструктуры на основе гибридной модели**

Здесь имеется в виду сочетание собственной, арендуемой и облачной инфраструктур, распределение используемых платформ между собственными площадками, коммерческими ЦОД и облаками сервис-провайдеров. Особенно эффективно гибридная инфраструктура работает в ситуациях, когда удаётся обеспечить динамическое перемещение ресурсов и задач между всеми компонентами модели.

Иными словами, если не устраивает количество, качество, цена или доступность ресурса или сервиса в арендуемом ЦОД, перенесите приложение в собственный ЦОД или в облако, либо же перераспределите нагрузку между различными сайтами. Разумеется, это нельзя сделать, если заранее не проанализированы доступные источники ИТ-ресурсов и услуг, не разработаны процедуры миграции приложений между платформами, провайдерами, сайтами. Но те компании, которые изначально опирались на несколько источников и моделей использования ресурсов, получили важное преимущество.

4. **Работа с большими данными и искусственным интеллектом**

Эти технологии применялись компаниями как для анализа собственного бизнеса, так и для обеспечения функционирования корпоративных ИТ. Многие предприятия искусственно ограничивали функциональность корпоративных ИТ обработкой оперативных (быстрых)

Александр Старыгин
директор департамента подготовки технических решений, Hewlett Packard Enterprise в России

данных. Они сосредоточились на транзакциях, вычислениях, отчётах, онлайн- и офлайн-доступе. Теперь эти компании испытывают трудности с анализом колебаний спроса, маржинальности товаров, услуг, потребителей, корреляцией событий, использованием прогнозной аналитики при решении самых разных задач, актуальных в условиях неопределённости рынка.

Что касается применения искусственного интеллекта в ИТ, то пандемия лишний раз обратила внимание менеджмента на «самое слабое звено» в обеспечении непрерывности бизнеса. Сегодня технологии искусственного интеллекта вышли на уровень промышленного использования и позволяют не только увеличить надёжность и эффективность ИТ, но и высвободить персонал для решения творческих задач, внедрения инноваций в бизнес-практику и, что особенно важно в текущих условиях, снизить риск угрозы здоровью сотрудников.

Что делать компаниям после пандемии

Что же должно измениться в подходах к корпоративному ИТ после пандемии коронавируса и как внедрить эти изменения в условиях предсказуемо ограниченных инвестиций в ИТ в ближайшее время? Антонио Нери (Antonio Neri), президент компании Hewlett Packard Enterprise, говоря о неизбежных изменениях в мире после коронавируса, отметил, что «нет возврата к тому, что было раньше. Есть только подготовка и построение того, что будет дальше».

Если опираться на текущий опыт, то можно выделить следующие наиболее важные направления трансформации корпоративных ИТ.

Александр Старыгин: Технологии искусственного интеллекта вышли на уровень промышленного использования и позволяют не только увеличить надёжность и эффективность ИТ, но и высвободить персонал для решения творческих задач, внедрения инноваций в бизнес-практику.

1. **Построение автономно функционирующей ИТ-инфраструктуры и/или автономного ЦОД**

В сущности, это преобразование аналогично переходу от традиционного автомобиля к автономному. Автономный ЦОД больше не нуждается в постоянном внимании, ручной настройке, реактивном (постфактум) поиске и устранении неисправностей. Он обеспечивает самоуправление на основе автоматизации текущих ежедневных операций, самовосстановление посредством выявления потенциальных проблем и их предотвращения, а также самооптимизацию баланса ресурсов, производительности и стоимости.

Решение этих задач строится на основе технологий **интернета вещей**, **искусственного интеллекта** и **глубокого обучения**. Сегодня система предиктивной аналитики **HPE Infosight** реализует этот подход для массивов **HPE Nimble** в наиболее развитом в индустрии виде.

2. **Самое широкое использование подхода «ИТ-инфраструктура как услуга»**

В рамках этого подхода каждое решение оплачивается по мере потребления и сопровождается услугами по проектированию и внедрению для быстрой интеграции в ИТ-окружение. В рамках сервисного контракта оговаривается архитектура и состав оборудования, начальный уровень использования ресурсов, а также планируемый рост их потребления.

Оплата происходит пропорционально количеству используемых ИТ-ресурсов за расчётный период. Поставщик поддерживает и восполняет по мере применения буфер дополнительных мощностей на площадке заказчика, который не оплачивается до тех пор, пока он не задействован. Наиболее зрелым на рынке примером такого подхода является сервис **HPE GreenLake**, который представляет собой комплекс технологических и финансовых решений для этой задачи с возможностью оплаты, привязанной к конечному бизнес-результату.

3. **Обеспечение независимости ИТ-инфраструктуры от источника ресурсов и услуг**

Достигается путём перехода к гибридному ИТ и обеспечивает возможность выбора наиболее подходящей платформы и источника ресурсов для данного типа нагрузки, требуемой мощности, ёмкости, производительности и цены ресурса или сервиса. Следует отметить, что полноценное использование этой возможности, а именно – перемещение приложений между различными ресурсами – основано на абстрагировании программного обеспечения от аппаратных платформ. Хотя современные контейнерные технологии, а также развивающиеся технологии serverless и cloudless направлены на решение этой задачи, говорить о полной аппаратной независимости пока рано.

В рамках этого направления компания HPE уделяет большое внимание обеспечению возможности **управления конфигурацией наших платформ из внешних программных систем**, **создания частных облаков**, **построения ИТ-платформ для цифровой трансформации**, использования **контейнерных платформ HPE**, участия ИТ-компаний в **партнёрской экосистеме HPE**.

Любой проект по обеспечению непрерывности бизнеса начинается с анализа внешних и внутренних рисков, определения тех из них, которые следует учитывать при планировании бизнеса, и тех, которыми можно пренебречь, ибо защита от соответствующих угроз потребует слишком больших инвестиций, либо же по причине невысокой вероятности наступления того или иного события.

До начала 2020 г. абсолютное большинство компаний относило пандемию к последней категории. Сегодня мы можем уверенно сказать, что учёт этой опасности должен стать нормой, устанавливающей новый класс требований и подходов к трансформации корпоративного ИТ.

История успеха: превращение мечты в реальность

Упорная работа и стремление к постоянному развитию – вот ключ к успешной карьере. Так считает наш сегодняшний герой – Святенко Александр Сергеевич, который прошёл путь от сборщика компьютеров до директора по управлению тестированием в крупнейших ИТ-проектах.

Александр Святенко

Александр Святенко родился в г.Махачкала, респ. Дагестан. Яркими воспоминаниями детства были комната в коммунальной квартире и мечта о компьютере, для покупки которого Александр подрабатывал на заправке, будучи ещё школьником.

Идея о переезде в другой город возникла после посещения Москвы. Увидев иной ритм жизни и широкие возможности в столице, Александр решил поступать в ВУЗ г. Москвы по перспективному направлению «Программное обеспечение вычислительной техники».

Первой его работой была сборка компьютеров. Для поиска заказов он с однокурсником расклеивал объявления о ремонте компьютерной техники, а после дневной учёбы занимался их выполнением. Серьёзным толчком для смены профиля стало желание работать с программными продуктами. Александр самостоятельно обучался тестированию ПО, с помощью интернет-ресурсов и параллельно искал работу в этой области. После нескольких собеседований он устроился инженером по тестированию в крупный московский депозитарий.

За первый год Александром было внедрено несколько значительных улучшений производственных процессов, что позволило оптимизировать работу компании. После чего ему предложили повышение до бизнес-аналитика. В этой должности он отвечал за развитие нескольких корпоративных систем и занимался управлением команды по тестированию.

Следующим этапом карьеры стало предложение о работе в проекте в Центральном депозитарии России. На тот момент в России внедряли реформу, суть которой заключалась в реорганизации корпоративных действий с ценными бумагами с целью увеличения привлекательности экономики РФ. Шанс поучаствовать в столь значимом для страны проекте нельзя было упустить.

Александр пришёл в проект в качестве руководителя команды по тестированию. В его зону ответственности входили управление командами ручного и автоматизированного тестирования и успешное внедрение новых продуктов и обновлений. Работа в НКО АО «Национальный расчётный депозитарий» много значила для карьерного и личностного роста. Решение сложных задач в условиях заданных сроков позволили быстро вырасти в профессиональном плане.

Проект реформы был внедрён в срок, количество ошибок, возникающих в «боевой среде», удалось сократить на 85%, большую часть рутинной работы автоматизировали, что позволило сократить расходы на тестирование.

Знания, накопленные за несколько лет работы, Александр решил преобразовать в формат курса, который в дальнейшем читал для повышения квалификации сотрудников компании. Было обучено более 100 человек. Материал и его подача была высоко оценена ими.

С целью дальнейшего развития и улучшения процессов автоматизации в НКО АО НРД Александру было предложено возглавить направление автоматизированного тестирования.

Среди основных задач, с которыми он успешно справился, были увеличение покрытия авто-тестами с целью снижения ручного тестирования и оптимизация процессов тестирования.

Параллельно с основной работой Александр посещал профильные курсы, одним из которых стал предмет по управлению проектами. Новая область привлекла своей широтой и возможностью улучшить в первую очередь не техническую базу, а управленческие навыки. В этот период представился шанс получить должность в крупном международном системном интеграторе EGAR Technology.

Новая позиция позволила получить опыт не только в области финансов и рынка ценных бумаг, но и в сфере страхования и ритейла. На текущей должности Александр развивает внутренние производственные процессы, привлекает новых клиентов, управляет распределёнными командами из разных стран и проводит оценку проектов.

Будучи перфекционистом по натуре, в работе он придерживается того же принципа – «Будь профессионалом во всём, что ты делаешь, только в этом случае тебя ждёт успех!»

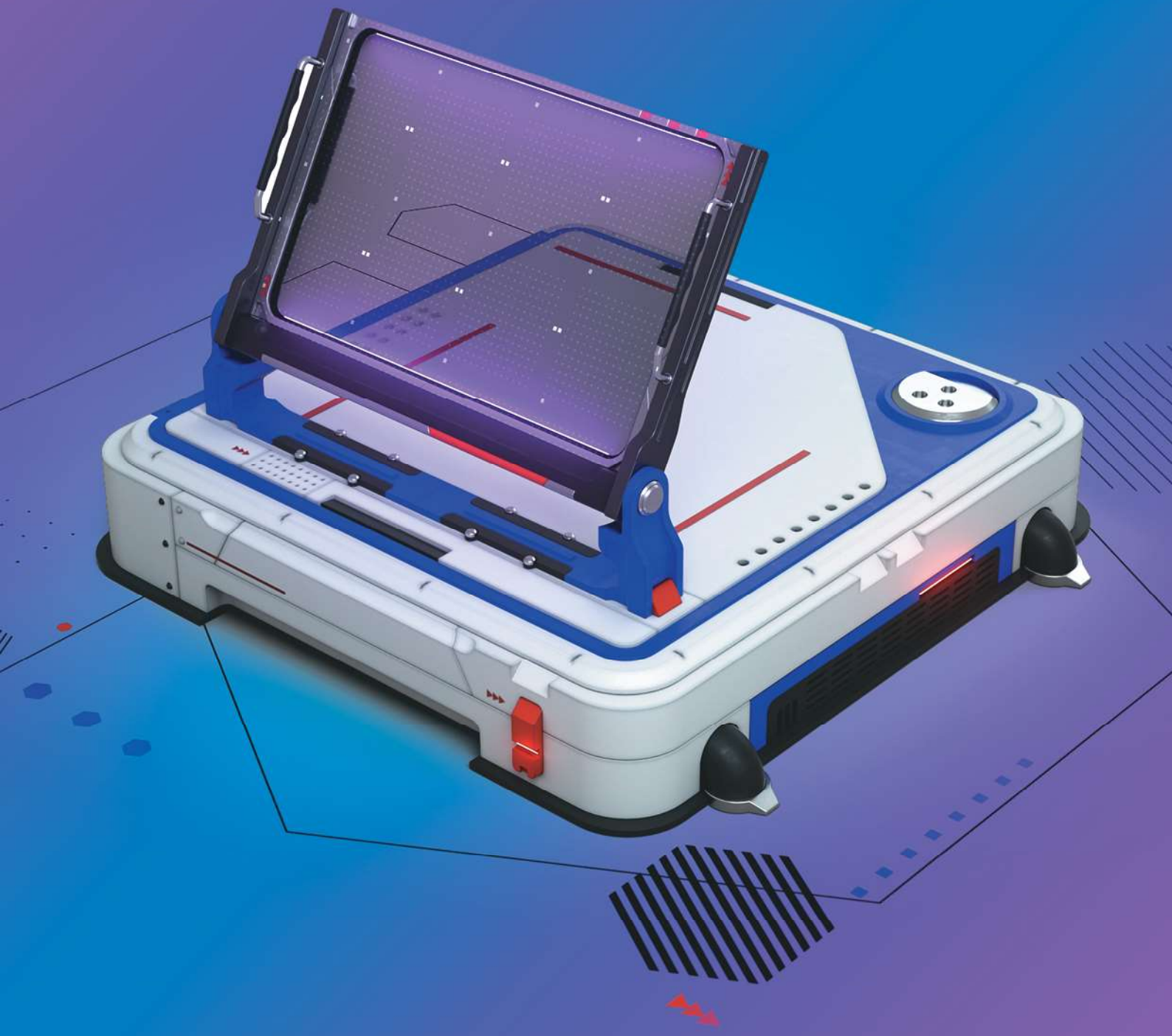
EGAR Technology

107564, г. Москва, ул. Краснобогатырская, д. 6 стр. 2

+7 (495) 120-05-33

CIS / № 3 (13) / 2020 / www.cis.ru

Запрет на дополнительные требования к квалифицированной электронной подписи



На что повлияло законодательное вето, и как избежать платы за «воздух» при получении цифрового инструмента в статье Единого портала Электронной подписи.

КЭП как двигатель прогресса

Квалифицированная электронная подпись (КЭП) – цифровой аналог подписи от руки, **пропуск в мир цифровой экономики.** С её помощью можно получить подтверждённую запись на портале Госуслуг, зарегистрировать компанию или ИП без явки в ФНС, принять участие в коммерческих или государственных торгах, сдать отчётность online, дистанционно установить трудовые отношения и многое другое. Важно помнить, что скорость и качество цифровых процессов многократно выше их «бумажных» аналогов, а стоимость и временные затраты ниже.

Если **подпись от руки «едина»** или, другими словами, действительна без соблюдения дополнительных правил вроде требования расписываться только по четвергам, то **как обстоят дела с КЭП?**

Полиморфизм рынка электронной подписи

Совсем недавно, **до 1 июля 2020 года,** пробелы в законодательстве были причиной расщепления рынка на крупные, средние, мелкие и даже микросектора, а всё потому, что **квалифицированная электронная подпись де-факто не являлась универсальной.** Оператор каждой информационной системы (ИС) имел возможность **отказать** владельцам КЭП **в доступе,** «отбраковывая» цифровой аналог подписи от руки. Основанием служило **отсутствие** в структуре предъявляемого клиентами квалифицированного сертификата ключа проверки электронной подписи (КСКПЭП) **объектного идентификатора** (OID-а или ОИД-а), который оператор ИС устанавливал в качестве обязательного элемента для работы в своей информсистеме по своему усмотрению.

Зачастую подобные ОИД-ы были платным. Чем выше стоимость, тем сильнее информационная система ограничивала количество её участников, перекладывая **расходы на плечи владельцев КЭП,** тем самым вводя скрытую комиссию за регистрацию в системе. Это позволяло обходить некоторые законодательные акты, например в сфере электронных торгов по банкротству. Только определённые пользователи могли заплатить существенную цену, будучи точно уверенными в своей победе, остальные просто отказывались от регистрации. К сожалению, подобная ситуация встречается и сейчас, и не только в системах из приведённого примера.

Удостоверяющим центрам (УЦ), помимо их основной деятельности по выдаче электронных подписей, сопряжённой с высокими рисками и ответственностью, **требовалось вести переговоры и заключать соглашения** с многочисленными электронными торговыми площадками (ЭТП) и прочими информационными системами. В случае установления партнёрства с какой-либо ИС УЦ получал право включать в структуру КСКПЭП определённый **ОИД.** Подобная особенность привела к тому, что порой пользователям приходилось получать **несколько КСКПЭП в разных удостоверяющих центрах** либо одну со всеми ОИД-ами. Известны случаи, что цена такой «мульти-ОИД-ной» подписи доходила **до 55000 рублей.**

«Мамай ушёл»

Столь хаотичный уклад, несомненно, вёл к падению эффективности системы в целом. Первые шаги к изменению подхода к использованию единой подписи и структурированию взаимодействия между субъектами в масштабах страны были предприняты **АО «Аналитический Центр»** в далёком 2009 году. Организация выстроила **порядок,** одними из главных элементов которого стали условно «универсальный» ОИД, позволявший работать на подавляющем большинстве торговых площадок, и единый реестр сертификатов. С его помощью Аналитический Центр избавил удостоверяющие центры и получателей электронной подписи от финансового и временного лага.

Законодательное вето

Успешно завершённая работа по корректировке законодательной базы позволила изменить положение ОИД-ов 1 июля 2020 года. С этой даты участники электронного взаимодействия, в том числе:

- операторы государственных и муниципальных ИС,
- ИС, использование которых предусмотрено нормативными правовыми актами,
- ИС общего пользования,

не вправе устанавливать ограничения признания КЭП, за исключением тех, что предусмотрены Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» (63-ФЗ) в редакции Федерального закона от 27.12.2019 № 476-ФЗ.

Вместе с тем **вето** накладывается на требование **вносить** в КСКПЭП **информацию, не являющуюся обязательной** согласно законодательству об использовании ЭП.

Что означает отмена ОИД-ов простым языком?

Теперь **доступ** к перечисленным выше ИС должен предоставляться владельцам квалифицированной электронной подписи **без внесения в КСКПЭП дополнительных ОИД-ов** за исключением ситуаций, когда того требует закон или иной нормативный правовой акт, например акт Центробанка. Подобную подпись можно получить **в любом** аккредитованном Минкомсвязью **удостоверяющем центре,** но важно учесть несколько моментов:

1. Ценовая политика УЦ

Отмена объектных идентификаторов, в том числе платных, однозначно, должна была сказаться на стоимости КЭП. Но, желая максимизировать собственную прибыль, некоторые удостоверяющие центры могут игнорировать этот факт для сохранения своей доходности, преднамеренно вводя клиента в заблуждение.

2. Позиция УЦ

Клиентам следует обратить особенно пристальное внимание на разъяснения и комментарии, которые предоставляет удостоверяющий центр. Позиция по отказу от дополнительных требований должна быть максимально открытой и прозрачной без предложений купить гарантированный доступ.

Что делать, когда отказываются принимать КЭП или навязывают платные услуги?

В рубрику «Вопрос эксперту» Единого портала Электронной подписи поступил ряд обращений, связанных с отказами ЭТП принимать КЭП без ОИД-ов, а также с попытками операторов навязать платные действия (требование активировать/зарегистрировать КЭП) после вступления в силу изменений 63-ФЗ.

Так, например, в середине июля Александра написала:

Здравствуйте! Получила в УЦ квалифицированную ЭП для участия в аукционе по реализации имущества банкрота, но торговая площадка отказала в регистрации из-за отсутствия ОИД-а. Правомерно ли это? Если нет, то куда мне жаловаться?

Ответ экспертов Единого портала Электронной подписи:

Здравствуйте, Александра! Действия оператора электронной площадки нарушают действующее законодательство в области использования электронной подписи. Согласно вступившей в силу с 01.07.2020 новой редакции Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» (Закон № 63-ФЗ) операторы государственных и муниципальных информационных систем, а также информационных систем, использование которых предусмотрено нормативными правовыми актами, или информационных систем общего пользования не вправе требовать наличие в квалифицированном сертификате информации, не являющейся обязательной в соответствии с Законом № 63-ФЗ и принимаемыми в соответствии с ним иными нормативными правовыми актами (п. 2.1 ст. 17).

Жалобу на незаконные действия оператора электронной площадки считаем целесообразным направить в Минкомсвязь России (уполномоченный госорган в сфере использования электронной подписи) и Минэкономразвития России (уполномоченный орган в сфере правоотношений, регулируемых Федеральным законом «О несостоятельности (банкротстве)»).

***

Редакция Единого портала Электронной подписи / iecp.ru / Свидетельство о регистрации средства массовой информации Эл №ФС77–61055 от 05 марта 2015 года выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) / 16+

***

Итого

В случае неправомерных действий (отказ в регистрации, навязывание платных услуг) продемонстрируйте оператору знание законодательства. Если это не изменит его линии поведения, то обратитесь с жалобой в Минкомсвязь России и уполномоченный орган исполнительной власти в той области общественных правоотношений, в которой работает оператор информационной системы, также не будет лишним направить официальную претензию на имя оператора самой ИС.

Перспективы

Участники рынка электронной подписи находятся в ожидании прочих, более масштабных трансформаций. Горизонт планирования – 2022 год, когда система претерпит фундаментальные изменения, в том числе расширение сфер использования КЭП физических лиц и внедрение машиночитаемых доверенностей, сокращение количества удостоверяющих центров, создание сервисов «доверенной третьей стороны», развитие всей цифровой экономики. Подробнее об этом можно прочитать в предыдущих номерах журнала CIS или в разделе «Статьи» Единого портала Электронной подписи.

АО «Аналитический Центр» *– организация, более чем 20-летний опыт сотрудников которой по структурированию и совершенствованию рынка электронного взаимодействия в России положен в базис удостоверяющего центра «Основание».*

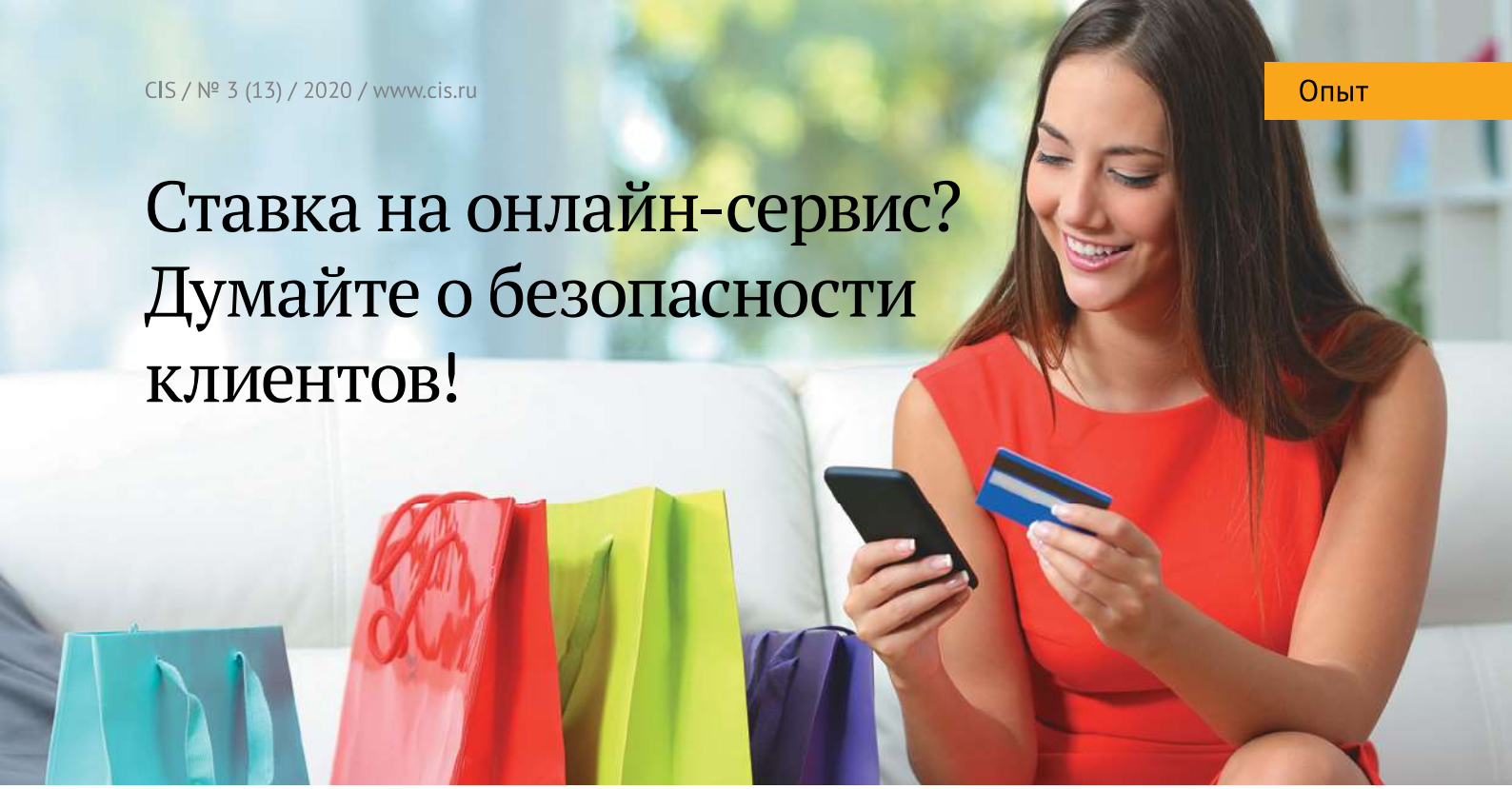
Удостоверяющий центр «Основание» *– надёжная цифровая экосистема идентификации и аутентификации граждан Российской Федерации при партнёрстве с госкорпорацией «Ростех».*

uc-osnovanie.ru

Единый портал Электронной подписи *– интернет-проект АО «Аналитический Центр», на котором представлена исчерпывающая информация об электронной подписи, преимуществах и принципах работы с ней, об электронных торгах, о системах электронного документооборота, защите информации и многом другом, без чего невозможно представить современный цифровой мир.*

iecp.ru

Ставка на онлайн-сервис? Думайте о безопасности клиентов!



Как прекрасно, что мы живём в таком веке, когда заказать продукты на дом, оформить доставку еды, оплатить коммунальные услуги, оформить платную подписку на сериал и прочее — всё можно сделать, не выходя из дома.

Ситуация с пандемией только подстегнула развитие онлайн-сервисов. К сожалению, для многих компаний сработал принцип, что если товара нет онлайн, то его не существует для конечного потребителя, который вынужден соблюдать режим самоизоляции. Чтобы пережить «коронокризис» бизнес пытается приспособиться к реалиям, чтобы уцелеть, привлекать новых клиентов и расти. Хорошие новости в том, что с началом покупательского ажиотажа, связанного с распространением коронавируса, рост онлайн-продаж увеличивался темпами, опережающими среднегодовые. И растёт не только онлайн-ритейл. Так, 33% миллениалов сейчас посещают онлайн-уроки вместо очных занятий или лекций, 53% предпочитают шопинг в интернете походам в торговые центры, а 18% делают выбор в пользу виртуальных туров по городам и музеям.

И все же нужно помнить, что ваши сайты и мобильные приложения с товарами и услугами онлайн доступны не только добросовестным пользователям, но могут попасть и под прицел злоумышленников. Мошенники всё так же нацелены на похищение денежных средств, личных данных пользователей, по-прежнему используют программы лояльности, находя лазейки в акциях и распродажах, и отмывают денежные средства через цифровые каналы обслуживания. По данным опроса «Лаборатории Касперского» 17% респондентов заявили, что сталкивались со взломом своего аккаунта.

Чем это опасно? Например, в случаях с компрометацией логина и пароля пользователя вашего онлайн-сервиса злоумышленники могут преследовать несколько целей: совершить кражу денег или бонусов, убедиться в подлинности учётных записей для последующей перепродажи, собрать дополнительную информацию о владельце (номер телефона, адрес и т.д.) для пополнения своей базы. В результате таких действий компании несут финансовые убытки за счёт необходимости возмещения украденных у пользователей средств, незапланированных расходов на отработку негативных отзывов, роста расходов на отправку второго фактора аутентификации через SMS, а их ресурсы могут перестать работать из-за большого количества авторизационных запросов ботов, что также влечёт репутационные риски.

Что делать?

- Обучайте и информируйте своих клиентов об уязвимостях, обнаруженных методах мошенничества, лайфхаках «как не стать жертвой мошенников» и о других рисках.
- Отслеживайте подозрительную активность в течение пользовательской сессии. Используйте передовые средства обнаружения мошеннической активности, такие как **Kaspersky Fraud Prevention** для раннего выявления кражи аккаунта, «фейковых» учётных записей и других мошеннических действий.
- Всегда анализируйте результаты обнаруженного мошенничества на своих цифровых сервисах и адаптируйте бизнес-логику соответственно.
- Реализуйте многофакторную авторизацию, безопасное шифрование пароля и другие защитные механизмы.
- Будьте готовы к инцидентам. Разработайте планы коммуникации с клиентом, восстановления репутации и реагирования в СМИ.

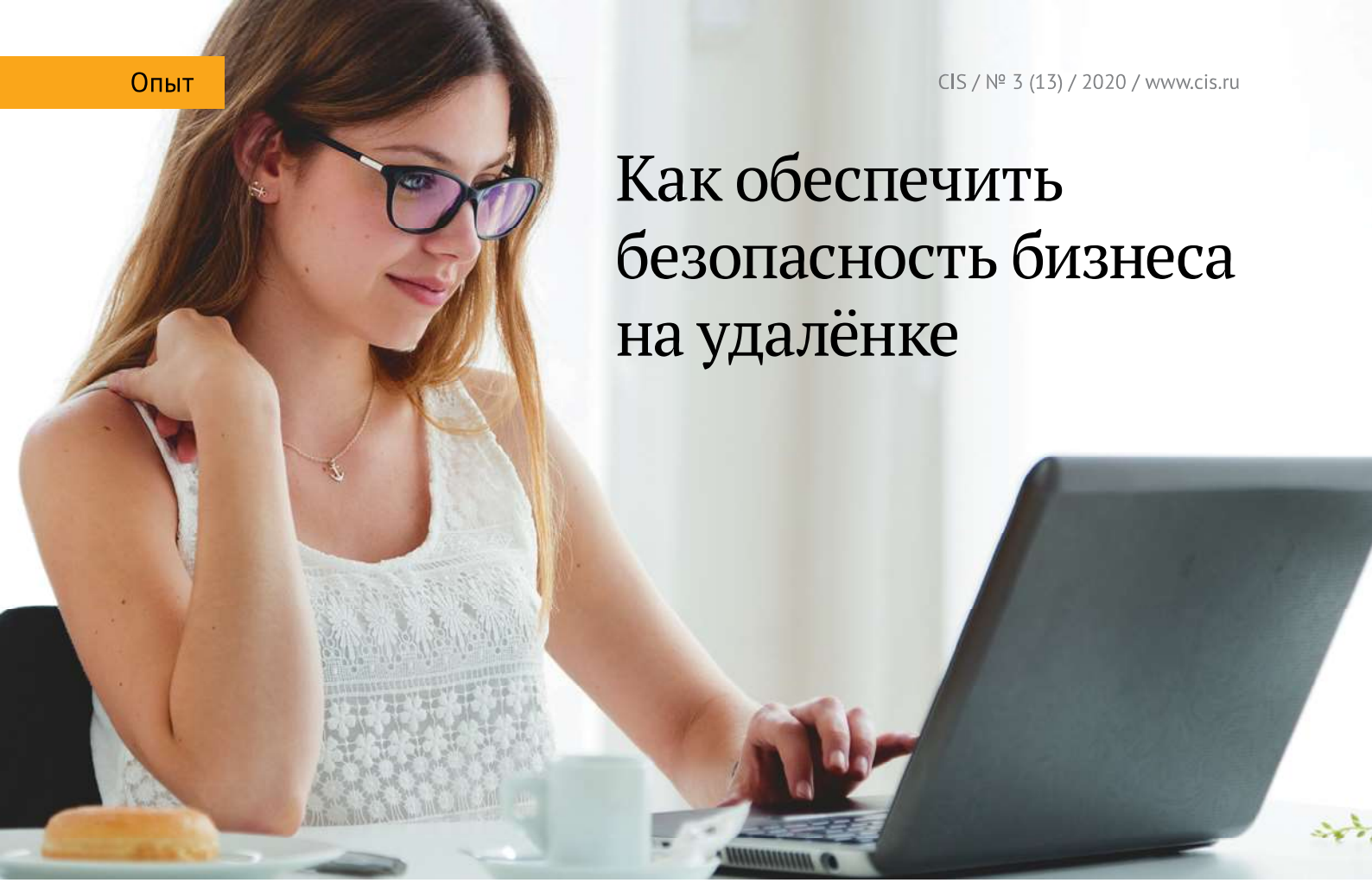
Екатерина Данилова
Менеджер по развитию бизнеса решений по предотвращению онлайн-мошенничества

kaspersky

***«Лаборатория Касперского»** – международная компания, работающая в сфере информационной безопасности.*

www.kaspersky.com

CIS / № 3 (13) / 2020 / www.cis.ru



Как обеспечить безопасность бизнеса на удалёнке

Тысячи компаний по всему миру перешли на удалённую работу. При этом персонал был и остаётся уязвимым звеном, через которое киберпреступники проникают в сеть.

И эта опасность только усиливается, когда сотрудники подключаются из дома к корпоративной инфраструктуре. Одновременно с этим важно не забывать о сохранении самого бизнеса и лояльности клиентов. Выход есть: обучить сотрудников основам кибербезопасности. В статье мы постараемся дать рекомендации по решению этого вопроса.

Сотрудник на удалёнке – WFH[1] или WTF?

Зачастую человеческий фактор обходится компаниям крайне дорого даже в обычное время. Отделы информационных технологий и безопасности в каждой второй компании считают, что наибольшую угрозу корпоративной безопасности представляют сотрудники. Многие пользователи не понимают важность компьютерной безопасности. По данным исследований «Лаборатории Касперского» больше половины сотрудников хранят на рабочих устройствах финансовую информацию, базы e-mail клиентов и поставщиков и другие конфиденциальные данные, при этом 30% – спокойно признаются в том, что делились логином и паролем от рабочего компьютера с коллегами.

1. Сокращение от термина WFH – Work From Home.

Сейчас в удалённом режиме работают даже правительства различных стран – заседание Британского правительства проходило по видеоконференции как пример для граждан, что можно эффективно исполнять свою обязанности и на удалёнке. Уже стала привычной картина, когда лидеры стран – самые влиятельные люди на планете – используют онлайн-конференции. Все, и мы с вами, привыкаем к новым условиям.

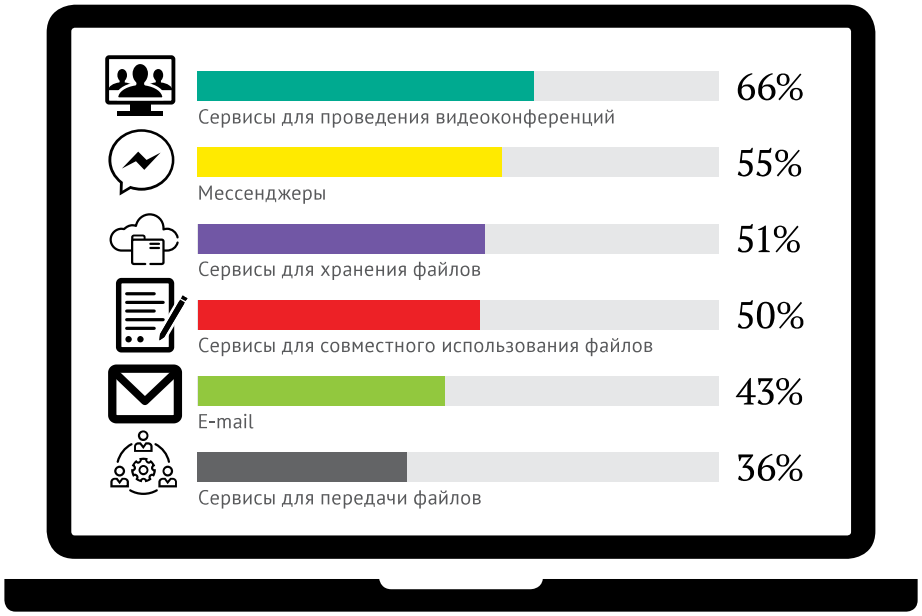
Но, как избежать рисков, когда формат работы Work From Home (WFH) внезапно может превратиться в WTF – малоприятную ситуацию?

Сегодня бизнесу важно сохранить производительность и эффективность рабочих процессов и в то же время обеспечить безопасный доступ сотрудников к необходимым сервисам. Работа в удалённом режиме может приводить к возникновению таких проблем, как подключение корпоративных пользователей к незащищённым точкам Wi-Fi или использование сотрудниками теневых ИТ-ресурсов. По данным исследования «Лаборатории Касперского» о влиянии COVID-19 на стиль работы, многие российские сотрудники стали больше использовать для работы онлайн-сервисы, которые не были одобрены ИТ-отделами компаний, в том числе платформы для проведения видеоконференций (66%), мессенджеры (55%), сервисы для передачи и совместного использования файлов (51%).

Несоблюдение правил информационной гигиены могут привести к негативным последствиям.

Использование сотрудниками теневых ИТ

Исследование «Лаборатории Касперского»*



Теневые IT – не одобренные компанией программы и сервисы, которые тем не менее применяются сотрудниками для работы.

79%

не получали рекомендаций по безопасной удалённой работе

18%

получали фишинговые письма, связанные с COVID-19

* Исследование «Влияние COVID-19 на стиль работы» проведено «Лабораторией Касперского» в апреле 2020 г. Опрошено 6016 сотрудников по всему миру.

Например, причиной могут послужить подключение компьютера сотрудника к незащищённой Wi-Fi сети, использование видеоконференций, неодобренных политиками службы ИБ, искушение использовать «простые» средства передачи данных: облачные и почтовые сервисы, мессенджеры, а также возможный доступ семьи к рабочему компьютеру. Последний фактор обычно недооценивают, потому что мы все доверяем своим семьям. Тем не менее члены семьи, имеющие физический доступ к компьютеру, также могут неосознанно нанести ущерб организации.

Что делать?

- Принимайте ключевые меры для защиты корпоративных данных и устройств, включая установку пароля, шифрование рабочих устройств и обеспечение резервного копирования данных.
- Запланируйте тренинги для повышения цифровой грамотности сотрудников. Чтобы понять, что из себя может представлять такое обучение, воспользуйтесь бесплатным пробным периодом нашего тренинга **Kaspersky Automated Security Awareness Platform** по адресу www.k-asap.com/ru.
- Убедитесь, что ваши сотрудники знают, к кому обратиться, если у них возникнут проблемы. Уделяйте особое внимание тем, кому приходится работать с личных устройств:
  - помогите им разделить учётные записи на компьютере. Подскажите, как создать надёжный и сложный пароль. Примените двухфакторную аутентификацию;
  - создайте список сотрудников, для которых обязательна виртуальная машина для доступа к конфиденциальным ресурсам. Научите использованию и объясните, почему работать надо именно в виртуальной среде;
  - обучите сотрудников пользоваться корпоративными ресурсами для передачи и хранения служебной и конфиденциальной информации.
- Убедитесь, что устройства, программное обеспечение, приложения и сервисы регулярно обновляются.
- Установите проверенное защитное ПО на все конечные устройства, включая мобильные девайсы.

В экстраординарной ситуации защитят самые простые навыки кибергигиены, если, конечно, эти навыки привиты! Это важно при работе из дома.

Елена Молчанова
Руководитель направления маркетинга и продаж Security Awareness

kaspersky

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности.

www.kaspersky.com

Высокоскоростные шифраторы СИС крипто «Палиндром»

Семейство высокоскоростных шифраторов (ВСШ) Ethernet серии «Палиндром» выпускает российская компания «СИС крипто». Это шифраторы Ethernet на L2 с поддержкой алгоритмов шифрования ГОСТ. Семейство состоит из двух серий: 4000-й в двух вариантах (с портами RJ45 или гнездами SFP) и скоростью 1 Гбит/с, и 6000-й с гнездами SFP+ и скоростью 10 Гбит/с.

ВСШ «Палиндром-6140».

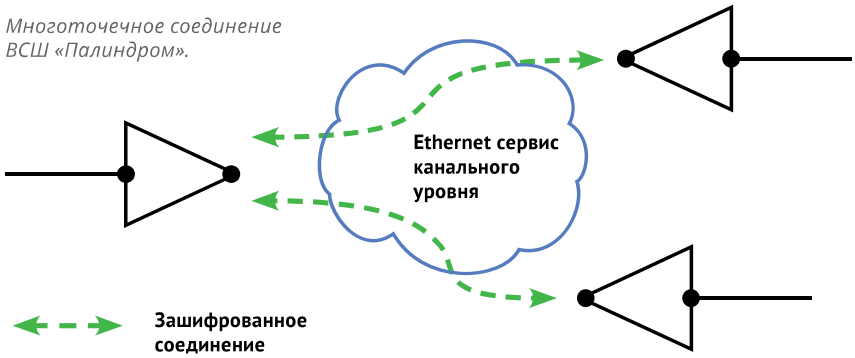
В отличие от многофункциональных шлюзов безопасности, описанных выше, это специализированные устройства, предназначенные исключительно для сетевого шифрования (защиты каналов) в сетях Ethernet L2. У шифратора есть только 2 сетевых порта (кроме выделенных для управления) – один к локальному сегменту, другой – к внешнему каналу. Устройства построены на специализированной платформе шифрования с ПЛИС и криптомодулем, реализующим шифрование ГОСТ. Используется блочный шифр 34.12-2015 «Кузнечик» в режиме гаммирования с алгоритмом согласования ключей VKO.

В шифраторах используется фирменный протокол шифрования Ethernet в транспортном режиме. Шифруется всё поле данных кадра – отсюда следует, что через сети L3 (с маршрутизацией по заголовку IP) такие устройства работать не смогут, перед каждым маршрутизатором кадры придётся расшифровывать. Так как заголовок кадра Ethernet не шифруется (и не изменяется), зашифрованные кадры могут быть скоммутированы через сеть L2, как обычно. Это делает возможным сквозное групповое многоточечное шифрование, при котором три и более шифраторов образуют единое защищённое соединение, через которое кадры будут доставляться только в нужный сегмент.

Шифраторы поддерживают работу на скорости линии во всем диапазоне длин кадров, то есть не теряют кадров почти никогда. Накладные расходы пропускной способности не превышают 8 байт на кадр, а в линейном режиме (между парой шифраторов), если опорная сеть между ними гарантирует надёжность и порядок доставки кадров, вообще равны нулю! В сочетании с рекордной задержкой (до 10 микросекунд) во всём диапазоне длин кадров это обеспечивает этим устройствам ощутимое преимущество. Их также можно устанавливать в агрегированном канале, позволяя кратно масштабировать пропускную способность.

Устройства умеют работать с кадрами Q-in-Q и MAC-in-MAC, применяющимися в больших операторских сетях, и таким образом обеспечивают поддержку VPN L2 со своим пространством MAC-адресов и VLAN. А вот организовать «своими силами» VPN L3 нельзя, это придётся делать другими средствами.

Многоточечное соединение ВСШ «Палиндром».



Единственным заметным ограничением на масштаб сети может стать количество VLAN, используемых как идентификаторы защищённых соединений – до 100. Но зато эти шифраторы никак не ограничивают гибкость сетей Ethernet, где они применяются: поддерживаются все виды топологий Carrier Ethernet («точка-точка», «дерево», многоточечное), разные виды физического транспорта Ethernet («тёмное» оптоволокно, сети OTN, Ethernet с коммутацией на L2, псевдопровода через MPLS и IP.) При использовании по модели управляемого сервиса шифраторы поддерживают мультитенантность (взаимную криптографическую изоляцию трафика разных абонентов одного оператора).

С точки зрения интеграции в сеть устройства полностью реализуют принцип «узел на проводе»: они совместимы с кадрами Ethernet любых форматов, не вмешиваются в работу протоколов слоя контроля L2 (тем более верхних уровней). Полноценно реализованы мутация (временная замена) Ethertype, отступ шифрования перед заголовками и пропуск незашифрованными кадров с особыми MAC-адресами, Ethertype и VLAN. Так как протокол шифрования фирменный, то ВСШ не могут работать в паре с другими устройствами шифрования, но зато совместимы между собой модели 4000-й и 6000-й серий.

Для управления используется интерфейс командной строки (через последовательный консольный порт) и фирменная система управления (станция управления под Windows через сеть во внеполосном или внутриполосном режимах). Отдельного сервера управления нет, и после отключения станции управления защищённая сеть может работать автономно. Ручные операции при начальной настройке устройства включают в себя загрузку начальной последовательности датчика случайных чисел, настройку IP-адреса, времени и даты, смену пароля по умолчанию и генерацию-подписывание-загрузку сертификатов, которые используются для централизованного автоматического управления ключами. Поддерживаются внутренний (встроенный в среду управления) или сторонние УЦ. Управление включает в себя в основном настройки, связанные с криптографией, защищёнными соединениями и политиками обработки кадров в зависимости от содержимого их полей. Защищённые соединения (туннели) могут устанавливаться автоматически, в том числе и в многоточечном режиме – главное, чтобы шифраторы были в одном широковещательном домене.

Шифраторы могут обнаруживать отказ других устройств в группе шифрования, а также сигнализировать о потере сигнала оборудованию, которое установлено у них «за спиной». Их можно встраивать в отказоустойчивые конфигурации с агрегацией портов и резервированием каналов. Модель 6140 имеет дублированные блоки питания и вентиляторы. Корпус шифраторов всех моделей защищён от физического взлома без вскрытия (зондирования), а также имеет датчик вскрытия. При срабатывании этого датчика устройство останавливается, вся ключевая информация стирается, и администратор получает уведомление о взломе.


ВОЖДЕНИЕ КАК ИСКУССТВО.
ЦЕНТР ВОДИТЕЛЬСКОГО МАСТЕРСТВА
BMW DRIVING EXPERIENCE.
Московская обл.,
Дмитровский район,
г/к Сорочаны,
деревня Курово 68А
Тел. +7 (495) 120-1000
www.bmwdrivingexperience.ru


BMW Driving Experience
Official Partner of M

Beauty & DigITal

ИТ-конкурс красоты

Я ИТ Ы

КЛУБ IT&DIGITAL ДИРЕКТОРОВ

CIS

Современные
Информационные
Системы

www.cismiss.ru

«Совинтегра»

«СОВИНТЕГРА» – инновационный проект, объединивший первоклассных специалистов с колоссальным опытом работы (более 15 лет) в области информационных технологий.

Направления деятельности

Наша основная специализация – защита ценных информационных активов, но, помимо этого, мы обеспечиваем полный спектр услуг и решений:

- консалтинг в области ИТ;
- комплексные решения по построению корпоративных ИС;
- решения в области виртуализации и облачных вычислений;
- специализированные решения по обеспечению информационной безопасности;
- сервис и комплексная техническая поддержка;
- разработка и внедрение программного обеспечения;
- специализированные решения.

Наша компания активно взаимодействует более чем с 1000 разработчиками ПО, такими как «Лаборатория Касперского», «Код безопасности», «Актив», Gemalto, HPE, Cisco, Citrix, Oracle, и т.д.

Наша миссия. Мы стремимся стать надёжным партнёром в деле повышения эффективности и безопасности бизнеса клиента. Наши специалисты работают для того, чтобы ваша компания не испытывала препятствий в ходе ведения деятельности.

Наши ценности. Мы – команда единомышленников, стремящихся решить вопросы заказчиков разных отраслей. Мы чётко видим цель, и для нас нет непреодолимых преград!

Наша философия. «СОВИНТЕГРА» работает, основываясь на принципах высокого качества предоставляемых услуг, ориентации на долгосрочные отношения с заказчиками и партнёрами, информационной открытости компании.

Мы можем решить практически все ваши проблемы с ИТ! Мы стремимся к тому, чтобы вам было максимально удобно и приятно работать с нами.

Анна Иванова
Компания «Совинтегра»

Мы знаем все основные подходы и решения по обеспечению безопасности ИС! Это позволяет нам реализовать проект любой сложности точно в срок и качественно.

Мы уже сделали сотни проектов по защите информации, виртуализации, аутентификации, решили множество проблем наших партнёров и заказчиков!

СОВИНТЕГРА

«Совинтегра» – инновационный проект, объединивший первоклассных специалистов с колоссальным опытом работы (более 15 лет) в области информационных технологий.

www.sovintegra.ru

«Datana»

Ольга Костяная
Компания «Datana»

Давайте знакомиться, меня зовут Ольга. Я работаю руководителем отдела маркетинга в компании реальных дел Datana.

Почему реальных, спросите вы? Отвечу: потому что мы не просто разрабатываем ИТ-системы на базе искусственного интеллекта, мы решаем конкретные задачи бизнеса с помощью технологий. Эффект от внедрения наших решений измеряется не абстрактным уровнем удовлетворённости, а конкретными цифрами, а это десятки миллионов рублей.

Так что же конкретно мы делаем. Datana занимается разработкой программно-аппаратных решений для повышения эффективности технологических и производственных процессов промышленных предприятий.

Наши решения представляют собой комплекс научных методологических разработок с применением глубокой отраслевой экспертизы и программного обеспечения, созданного с применением принципов Индустрии 4.0.

Мы помогаем заказчикам:

- повышать производительность и эффективную загрузку оборудования;
- снижать себестоимость единицы продукции;
- снижать негативное влияние человеческого фактора.

Мы делаем реальные дела в реальном секторе экономики!

Основной фокус компании сейчас направлен на предприятия чёрной металлургии, позже мы пойдём в цветную, а затем и в другие отрасли.

В промышленности в одиночку ничего не сделать, поэтому наша команда состоит из специалистов в области чёрной металлургии, профессионалов математического моделирования, а также разработчиков высоконагруженных и высокопроизводительных информационных систем и конечно же маркетологов. Кто-то должен продвигать наши решения и рассказывать о них миру промышленности.

Я занимаюсь всеми маркетинговыми и рекламными проектами. Я маркетолог-универсал, который может собственноручно настраивать контекстную рекламу, организовывать конференции, писать статьи, выступать с докладом, искать подрядчиков для разных проектов и ещё много чего. А ещё я бываю на крупнейших металлургических комбинатах страны и воочию наблюдаю масштабы производства и то, как плавится сталь. Это невероятное зрелище!

Наш девиз – «Экспертиза. Математика. Технологии». Мы считаем, что сочетание этих ключевых основ позволяет наиболее эффективно решать задачи, стоящие перед отраслью.

Мы любим то, что делаем, и стараемся делать это лучше всех!

Datana

Компания «Datana» *занимается разработкой программно-аппаратных решений для повышения эффективности технологических и производственных процессов промышленных предприятий.*

datana.ru

«ФЦНИВТ «СНПО «Элерон»

АО «ФЦНИВТ «СНПО «Элерон» – инжиниринговая компания в составе ядерного оружейного комплекса Государственной корпорации по атомной энергии «Росатом».

Крупнейшее в стране и отрасли предприятие по созданию и внедрению систем физической безопасности как по численности персонала, так и по номенклатуре выпускаемой продукции. Стратегическими заказчиками предприятия являются объекты ГК «Росатом» и федеральных силовых ведомств.

Основным направлением деятельности предприятия можно назвать реализацию «комплексного инжинирингового решения», в результате которого заказчик получает полный пакет услуг по проведению НИОКР, проектированию, производству, поставкам, строительству, монтажу, пусконаладке, а также сервисному обслуживанию.

При осуществлении деятельности наша организация решает следующие основные задачи:

- качественное выполнение государственного оборонного заказа в целях укрепления оборонного потенциала России;
- обеспечение безопасного функционирования объектов Госкорпорации «Росатом», особо важных государственных объектов, промышленных предприятий, компаний топливно-энергетического комплекса, организаций транспортной инфраструктуры;
- снижение стоимости и сроков работ в сфере капитального строительства атомной отрасли;
- расширение и модернизация линейки продуктов и услуг, увеличение выручки на новых рынках сбыта.

Продукцию АО «ФЦНИВТ «СНПО «Элерон» выбирают министерства, ведомства и иные структуры, чья деятельность связана с обеспечением государственной и общественной безопасности РФ. Наше предприятие имеет награды многих престижных отраслевых и международных выставок, а также было неоднократно признано лучшим поставщиком отрасли.

Моя роль в обществе – создание систем защиты информации в автоматизированных системах физической защиты на объектах атомной отрасли.

Основная деятельность нашего отдела – составление предпроектной и проектной документации, что является неотъемлемой частью

на пути к созданию систем защиты информации. Сбор исходных данных, анализ объекта, выявление угроз безопасности и по итогу защита объекта – всё это увлекательный и непростой процесс.

Сложность в комплексном обеспечении информационной безопасности заключается в том, что, несмотря на некоторые схожести, каждая проектируемая автоматизированная система является индивидуальной и требует своего уникального решения по защите информации.

Ещё одна сложность – это всегда быть в курсе актуальной нормативно- методической базы и всех её изменений, при этом учитывать современные, используемые на практике подходы и решения по защите информации. Также необходимо иметь знания в области продуктов, применяемых для обеспечения информационной безопасности, умение в них разбираться, анализировать рынок и знать лидирующие компании с продукцией, обладающей необходимыми сертификатами соответствия ФСТЭК и ФСБ России.

Но, несмотря на многие трудности, эта профессия – Специалист по защите информации – не может не нравиться, ведь чувство, которое испытываешь по завершении проекта, стоит всех сложностей!

Вера Долганина
Компания «ФЦНИВТ «СНПО «Элерон»

РОСАТОМ

АО «ФЦНИВТ «СНПО «Элерон» – инжиниринговая компания в составе ядерного оружейного комплекса Государственной корпорации по атомной энергии «Росатом».

www.eleron.ru

ИТ-компания «Азон»

Валентина Шумакова
ИТ-компания «Азон»

Огромный поток информации, возможность найти ответ на большинство вопросов – интернет даёт нам многое, но он же способен и нанести ущерб. «Если вас можно атаковать, вас атакуют» – следствие основного закона Мёрфи.

Защищённая информационная система – один из элементов стабильности бизнес-процессов компании, поэтому внедрение и поддержка экспертами систем обеспечения ИТ-безопасности призваны устранять возможные проблемы в виде DDoS-атак, вирусов, саботажа, кражи конфиденциальных данных и других киберугроз.

Появление направления информационной безопасности было лишь вопросом времени, и сейчас ИБ движется вперёд семимильными шагами.

«Трудные задачи выполняем немедленно, невозможные – после изучения матчасти»

Я сотрудник отдела информационной безопасности в небольшом системном интеграторе – ИТ-компании «Азон», созданной в 2003 году. Сегодня «Азон» – это около 70 человек, 2 офиса в Москве, собственная лаборатория по специальным проверкам и исследованиям технических средств.

Компания предоставляет полный спектр ИТ-услуг: от проектирования, внедрения и обслуживания ИТ-инфраструктуры, разработки и внедрения решений по информационной безопасности, в том числе для защиты персональных данных и «гостайны», до виртуализации серверов и рабочих станций (VDI).

Остаться на «светлой стороне»

Специалист по ИБ – это аудиты всех информационных систем, кропотливое составление документации для внедрения средств защиты информации в ИСПДн и ГИС, предаттестационная подготовка ИСПДн. Именно этим я занимаюсь в компании, и мне это безумно нравится.

Моя история в «Азон» началась 8 лет назад, когда я пришла в отдел по работе с государственными заказчиками. В ходе выполнения своих обязанностей приходилось часто сталкиваться с конкурсами по ИТ-безопасности, и я дотошно расспрашивала коллег о нюансах решений, просто потому что это было интересно. Когда встал вопрос о получении лицензии ФСБ для деятельности компании, потребовался сотрудник, соответствующий ряду требований, готовый пройти обучение по информационной безопасности, – я подходила идеально, и конечно же согласилась.

Мои знания и навыки, полученные при работе с тендерами, математическое образование, логическое мышление, любопытство – всё это помогает сопоставлять информацию из разных источников, грамотно оформлять документацию, легче понимать структурную схему комплекса технических средств компонента защиты информации.

Мне импонирует то, что за эти годы мы смогли сохранить бутиковый подход в работе с заказчиками и продолжаем поддерживать высочайший уровень требований к сервису оказания услуг. Стремление работать на поток, длительные неконструктивные совещания, строгий дресс-код – всё это не входит в нашу систему ценностей. Создание решения, максимально отвечающего технологическим возможностям и задачам бизнеса заказчика – вот приоритетный элемент нашей стратегии.

И я рада, что Вселенная предоставила мне шанс оказаться на «светлой» стороне интернета именно здесь и сейчас.

AZONE IT

ИТ-компания «Азон» *– специализируется на выполнении задач любой сложности в области информационных технологий – от поставок лицензионного программного обеспечения и оборудования до комплексного обслуживания ИТ-инфраструктуры.*

www.azone-it.ru

«РТП-Медиа»

«РТП-Медиа» – компания в сфере предоставления профессиональных услуг медалогитики. У компании интересная история, истоки которой в 2000-х годах. Все началось с предоставления услуг кабельного телевидения в одном из московских домов, в сетке вещания на тот момент было всего 10 каналов, зато на 4 телеканала больше, чем в соседних домах.

И это был первый успех! Дальше – больше. Подключались новые дома, объединялись в сети с районными телевизионными ГС посредством ВОЛС. Спустя несколько лет, под брендом «Столичные Кабельные Сети» началось объединение районных СКТВ в единую сеть с централизованным ядром на Шаболовке. Одновременно с расширением территории охвата сети увеличивался и спектр предоставляемых услуг. Помимо кабельного ТВ, компания стала заниматься профессиональным проектированием, строительством и обслуживанием ВОЛС, СКС, СКУД и других сетей, предоставлением в аренду волокон, окон прозрачности и каналов связи в них.

В начале 2017 года с изменением запросов пользователей рынка ТВ-услуг, следуя новым тенденциям развития телекоммуникаций, компания начала делать значительные капиталовложения именно в качество вещания ТВ-сигнала в своей сети. Это послужило новым толчком к развитию «наземной» доставки сигналов. Был построен с нуля собственный ЦОД для нужд компании в сфере медалогистики и межоператорского взаимодействия с телеканалами и другими операторами вещания. Так появилась отдельная компания под брендом «РТП-Медиа».

Сегодня мы предоставляем такие услуги, как:

1. **Приём сигнала** из точек обмена трафиком (в том числе ММТС-9, ММТС-10, РТРС, ГПКС и др.), со спутника, из аппаратных телеканалов и пр.
2. **Обработка сигнала:** преобразуем полученный сигнал в любой требуемый формат, производим конвертацию, энкодирование и декодирование, транскодинг и трансрейтинг, изменяем формат и разрешение кадра.
3. **Доставка сигнала,** в т.ч. наземным способом по собственным ВОЛС, сопряжённых со многими операторскими сетями, протяжённостью более 2500 км в Москве и МО.
4. **Перегон сигнала** прямых трансляций с сохранением высокого качества изображения и звука.
5. **Услуги резервного антенного поста.** Обладая 2-мя собственными разнесёнными АП, удалёнными друг от друга на 40 км, организуем резервный приём и передачу сигнала.
6. **Услуга Playout** – круглосуточного выхода телеканала в эфир.
7. **Контент-агрегация.** Операторы могут получить доступ к большинству телеканалов (у нас более 200 каналов). Также мы являемся точкой раздачи телеканалов 1 и 2 Мультиплексов.
8. **Аренда технологических ресурсов связи.** Предоставляем в аренду каналы связи высокого качества на базе собственной сети, построенной на принципах надёжности с использованием технологии резервирования. Предлагаем в аренду оптическое волокно, выделенные спектры (лямбды) или каналы связи.

В «РТП-Медиа» я являюсь руководителем межоператорского взаимодействия, работаю непосредственно в B2O сегменте. Взаимодействую с клиентами и партнёрами по вопросам предоставления технологических ресурсов связи, телевизионных сигналов, организации «последней мили», контролирую выполнение проектов в срок, веду документооборот. В этой сфере я уже более 5 лет, знаю всех ведущих игроков, основных конкурентов и потенциальных клиентов. Мне нравится вести переговоры и предлагать клиентам именно то, что они хотят, помогать им реализовывать самые сложные и амбициозные проекты.

Наталья Деркач

Компания: «РТП-медиа»

«РТП медиа» – компания с комплексными технологическими решениями в сфере логистики медиаконтента, занимающаяся приемом, обработкой и доставкой телевизионных сигналов любого формата от вещателей до операторов кабельного и спутникового телевидения и конечных потребителей контента.

rtp.media

Банк «Открытие»

Алёна Петунина
Банк «Открытие»

В современном мире информация стала главным активом. Поэтому так важен вопрос её защиты, и особенно в банках. Большая часть информации, которая обрабатывается в банке, относится к конфиденциальной, в том числе: персональные данные клиентов и сотрудников, банковская тайна, коммерческая тайна. Клиенты доверяют банку, в свою очередь банк делает всё для обеспечения информационной безопасности.

Я работаю в банке «Открытие». Банк – это только часть большой финансовой корпорации «Открытие», которая является одной из ведущих групп компаний на банковском, страховом, пенсионном и брокерском рынке России. Сегодня в состав группы входят 66 компаний, а сам банк в списке системно значимых банков ЦБ РФ.

У банка «Открытие» богатая история. Что интересно, банк мой ровесник и уже пережил множество реорганизаций и объединений. Он был сформирован в результате интеграции более чем 10 банков, в том числе Номос-банка, Ханты-Мансийского банка, банка «Петрокоммерц» и других.

Впервые я услышала о нём, когда он был банком «Петрокоммерц». В те годы он был спонсором игр КВН, которые я постоянно смотрела. А в 2018 году моё резюме удачно нашёл руководитель отдела, и я стала частью команды.

Продукты банка получают признания и награды профессионального сообщества. В 2019 году награду получила карта OpenCard как самая выгодная для клиента дебетовая карта с функцией cash-back (по решению пользователей сервиса «Выберу.ру»). Аналитическое агентство Markswebb Rank & Report назвало «Открытие» самым выгодным банком для предпринимателей. Банк победил в конкурсе «Лучшая банковская программа для малого и среднего бизнеса — 2019» Национальной премии в области предпринимательской деятельности «Золотой Меркурий».

И особенно значимая для меня награда — банк стал победителем Национальной банковской премии — 2019 в номинации «ИТ-решение в области информационной безопасности». Эту награду получил проект автоматизации реагирования на инциденты кибербезопасности путём внедрения системы Security Vision IRP!

В банке столько возможностей для личного и профессионального развития! Это различные вебинары и курсы, марафоны и тренинги, лекции «Открытого университета» и совместные спортивные тренировки. Банк является участником Национального совета корпоративного волонтёрства. Ежегодно проводится новогодняя акция, где любой сотрудник может стать Дедом Морозом, отправив подарок детям — подопечным дружественных Фондов.

Забота о близких — одна из важнейших ценностей нашего банка. В условиях пандемии банк одним из первых создал условия для удалённой работы своих сотрудников. А также принял участие в акции #изотворительность совместно в Фондом Константина Хабенского.

В нашем банке очень развита корпоративная культура и всячески поддерживаются истинные человеческие ценности. Можно поблагодарить коллегу за помощь, отправив открытку на портале, пригласить на чашечку кофе ещё незнакомого сотрудника через Кофебот, а по пятницам почитать интересные ответы на «Вопрос недели». Приятно быть частью не просто такого крупного банка, а дружного коллектива единомышленников. Теперь в моей жизни всегда есть место Открытию.

открытие
Банк

Банк «Открытие» *– универсальный банк, который развивает различные направления бизнеса: корпоративный, инвестиционный, розничный, МСБ и Private Banking.*

www.open.ru

«Высшая Школа Программирования»

Команда профессионалов своего дела – наша отличительная особенность. Мы объединяем самых лучших специалистов в области информационных технологий, параллельно занимаясь образовательной деятельностью, обучением учащихся тому, что умеем сами.

Наша компания основана в 1996 году и специализируется на проектировании, разработке, внедрении программного обеспечения и образовании детей и взрослых в сфере ИТ-технологий.

Я работаю в компании с 2011 года, на данный момент занимаю должность руководителя департамента программной инженерии.

Мы разрабатываем программное обеспечение с применением более чем 200 технологий, фреймворков, библиотек, языков программирования, сервисов и платформ. Занимаемся автоматизацией бизнес-процессов наших клиентов, снижаем издержки и увеличиваем прибыль.

Разработка программного обеспечения – важная составляющая для успешной работы компании или предприятия. Без специального программного обеспечения, мало какая организация может добиться успеха.

Современные технологии развиваются очень быстро! Сегодня автоматизация позволяет использовать передовые технологии, такие как машинное обучение, искусственный интеллект и нейронные сети. Это позволяет нам визуализировать взаимодействие функций, процессов и ключевых показателей производительности.

Автоматизация процессов позволяет существенно повысить качество управления и продукта.

Преимущества автоматизации:

- увеличивается скорость выполнения повторяющихся задач
- повышается качество работы
- повышается точность управления
- параллельное выполнение задач
- быстрое принятие решений в типовых ситуациях

На сегодняшний день автоматизация охватила многие отрасли промышленности и сферы деятельности: от производственных процессов до совершения покупок в магазинах. Вне зависимости от размера и направления организации, практически в каждой компании существуют автоматизированные процессы.

Нами успешно реализованы десятки крупных проектов в области проектирования и разработки заказного программного обеспечения, системной интеграции, электронной коммерции и управления информационной инфраструктурой. Так же мы консультируем как государственные структуры, так и бизнес-сектор, сотрудничаем с более чем 1000 ИТ-компаниями по всему миру.

Юное поколение погружено в виртуальную реальность изначально. Для них ИТ естественно, как воздух. В этот момент на помощь приходим мы. Мы объясняем что YouTube, «Вконтакте», Instagram – это не весь интернет, люди живут не только этим. Они программируют телефоны, автомобили, умные дома, банковские карточки. Наша задача показать новому поколению, что ИТ – большой мир, в котором есть, что изучать.

Мы любим то, что мы делаем!

Юлия Соколова

Компания «Высшая Школа Программирования»

ВЫСШАЯ ШКОЛА ПРОГРАММИРОВАНИЯ

«Высшая Школа Программирования» *– образование в сфере ИТ/аутсорсинг компаний в сфере системной инженерии, программирования, web разработки и графического дизайна.*

itproger.com

CIS / № 3 (13) / 2020 / www.cis.ru

«Высшая Школа Программирования»

Светлана Калачева

Компания «Высшая Школа Программирования»

Высшая Школа Программирования – ИТ-компания, которая сформировалась на юге России в городе Краснодаре. Основной деятельностью является аутсорсинг в сфере ИТ и качественное ИТ-образование. В этой статье речь пойдёт об обучении и воспитании юного поколения будущих айтишников.

Помимо web-разработки, я занимаюсь педагогикой, а именно обучением детей и взрослых ИТ-дисциплинам – от языков программирования и системной инженерии до графических редакторов.

Вернёмся к процессу освоения этого сложного удивительного мира. Все, кто мечтает стать программистом и думает, что это возможно сделать за месяц, увы, ошибается. Взрослому человеку нужно потратить минимум год на обучение и на работу с языком программирования, чтобы с уверенностью сказать, что он в нём хорошо разбирается. Это при условии, что, помимо обучения в специализированном учебном заведении, он учится ещё и дома, уделяя дополнительно хотя бы 5 часов в неделю… Впрочем, на любую другую дисциплину уходит примерно столько же времени.

Детям проще, так как у них больше времени и они получают эту информацию дозировано в течение нескольких лет. Задача всех наставников и родителей таких детей – курировать процесс образования, давать новые знания, поддерживать живой интерес и не мешать, когда ребёнок хочет переориентироваться, допустим, из программирования в графический дизайн или наоборот. Графический дизайн нисколько не легче программирования: это по-своему очень сложное направление.

В целом все профессии ИТ-сферы достаточно сложные, они требуют определённого склада ума, характера. Но, пожалуй, самый главный навык – учиться. Технологии развиваются очень быстро, и чтобы не покрыться пылью на рынке труда, необходимо успевать.

Текущее взрослое поколение айтишников – в большей степени самоучки, институты как раньше не давали серьёзного погружения в профессию, так и не дают его сейчас. Но, к счастью, появились специализированные учебные центры, такие как Высшая Школа Программирования, которые имеют возможность и желание идти в ногу со временем, давать адекватную подготовку специалистам.

В нашей школе к каждому учащемуся индивидуальный подход. Мы помогаем уже на начальном этапе выявить склонности к конкретному направлению, даём фундаментальные знания, опираясь на которые можно освоить любое ответвление в ИТ.

Мир меняется с каждым годом, становится всё более технологичным, и, конечно, любая профессия, связанная с технологиями, будет востребована всегда. Детей уже сегодня нужно активно ориентировать и развивать в этом направлении. Даже если они не станут известными учёными, разработчиками, графическими дизайнерами, у них будет совершенно другой уровень компьютерной грамотности, а она сегодня необходима для любой сферы. Современный родитель должен это понимать, а ещё осознавать, что играть в компьютерные игры, заводить канал на YouTube – это полезно. Я как преподаватель могу сказать, что с каждым новым потоком учащихся воочию наблюдаю объективность этого заключения. Дети, у которых есть доступ к компьютеру, приставке, телефону, более развиты по всем аспектам: от скорости печати до усвоения новой сложной информации. Такие дети уже в возрасте 10 лет умеют учиться, а умение самообучаться очень важный навык.

Развивайтесь, развивайте своих детей, ведь жить в образованном обществе куда приятнее.

ВЫСШАЯ ШКОЛА ПРОГРАММИРОВАНИЯ

«Высшая Школа Программирования» *– образование в сфере ИТ/аутсорсинг компаний в сфере системной инженерии, программирования, web разработки и графического дизайна.*

itproger.com

«Манго Телеком»

— Девушка, а Вы где работаете?
— Я в облаках работаю!
— Вы стюардесса?
— Нет, ведь облака могут быть не только в небе, но и виртуальные. Я работаю в облачной компании страны «Манго Телеком»...

Я — та самая цепь взаимодействия между клиентами и сервисами; хочу, чтобы люди, с которыми коммуницирую изо дня в день, были счастливее и лучше, а их бизнес только рос и развивался.

Телекоммуникационная отрасль активно развивается, а вместе с ней — продукты и инструменты, которые позволят найти новые решения для оптимизации бизнес-процессов. Время требует высоких скоростей, хранения больших объёмов данных, надёжности и сохранности их передачи, а также бесперебойной связи.

«Манго Телеком» — крупная телекоммуникационная компания страны, один из ведущих поставщиков Saas-решений и абсолютный лидер российского рынка виртуальных АТС. MANGO OFFICE помогает клиентам найти современные решения для эффективного ведения бизнеса. Мы традиционно работаем на стыке телекома и ИТ, предоставляя одновременно облачные бизнес-приложения и услуги связи.

Услуги телефонии для бизнеса мы начали предоставлять с 2000 года и первыми запустили Виртуальную АТС в России. Сегодня у нас лидирующее по возможностям обработки звонков облачное решение, удостоенное множества наград и отмеченное профессиональным признанием. Обеспечиваем сервис высокого класса — 99,99% бесперебойности. Портфель «Манго Телеком» содержит 48 000 клиентов. **Наша главная цель** — помогать предпринимателям управлять бизнесом, а бизнесу — расти.

Мы сами разрабатываем софт и являемся главными пользователями своего продукта. Ориентируясь на потребности бизнеса любого клиента как новым компаниям на этапе стартап, так и крупным с филиальной сетью, MANGO OFFICE предоставляет софт:

- **Виртуальная АТС MANGO OFFICE**
  Облачная телефония для организации продаж, обслуживания и связи внутри бизнеса.
- **Коллтрекинг MANGO OFFICE**
  Профессиональный инструмент для оценки эффективности рекламы и её конверсии в сделки.
- **Контакт-центр MANGO OFFICE**
  Профессиональное облачное бизнес-приложение для управления и обработки обращений клиентов через голосовые и текстовые каналы.

Большим потенциалом для решения задач любого бизнеса обладает сервис «Виртуальная АТС» — это недорогое и не требующее первоначальных затрат решение, которое обеспечит полноценный контроль работы менеджеров, решит проблему потери звонков, позволит оценивать эффективность работы отдела продаж, контролировать и улучшать качество работы call-центра.

Все решения Mango Office — это не просто замена традиционной телефонии, но и инструмент для обеспечения роста бизнеса — роста продаж, качества обслуживания клиентов, улучшения бизнес-процессов, повышения квалификации и контроля сотрудников. Можно добиться снижения количества пропущенных вызовов, расширения воронки продаж, уменьшения времени обслуживания клиентов, увеличения индекса удовлетворённости клиентов, повышения эффективности рекламы.

Качественные услуги связи — неотъемлемая составляющая бизнес-процессов в компании, с их помощью выстраивается работа баз данных, внешних и внутренних систем и сервисов, а также обеспечивается безопасная передача информации.

Виртуальная АТС — это следующий эволюционный шаг, ещё более новое поколение офисных АТС, современного преемника устаревших «Железных» аналогов.

Ярослава Страшко
Компания «Манго Телеком»

MANGO OFFICE

Телекоммуникационная компания страны «Манго Телеком» *– один из ведущих поставщиков SaaS-решений и абсолютный лидер российского рынка виртуальных АТС.*

www.mango-office.ru

«РелКом»

Ирина Фролова
Компания «РелКом»

Современному человеку сложно представить жизнь без интернета. На мой взгляд, около 99 % бизнеса нуждается в получении качественных ИТ-услуг, без которых работа может просто «встать».

Сфера телекоммуникационных услуг является одной из самых перспективных, быстро развивающихся отраслей. Она охватывает широкое поле деятельности: от торговли и транспорта до финансирования, страхования и посредничества самого разного рода. Гостиницы и рестораны, прачечные и парикмахерские, учебные и спортивные заведения, туристические фирмы, радио- и телестанции, консультационные фирмы, медицинские учреждения, музеи, театры и кинотеатры – все они нуждаются в телекоммуникационных услугах.

В одной из таких компаний тружусь и я.

Группа компаний «Спарк Телл» оказывает услуги для качественного ведения бизнеса: предоставляет не только интернет и телефонию, но и ИТ-обслуживание и размещение в крупных ЦОДах.

В этой компании, как и в телекоммуникационной сфере, я работаю 3 года. На рынке «Спарк Телл» существует уже 12 лет. Свою деятельность она начала с обслуживания бизнес-центра, и по сей день многократно и эффективно реализовывает проекты по оснащению зданий и помещений внутренними слаботочными сетями, сетями электроснабжения, коммуникационным оборудованием, оборудованием бесперебойного электроснабжения, организации систем видеонаблюдения и охранной сигнализации и т.д.

За годы успешной работы накоплен богатый опыт, позволяющий компании предоставлять клиентам полный спектр телекоммуникационных услуг, гарантируя высокое качество сервиса и надёжность связи.

Ресурсное обеспечение – собственная обширная высокоскоростная волоконно-оптическая SDH-сеть на территории г. Москвы и Московской области, собственные технологические площадки, автономные системы, коммуникационные узлы, непосредственное присутствие на Московской Международной Телефонной Станции, тесные партнёрские отношения с более чем 1300 Операторами связи в России и за рубежом.

Мы сфокусированы на инфраструктурных проектах и не отвлекаемся на смежные области, решаем любую задачу, которая касается ИТ-инфраструктуры.

В данный момент наша компания открыла новое направление в предоставлении услуг, именуемое как «Агентство связи». Так как на рынке это достаточно новое направление, первоначально продажа и внедрение данной услуги являлись для меня и моих коллег чем-то необычным, неизвестным, а для наших клиентов и вовсе «тёмным лесом». Но в данный момент мы успешно продаём данную услугу, благодаря большому количеству партнёрских связей с другими поставщиками услуг.

Коллектив компании – главная её ценность – профессионалы с многолетним опытом работы на рынке телекоммуникационных услуг. Специалисты компании «РелКом» всегда предложат оптимальное решение конкретных задач клиента с учётом его материальных и технических возможностей, а также специфики бизнеса. А наша главная политика – индивидуальный подход к каждому клиенту с учётом его потребностей. Больше всего мы ценим доверие клиента.

В заключение я благодарю редакцию журнала «CIS» за предоставленную возможность рассказать о компании, которая вносит значительный вклад в ведение бизнеса различных отраслей. Также благодарю коллег, которые в начале моего пути поделились знаниями. И сегодня они являются моей второй семьёй, одним словом – Люди с большой буквы.

SPARK TELL

*Когда-то 12 лет назад **ООО «РелКом»** были маленьким местячковым провайдером с небольшим оборотом. Благодаря опытным сотрудником наша сеть и клиентская база выросла.*

А сейчас мы полноценное агентство связи информационных технологий, у нашей компании имеется собственная разветвленная сеть с точками присутствия на основных телекоммуникационных узлах Москвы.

sparktell.net

«Connect+»

Блондинка в ИТ. Как организовать успешный стартап?

Тяжело ли учиться красивой девушке в техническом ВУЗе на «мужской» специальности? Да, особенно если учесть все гендерные стереотипы, которые крепко укоренились в нашем обществе. Судьба занесла меня в МГТУ имени Баумана на факультет информатики и систем управления. Стоит ли говорить, что 95% обучающихся были парнями?

Постоянно приходилось доказывать, что тебя в мир информационных технологий занесло не случайно, а по велению души. Окончив ВУЗ с красным дипломом, я поняла, что большинство моих одногруппников обладали огромным количеством интересных идей, но многие их стартапы и задумки так и оставались в голове. Почему-то мужчинам-айтишникам тяжелее налаживать контакты и развивать свои проекты. К сожалению, технический склад ума не предполагает врождённый маркетинговый талант.

Моей мечтой было познакомить превосходных ИТ-специалистов с известными маркетологами и успешными предпринимателями. На мой взгляд, один из секретов построения успешного бизнеса – эффективный нетворкинг. Но я понимала, что начинающим стартаперам очень трудно заводить полезные бизнес-контакты. Так родилась идея создать приложение для бизнес-знакомств.

Увы, люди из одного профессионального круга редко выходят из зоны комфорта для поиска новых контактов и полезных связей. Будучи студенткой Бауманки, я решила получить дополнительное образование в бизнес-школе Ernst and Young. Мною двигали 2 цели: получение новых знаний и расширение круга знакомых. Мне хотелось общаться не только с айтишниками, но и с людьми из других интересных профессиональных сфер.

Цель была достигнута! Я познакомилась с замечательными специалистами, и мне пришла в голову идея создать приложение для оптимизации нетворкинга. Теперь я возглавляю свой проект Connect+. Основное образование позволяет мне разбираться в технической составляющей вопроса, а с помощью знакомых маркетологов получается прогрессивно развивать стартап.

Приложение является неким «Тиндером» для бизнеса, однако здесь люди ищут не любовь, а полезные контакты. В период пандемии наш проект обретает особую популярность: бизнес-встречи можно проводить, не выходя из дома, а также искать новых партнёров. В сложное нынешнее время мы за безопасный и бесконтактный нетворкинг.

Пандемия стала для меня настоящим толчком! Кто знает, каким мир будет после неё? Возможно, нам надолго придётся «зависнуть» онлайн. Я как руководитель проекта понимаю, что для бизнесменов из абсолютно разных сфер наступают непростые времена, многие страны опасаются повторной волны короновирусной инфекции. Мой проект позволяет искать подходящих бизнес-партнёров рядом с вами. По профилям пользователей можно понять, будет ли полезен новый контакт именно для вашей сферы. Все конференции и стримы переносим в приложение.

Я уверена, что для создания своего бизнес-проекта нужны не только знания и мотивация, но и помощь опытных знакомых. Возможно, мне было легче наладить связь с «внешним» миром, потому что я не боюсь коммуникации с другими людьми, всегда за общение и эффективный нетворкинг!

Анастасия Староверова

Компания «Connect+»

Connect+

***Connect+**: «тиндер» для бизнеса.*

95% россиян стесняются знакомиться на бизнес-мероприятиях и за их пределами. Команда российских разработчиков придумала, как преодолеть эти страхи. Они разработали мобильное приложение на базе искусственного интеллекта, которое анализирует интересы пользователей и подсказывает полезных специалистов, даёт качественные рекомендации.

connectim. pro

«РДТЕХ»

Ольга Горохова
Компания «РДТЕХ»

Работать в ИТ – значит, быть в курсе инноваций. Даже если вы не являетесь техническим специалистом, то всегда обязаны быть на передовой технологий.

Например, мы – ИТ-маркетологи – используем в своей работе все возможные и максимально технологичные рекламные, PR- и аналитические инструменты и таким образом находимся в постоянном развитии. И это как минимум не скучно!

Начав работать в РДТЕХ, я, конечно, хотела включиться в развитие digital-инструментов, применяемых маркетологами. Наша команда очень профессиональная, поэтому всегда есть чему научиться друг у друга. Постоянно повышая свою квалификацию, приобретая новые умения и навыки, мы делимся ими с коллегами. Таким образом работа отдела получается кросс-функциональной и более эффективной.

Безусловно, мы не концентрируемся только на цифровых методах работы. Классический подход к B2B-маркетингу, оправдывающий себя на протяжении многих лет, предполагает активное участие в офлайн-мероприятиях. И это тоже замечательная возможность поддерживать себя в профессиональном тонусе: на ИТ-выставках и конференциях можно отслеживать существующие тренды и тенденции, общаться с коллегами, работающими в различных областях.

Период удалённой работы во время самоизоляции также не прошёл без новых идей, проектов и технологий. Мы получили возможность сосредоточиться на инструментах, которым до этого уделяли чуть меньше внимания. Например, мы активно занялись созданием видео-контента и его использованием в продвижении бренда и услуг компании. Кроме этого, мы реализовали несколько интереснейших проектов на стыке маркетинга, HR и PR. И, на удивление, стали ещё ближе и чаще общаться с коллегами из других подразделений.

О компании «РДТЕХ»

Компания «РДТЕХ» была основана в 1992 году, и на протяжении 28 лет она реализует проекты, направленные на повышение эффективности и конкурентоспособности бизнеса своих заказчиков.

РДТЕХ – Разумные Деловые Технологии. Это означает, что компания применяет весь интеллектуальный потенциал, чтобы технические возможности способствовали р азвитию и упрощали бизнес-процессы. РДТЕХ обеспечивает максимальную синергию ИТ и бизнеса и, как навигатор, помогает заказчику найти наиболее разумный путь к успеху, налаживая правильное взаимодействие между технологиями и деловыми процессами. Основная задача РДТЕХ – успешное развитие бизнеса клиентов за счёт перевода на более высокий уровень регулирования, эффективности, надёжности управленческих систем и ИТ-инфраструктуры.

Комплекс услуг РДТЕХ включает управленческий и технологический консалтинг, разработку и внедрение информационных систем.

РДТЕХ успешно выполнено свыше 700 проектов, созданы уникальные информационно-аналитические системы и типовые решения для крупных государственных и коммерческих структур на базе программных продуктов ведущих мировых производителей – лидеров рынка корпоративного программного обеспечения: Oracle, ABBYY, FICO, Huawei, IBM, Informatica, Microsoft, SAS, TmaxSoft.

РДТЕХ

Компания «РДТЕХ» *основана в 1992 году и более 25 лет реализует проекты, направленные на повышение эффективности и конкурентоспособности бизнеса своих заказчиков. Комплекс услуг «РДТЕХ» включает управленческий консалтинг, разработку и внедрение информационных систем, технологический консалтинг.*

rdtex.ru

«ПраймЛинк Телекоммуникации»

Компания «ПраймЛинк Телекоммуникации» предоставляет телекоммуникационные услуги на базе широкополосной сети передачи данных, построенной по технологии IP/MPLS/Ethernet и CWDM, охватывающей крупные города России: Москву, Санкт-Петербург, Тверь, Великий Новгород.

Высокоскоростная IP-магистраль соединяет сеть ПраймЛинк с крупными центрами в Европе: Стокгольмом, Лондоном, Амстердамом, Франкфуртом-на-Майне и другими. Организация работает со многими операторами России. Заключены долгосрочные договоры с крупными государственными компаниями. Более подробно опишу об интернете, без которого невозможно существовать в наше время.

«ПраймЛинк Телекоммуникации» образована в 2003 году, а в 2019 – вошла в группу компаний SparkTell. Небольшой коллектив нашей компании профессионально обслуживает сферу ИТ-услуг. Моя задача выяснять, какие услуги необходимы клиенту, и контролировать подключение таковых точно в срок (я – менеджер по работе с клиентами). В компании работаю уже более трёх лет и с интересом слежу за новинками в ИТ-сфере.

Благодарна нашему коллективу и руководству компании за поддержку и помощь!

Спасибо большое сотрудникам журнала Beauty & Digital – 2020 за возможность рассказать о своей компании!

Подробнее об услугах компании:

1. Предоставление интернета по LTE

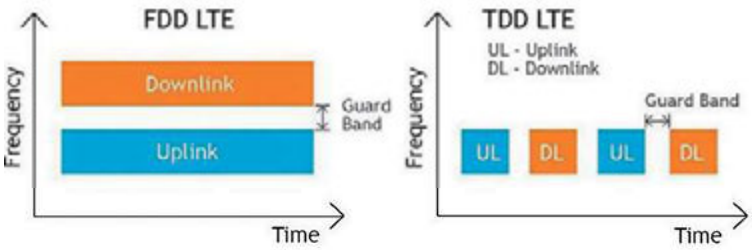
LTE (от англ. Long-Term Evolution) – это стандарт беспроводной высокоскоростной передачи данных для мобильных устройств, а также точечное подключение одного рабочего места.

Основан он на всё тех же GSM/UMTS протоколах, но теоретические и реальные скорости передачи данных в сетях LTE значительно выше, порой превосходят проводные соединения.

Стандарт LTE бывает двух видов, различия между которыми довольно существенны. FDD (Frequency Division Duplex) – частотный разнос входящего и исходящего канала. TDD (Time Division Duplex) – временной разнос входящего и исходящего канала. Можно сказать, что FDD – это параллельный LTE, а TDD – последовательный. Например, при ширине канала в 20 МГц в FDD LTE часть диапазона (15 МГц) отдаётся для загрузки (download), а часть (5 МГц) – для выгрузки (upload). Таким образом, каналы не пересекаются по частотам, что позволяет работать одновременно и стабильно для загрузки и выгрузки данных. В TDD LTE всё тот же канал в 20 МГц полностью отдаётся как для загрузки, так и для выгрузки, а данные передаются и в ту, и в другую сторону поочерёдно, при этом приоритет имеет всё-таки загрузка. В целом FDD LTE предпочтительнее, т. к. он работает быстрее и стабильнее.

Яна Бильданова

Компания «ПраймЛинк Телекоммуникации»



LTE FDD и LTE TDD: в чём отличия?

Оборудование для установки и подключения

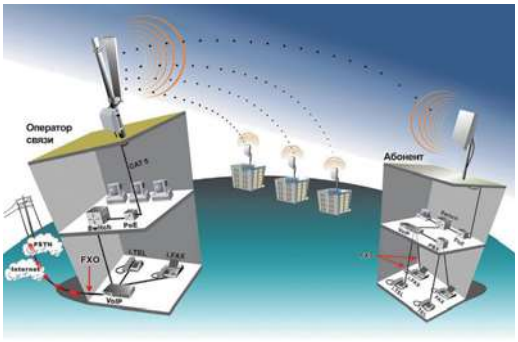
Маршрутизатор MikroTik SXT LTE kit, крепление, зарядка, кабель.

Антенна MIMO, роутер, кабель, крепеж для антенны.

Фото работ наших специалистов по установке оборудования LTE

Установка оборудования на стройке.

2. Предоставление интернета по радио-каналу



Этот вид интернет-соединения построен на оборудовании операторского класса. При данном методе подключения используются направленные антенны, которые направляются на антенны-сектора, установленные на базовых станциях. К одному сектору может быть привязан как один клиент (если ему нужна высокая скорость и доступность), так и несколько клиентов с невысокими параметрами подключения.

Преимущество такого метода подключения заключается в том, что можно обеспечить высокоскоростной связью удалённый объект, до которого нецелесообразно прокладывать оптические линии связи либо проложить их не представляется технически возможным. Расстояния, на которые можно подключить абонента по такой технологии с гарантированной скоростью – до 20 км! При этом себестоимость подключения в разы дешевле «оптики».

Ещё одно преимущество интернета по радиоканалам – быстрое восстановление связи в случае повреждения оборудования. В отличие от долгого восстановления оптоволоконной линии в случае повреждения базовой станции, клиентская антенна просто поворачивается на соседнюю базу, и клиент продолжает работать, пока инженеры восстанавливают прежнюю базу. То же самое происходит при возникновении какой-то помехи (например, если кто-то установил на вашей частоте другие радиоустройства, что приводит к ухудшению связи): либо развернуть антенну клиента на другую базовую станцию на время устранения помехи, либо перевести на другую частоту. Это обеспечивает стабильность и постоянную заявленную скорость, в отличие от мобильных операторов.

Ещё один большой плюс технологии радиоканала заключается в скорости его развёртывания. Для подключения клиента требуется не более 4-х часов, в отличие, например, от подключения по волоконно-оптическим линиям, когда процесс может растянуться на месяцы, поскольку придётся получать разрешения и согласовывать с разными службами трассу прокладки «оптики».

Оборудование для установки и подключения

Ubiquiti UniFi AP LR-антенна.

Фото работ наших специалистов по установке оборудования

Установка антенны на крыше дома.

3. Предоставление интернета по ВОЛС или UTP

UTP кабель

ВОЛС кабель.

Волоконно-оптическая система передачи (ВОСП – официальный термин, определённый в ГОСТ Р 54417-2011), Волоконно-оптическая линия связи (ВОЛС – устоявшееся название) – волоконно-оптическая система, состоящая из пассивных и активных элементов, предназначенная для передачи информации в оптическом (как правило, ближнем инфракрасном) диапазоне.

ВОЛС в основном используются при строительстве объектов, при котором монтаж СКС должен объединить многоэтажное здание или здание большой протяжённости, а также при объединении территориально-разрозненных зданий.

Оборудование для установки и подключения

Оптоволоконное оборудование

Медиаконвертеры

Модули SFP, трансиверы

Сварочный аппарат для оптических волокон.

Фото работ наших специалистов по прокладке кабеля и установке оборудования

4. Виртуальный АТС

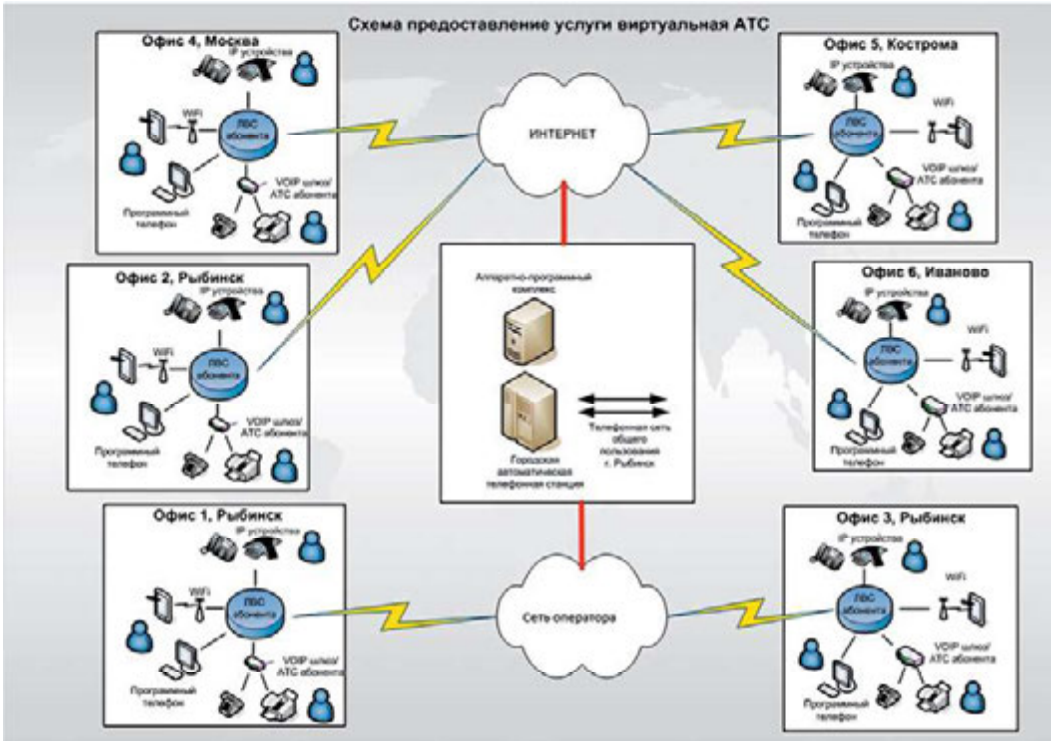


Схема предоставления Виртуальной АТС

Виртуальная АТС (от англ. — Hosted PBX), или облачная АТС — это услуга обеспечения телефонной связи для компаний, которая заменяет физическую офисную мини-АТС и даже колл-центр. Суть услуги состоит в том, что клиент (компания) получает в полное пользование IP-АТС, физически размещённую у провайдера (отсюда и слово — виртуальная), и оплачивает единовременно стоимость подключения услуги или абонентскую/арендную плату за использование на постоянной основе.

Виртуальная АТС предоставляет все стандартные возможности IP-АТС: многоканальный номер, запись разговора, голосовое приветствие, перевод вызова — всё это и многое другое доступно через Интернет без приобретения специализированного коммутационного оборудования. Конечные пользователи используют VoIP-телефоны или программные приложения IP-телефонии.

Наша компания предлагает в базовой комплектации минимальные возможности (например, 1 городской номер и 2-5 учётных записей конечных пользователей без каких-либо расширенных функций АТС). Расширение числа сотрудников и дополнительные возможности в этом случае активируются за дополнительную плату.

5. Облачный сервер

Виртуальный или облачный сервер (он же VPS — Virtual Private Server или VDS — Virtual Dedicated Server) — услуга хостинг-провайдеров, когда клиент получает в своё распоряжение эмуляцию физического сервера со всеми компонентами: процессором, оперативной памятью, дисковым пространством. Можно установить на него любую серверную ОС и программное обеспечение.

По функциональности виртуальный сервер ничем не отличается от физического, но на одном таком сервере может запускаться несколько виртуальных. Именно благодаря этому цены на виртуальные серверы ниже, а возможности такие же.

Так же одним из главных преимуществ виртуального сервера является возможность в любой момент увеличить его производительность: количество ядер процессора, объём оперативной памяти или ёмкость дискового пространства.

«Smart Meal Service»

Анна Никитченко

Компания «Smart Meal Service»

Жизнь слишком коротка, чтобы работать над задачами, которые вам не интересны. В первом классе я хотела быть актрисой. Потом владелицей книжного магазина или ресторана. Но сейчас прекрасно понимаю, что я на своём месте.

Сегодня я являюсь управляющим партнёром консалтинговой компании O2Consulting и генеральным директором технологического стартапа Smart Meal Service. Я осознаю, что занимаюсь любимым делом, чем-то действительно значимым для огромного числа людей, в этом есть драйв, радость, азарт и даже порой отчаяние. Ничто не мотивирует лучше, чем движение к великой, значимой лично для тебя цели, формируется желание действовать, улучшать мир шаг за шагом. Каждую сферу своей жизни я стараюсь модернизировать, целенаправленно работая над ней. При этом если обобщить мою деятельность, то я стараюсь быть абсолютно чистой в мыслях и действиях. Поэтому сегодня я достигла заветного баланса между любимым делом и счастливой семьёй.

В O2Consulting мы работаем на стыке государства и бизнеса, помогая и тем, и другим. Например, помогаем регионам не просто создавать ТОР (территории опережающего развития), стратегии социально-экономического развития, но и под концептуальные решения сразу заключать соглашения о намерениях с ключевыми контрагентами – с крупнейшими инвесторами по всему миру, в результате чего привлекаются реальные инвестиции и создаются новые рабочие места. А бизнесу помогаем выстраивать отношения с властями: получать различные меры поддержки, подбирать наиболее подходящее место размещения производства. Также мы занимаемся внедрением инструментов открытых инноваций и решаем задачи, связанные с цифровизацией экономики регионов Российской Федерации.

В 2019 году мы вышли за рамки чистого консалтинга и создали свой технологический стартап – Smart Meal Service, у которого уже есть первые продажи и нейросеть, практически не имеющая аналогов во всём мире. Целью проекта является создание и коммерциализация робота кассира Lunch fastPass, представляющего собой кассовый терминал для самообслуживания в столовых и заведениях формата fast casual. Терминал способен заменить кассира, поскольку может быстро и точно распознавать блюда, используя специально созданную архитектуру нейронных сетей. Комплексное программно-аппаратное решение Lunch fastPass включает в себя модули распознавания блюд, учёта скидки и оплаты (идентификация и оплата по RFID-карте, QR-коду, распознаванию лица), сбора больших данных и анализа пищевого поведения. В настоящее время готова первая версия терминала, ведётся подготовка к тестированию на площадках потенциальных клиентов – крупнейших кейтеринговых операторов в России.

Работа наших компаний уникальна и эффективна, а секрет успеха в команде – в постоянном мощном развитии. Каждый год мы бьём рекорды прошлого года и на грани невозможного намечаем новые горизонты. Верим, что мир меняется только тогда, когда сами прилагаем усилия к его изменению. И мы точно знаем, что миссия выполнима!

O2CONSULTING

*Сферой деятельности **«Smart Meal Service»** являются работы в области компьютерных технологий и консультативная деятельность в области организации общественного питания.*

smartmealservice.com

CISummIT

Мероприятие журнала CIS

Благотворительная ИТ-конференция Digital Hearts

15 октября, 2020

Площадка «Москва-Сити»

Фонд Хабенского

Мероприятие журнала CIS в поддержку Фонда Константина Хабенского

Заполните регистрационную форму для участия на мероприятии

Ждём вас на благотворительной ИТ-конференции CISummIT Digital Hearts, которая объединит самых активных участников ИТ-рынка, ведущих производителей и экспертов, чтобы собрать средства для помощи детям с заболеваниями головного мозга.

CIS Современные Информационные Системы

www.cisevent.ru
www.cismag.news
www.cis.ru

«Всё своё ношу с собой»

BYOD и карантин

Эпидемия COVID-19 выявила массу проблем, к которым, как оказалось, никто не был готов. Мало того, об этом никто даже не задумывался. Одна из таких проблем — использование персональных устройств для рабочих целей.

Вспомним, что такое BYOD?

Технология BYOD – Bring Your Own Device – это модная в последнее десятилетие (после кризиса в 2008 году, если точнее) тема экономии на рабочих станциях для сотрудников. Логика проста: если для работы людям не покупать оборудование, а предлагать приносить своё (ноутбуки, смартфоны), то это получается гораздо дешевле как в разовой покупке, так и в обновлении парка техники, и в обслуживании.

С последним, конечно, всё не так однозначно: по факту первичная экономия быстро снижается из-за резкого роста расходов на поддержку и обеспечение безопасности. Одно дело, когда люди работают на рабочей станции компании, к которой применяются жёсткие централизованные политики по установке ПО и настройкам, другое – когда это личный компьютер сотрудника, где нельзя выставить нужные настройки, так как это «не твоё».

Однако тема экономии средств в связи с кризисом отошла на второй план. Нам с вами может нравиться или не нравиться, но в карантин всё же большинство сотрудников вынуждено работать на своих устройствах (как компьютерах, так и смартфонах). Естественно, это приводит к образованию своего рода зоопарка, а следовательно, и к появлению головной боли как у ИТ, так и у ИБ.

В **Отчёте об интеллектуальном управлении информацией** за **2019 г.** респонденты указали, что:

- Более 60% сотрудников используют персональные приложения для обмена файлами и/или персональные устройства для доступа и обмена информацией о компании
- Более половины компаний (52%) не одобряют или запрещают использование персональных устройств

Самые страшные угрозы безопасности BYOD

Группа информационной безопасности LinkedIn и исследование **BYOD & Mobile Security**, проведённое Crowd Research Partner в 2016 году, обнаружили, что затраты не всегда являются основным мотиватором внедрения BYOD. К основным мотивам можно отнести:

- Увеличение мобильности сотрудников (63%)
- Удовлетворённость сотрудников (56%)
- Производительность (55%)

Сегодня к этим мотивам, несомненно, добавился карантин.

Несмотря на преимущества, более трети профессионалов в области безопасности признают, что программа BYOD накладывает серьёзное бремя на ресурсы безопасности компании, согласно тому же исследованию.

Риски безопасности BYOD

Утечка данных

Независимо от того, нужен ли вашим сотрудникам доступ к корпоративной электронной почте или защищённой информации о заработной плате через мобильный телефон (персональный компьютер), утечка данных возможна, когда в игру вступают персональные устройства. Данные могут быть утеряны или раскрыты, если устройства утеряны или украдены, или если на персональном устройстве установлено вредоносное ПО. В то время как облачные технологии снизили большую часть потерь данных из-за повреждения устройства, резервные копии имеют решающее значение для работоспособной программы BYOD.

Способы предотвращения утечки данных включают в себя:

- **Управление мобильными устройствами.** В случае потери или кражи программа MDM может позволить ИТ-специалистам удалённо очистить устройство, чтобы обеспечить защиту конфиденциальной информации
- **Более разумное предоставление данных** – предоставление минимально необходимых прав доступа к данным
- **Использование сегрегации приложений и/или VPN.** Сегрегация и VPN предотвращают утечку конфиденциальных данных через схематичные общедоступные беспроводные точки доступа и могут создавать барьеры между личным и рабочим контентом на персональном устройстве

Вредоносные приложения

Далеко не все приложения, установленные пользователями, являются такими, какими они кажутся. Ещё не так давно закончилось всеобщее увлечение Pokemon Go, пришла пора новых игр. И так будет всегда. Увы, это порождает огромное количество подделок и вредоносных приложений. Некоторые из подтверждённых вредоносных приложений включали в себя такие названия, как Pokémon Go Ultimate, Guide & Cheats for Pokémon GO и Install Pokémongo, чтобы привлечь внимание поклонников игры.

Кроме того, далеко не всегда на домашних ПК установлено лицензионное программное обеспечение. Да и вспомним, что редко где соблюдается правило, при котором каждый пользователь работает под своей учётной записью.

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

В некоторых случаях вредоносные приложения могут взять под контроль мобильное устройство пользователя. Это может привести к слежке, а также к потере личной или рабочей информации. Поэтому ваши пользователи нуждаются в обучении передовым методам защиты приложений. Это основанное на глубоких знаниях обучение должно включать в себя важность загрузки контента только из магазинов приложений. Во многих случаях вредоносные приложения загружаются через веб-страницы.

Возможность кражи данных

Политика BYOD позволяет легко оставаться на связи с вашими сотрудниками. Но что, если они в аэропорту отправят файл по незащищённой сети Wi-Fi? Подумайте о рисках раскрытия этой информации хакерами, которые ищут доступ к критически важным системам компании, ведь интересно, как подключиться к системам, используя информацию (учётки/пароли/адреса), которую можно перехватить в аэропорту.

Хакеры найдут возможности для кражи данных, и практика BYOD может стать для них отличной средой для этого.

Потенциальные правовые вопросы

Репутация организации может быть серьёзно повреждена, если нарушение безопасности через устройство сотрудника приводит к утечке важной информации о ваших клиентах или деловых партнёрах. Это означает, что возможно иметь дело с судебными разбирательствами с разных сторон.

Утеря или кража устройства

Сотрудник потерявший устройство может превратиться из большого неудобства в катастрофу для всей вашей компании, если не будет соблюдать рекомендуемые меры безопасности. Что, если у него не было безопасного пароля для входа в систему компании? Что, если этот пароль легко найти, например он хранил его где-то на своём устройстве?

Даже если работник всё сделал правильно, хакеры теперь имеют доступ к более сложным технологиям. Кто-то с достаточной решимостью и навыком может взломать безопасный пароль или идентификатор отпечатка пальца.

Недостаток обучения сотрудников

Многие нарушения безопасности происходят в результате ошибок, допущенных сотрудниками. Они могут не полностью понимать требования компании, когда речь идёт о защите их устройства. Требуете ли вы, чтобы сотрудники посещали практические занятия или просто подписывали документ, подтверждающий, что они понимают политику компании? Неадекватное обучение может привести к ошибкам сотрудников, которые могут поставить под угрозу безопасность систем вашей компании.

Недостаток управления

С любым мобильным устройством сотрудника или владельца компании есть риск, связанный с потерей контроля над ним. Когда устройство «выходит» из здания компании, его трудно контролировать или невозможно: использует ли оно сомнительные бесплатные беспроводные соединения или будет утеряно либо украдено.

Ещё сложнее контролировать домашнее устройство. Более того, очень часто пользователи возражают против подобного контроля.

Защита мобильных устройств и ноутбуков требует от ИТ-специалистов сосредоточения внимания на сочетании безопасности устройств, многоуровневой защиты и более разумного обеспечения.

- **Управление мобильными устройствами** – MDM позволяет сотрудникам удалённо контролировать содержимое и безопасность устройства сотрудника. В сочетании с мониторингом целостности файлов ИТ-специалисты могут установить оптимальный уровень контроля
- **MAM (Mobile Application Management)** – управление мобильными приложениями, добавление политик безопасности, разделение мобильного устройства на личное и рабочее пространства и т. д.
- **Единая регистрация** – экран блокировки, защищённый паролем, вероятно, недостаточно защищён для конечных точек. Отделяя и защищая ваши мобильные приложения с помощью требования единого входа (SSO), ИТ-специалисты могут включить интеллектуальную аутентификацию пользователей без ущерба для производительности
- **Если же речь идёт о работе на домашнем компьютере, стоит понимать необходимость настройки VPN и удалённого доступа.** Более того, на мой взгляд, идеальным является вариант, когда пользователь использует домашнее устройство в режиме терминала, не имея доступа к личному жёсткому диску

Заражение устройства

Подавляющее большинство пользователей с заражённым смартфоном не знают, что на их устройстве находится вредоносное ПО.

Устаревшие мобильные операционные системы могут быть основным фактором риска, поскольку некоторые из форм вредоносного ПО в первую очередь влияют на устаревшие ОС. В любой программе BYOD ИТ-специалисты должны следить за тем, чтобы мобильные операционные системы были обновлены. Чрезвычайно важно вовремя обнаруживать рутованность или jail break устройств, чтобы не допускать их в корпоративную сеть.

На мой взгляд, хорошей практикой является, увы, чаще всего неосуществимое требование: пользователь должен работать со смартфоном, на котором установлена последняя или пред-

последняя версия ОС. Почему это неосуществимо? Потому что в случае применения Android пользователь должен максимум раз в два года менять свой смартфон. В наших условиях это маловероятно.

Наличие и настройка политик безопасности

Возможно попробовать программу BYOD без эффективных политик безопасности, но это, безусловно, рискованно. Если ваша организация обязана соблюдать требования PCI DSS, HIPAA или любые другие нормативные требования, необходима эффективная политика, чтобы избежать штрафов.

Используя комбинацию письменной политики и администрирования на основе политик, ИТ-специалистам следует:

- Использовать устойчивые пароли, экраны блокировки и единый вход
- Помнить о необходимости защищённого подключения к сети
- Обязательно использовать VPN
- Обязательно устанавливать обновления и исправления в реальном времени
- Помнить, что отслеживать местоположение могут многие приложения. Не забывать смотреть, какие права нужны тому или иному приложению
- Управлять мобильными устройствами

Смешивание личного и делового использования

С BYOD сочетание личного использования и использования в рабочих целях неизбежно. Вы не можете контролировать, будут ли ваши сотрудники совершать покупки в Интернете на скомпрометированных веб-сайтах или неправильно устанавливать новые приложения (игры) на устройство. Несмотря на то, что вы можете много знать о передовых методах обеспечения безопасности, но не сможете гарантировать, что ваши сотрудники не будут одалживать своё устройство другу или использовать общедоступные беспроводные соединения для сохранения данных.

В связи с этим вашей службе безопасности придётся использовать наиболее разумные методы защиты, включающие в себя:

- **Разделение приложений** – создание барьера между личным и рабочим использованием устройства может предотвратить случайный доступ к рабочим данным
- **Использование VPN** – может защитить данные от перехвата, даже если сотрудники попытаются использовать беспроводную сеть кафе
- **Мониторинг целостности файлов** – ИТ-специалисты могут получить доступ к негативным изменениям критических системных файлов, что позволяет им действовать немедленно

Кроме того:

- **Продумайте и протестируйте свою политику BYOD,** прежде чем применять её в масштабах всей компании
- **Проведите инвентаризацию каждого персонального устройства,** подключённого к вашей сети
- **Проводите периодические проверки вашей политики BYOD**

Неспособность управлять устройствами

Что, если сотрудник покидает организацию или теряет мобильное устройство? Во многих программах BYOD большая часть проблем безопасности связана с отсутствием контроля над устройствами. Сотрудники не всегда осторожны, а недовольные сотрудники могут нанести большой ущерб.

Важное значение имеют управление мобильными устройствами и разумное управление доступом. Если сотрудник уволен или начинает демонстрировать сомнительное поведение, политика должна поддерживать вашу способность немедленно отозвать доступ к конфиденциальным данным, прежде чем произойдут утечки.

Возможна ли безопасность BYOD?

Обеспечить безопасность личного устройства не так просто. В целом проблема решаема, многое зависит от топ-менеджмента, который привносит идеологию BYOD в компанию, а потом начинается… Подобные привилегии для себя пробивают приближённые к руководству топ-менеджеры, потом их замы и руководители среднего звена и т.д. Поэтому здесь лучше последовать правилу: не можешь предотвратить – возглавь. И тогда, составив грамотные политики, выбрав правильные инструменты, подписав с сотрудником дополнительное соглашение (что тоже важно), можно построить защищённый BYOD, который будет удобен пользователям и соответствовать требованиям компании с точки зрения безопасности.

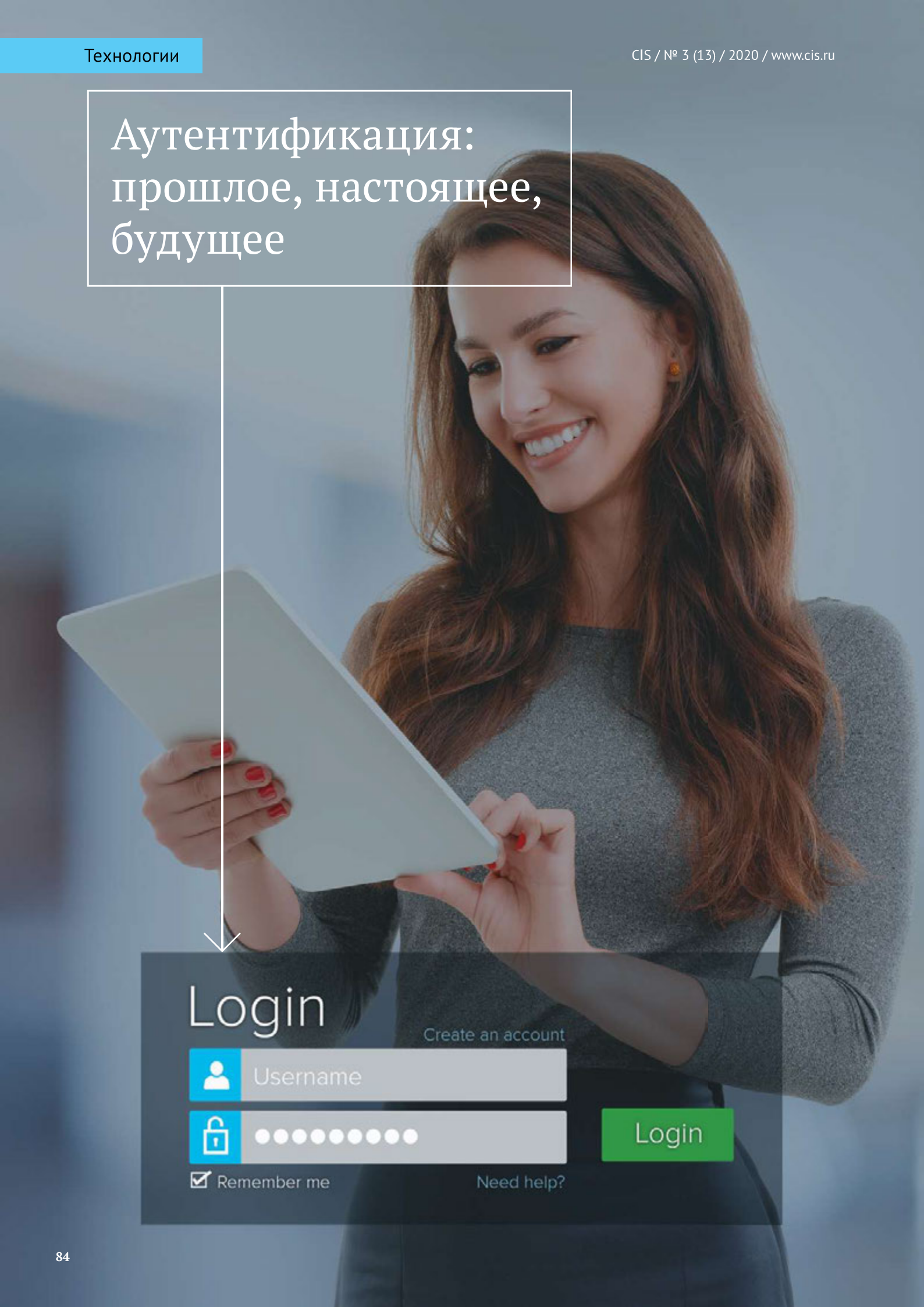
Да, гораздо проще контролировать принадлежащие компании мобильные устройства, особенно если все сотрудники используют единую модель и операционную систему. Тем не менее безопасность BYOD возможна с помощью правильных инструментов.

В дополнение к лучшим техническим практикам, таким как использование VPN, SSO, MDM, MAM, VDI, терминальные сервисы, контейнеризация приложений и т.д., командам безопасности также необходимы инструменты для оценки целостности устройства.

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

CIS / № 3 (13) / 2020 / www.cis.ru

Аутентификация: прошлое, настоящее, будущее



Одной из основных проблем информационной безопасности, особенно с увеличением количества сотрудников, работающих удалённо, является проблема аутентификации.

С давних пор решение доступа было связано с использованием паролей. Но сегодня с учётом психологии пользователей применение паролей становится небезопасным по целому ряду причин:

- всё больше пользователей применяет один и тот же пароль и в корпоративной сети, и для личных нужд
- пароли пользователей, как правило, содержат словарные слова либо так или иначе связаны с личностью самого пользователя (имя жены, ребёнка, название любимой футбольной команды, номер и марка автомобиля и т.д.), а так как сегодня многие описывают свою жизнь в социальных сетях достаточно подробно, то такие пароли легко взламываются.

В дальнейшем эти требования будут только ужесточаться. К чему это приведёт, вернее, уже привело? Чем сложнее пароли, чем больше приложений требуют ввод пароля, тем выше вероятность того, что пользователи для всех приложений, в том числе и для аутентификации в ОС, будут использовать один и тот же пароль, к тому же записывая его на бумаге. Хорошо это или плохо? Допустимо ли?

С одной стороны – явно недопустимо, так как резко возрастает риск компрометации пароля, с другой – слишком сложный пароль (например, PqSh*98+) трудно удержать в памяти. Вероятно, что пользователи будут или выбирать простой пароль, или постоянно забывать сложный и отвлекать администратора от более важных дел.

Исследования Gartner показывают, что от 10 до 30% звонков в службу технической поддержки компаний составляют просьбы сотрудников восстановить забытые ими пароли.

По данным IDC, каждый забытый пароль обходится организации в 10-25 долл. Добавим сюда ещё необходимость его постоянной смены и требование оригинальности паролей. Что делать? Какой выход?

Но уже сегодня существует несколько вариантов решения этой проблемы.

Первый вариант. На видном месте в комнате (на стене, на столе) вывешивается плакат с лозунгом. После этого в качестве пароля используется текст, содержащий, предположим, каждый третий символ лозунга, включая пробелы и знаки препинания. Не зная алгоритма выбора знаков, подобный пароль подобрать довольно сложно.

Второй вариант. В качестве пароля выбирается (генерируется с помощью специального ПО) случайная последовательность букв, цифр и специальных символов. При этом указанный пароль распечатывается на матричном принтере на специальных конвертах, которые нельзя вскрыть, не нарушив их целостность. Примером такого конверта может служить конверт с PIN-кодом к платёжной карте. Эти конверты хранятся в сейфе начальника подразделения или в сейфе службы информационной безопасности. Единственной сложностью при таком способе является необходимость немедленной смены пароля сразу после вскрытия конверта и изготовления другого подобного конверта с новым паролем, а также организация учёта конвертов. Но если принять во внимание экономию времени администраторов сети и приложений, то эта плата не является чрезмерной.

Третий вариант – использование многофакторной аутентификации на базе новейших технологий аутентификации. В качестве примера рассмотрим двухфакторную аутентификацию. Основным преимуществом такой аутентификации является наличие физического ключа и PIN-кода к нему, что обеспечивает дополнительную устойчивость к взлому. Ведь утрата аппаратного ключа не влечёт за собой компрометацию пароля, поскольку, кроме ключа, для доступа к системе нужен ещё и PIN-код.

Отдельно стоит рассмотреть системы с применением разовых паролей, которые получают всё большее распространение в связи с широким развитием интернет-технологий, и системы биометрической аутентификации.

Системы биометрической аутентификации

Технологией, особенно широко рекламируемой при использовании смартфона, является биометрическая аутентификация на основе использования отпечатка пальца, радужки глаза. Реже встречается трёхмерный снимок лица или так называемый «клавиатурный» почерк.

Наиболее распространены следующие виды биометрической аутентификации:

- по отпечатку пальца
- по лицу, как по двухмерному, так и по трёхмерному изображению
- по голосу
- по радужной оболочке глаза
- по геометрии ладони или рисунку вен на ладони

Классификация средств идентификации и аутентификации

Современные программно-аппаратные средства идентификации и аутентификации по виду идентификационных признаков можно разделить на электронные, биометрические и комбинированные (рис. 1). В отдельную подгруппу в связи с их специфическим применением можно выделить входящие в состав электронных средств системы одноразовых паролей.

В электронных системах идентификационные признаки представляются в виде кода, хранящегося в защищённой области памяти идентификатора (носителя) и, за редким

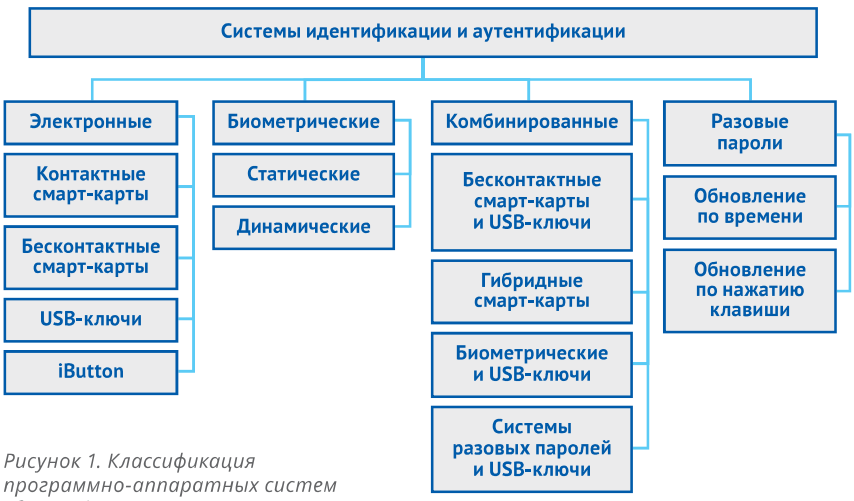


Рисунок 1. Классификация программно-аппаратных систем идентификации.

исключением, фактически не покидающего её. Идентификаторы в этом случае бывают следующие:

- контактные смарт-карты
- бесконтактные смарт-карты
- USB-ключи (USB-token)
- iButton

В биометрических системах идентификационными являются индивидуальные особенности человека, которые в данном случае называются биометрическими признаками. Идентификация производится за счёт сравнения полученных биометрических характеристик и хранящихся в базе шаблонов. В зависимости от характеристик, которые при этом используются, биометрические системы делятся на статические и динамические.

Статическая биометрия основывается на данных (шаблонах), полученных путём измерения анатомических особенностей человека (отпечатки пальцев, узор радужки глаза и т.д.), а динамическая – на анализе действий человека (голос, параметры подписи, её динамика).

На мой взгляд, биометрические системы аутентификации не получили широкого распространения по нескольким причинам:

- высокая стоимость подобных систем
- отсутствие хорошо подготовленного профессионального персонала
- сложность настройки таких систем
- противодействие со стороны сотрудников, так как руководство получает возможность контролировать все их перемещения и фактически производить контроль рабочего времени

В комбинированных системах применяется одновременно несколько признаков, причём они могут принадлежать как к системам одного класса, так и к разным.

Биоэлектронные системы

Как правило, для защиты компьютерных систем от несанкционированного доступа применяется комбинация из двух систем: биометрической и контактной на базе смарт-карт или USB-ключей.

Что скрывается за понятием «биометрия»? Фактически мы используем такие технологии каждый день, но как технический способ аутентификации биометрия стала применяться относительно недавно. Биометрия – это идентификация пользователя по уникальным, присущим только ему одному биологическим признакам. Такие системы являются самыми удобными, с точки зрения самих пользователей, поскольку не нужно ничего запоминать, а потерять биологические характеристики весьма сложно.

При биометрической идентификации в базе данных хранится цифровой код, ассоциированный с определённым человеком. Сканер или другое устройство, используемое для аутентификации, считывает конкретный биологический параметр. Далее он обрабатывается по определённым алгоритмам и сравнивается с кодом, содержащимся в базе данных.

Просто? С точки зрения пользователя – безусловно. Но у данного метода существуют как достоинства, так и недостатки.

К **достоинствам** биометрических сканеров обычно относят то, что они никак не зависят от пользователя (например, пользователь может ошибиться при вводе пароля) и тот не может передать свой биологический идентификатор другому человеку, в отличие от пароля. А подделать уникальный узор, имеющийся на пальце у каждого человека, практически невозможно. Но, как показали исследования, проведённые в США, биометрические сканеры, основанные на отпечатках пальцев, довольно легко вводили в заблуждение с помощью муляжа отпечатка пальца или даже пальца трупа. Распространён также отказ в доступе, осуществляемый на основании распознавания голоса, если человек, например, простыл. Но самый большой недостаток биометрических систем – это их высокая цена.

Все биометрические технологии можно разделить на две группы:

- статические методы, которые основываются на физиологической (статической) характеристике человека, то есть уникальном свойстве, присущем ему от рождения и неотъемлемом от него. К статическим биологическим признакам относятся форма ладони, отпечатки пальцев, радужная оболочка, сетчатка глаза, форма лица, расположение вен на кисти руки и т.д.
- динамические методы, которые основываются на поведенческой (динамической) характеристике человека – особенностях, характерных для подсознательных движений в процессе воспроизведения какого-либо действия (подписи, речи, динамики клавиатурного набора)

Идеальная биометрическая характеристика человека (БХЧ) должна быть универсальной, уникальной, стабильной и собираемой.

- **Универсальность** – наличие биометрической характеристики у каждого человека
- **Уникальность** – не может быть двух человек, имеющих идентичные значения БХЧ
- **Стабильность** – независимость БХЧ от времени
- **Собираемость** – возможность получения биометрической характеристики от каждого индивидуума

Реальные БХЧ не идеальны, и это ограничивает их применение. В результате экспертной оценки таких источников БХЧ, как форма и термограмма лица, отпечатки пальцев, геометрия руки, структура радужной оболочки глаза (РОГ), узор сосудов сетчатки, подпись, особенности голоса, форма губ и ушей, динамика почерка и походки было установлено, что ни один из них не удовлетворяет всем требованиям по перечисленным выше свойствам. Необходимым условием использования тех или иных БХЧ является их универсальность и уникальность, что косвенно может быть обосновано их взаимосвязью с генотипом или кариотипом человека.

Распознавание по отпечаткам пальцев

Это самый распространённый статический метод биометрической идентификации, в основе которого лежит уникальность для каждого человека рисунка папиллярных узоров на пальцах. Изображение отпечатка пальца, полученное с помощью специального сканера, преобразуется в цифровой код (свёртку) и сравнивается с ранее введённым шаблоном (эталоном) или набором шаблонов (в случае аутентификации).

Ведущие производители сканеров отпечатков пальцев:

- BioLink – www.biolink.ru
- Bioscrypt – www.bioscrypt.com
- DigitalPersona – www.digitalpersona.com
- Precise Biometrics – www.precisebiometrics.com

Ведущие производители сенсоров (считывающих элементов для сканирующих устройств):

• Atmel – www.atmel.com
• Fujitsu – www.fujitsu.com

Распознавание по форме руки

Данный статический метод построен на распознавании геометрии кисти руки, также являющейся уникальной биометрической характеристикой человека. С помощью специального устройства, позволяющего получать трёхмерный образ кисти руки (некоторые производители сканируют форму нескольких пальцев), делаются измерения, необходимые для получения уникальной цифровой свёртки, идентифицирующей человека.

Ведущий производитель такого оборудования:

• Recognition Systems – www.recogsys.com

Распознавание по радужной оболочке глаза

Данный метод распознавания основан на уникальности рисунка радужной оболочки глаза. Для реализации этого метода необходима камера, позволяющая получить изображение глаза человека с достаточным разрешением, и специализированное программное обеспечение, выделяющее из полученного изображения рисунок радужной оболочки глаза, по которому строится цифровой код для идентификации человека.

Фирма Iridian (www.iridiantech.com) – крупнейший производитель в данной области, на её решениях базируются практически все разработки таких компаний, как LG, Panasonic, OKI, Saflink и др.

Распознавание по форме лица

В данном статическом методе идентификации строится двух- или трёхмерный образ лица человека. С помощью камеры и специализированного программного обеспечения на изображении или наборе изображений лица выделяются контуры бровей, глаз, носа, губ и т.д., вычисляются расстояния между ними и другие параметры в зависимости от используемого алгоритма. По этим данным строится образ, который преобразуется в цифровую форму для сравнения. Причём количество, качество и разнообразие (разные углы поворота головы, изменение нижней части лица при произношении ключевого слова и т.д.) считываемых образов может варьироваться в зависимости от алгоритмов и функций системы, реализующей данный метод.

Ведущие производители подобных устройств:

• Cognitec Systems – www.cognitec.com
• Vicar Vision – www.vicarvision.nl
• ZN Vision – www.zn-ag.com

Распознавание по почерку

Как правило, для этого динамического метода идентификации человека используется его подпись или написание кодового слова.

Цифровой код идентификации формируется по динамическим характеристикам написания, то есть для идентификации строится свёртка, в которую входит информация по графическим параметрам подписи, временным характеристикам нанесения подписи и динамике нажима на поверхность в зависимости от возможностей оборудования (графический планшет, экран карманного компьютера и т.д.).

Распознавание по набору на клавиатуре

Метод в целом аналогичен вышеописанному, но вместо подписи в нём используется некое кодовое слово, а из оборудования требуется только стандартная клавиатура. Основная характеристика, по которой строится свёртка для идентификации, – динамика набора кодового слова.

Ведущий производитель подобного оборудования:

• Checco – www.biochec.com

Распознавание по голосу

В настоящее время развитие этой одной из старейших технологий ускорилось, так как предполагается её широкое использование при сооружении интеллектуальных зданий. Существует достаточно много способов построения кода идентификации по голосу – это, как правило, различные сочетания частотных и статистических характеристик последнего.

Ведущие производители таких устройств:

• Nuance – www.nuance.com
• Voicevault – www.voicevault.com

Стоит учесть, что идентификация по статическим характеристикам более надёжна, так как не зависит от психоэмоционального состояния идентифицируемого субъекта.

Middleware

Кроме вышеуказанных производителей, в настоящее время на рынке биометрии появилась новая группа компаний, решения которых называются middleware. Как правило, это «программное обеспечение – посредник между конечным оборудованием и программными системами, в которые интегрируются процедуры биометрической идентификации. Причём middleware может реализовать как просто вход в систему с использованием измерений биометрического сканера (например, Windows Logon), так и самостоятельную функциональность, например создание криптографических контейнеров с помощью ключа, получаемого только по определённому отпечатку пальца.

Недостатки биометрической аутентификации

В биометрической аутентификации есть свои недостатки.

Во-первых, это недостатки самих биометрических сканеров. Конечно, они будут разными у различных типов сканеров. Но их объединяет то, что они есть! Например, сканеры отпечатков пальцев могут быть оптическими и электронными. Первые обеспечивают более качественное изображение, но быстрее загрязняются и более требовательны к чистоте рук. Вторые – менее надёжные и качественные, однако могут распознавать даже грязные руки. Можно сделать вывод, что выбор биометрической технологии для каждого конкретного случая должен быть разным.

Во-вторых, это крайне сложная корректная настройка оборудования, точнее, установка корректного порогового значения ошибки. FAR (False Acceptance Rate) – это процент ложных отказов в допуске, FRR (False Rejection Rate) – вероятность допуска в систему незарегистрированного человека. Порог чувствительности является своеобразной гранью идентификации. Человек, имеющий сходство какой-либо характеристики выше предельного, будет допущен в систему, и наоборот. Значение порога администратор может изменять по своему усмотрению, то есть это предъявляет к нему весьма высокие требования, ведь поддержка баланса между удобством и надёжностью требует больших усилий.

В-третьих, при внедрении биометрических систем можно столкнуться с сопротивлением сотрудников компаний, обусловленным возможностью контроля их рабочего времени. Тем более что системы для учёта рабочего времени сотрудников тоже существуют.

Биометрические сканеры невозможно применять для идентификации людей с некоторыми физическими недостатками, утверждает профессор антропологии Университетского колледжа (University College) Лондона Анжела Сесс (Angela Sasse). Так, применение сканеров сетчатки глаза будет сложным для тех, кто носит очки или контактные линзы, а человек, больной артритом, не сможет ровно положить палец на сканер отпечатка.

Ещё одна проблема – рост. Сканирование лица может стать затруднительным, если рост человека менее 1,55 метра или более 2,1 метра. Преступники, по словам г-жи Сесс, смогут легко обмануть биометрические системы. Некоторые срезают свои отпечатки пальцев или сжигают их кислотой. Есть и неумышленные случаи: например люди с повреждённой кожей рук.

К недостаткам такого способа идентификации можно отнести возможность воспользоваться муляжом отпечатка, что было успешно продемонстрировано заключёнными шотландской тюрьмы строгого режима Glenochil.

Анализ мер по снижению риска биометрической аутентификации

Если на предприятии вместе с Windows 7 планируется внедрение биометрического механизма проверки, например сканирования отпечатков пальцев, следует заранее учесть следующие соображения:

- биометрические системы обычно требуют хранения на компьютере информации, которая может использоваться для установления личности. По этой причине предприятию придётся заниматься обеспечением конфиденциальности
- многие современные переносные компьютеры обладают встроенными сканерами отпечатков пальцев, что может упростить внедрение биометрического решения, но по функциональности и качеству распознавания такие встроенные устройства уступают специализированному оборудованию. Следует сравнить относительное качество по таким показателям, как коэффициент ложного пропуска, коэффициент ложного отказа, коэффициент ошибок кроссовера, коэффициент ошибок регистрации и пропускная способность
- если по характеру работы пользователи или компьютеры оказываются в загрязнённых помещениях, где сложно поддерживать чистоту рук или требуются перчатки, сканеры отпечатков использовать не удастся. Эту проблему можно решить за счёт систем анализа других физиологических параметров, например геометрии лица, радужной оболочки глаза или ладони
- наряду с биометрическим подтверждением пользователю необходимо предоставлять какое-либо иное свидетельство, например ключевую фразу, PIN-код или смарт-карту, поскольку биометрические устройства можно обмануть

Процесс снижения рисков

Особенности внедрения биометрических средств на каждом предприятии свои. Но общую последовательность действий определить можно.

1. Установить, какие из имеющихся механизмов проверки биометрических данных больше подходят нуждам предприятия.
2. Проанализировать внутреннюю документацию по обеспечению конфиденциальности, чтобы убедиться в возможности управления конфиденциальными биометрическими данными.
3. Определить требования к оборудованию, используемому при биометрическом сканировании, и наметить сроки выполнения этих требований.
4. Определить элементы инфраструктуры, необходимые для биометрического сканирования, такие как инфраструктура публичных ключей или требования к клиентскому программному обеспечению.
5. Установить, у каких сотрудников могут возникнуть проблемы с использованием биометрической системы, и подобрать для них альтернативные варианты, например проверку по имени пользователя и паролю или смарт-карте с PIN-кодом.
6. Заранее обучить пользователей обращению с системой биометрической проверки подлинности, а тех, кто не сможет ею пользоваться, – альтернативным методам проверки.
7. Провести масштабный пилотный запуск в целях выявления и разрешения проблем до начала повсеместного внедрения.
8. Следуя инструкциям производителя по сканированию и проверке, ввести данные о пользователях в биометрическую систему.
9. Обучить пользователей обращению с системой, обеспечить помощь для тех, кто испытывает трудности.
10. Необходимо учесть, что некоторые пользователи могут категорически отказаться применять биометрическую систему. Для них следует предусмотреть альтернативный способ проверки подлинности.

В заключение подчеркнём, что биометрическая аутентификация пока не может служить альтернативой многофакторной аутентификации на смарт-картах. На сегодня, по моему мнению, это скорее удобство, чем полноценная технология безопасности. Но, может быть, это поможет пользователям не забывать свои пароли, кто знает?

Электронные системы идентификации и аутентификации

В состав электронных систем идентификации и аутентификации входят контактные, бесконтактные и виртуальные смарт-карты и USB-ключи (USB-token).

Контактные смарт-карты и USB-ключи

USB-ключи работают с USB-портом компьютера и изготавливаются в виде брелоков. Что такое USB-ключ, мы рассмотрим на примере токенов от компании Thales.

Поддерживаемые методы аутентификации включают контекстную аутентификацию, одноразовый пароль (OTP) и решения на основе сертификатов X.509. Все методы аутентификации доступны в различных форм-факторах, включая смарт-карты, USB-токены, программное обеспечение, мобильные приложения и аппаратные токены.

USB-токены на основе сертификатов

USB-токены на основе сертификатов Thales обеспечивают безопасный удалённый доступ, а также другие приложения, включая цифровую подпись, управление паролями, вход в сеть и комбинированный физический/логический доступ в одном USB-токене безопасности.

До сих пор можно услышать вопрос, а в чём же разница между eToken и смарт-картой?

eToken – персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и элек-

тронными цифровыми подписями (ЭЦП). eToken может быть выполнен в виде стандартной смарт-карты или USB-ключа.

- Смарт-карта требует для подключения к компьютеру PC/SC-совместимого устройства чтения смарт-карт. Она может применяться как средство визуальной идентификации (на смарт-карте может быть размещена информация о её владельце и фотография (ID-бэдж) для использования службой безопасности предприятия). Смарт-карты могут быть изготовлены из белого пластика для последующей печати (фотографии, персональных данных и т.д.) с предварительной надпечаткой, а также с наклеенной магнитной полосой либо в виде эмбосированных карт (с выдавленными символами).
- USB-ключ – напрямую подключается к компьютеру через порт USB (Universal Serial Bus), совмещая в себе функции смарт-карты и устройства для её считывания.

Если сравнивать две эти технологии, то становится очевидно, что выбор одной из них зависит от технологии безопасности, принятой в компании. Так, если планируется введение автоматизированного пропускного режима и при этом на пропусках должны быть фотография, имя владельца и прочая информация, то предпочтительно воспользоваться смарт-картами. Но стоит учесть, что потребуется купить также устройства чтения смарт-карт.

Если пропускной режим уже введён и необходимо лишь обеспечить дополнительный контроль и ужесточить режим входа в некоторые помещения, то стоит обратить внимание на eToken PRO со встроенными радиометками. Ведь службе физической безопасности, отвечающей за пропускной режим, гораздо проще контролировать пропуска при наличии на них фотографии, фамилии и имени владельца, хотя eToken PRO со встроенным RFID-чипом и аналогичная смарт-карта одинаковы по функциональности.

Основные области применения eToken

- двухфакторная аутентификация пользователей при доступе к серверам, базам данных, приложениям, разделам веб-сайтов
- безопасное хранение секретной информации: паролей, ключей ЭЦП и шифрования, цифровых сертификатов
- защита электронной почты (цифровая подпись и шифрование, доступ)
- защита компьютеров от несанкционированного доступа (НСД)
- защита сетей и каналов передачи данных (VPN, SSL)
- клиент-банк, системы типа e-banking и e-commerce

При работе с многофакторной аутентификацией пользователь получает целый ряд преимуществ. В частности, ему требуется помнить всего один пароль к eToken вместо нескольких паролей к приложениям. Кроме того, теперь отпадает необходимость в регулярной смене паролей. И в случае утери eToken ничего страшного не произойдёт: чтобы воспользоваться найденным (украденным) eToken, необходимо ещё знать его пароль. Всё это существенно повышает уровень безопасности организации. Вместе с тем нужно понимать, что eToken поддерживает работу и интегрируется со всеми основными системами и приложениями, использующими технологии смарт-карт или PKI (Public Key Infrastructure), так называемыми PKI-ready-приложениями.

Основное назначение eToken

- строгая двухфакторная аутентификация пользователей при доступе к защищённым ресурсам (компьютерам, сетям, приложениям)
- безопасное хранение закрытых ключей цифровых сертификатов, криптографических ключей, профилей пользователей, настроек приложений и пр. в энергонезависимой памяти ключа
- аппаратное выполнение криптографических операций в доверенной среде (генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хеш-функции, формирование ЭЦП)
- продукты для многофакторной аутентификации на основе мобильных телефонов и программного обеспечения, при использовании которых пользователи не нуждаются в отдельном аппаратном токене
- программные решения для аутентификации с использованием технологии OTP (One Time Password) – одноразовый пароль
- токены OTP для смартфонов SafeNet сочетают в себе безопасность проверенной двухфакторной строгой аутентификации с удобством и простотой использования OTP, генерируемых на мобильном телефоне. Токены для смартфонов SafeNet доступны для всех мобильных устройств, включая iOS, Android

Если использование аппаратных токенов известно довольно давно, то, на мой взгляд, использование мобильных телефонов в качестве токенов OTP становится особо актуальным в сложное время пандемии. Тем более что пользователи внутренне уже готовы к этому. Ведь мультифакторная аутентификация сегодня применяется как во многих сервисах электронной почты, так и социальных сетях.

Не буду подробно на этом останавливаться, тем более что не так давно уже вышли подобные статьи и видео.

В качестве средства аутентификации eToken поддерживается большинством современных операционных систем, бизнес-приложений и продуктов по информационной безопасности и может применяться для решения следующих задач:

- строгая аутентификация пользователей при доступе к информационным ресурсам: серверам, базам данных, разделам веб-сайтов, защищённым хранилищам, зашифрованным дискам и пр.
- вход в операционные системы, службы каталога, гетерогенные сети и бизнес-приложения
- внедрение систем PKI (Entrust, Microsoft CA, RSA Keon, а также в удостоверяющих центрах и системах с использованием отечественных криптопровайдеров «Крипто-Про», «Сигнал-Ком» и т.д.) – хранение ключевой информации, аппаратная генерация ключевых пар и выполнение криптографических операций в доверенной среде (на чипе смарт-карты)
- построение систем документооборота, защищённых почтовых систем – ЭЦП и шифрование данных, хранение сертификатов и закрытых ключей
- организация защищённых каналов передачи данных с использованием транспорта Интернет (технология VPN, протоколы IPSec и SSL) – аутентификация пользователей, генерация ключей, обмен ключами
- межсетевые экраны и защита периметра сети (продукты Cisco Systems, Check Point) – аутентификация пользователей
- шифрование данных на дисках – аутентификация пользователей, генерация ключей шифрования, хранение ключевой информации

- единая точка входа пользователя в информационные системы и порталы (в продуктах eTrust SSO, IBM Tivoli Access Manager, WebSphere, mySAP Enterprise Portal) и приложения под управлением СУБД Oracle – строгая двухфакторная аутентификация
- защита веб-серверов и приложений электронной коммерции – аутентификация пользователей, генерация ключей, обмен ключами
- управление безопасностью корпоративных информационных систем, интеграция систем защиты информации – eToken является единым универсальным идентификатором для доступа к различным приложениям
- поддержка унаследованных приложений и разработка собственных решений в области ИБ

USB-ключи – это преемники смарт-карт, поэтому структура USB-ключей и смарт-карт идентична.

Бесконтактные смарт-карты

Бесконтактные смарт-карты (БСК) широко используются в различных приложениях как для аутентификации (режим электронного пропуска, электронный ключ к двери и т.д.), так и для разного рода транспортных, идентификационных, расчётных и дисконтных приложений.

Важным свойством БСК, выделяющим её из ряда других смарт-карт, является отсутствие механического контакта с устройством, обрабатывающим данные с карты. Фактически надёжность технических элементов систем, использующих БСК, определяется надёжностью микросхем. Последнее обстоятельство приводит к существенному снижению эксплуатационных расходов на систему по сравнению с аналогичными системами, применяющими смарт-карты с внешними контактами.

Порядок проведения операций с БСК и устройством чтения/записи памяти карты (далее – считывателем) определяется программным приложением. При поднесении пользователем карты к считывателю происходит транзакция, то есть обмен данными между картой и считывателем и возможное изменение информации в памяти карты. Максимальное расстояние для осуществления транзакций между считывателем и картой составляет 10 см. При этом карту можно и не вынимать из бумажника. С одной стороны, это позволяет пользователю удобно и быстро произвести транзакцию, а с другой – при попадании в поле антенны карта вовлекается в процесс обмена информацией независимо от того, желал этого пользователь или нет.

Типичная начальная последовательность команд для работы приложения с картой включает следующее:

- захват карты (выбирается первая находящаяся в поле антенны считывателя карта), если необходимо – включение антиколлизионного алгоритма (команда антиколлизии сообщает приложению уникальный серийный номер захваченной карты, точнее, уникальный номер встроенной в карту микросхемы)
- выбор карты с данным серийным номером для последующей работы с памятью карты или её серийным номером.

Указанная последовательность команд выполняется за 3 мс, то есть практически мгновенно.

Далее следует аутентификация выбранной области памяти карты. Она основана на использовании секретных ключей и будет описана ниже. Если карта и считыватель узнали друг друга, то данная область памяти открывается для обмена данными и в зависимости от условий доступа могут быть выполнены команды чтения и записи, а также специализированные команды электронного кошелька (если, конечно, область соответствующим образом была размечена при персонализации карты). Команда чтения 16 байтов памяти карты выполняется за 2,5 мс, команды чтения и изменения баланса кошелька – за 9-10 мс. Таким образом, типичная транзакция, начинающаяся с захвата карты и приводящая к изменению 16 байтов памяти, совершается максимум за 16 мс.

Для аутентификации сектора памяти карты применяется трёхпроходный алгоритм с использованием случайных чисел и секретных ключей согласно стандарту ISO/IEC DIS 9798-2.

В общих чертах процесс аутентификации можно представить так. Чипы карты и устройства для работы с ней обмениваются случайными числами. На первом шаге карта посылает считывателю сформированное ею случайное число. Считыватель добавляет к нему своё случайное число, шифрует сообщение и отправляет его карте. Карта расшифровывает полученное сообщение, сравнивает своё случайное число с числом, полученным в сообщении; при совпадении она заново зашифровывает сообщение и направляет его считывателю. Считыватель расшифровывает послание карты, сравнивает своё случайное число с числом, полученным в сообщении, и при совпадении чисел аутентификация сектора считается успешной.

Итак, работа с сектором памяти возможна только после успешной аутентификации сектора выбранной карты и пока карта находится в поле антенны считывателя. При этом все данные, передаваемые по радиочастотному каналу, всегда шифруются.

Начальные (так называемые транспортные) ключи, а также условия доступа к секторам задаются во время первичной персонализации карты на заводе-изготовителе и секретным образом сообщаются эмитенту. В процессе вторичной персонализации карточки эмитентом или пользователем приложения ключи обычно меняются на другие, известные только эмитенту или пользователю. Так же (это определяется конкретным приложением) при вторичной персонализации изменяются и условия доступа к секторам памяти карты.

Бесконтактные смарт-карты разделяются на идентификаторы PROximity и смарт-карты, базирующиеся на международных стандартах ISO/IEC 15693 и ISO/IEC 14443. В основе большинства устройств на базе бесконтактных смарт-карт лежит технология радиочастотной идентификации.

Основными компонентами бесконтактных устройств являются чип и антенна. Идентификаторы могут быть как активными (с батареями), так и пассивными (без источника питания). Идентификаторы имеют уникальные 32/64-разрядные серийные номера.

Системы идентификации на базе PROximity криптографически не защищены, за исключением специальных заказных систем.

Каждый ключ имеет прошиваемый 32/64-разрядный серийный номер.

Комбинированные системы

Внедрение комбинированных систем существенно увеличивает количество идентификационных признаков и тем самым повышает безопасность.

В настоящее время существуют комбинированные системы следующих типов:

- системы на базе бесконтактных смарт-карт и USB-ключей
- системы на базе гибридных смарт-карт
- биоэлектронные системы

В корпус брелока USB-ключа встраиваются антенна и микросхема для создания бесконтактного интерфейса. Это позволяет организовать управление доступом в помещение и к компьютеру, используя один идентификатор. Такая схема применения идентификатора исключает ситуацию, когда сотрудник, покидая рабочее место, оставляет USB-ключ в разъёме компьютера, что даёт возможность работать под его идентификатором.

Применение eToken для контроля физического доступа

RFID-технология (Radio Frequency IDentification – радиочастотная идентификация) является наиболее популярной сегодня технологией бесконтактной идентификации. Радиочастотное распознавание осуществляется с помощью закреплённых за объектом так называемых RFID-меток, несущих идентификационную и другую информацию.

Помимо традиционных преимуществ RFID-технологий, комбинированные USB-ключи и смарт-карты eToken, используя единый «электронный пропуск» для контроля доступа в помещения и к информационным ресурсам, позволяют:

- сократить расходы
- защитить инвестиции, сделанные в ранее приобретённые СКУД, за счёт интеграции eToken с большинством типов RFID-меток
- уменьшить влияние человеческого фактора на уровень информационной безопасности организации: сотрудник не сможет покинуть помещение, оставив комбинированную карту на рабочем месте
- автоматизировать учёт рабочего времени и перемещений сотрудников по офису
- провести поэтапное внедрение путём постепенной замены выходящих из эксплуатации идентификаторов

Применение гибридных смарт-карт для контроля физического доступа

Гибридные смарт-карты содержат разнородные чипы: один чип поддерживает контактный интерфейс, другой – бесконтактный. Как и в случае гибридных USB-ключей, гибридные смарт-карты решают две задачи: контроль доступа в помещение и к компьютеру. Дополнительно на карту можно нанести логотип компании, фотографию сотрудника или магнитную полосу, что позволяет заменить на такие карты обычные пропуска и перейти к единому электронному пропуску.

Электронные ключи с одноразовыми паролями

Идентификаторы на базе генераторов разовых паролей применяются чаще всего для организации веб-доступа или систем типа e-banking.

Аппаратные реализации генераторов одноразовых паролей называют OTP-токенами. Они имеют небольшой размер и выпускаются в различных форм-факторах:

- карманный калькулятор
- брелок
- смарт-карта
- устройство, комбинированное с USB-ключом
- специальное программное обеспечение для карманных компьютеров

Одной из распространённых аппаратных реализаций одноразовых паролей является технология SecurID, предлагаемая компанией RSA Security. Она основана на специальных калькуляторах – токенах, которые ежеминутно генерируют новый код. В токен встроена батарейка, заряда которой хватает на 3-5 лет, после чего токен нужно менять. Существуют и другие реализации одноразовых паролей. Например, можно генерировать пароль по событию – нажатию клавиши на устройстве. Такое решение предлагает компания Secure Computing в виде продукта Safeword. Аппаратную реализацию технологии «запрос-ответ» представляет корпорация Thales.

Различие между технологиями RSA Security ID и eToken Pass заключается в том, что разовый пароль в RSA SecurID изменяется через заранее заданные промежутки времени (синхронизация по времени), а в продукте eToken Pass смена разового пароля производится по нажатию кнопки (синхронизация по событию).

При необходимости получить соединение с сетью пользователь вводит PIN-код, а затем генерирует разовый пароль, нажимая кнопку на eToken Pass. При этом пароль формируется как PIN-код плюс Token-код. На стороне сети этот пароль проверяется с помощью специального серверного ПО.

Второй вариант такого подхода реализован в продуктах компании RSA Security. С точки зрения конечного пользователя, разница между обычной процедурой регистрации в системе Windows и аутентификацией в системе RSA SecurID состоит лишь в том, что вместо стандартного пароля требуется ввести составной код доступа, состоящий из личного PIN-кода и комбинации цифр, которая в данный момент отображается на экране жетона-аутентификатора. Затем этот код доступа отсылается серверу RSA Authentication Manager, который и выполняет проверку подлинности пользователя.

RSA SecurID for Microsoft Windows обеспечивает интеграцию с контроллерами доменов Windows и каталогами Active Directory. База данных пользователей и групп сервера аутентификации RSA Authentication Manager синхронизирована с каталогом Active Directory.

Выводы

Рассмотрев различные технологии аппаратно-программной и парольной аутентификации, можно сделать вывод, что применение паролей всё меньше соответствует требованиям безопасности, так как с увеличением сложности паролей и количества их для запоминания будет возрастать роль человеческого фактора, а значит:

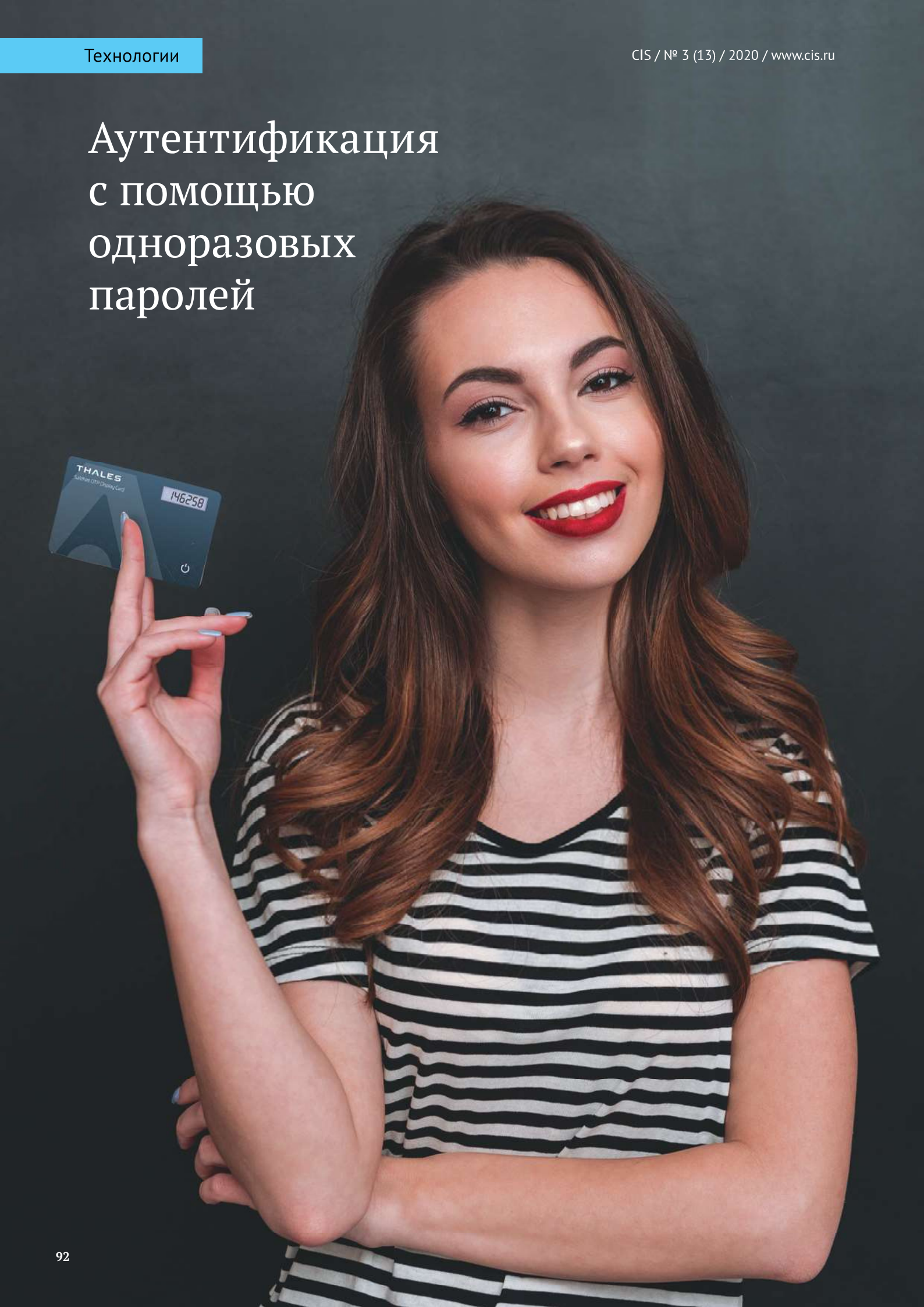
- пользователи всегда будут выбирать наиболее простые, с их точки зрения, пароли
- при ужесточении политики паролей пользователи будут идти на всяческие ухищрения, облегчающие им пользование паролями, но снижающие безопасность (например, наклеивать стикеры с паролем на монитор, клавиатуру, записывать пароль в блокнот и т.д.)
- с ростом вычислительных мощностей процесс подбора паролей будет происходить всё быстрее.

В связи с этим необходим переход на многофакторную аутентификацию, из всех видов которой самым надёжным сегодня является применение USB-ключей (смарт-карт).

Владимир Безмалый
Kaspersky Certified Trainer

CIS / № 3 (13) / 2020 / www.cis.ru

Аутентификация с помощью одноразовых паролей



Наступление карантина во всём мире привело к необходимости пересмотра привычных подходов к аутентификации. Увы, но стоит признать, что аутентификация с помощью привычных нам паролей не оправдала себя. А если добавить к этому то, что большинство пользователей и ранее использовали не стойкие, а главное, не уникальные пароли, то это привело к тому, что такая защита на сегодня обеспечивает крайне низкий уровень стойкости.

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

Биометрическая аутентификация, на которую возлагались такие огромные надежды, также не получила широкое распространение. Причина вполне понятна. Увы, но хорошие биометрические датчики стоят дорого, вернее, очень дорого. Большинство существующих таких датчиков не могут отличить живое от неживого. Как быть?

Пожалуй, вполне достойным выходом может быть применение аппаратных токенов. Но здесь тоже есть своя цена. Ведь при оставлении компьютера без присмотра, токен чаще всего остаётся подключённым в USB-порт. Это огромная проблема. И если на работе это ещё как-то отслеживается, то дома следить некому и некогда. Как быть?

Одним из выходов из сложившейся ситуации будет использование технологии, получившей название One Time Password (OTP) или применение одноразовых паролей. Наверное, кто-то из читателей, как и я, применяет подобный подход при использовании сервисов Microsoft (например, Outlook, Skype и т.д.) или сервисов Google. В обоих случаях необходимо заранее установить на свой смартфон соответствующие приложения Microsoft Authenticator и Google Authenticator. Это необходимо, чтобы не использовать для получения одноразового пароля SMS: использование SMS признано небезопасным.

Какие виды OTP существуют в этом случае, рассмотрим на примере OTP-аутентификаторов и продуктов OTP-аутентификации семейства SafeNet компании Thales.

SafeNet OTP 110 токен

SafeNet OTP 110 (ранее IDProve) – это аппаратный токен OTP, обеспечивающий двухфакторную аутентификацию для широкого спектра ресурсов и поддерживает функции протоколов OATH TOTP и HOTP.

SafeNet Trusted Access поддерживает токены аутентификации OATH и позволяет организациям сохранить свои текущие инвестиции для эффективной и действенной защиты от несанкционированного входа в систему из-за скомпрометированных статических паролей.

Что такое OATH-аутентификация?

OATH – это открытая эталонная архитектура для реализации строгой аутентификации, созданная отраслевым сообществом поставщиков безопасности для универсального применения строгой аутентификации.

Стандарт OATH может использоваться ИТ-специалистами и специалистами по безопасности в качестве шаблона для интеграции строгой аутентификации в существующую инфраструктуру их организации.

Для получения дополнительной информации посетите openauthentication.org.

Описание токена

SafeNet OTP 110 представляет собой аппаратный токен OTP, сертифицированный OATH, который обеспечивает многофакторную аутентификацию для широкого спектра ресурсов. Работа SafeNet OTP 110 основана на смене одноразового пароля через определённый промежуток времени и может применяться везде, где используется обычный статистический пароль, что существенно повышает безопасность.

При этом OTP-аутентификация помогает организациям устранить риски, связанные с фиксированными паролями, и повысить безопасность контроля доступа пользователей, реализованного для защиты доступа к локальной сети, доступа к удалённой сети (VPN), облачных приложений, VDI, веб-порталов и пользовательских приложений.

Проблемы, которые могут возникнуть при использовании аппаратных токенов OTP

Прежде всего это несовпадение временных интервалов между токеном и вашим сервером. Как это решается? Можно увеличить (уменьшить) интервал действия пароля. Могу сказать одно: данная проблема вполне решаема.

Удобство:

- Пожизненная гарантия на SafeNet OTP 110 предоставляется на весь срок действия подписки SafeNet Trusted Access, включая бесплатную замену
- Безопасный удалённый доступ к сетям (Vpns), приложениям SaaS, VDI, веб-порталам и пользовательским приложениям
- Пользователи могут легко носить устройство с собой, куда бы ни отправились
- Простое управление благодаря лёгкой внутренней конфигурации, низкому техническому обслуживанию и длительному сроку службы аккумулятора
- Обеспечивает соответствие отраслевым нормам

Особенности:

- Устройство аутентификации OTP с ЖК-дисплеем, батареей и кнопкой генерации OTP
- Поддержка протоколов OATH TOTP и HOTP

SafeNet OTP Display Card

В данном случае мы имеем OTP-карту SafeNet. При нажатии кнопки карта сгенерирует одноразовый пароль, привязанный к данной карте.

При этом одноразовый пароль, сгенерированный картой, может объединяться с другими факторами аутентификации, например PIN-кодом или паролем. Ведь необходимо убедиться, что карта находится в руках подлинного владельца.

OTP-карта SafeNet взаимодействует с SafeNet Trusted Access, сервисом управления облачным доступом, который предлагает единый вход, защищённый детальными политиками доступа.

Удобства

- Легко переносить: помещается в ваш кошелёк
- Простота в использовании: нажмите кнопку и получите свой OTP
- Пожизненная гарантия. Гарантийный талон на SafeNet OTP Display Card предоставляется на весь срок действия подписки Gemalto, включая бесплатную замену. Как и все аутентификаторы Gemalto, токен никогда не истекает
- Безопасный доступ к удалённым сетям (VPN), облачным (SaaS) приложениям, VDI, веб-порталам и пользовательским приложениям
- Простое управление с лёгкой внутренней конфигурацией и автоматизированными рабочими процессами администрирования
- Обеспечивает соответствие отраслевым нормам, требующим многофакторной аутентификации

Особенности:

- OTP-токен в форм-факторе кредитной карты
- Высокая читаемость экрана ePaper
- Синхронизация времени – OATH TOTP

eToken PASS OTP Аутентификатор

eToken PASS — это компактное и портативное устройство строгой аутентификации с использованием одноразовых паролей (OTP), которое позволяет организациям удобно и эффективно устанавливать контроль доступа на основе OTP. Он поддерживает протоколы OATH TOTP и HOTP, а также стандартную поддержку RADIUS OTP и многое другое.

Thales SafeNet GOLD

Разработан для защиты идентификационных данных и безопасного доступа, представляет собой высокоэффективное двухфакторное OTP-устройство, обеспечивающее дополнительную защиту с помощью **PIN-кода и ответа на вызов**.

GOLD активируется с помощью персонального идентификационного номера (ПИН), который запрашивает у аутентификатора одноразовый динамический пароль. Затем пользователь вводит этот пароль в веб или сетевое приложение для аутентификации своей личности.

Как работает GOLD

GOLD предоставляет провайдерам онлайн-услуг, таким как банки, платёжные порталы, очень надёжное средство предложить своим клиентам защищённую онлайн-среду для проведения финансовых транзакций и доступа к конфиденциальной информации.

В дополнение к защите ПИН-кодами расширенные возможности OTP и ответа на вызовы GOLD предназначены для борьбы с мошенничеством в Интернете, таким как фишинг, и помогают поставщикам онлайн-услуг и банкам поддерживать целостность пароля, усложняя для клиентов потерю или обмен паролями.

Доступен на корпоративной платформе SafeNet Trusted Access. Эта уникальная платформа управления доступом обеспечивает гибкость и масштабируемость, позволяя организациям централизованно управлять GOLD с помощью других аутентификаторов Thales SafeNet или добавлять их в будущем по мере роста потребностей бизнеса. STA позволяет организациям защищать доступ ко всем ресурсам и переходить в облако.

Преимущества

- Безопасный удалённый доступ
- Аппаратная защита PIN-кода и ответ на вызов
- Портативность
- Большой удобный дисплей

Но стоит помнить, что кроме аппаратных токенов, можно использовать и программный токен SafeNet MobilePASS+ — программный токен следующего поколения, который обеспечивает безопасную одноразовую генерацию пароля на мобильных устройствах, а также аутентификацию одним нажатием для повышения удобства пользователя.

SafeNet MobilePASS+ интегрируется с ведущими облачными приложениями, шлюзами безопасности и виртуальными частными сетями и обеспечивает администрирование жизненного цикла без каких-либо ограничений, что делает его идеальным для обеспечения безопасного доступа к консультантам, партнёрам и разрозненной рабочей силе.

Для пользователей SafeNet MobilePASS+ предлагает удобный доступ благодаря простой активации QR-кода, дополнительному биометрическому PIN-коду и выбору стандартных режимов OTP и push-аутентификации. В режиме push при каждом обращении к защищённому ресурсу на устройство пользователя автоматически отправляется push-уведомление. Пользователь нажимает на уведомление MobilePASS+, затем, чтобы подтвердить запрос на вход в систему, а после входит в систему на ресурсе. Если политика ПИН была определена, пользователь вводит свой буквенно-цифровой ПИН или использует TouchID/FaceID для ввода своего биометрического ПИН (необязательно).

Можно также утверждать запросы входа в систему прямо с экрана блокировки — просто откройте push-уведомление, нажмите «Утвердить», а затем авторизуйтесь на своём устройстве, чтобы получить доступ к онлайн-ресурсу.

Начиная с MobilePASS+ v1.6, теперь можно проходить сквозной процесс аутентификации для доступа к личным токенам и паролям с полностью обновлённым пользовательским интерфейсом.

По аналогии с MobilePASS+ v1.6 работают существующие средства аутентификации сервисов Google и Microsoft, в частности push-аутентификация Microsoft и Google на iPhone.

Достоинство мобильной аутентификации состоит прежде всего в том, что это удобно и дёшево. Сегодня у большинства пользователей есть смартфоны. Вместе с тем это и недостаток данного способа аутентификации, ведь в таком случае необходимо контролировать смартфоны пользователей. А позволят ли это пользователи?

Необходимо убедиться в том, что смартфоны пользователей не взломаны, не заражены, на них не проведён rooting или jailbreak и для их блокирования используется устойчивый PIN-код.

Вы можете это гарантировать? Я — нет!

Вывод

На мой взгляд, с точки зрения безопасности, альтернативы использованию аппаратных токенов OTP сегодня просто не существует. Заставить пользователей использовать свои смартфоны для OTP и тем более заставить их безопасно использовать, увы, невозможно!

CIS / № 3 (13) / 2020 / www.cis.ru

Использование технологии IIoT для мониторинга промышленных роботов

В статье рассмотрены перспективы использования одной из современных платформ промышленного интернета вещей в качестве инструмента для мониторинга промышленных роботов. Также представлены перспективы этого направления и реализация таких решений.

Перспективы использования промышленных роботов на предприятии

Несмотря на то, что разработки промышленных роботов в СССР были начаты ещё в конце 40-х годов прошлого века, интенсивная работа над их созданием в данном сегменте началась с конца 1960-х. Всего в период с 1970 по 1980 гг. в стране было разработано свыше 50 различных типов автоматических манипуляторов с программным управлением. СССР в те годы занимал одну из лидирующих позиций в роботостроении и применении роботизированных систем на производстве. В 1989 году в нашей стране эксплуатировалось свыше 59 тыс. таких систем, включая страны восточной Европы – 65 тыс. Эффективность роботизации в то время подтверждается следующими показателями: сокращением времени производственного цикла до 30 раз, повышением коэффициента сменности оборудования до 2,5-2,7 при экономии производственной площади на 30-40% [1].

В настоящее время данная технология утратила свою популярность в российском промышленном производстве. По состоянию на 2019 год в мировом производстве используется порядка 2,6 млн промышленных роботов, а в России только 8 тыс., то есть 2 робота на 10 тыс. занятых при среднемировых – 55 роботов на 10 тыс. [2]. Но эта ситуация имеет тенденцию к улучшению.

На машиностроительных предприятиях роботы по-прежнему применяются на участках, где необходим монотонный труд: дефектоскопия, сварка, нанесение маркировки. Руководители предприятий с большим интересом смотрят на использование роботизированных систем и манипуляторов на потенциально опасных участках производства, но к внедрению таких систем относятся без энтузиазма.

Рисунок 1. Роботизированный комплекс завода КАМАЗ с использованием «БРИГ-10 ЗАЗ». 1983 год.

Факторы, ограничивающие роботизацию

Множество исследований на тему текущих трудностей с роботизацией часто концентрируются на проблемах технологического и социального характера.

Отмечается, что «в настоящее время в России промышленные роботы серийно не производятся, а закупка готового оборудования, как правило, приводит к заведомому отставанию в технологиях. К тому же на импортируемое роботизированное оборудование зарубежными производителями применяются запретительные ограничения для ряда отраслей нашей промышленности» [2].

Немаловажным фактором является недостаточное финансирование на предприятиях с высокой долей государственного участия.

По наблюдениям автора статьи, для руководителя предприятия самыми значимыми факторами являются:

- целесообразность применения роботизированных технологий;
- отсутствие организационных связей на предприятии как предпосылок использования промышленных роботов.

В «Общих предложениях роботизации РД 50-355-82» сказано: «3.3.3. Под организационными связями понимается совместное обслуживание ряда комплексов операторами, наладчиками, ремонтниками и другими специалистами, а также совместные планирование и учёт работы этих комплексов» [3].

Таким образом, одним из сдерживающих факторов является низкий уровень зрелости процессов эксплуатации промышленных роботов на предприятии. Это обуславливает следующее:

- неэффективное использование промышленных роботов, их низкая загрузка;
- отсутствие у ремонтников информации о текущем техническом состоянии роботов и тех режимов, в которых они работали;
- децентрализованное программирование роботов, затрудняющее их быструю интеграцию в технологические процессы и переналадку;
- информационный вакуум руководства, не позволяющий понимать фактическое положение дел роботизированных систем на своём предприятии, тем самым затрудняющий принятие соответствующих управленческих решений.

Один из способов, который будет способствовать изменению ситуации, – обеспечение точной и достоверной информацией всех служб и вертикалей о состоянии дел роботизированных систем на предприятии, что позволит выстроить интегрированные процессы обслуживания, планирования и производства.

Опыт общения с заказчиками показал, что решить эти задачи можно благодаря информационной системе, которая позволит интегрировать все данные, связанные с роботами, и предоставлять непротиворечивую информацию в соответствующих ракурсах заинтересованным службам.

Мониторинг промышленных роботов. Инструмент повышения эффективности

Наиболее близкой системой для решения таких задач является система мониторинга. Она позволяет автоматически и без участия человека получить объективные данные с роботизированных систем, обеспечив необходимой информацией участников производственного процесса.

Современные производители роботов предусматривают их мониторинг, разрабатывая соответствующие утилиты. Они позволяют получать данные и предоставлять их оператору в удобном формате.

Эти возможности, с одной стороны, позволяют несколько облегчить работу ремонтных служб предприятия, но с другой – используются только самими производителями оборудования для постпродажного обслуживания своих систем.

Рисунок 2. Пример цифрового двойника роботизированной ячейки.

Их ценность для предприятия не велика. В первую очередь такие системы привязаны к конкретному оборудованию. Предприятия в силу своей специфики не хотят быть завязаны на конкретного производителя. Например, для одних задач подходят манипуляторы Fanuc, но на сварочном участке предпочтительно применять аппаратуру другого производителя.

Таким образом, встроенные системы мониторинга и управления будут разными, что не удобно для персонала.

Удачным решением станет применение единой системы мониторинга для всех моделей роботов и остального производственного оборудования.

Благодаря современным технологиям —промышленному интернету вещей (IIoT) и большим данным (Big Data) – построение универсальной информационной системы становится выполнимой задачей. IIoT позволит собирать сырые данные со всех производственных систем вне зависимости от производителя, а хранилище и механизмы обработки Big Data – выполнять необходимые математические преобразования.

Данный подход гораздо шире обычного контроля технического состояния и ошибок. Он даёт возможность в едином информационном пространстве отслеживать и эксплуатационные характеристики оборудования, и технологические цепочки предприятия как единого организма, то есть перейти от отдельных разрозненных систем АСУ ТП к комплексному управлению предприятием через его цифровой двойник.

Например, на рисунке 2, представлен цифровой двойник роботизированной производственной ячейки, который позволяет:

- отслеживать кинематику всех узлов манипулятора для контроля загрузки заготовки в обрабатывающий центр ЧПУ в реальном времени;
- контролировать техническое состояние и режимы работы как манипулятора, так и обрабатывающего центра;
- обеспечивать взаимодействие человек-машина для своевременной переналадки, загрузке управляющих программ и синхронизации совместной работы компонентов роботизированной ячейки.

Подобные цифровые двойники позволят решать и задачи моделирования технологических процессов с целью их оптимизации, и задачи эффективного информирования руководства о фактическом состоянии производства.

Такой подход обеспечит германизацию организационных связей на производстве, тем самым дав дополнительный толчок к развитию роботизации предприятий.

Ниже автор, основываясь на своём опыте, предлагает пример такой системы.

Платформа Winnum для мониторинга роботов

Краткая характеристика платформы. Назначение и основные варианты использования. Пример решения для мониторинга промышленных роботов. Эффект.

Компания «Техносерв» с 2017 года вплотную начала заниматься вопросами цифровизации производства. Тогда же, проанализировав рынок,

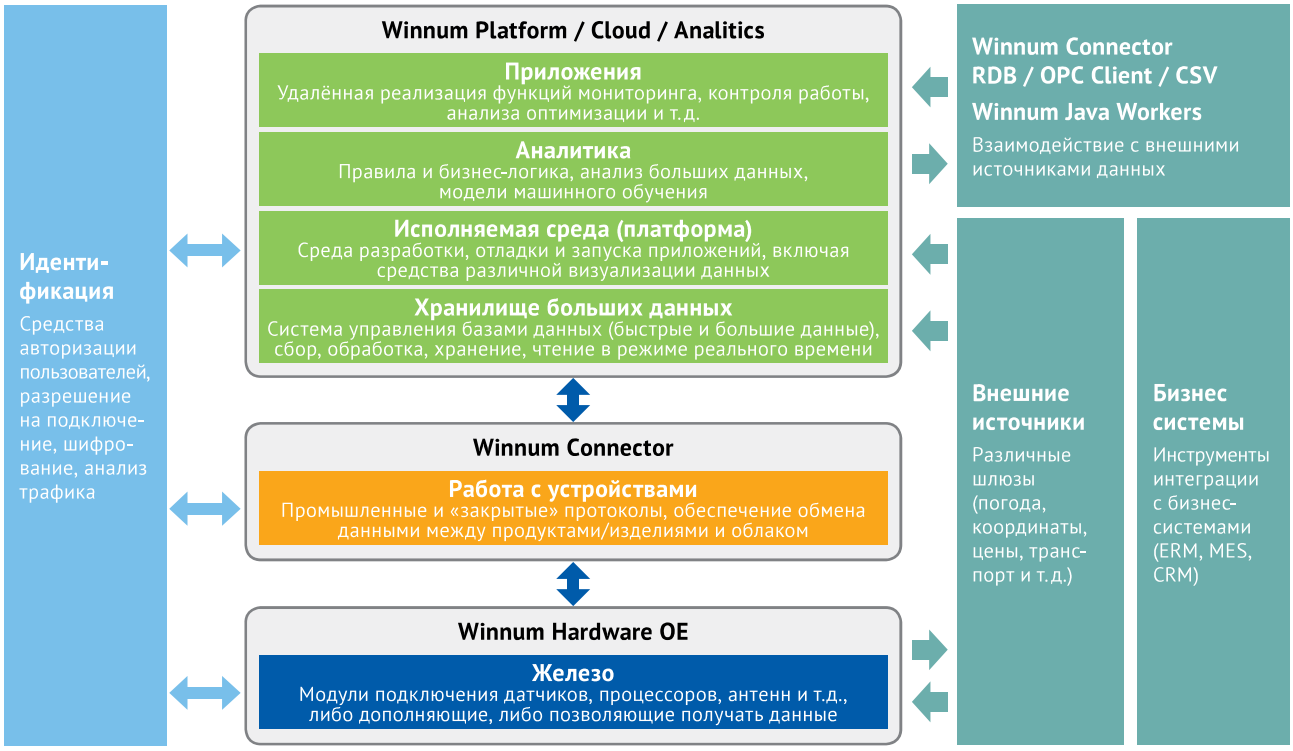


Рисунок 3. Структура IIoT-платформы Winnum

ею был сделан выбор в пользу российского решения Winnum в качестве платформы промышленного интернета вещей.

Она представляет из себя стек интегрированных, но физически независимых компонентов (каждый из которых может быть отдельной программно-аппаратной реализацией), показанных на рисунке 3.

Ниже кратко представлено описание основных компонентов платформы.

Winnum Platform

Winnum Platform содержит полный набор инструментов для мониторинга, управления и оптимизации производственных систем, в том числе роботизированных, и разработки приложения. Winnum Platform предоставляет расширенный функционал по администрированию как стандартно поставляемых приложений, уже разработанных производителем, так и тех, что разрабатываются потребителями с использованием встроенного SDK:

- единая классовая модель, которая без программирования позволяет настраивать подключение различных устройств;
- просмотр контента и администрирования выполняется исключительно в WEB-браузере для вынесения в пользовательский интерфейс настроенных графических показателей, отображающих текущую информацию по работе оборудования, отображения информации на графиках работы и загрузки;
- учёт и управление изделиями с подключёнными к ним коннекторами (см. ниже). Градация по типу коннекторов и статусам подключения оборудования;
- реализация механизма управления жизненным циклом объектов (создание, просмотр и редактирование шаблонов) с возможностью вставки автоматизированных действий (триггеров).

Моделирование функциональной составляющей изделий и их сигналов начинается с шаблонов, описывающие группу конкретных изделий и перечни сигналов. Для моделирования Winnum Platform содержит интерфейс, позволяющий быстро создавать шаблоны для любых новых изделий, и возможность описывать сигналы любых типов.

Хранилище больших данных Winnum Cloud

Winnum Cloud[1] используется для консолидации данных от разных источников (например, АСУТП, SCADA, контроллеры, датчики, файлы и пр.) и их использования для визуализации, обработки и передачи данных в корпоративные ИТ-системы и приложения бизнес-аналитики.

Технологии Winnum Cloud в части работы с данными временных рядов (в основе Winnum Cloud – NoSQL хранилище) является основой для построения корпоративных распределённых систем и обеспечивают возможность сбора сотен тысяч сигналов оборудования в секунду и их хранение без интерполяции и агрегации данных.

Winnum Connector

Winnum Connector – это семейство микропрограммного обеспечения линейки Winnum, которое предназначено для сбора данных с различных устройств и их записи в хранилище.

Описанные выше возможности позволяют нам создавать системы мониторинга и цифровые двойники производства для наших заказчиков. Так, совместно с одним из мировых производителей роботов мы и реализовали подобное решение.

Благодаря тому, что робот поддерживает взаимодействие по протоколу OPC UA, мы, используя стандартные возможности Winnum, без программирования подключили его к платформе в нашем облаке.

1. По мнению автора, название не совсем удачное, т.к. платформа полностью или частично может работать как облачный сервис и в общем случае наличие облака для её работы не требуется.

Во-первых, потребовалось настроить само подключение. Для этого у заказчика был развёрнут отдельный сервер, на котором, согласно модной сейчас концепции «туманных вычислений»[2], мы разместили коннектор, поддерживающий OPC UA. Сервер имел физическое подключение к стойке робота по Ethernet TCP/IP.

Во-вторых, настроили модель данных (шаблон изделия) для робота (рисунок 4). Это делается благодаря возможностям выборки конкретных OPC-тегов с робота и их ассоциации с элементами визуализации.

В-третьих, настроили панели мониторинга и цифровой двойник (рисунки 5, 6).

Заключение. IIoT как драйвер роботизации.

В завершение несколько слов о связи решения с четвёртой промышленной революцией (Индустрия 4.0).

Самой главной чертой нового технологического уклада будут кибер-физические системы: «Кибер-физические системы (CPS) – это умные системы, которые включают интерактивные инженерные сети из физических и коммуникационных компонент. CPS и связанные с ним системы (включая интернет вещей (IoT) и индустриальный интернет) являются общепризнанными инструментами, имеющими огромный потенциал внедрения, создающий пути реализации инновационных приложений, которые оказывают огромное влияние на множество секторов мировой экономики. В числе этих секторов NIST[3] называет в первую очередь промышленность, транспорт, энергетику и здравоохранение» [4].

Таким образом, в статье автор постарался привести понятный прикладной пример реализации CIS, показать, как современные технологии помогут развитию производства и как они могут дополнять, стимулировать и поддерживать друг друга.

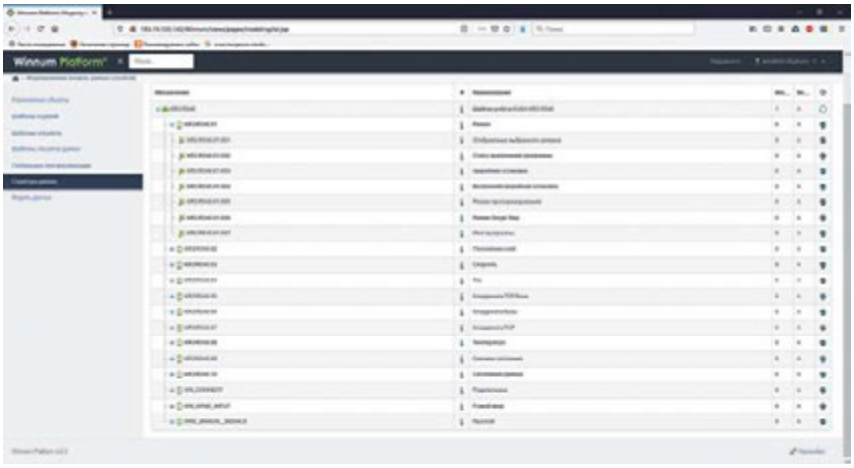


Рисунок 4. Пример настройки шаблона для подключения нового устройства

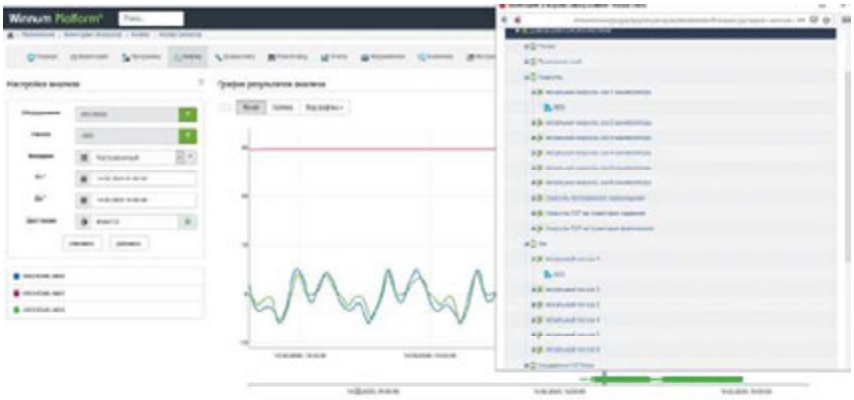


Рисунок 5. График зависимости скорости и тока для оси A. Исторические данные

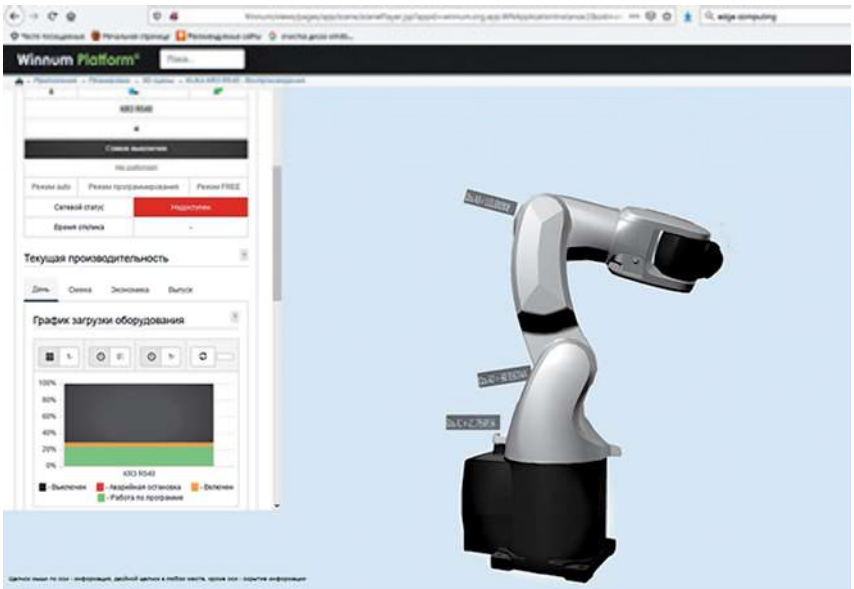


Рисунок 6. Пример реализации цифрового двойника и панели мониторинга робота-манипулятора

2. Edge (Fog) Computing можно трактовать, как все вычисления вне облака, происходящие на краю сети, и более конкретно в самих точках получения информации, в приложениях, где требуется обработка данных в реальном масштабе времени.

3. National Institute of Standards and Technology.

ТЕХНОСЕРВ

Автор статьи Андрей Шуравин, директор центра отраслевой экспертизы департамента по работе с промышленными предприятиями компании «Техносерв».

www.technoserv.com

Выставка ERRANT SOUND BERLIN

24 июня в галерее Звукового Искусства – SA)) gallery, расположенной в галерее «Электромузей в Ростокино» Объединения «Выставочные залы Москвы», в рамках проекта «Искусство звука 3-20» открылась выставка ERRANT SOUND BERLIN.

Errant Sound – это сообщество саунд-артистов из разных стран, базирующееся в Берлине в пространстве Errant Sound project на Рунгештрассе, Берлин-Митте. Проект был основан в 2010 году Брэндоном ЛаБеллем под названием Errant Bodies, а в 2013 году была образована группа Errant Sound с целью дальнейшего развития пространства как специализированной площадки для саунд-арт-проектов. В 2016 году Errant Sound был удостоен премии Project Space Prize, учреждённой Сенатом Берлина.

Деятельность проекта нацелена на приобщение широкой аудитории к теории и практикам таких областей современного искусства, как саунд-арт, аудиовизуальное искусство, паблик-арт и радио-арт. Благодаря проекту зрители получают возможность познакомиться с художественными произведениями и узнать о перспективах развития этих сфер искусства. Выставки и события, проводимые в рамках проекта, имеют тематическую направленность и посвящены не только эстетическим, но и социальным и политическим вопросам. В фокусе внимания проекта Errant Sound вопросы взаимодействия между искусством и публикой, а также обсуждение социально значимых художественных стратегий и концепций.

На выставке представлены работы восьми резидентов Errant Sound: **Kirsten Reese, Daniela Fromberg and Stefan Roigk, Thom Kubli, Georg Klein, Max Joy, Jeremy Woodruff, Jutta Ravenna.**

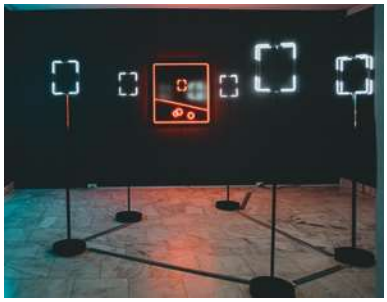
Выставка FREE WI-FI

23 июня галерея «Электромузей в Ростокино» Объединения «Выставочные залы Москвы» открывает персональную выставку победителя конкурса NOVA ART в 2019 году Григория Сельского FREE WI-FI.

Находясь в 20-м году XXI века, зритель смотрит на музей современной этнографии нового этноса «хомо-селфикус», ареал обитания которого распространился по всему миру. Это музей новой антропологии, хранящий не предметы быта и орудия труда, а скорее модели поведения человека.

Художник Григорий Сельский материализует цифровую среду, позволяя зрителю оказаться в ситуации расширенной реальности, где материальное и нематериальное перемешаны. Музей Сельского хранит отпечатки и следы деятельности человеческого аватара, созданного в цифровой среде. Персональный выставочный проект Григория – это эпитафия «хомо-селфикус», чья деятельность сосредоточена на том, чтобы получать одобрение и «социальные поглаживания».

Художник работает с артефактами нового общества – общества потребления и спектакля. Оно насыщается уже не кока-колой или супом из консервной банки, а наблюдением за теми, кто их пьёт или ест. Если Энди Уорхол непосредственно обращался к условной «продуктовой корзине», то сегодня потребление неотделимо от вуайеризма. Социальные сети удовлетворяют потребности в том, чтобы обнажить свою приватную жизнь, поделиться сокровенными мыслями или ритуалами из ванной комнаты или являются возможностью пристально следить за тем, что делает, о чём думает и что ест другой человек.



Департамент культуры города Москвы

ВЫСТАВОЧНЫЕ ОБЪЕДИНЕНИЕ ЭЛЕКТРО МУЗЕЙ

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

Positive Technologies: действия хакеров сложно отличить от действий обычных пользователей

Эксперты Positive Technologies представили результаты работ по внутреннему тестированию на проникновение[1]. Анализ показал, что почти половина всех действий преступников может не отличаться от обычной деятельности пользователей и администраторов, а в большинстве компаний контроль над инфраструктурой может получить даже низкоквалифицированный хакер.

По данным отчёта, в 2019 году во всех протестированных компаниях удалось получить полный контроль над инфраструктурой от лица внутреннего нарушителя[2]. Как правило, на это уходило около трёх дней, а в одной сети потребовалось всего 10 минут. В 61% компаний был выявлен хотя бы один простой способ получить контроль над инфраструктурой, который под силу даже низкоквалифицированному хакеру.

Как отмечают эксперты, легитимные действия, которые позволяют развить вектор атаки, составили 47% от всех действий пентестеров. К ним относятся, например, создание новых привилегированных пользователей на узлах сети, создание дампа памяти процесса lsass.exe, выгрузка ветвей реестра или отправка запросов к контроллёру домена. Все эти действия позволяют получить учётные данные пользователей корпоративных сетей или информацию, необходимую для развития атаки. Опасность состоит в том, что такие действия сложно отличить от обычной деятельности пользователей или администраторов, а значит, атака остаётся незамеченной. Детектировать перечисленные инциденты можно с помощью систем для выявления инцидентов информационной безопасности.

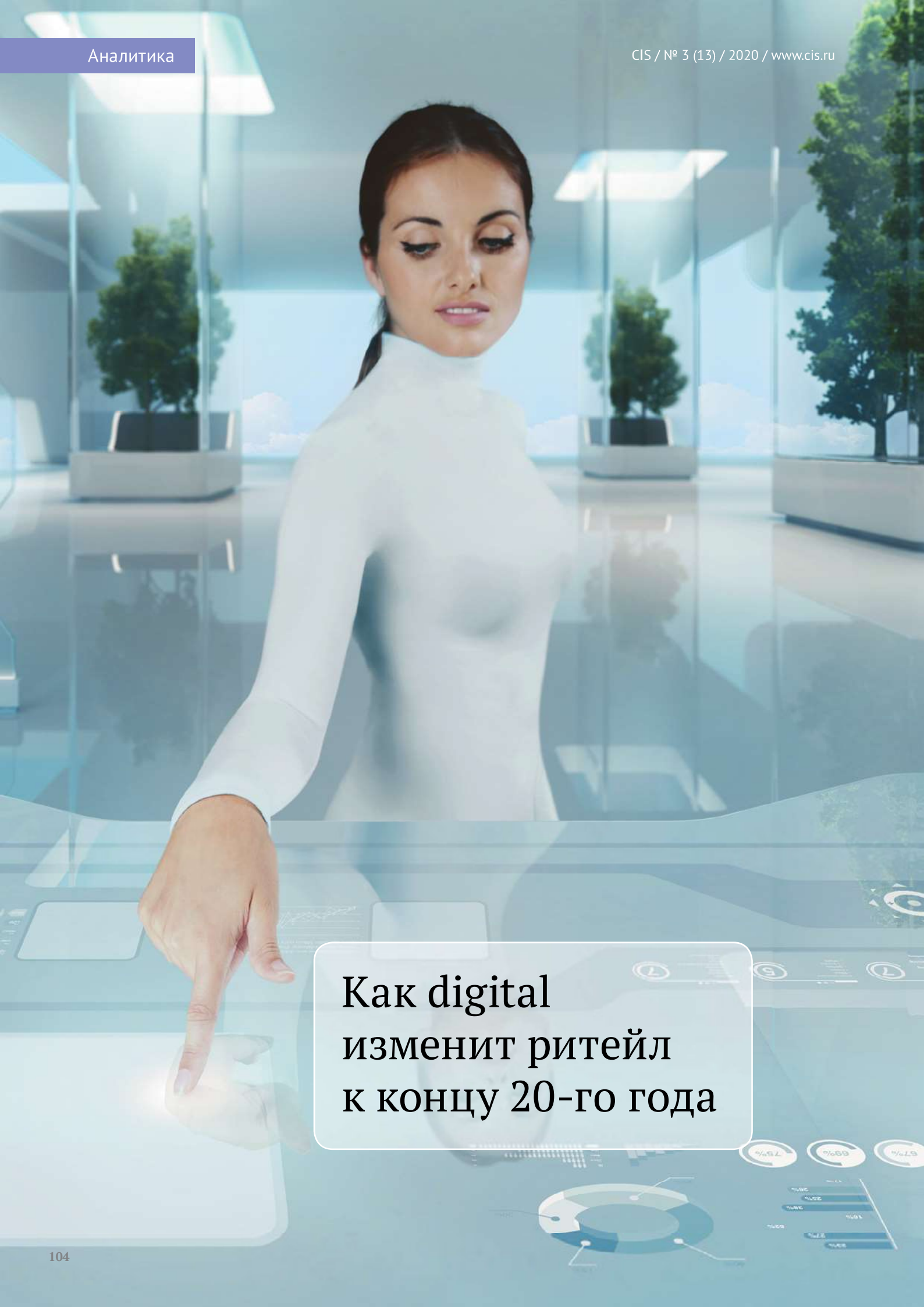
«В ходе атак во внутренних сетях для сбора учётных данных и перемещения между компьютерами, как правило, используются архитектурные особенности ОС и механизмов аутентификации Kerberos и NTLM. Например, учётные данные злоумышленник может извлечь из памяти ОС с помощью специальных утилит, таких как mimikatz, secretsdump, procdump или встроенных средств ОС, например taskmgr для создания дампа памяти процесса lsass.exe, – **отмечает директор по анализу защищённости Дмитрий Серебрянников.** – Мы рекомендуем использовать актуальные версии Windows (выше 8.1 на рабочих станциях или Windows Server 2012 R2 на серверах). Привилегированных пользователей домена следует включить в группу Protected Users. В современных версиях Windows 10 и Windows Server 2016 реализована технология Credential Guard, позволяющая изолировать и защитить системный процесс lsass.exe от несанкционированного доступа. Для дополнительной защиты привилегированных учётных записей, в частности администраторов домена, стоит использовать двухфакторную аутентификацию».

«В рамках внутреннего пентеста специалисты могут продемонстрировать возможность реализации бизнес-рисков или доступа к бизнес-системам, – **отмечает руководитель исследовательской группы отдела аналитики Positive Technologies Екатерина Килюшева.** – Для каждой компании перечень рисков будет отличаться, хотя есть и общие пункты, например компрометация критически важной информации в случае доступа к рабочим станциям руководства. В ходе проведения внутренних пентестов нашим экспертам удавалось, например, получить доступ к технологическим сетям промышленных компаний и системам управления банкоматами в банках, то есть показать на практике возможность осуществить атаку, которая представляет реальную опасность для компании. Тестирование на проникновение с проверкой возможности реализации бизнес-рисков позволяет максимально эффективно выстроить систему защиты».

Тестирование также показало, что злоумышленник может эксплуатировать известные уязвимости, которые содержатся в устаревших версиях ПО и позволяют удалённо выполнить произвольный код на рабочей станции, повысить привилегии или узнать важную информацию. Чаще всего в ходе тестирования эксперты сталкивались с отсутствием актуальных обновлений ОС. Так, по данным пентестеров Positive Technologies, в 30% компаний до сих пор можно обнаружить уязвимости ОС Windows, описанные в бюллетене безопасности 2017 года MS17–010, а в некоторых даже MS08–067 (октябрь 2008 года).

1. Для подготовки исследования были выбраны 23 проекта по внутреннему тестированию на проникновение за 2019 год из числа тех компаний, которые разрешили использовать обезличенные данные.
2. При проведении внутреннего пентеста моделируются атаки со стороны нарушителя, который находится внутри компании (например, с типовым набором привилегий сотрудника или от лица случайного посетителя).

CIS / № 3 (13) / 2020 / www.cis.ru



Как digital изменит ритейл к концу 20-го года

Направляй

Лояльность клиента формируется с первых минут нахождения в торговом центре. Чем удобнее пройдёт первый визит, тем больше шансов, что ваш гость ещё вернётся.

Если посетитель не может найти нужный магазин, тратит много времени на ориентирование – у вас плохая навигация. У гостя возникает стресс и он стремится поскорее выйти из зоны раздражения – вашего торгового центра.

Полноценная интерактивная навигация – недешёвое решение, так как предполагает покупку оборудования, сложного программного обеспечения. Сейчас тратиться на интеграцию дорогостоящих цифровых технологий готов не каждый. Но бюджетное решение вопроса тоже есть – это QR-навигация.

Пользователю достаточно навести камеру смартфона на специальную метку – QR-код, после чего в браузере появится карта торгового центра с маршрутом до нужного магазина или припаркованной машины.

Никаких контактов с персоналом на стойке информации, покупатель сам ориентируется в пространстве, чувствует себя комфортно и, как правило, возвращается в удобный ТРК.

Рисунок 1. QR-навигация

Вовлекай

Никто не будет спорить, что коммерция постепенно уходит в интернет. Физическое посещение точки продаж всё больше связано с потребностью получения позитивного опыта и эмоций.

Вы идёте в реальный магазин пощупать предмет покупки или же вам нравится тот «ритуал», который сопровождает покупку.

Если вы хотите, чтобы процесс покупки продолжал быть интересным, мотивировал вернуться в магазин и рассказать о нём друзьям, то вам поможет дополненная реальность.

Дополненная реальность (AR) может ближе познакомить покупателя с вашим продуктом или вовлечь его в процесс покупки.

Дополнительным плюсом становится возможность получения контактных данных. Например, различные рекламные акции с дополненной реальностью предлагают сделать пост в социальных сетях или послать какую-то информацию себе на почту. Вот вам и контакты активных клиентов.

Демонстрируй

Искусственный интеллект позволяет творить удивительные вещи. Представьте, что цифровое око видит вашего покупателя, определяет его пол, возраст, детали его образа и рекомендует ему что-нибудь из вашего ассортимента.

Это уже реальность! Система может работать как незаметно, тайно давая подсказки вашим сотрудникам, так и напрямую по запросу клиента. Второй вариант дарит незабываемый опыт, о котором мы говорили в начале статьи.

Рисунок 2. Искусственный интеллект

Адаптируй

Желание человека купить тот или иной товар, услугу зависит от множества факторов. Нет никакого смысла предлагать кофе в жару, а мороженое в дождь. Может, лучше продавать зонтики?

Современные возможности интерактивных систем позволяют настраивать целые сценарии. Допустим, товар, которого много на складе, будет демонстрироваться на вывесках чаще.

Отдельные объявления могут выходить в эфир только при определённых событиях. Утром система автоматически показывает доступный завтрак, пошёл дождь – запустилась реклама зонтов и согревающего кофе.

Сценарии выбираете вы, а комплексное решение самостоятельно следит за нужными условиями и подбирает подходящие кейсы.

Рисунок 3. Рекламные сценарии

Анализируй

Любое интерактивное решение собирает полезную статистику. Вы получаете актуальные данные о вашей аудитории, её предпочтениях. Кто, как и когда! С точностью до каждого конкретного клиента.

Машинное зрение может оценивать самые посещаемые зоны в магазине, выделять основные маршруты перемещения посетителей. Точечная настройка системы позволяет определять интерес вплоть до конкретной полки.

Как ваши гости смотрят на рекламу? Носят ли они маски? Всё это может отслеживаться автоматически.

Подумайте, технологии постоянно развиваются, и недооценивать их возможности нельзя. А мы готовы рассказать о них чуточку подробнее, свяжитесь с нами, и мы расскажем обо всех деталях.

---

initium

«Инициум»

www.initium.ru

CIS / № 3 (13) / 2020 / www.cis.ru

Управление внутренними изменениями в режиме удалённой работы

Коротко о Банке

НА РЫНКЕ С 1993 ГОДА

Акционерный коммерческий банк «АК БАРС» (публичное акционерное общество) зарегистрирован в ЦБ РФ и успешно работает на финансовом рынке.

БОЛЕЕ 100 ВИДОВ УСЛУГ

Банк располагает всеми видами существующих в Российской Федерации банковских лицензий и оказывает огромный спектр банковских услуг для корпоративных и частных клиентов.

КАПИТАЛ 73,5 МЛРД РУБ.

Величина собственного капитала на 1 января 2020 года.

226 ОФИСОВ ПО РОССИИ

На 1 марта 2020 года территориальная сеть банка – 226 отделений в городах России.

УПОЛНОМОЧЕННЫЙ БАНК РТ

Банк является уполномоченным агентом республики Татарстан по обслуживанию счетов бюджета и реализации социальной политики республики.

ЗНАЧИМЫЙ БАНК РФ

Ак Барс Банк по приказу Центрального Банка России входит в реестр значимых кредитных организаций на рынке платежных услуг РФ.

Елена Савосина

- Руководитель направления методологии Финансового департамента
- Более 10 лет работы в сфере банковской методологии
- ICAgile Certified Proffesional
- SAFe Agilist (SAFe 4.6)
- Опыт трансформации подразделения банковских технологий
- Руководитель проектов по внедрению новых процессов и продуктов
- Тренер внутренних обучений (обучено более 300 человек)

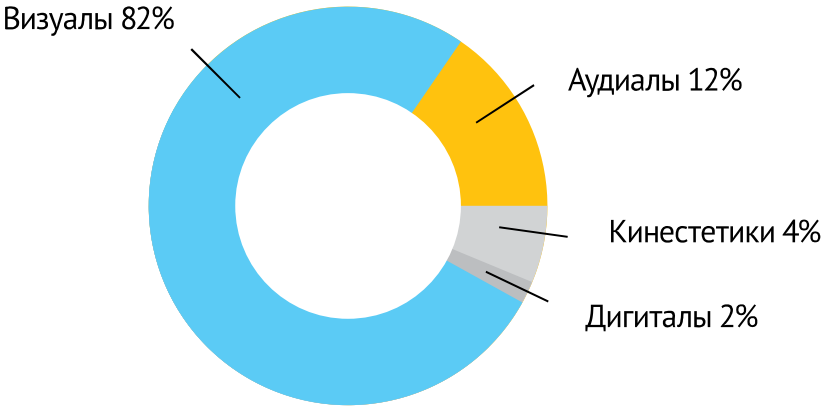
Вовлечённость

И что теперь делать?

С кем мы работаем? Как они воспринимают информацию?

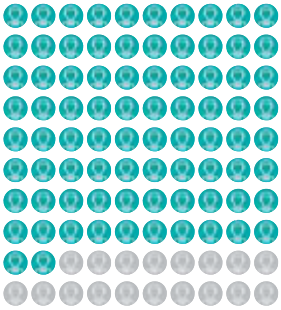
Хорошая новость:

94% людей воспринимают информацию глазами и ушами



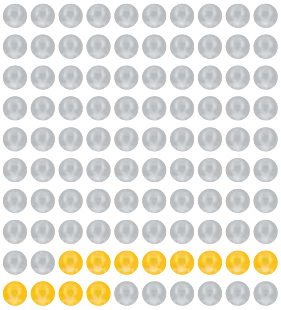
ВИЗУАЛЫ
- Презентации
- Расшариваем экран
- Используем видеозвонки

«ХОЧУ ВИДЕТЬ!»
- Цвета
- Форма
- Красота



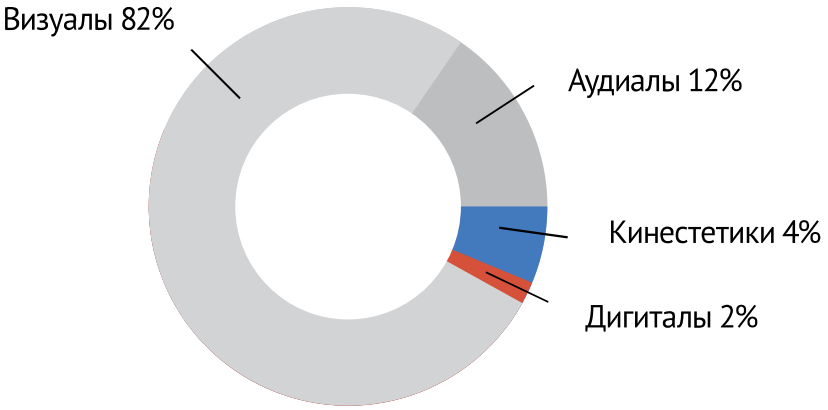
АУДИАЛЫ
- Звонки БЕЗ видео
- Объясняем словами
- Можно без презентаций (не оценят)

«ХОЧУ СЛЫШАТЬ!»
- Голос
- Словесные пояснения



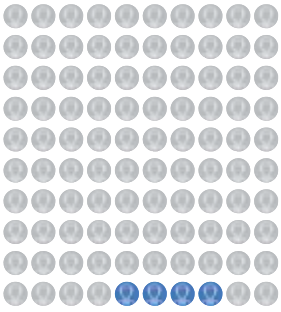
Плохая новость:

6% людей воспринимают информацию через жесты, «на ощупь», и анализируя (логически)



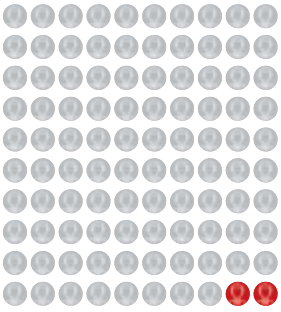
КИНЕСТЕТИКИ (ДИСКРЕТЫ, СЕНСОРИКИ)
- Права управления презентацией
- Одновременная работа на досках
- Совместное редактирование документов
- Беспроводная гарнитура

«ХОЧУ ПОЩУПАТЬ!»
- Движения
- Действия



ДИГИТАЛЫ
- Схема
- Первое, второе, третье...
- MindMap
- юююневажно, КАК вы излагаете свою ЛОГИЧНУЮ мысль

«ХОЧУ ПОНЯТЬ!»
- Логика
- Смысл



	MindMap с одновременным редактированием	RoadMap с общим доступом	Конфколлы без видео!
 КИНЕСТЕТИКИ	Можно подвигать стикеры, самому порисовать.	Можно самому вписывать шаги, менять последовательность.	
 ДИГИТАЛЫ	Появляются цели и логика.	Выстраивается логичная последовательность действий.	
 АУДИАЛЫ			Может слышать, что происходит.
	miro	Google Drive	Microsoft Teams

- Текущие проблемы
- Цели изменений
- Ключевые направления
- Следующие шаги
- Ключевые помощники
- Не сделали НИ ОДНОЙ презентации!

- Готовим сценарии стратсессий
- Запасаемся стикерами
- Заправляем маркеры
- Думаем над неформальными мероприятиями по вовлечению
- И делаем презентации!

Елена Савосина

Руководитель направления методологии Финансового департамента

Ак Барс Банк

Сбербанк и BI.ZONE подготовили ежегодное исследование «Threat Zone 2020: не дожидаясь бури»

Аналитический материал посвящён ключевым трендам киберпреступности и их влиянию на экономику

18 июня 2020 года, Москва – было опубликовано ежегодное аналитическое исследование «Threat Zone 2020: не дожидаясь бури», подготовленное экспертами Сбербанка и компании BI.ZONE.

Threat Zone 2020 – уже третий аналитический материал из серии ежегодных исследований киберугроз современности. В 2018 году основной темой Threat Zone стали вызовы цифровизации. Прошлогоднее исследование было посвящено методам киберпреступников и наиболее популярным кибератакам. В этот раз центральной темой Threat Zone 2020 стали основные тенденции развития цифровых угроз и вызовов защиты организаций, возникших в том числе в результате кризиса из-за пандемии. Эксперты сравнивают уровни защищённости систем в конкретных отраслях и дают рекомендации для повышения устойчивости перед новейшими киберугрозами.

«2020 год изменил жизнь сотен миллионов людей. Цифровизация ускоряется и риски растут: мы начинаем всё больше зависеть от цифровых каналов связи, и шансы кибер-кризиса многократно возрастают. Поэтому наше третье исследование мы назвали «Не дожидаясь бури». В нём мы анализируем тренды существующих и новых угроз, а также предлагаем читателям прикладные инструменты для оценки киберустойчивости бизнеса и рекомендации, как защитить себя и своих клиентов в новых условиях», – отметил заместитель председателя правления Сбербанка **Станислав Кузнецов.**

EXECUTIVE SUMMARY

Источниками кризисов обычно становятся факторы, связанные с нестабильностью отдельных рынков, экономики в целом или общественнополитической обстановки. Бизнес и государство уже привыкли к такого рода угрозам: в риск-департаментах и профильных министерствах на этот случай всегда существует план Б.

Однако сейчас аналитикам стоит сосредоточиться на проработке рисков киберкризиса. Его вероятность с каждым днём растёт, последствия по разрушительности сопоставимы с результатами традиционных катаклизмов, при этом большинство компаний (77%[1]) к такому повороту событий не готовы.

Хорошая новость в том, что способы защиты от киберкризиса существуют. Но они требуют постоянного вложения ресурсов и желания сотрудничать – это касается как отдельных организаций, так и целых государств.

О необходимости объединять усилия говорят уже не только аналитические центры и профильные институты, но и ведущие международные организации, например, ООН, которая призывает экспертов национальных центров реагирования на инциденты (CERT) ставить в приоритет кооперацию и обмен информацией[2].

Ведь в мире, объединённом интернетом, всё взаимосвязано, и связи эти становятся только теснее. По данным Международного союза электросвязи (МСЭ), с 2005 г. число пользователей сети ежегодно росло

на 10% и в 2019-м, предположительно, достигло 4,1 млрд человек[3]3.

Готовность к киберкризисам – необходимое, но не единственное условие успешной защиты. Хорошо разбираться в угрозах по-прежнему важно. В ближайшие годы ландшафт киберпреступности будут формировать два основных фактора: внутренние угрозы и развитие технологий. Несомненно, свой след в этом пространстве уже оставила и пандемия COVID-19, в результате которой экономика оказалась в состоянии кризиса, а компаниям по всему миру пришлось осваивать методы дистанционной работы.

1. IBM study: more than half of organizations with cybersecurity incident response plans fail to test them // IBM Newsroom.

2. The age of digital interdependence // UN.

3. Measuring digital development: facts & figures 2019 // ITU.

Доля населения Земли, подключенного к интернету, в 2005–2019 гг.
Источник: Международный союз электросвязи (МСЭ).

Внутренние угрозы

2019 год не раз напомнил миру, что, защищая внешний периметр, нельзя забывать о рисках, исходящих изнутри.

69%
компаний признали, что их данные утекли по вине сотрудников или подрядчиков[4]

Согласно одному из опросов, 69% организаций связывают утечки данных с внутренними злоумышленниками[4] – о некоторых случаях вы даже слышали в новостях. Например, в сентябре прошлого года два сотрудника фирмы – подрядчика малайзийской авиакомпании Malindo Air выкрали данные 45 млн пассажиров[5].

Даже в самой сфере кибербезопасности не все компании надёжно защищены от таких угроз: в феврале из-за ошибки подрядчика в сеть попали личные данные семи сотрудников компании Palo Alto Networks[6].

Впрочем, человеческий фактор не всегда сопряжён со злым умыслом или ошибками в работе: нередко компрометация происходит просто из-за недостатка киберграмотности.

Как утверждает МСЭ, в 40 из 84 стран, о которых есть данные, меньше половины населения обладает базовыми навыками работы с компьютером (умеет копировать файлы и работать с электронной почтой).

Доля тех, кто может совершить более сложные операции, ещё меньше[7]. Такой уровень компьютерной грамотности вряд ли предполагает знакомство хотя бы с азами компьютерной гигиены. Хороший пример – атака группировки Lazarus на чилийскую компанию Redbanc: IT-специалист банка открыл вредоносное ПО, замаскированное под программу для заполнения заявки на работу, и скомпрометировал корпоративную сеть организации[8].

Развитие технологий

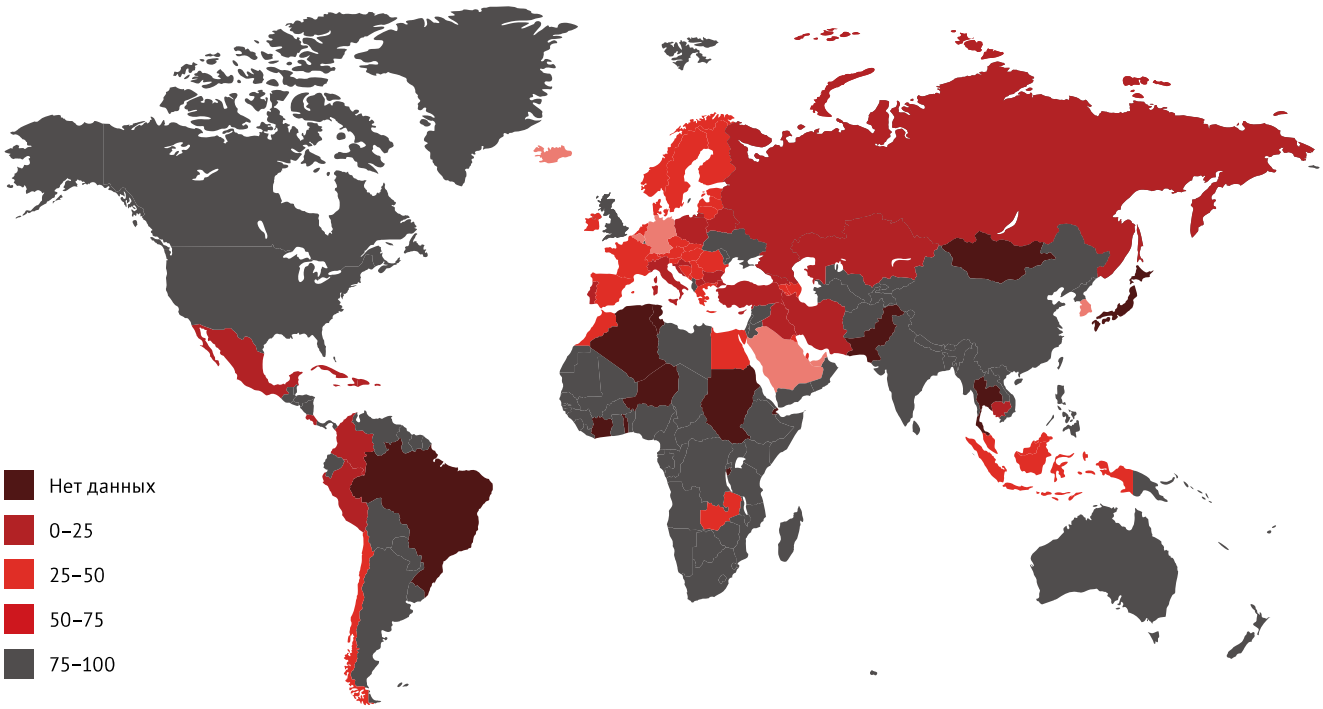
Каждая новая технология не только привносит в нашу жизнь комфорт, но и бросает новые вызовы с точки зрения кибербезопасности.

Индустрия IoT-устройств (чайники, холодильники и прочие бытовые приборы, подключаемые к интернету) развивалась с упором на большие объёмы выпуска при минимальных расходах – такой подход сказался в том числе на защищённости устройств от вторжений.

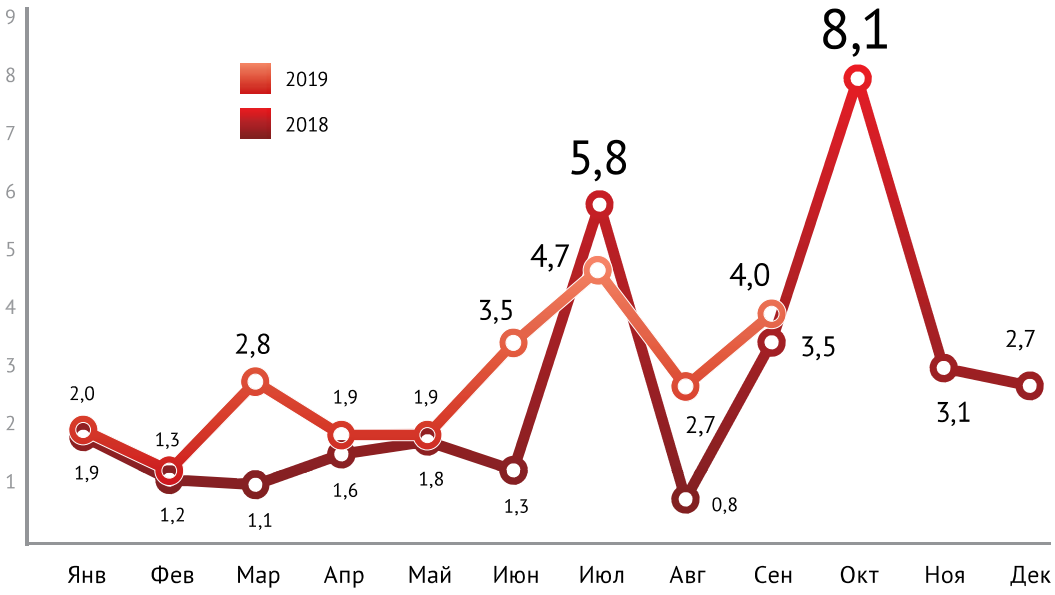
В результате злоумышленники получили в своё распоряжение миллиарды устройств, из которых сейчас состоит основная масса сетей для DDoS-атак.

В сотовых сетях нового поколения 5G данные будут передаваться со скоростью от 20 гигабит в се-

4. 2019 data exposure report // Code42.
5. Malindo Air says data leak caused by ex-staffers at contractor firm // Reuters.
6. 7 employees who worked at cybersecurity giant Palo Alto Networks had their social security numbers exposed after a partner «inadvertently» posted personal info to a website // Business Insider.
7. Measuring digital development: facts & figures 2019 // ITU.
8. North Korean hackers infiltrate Chile»s ATM network after Skype job interview // ZDNet.
9. IoT 2019 in review: the 10 most relevant IoT developments of the year // IoT Analytics.



Процент пользователей, владеющих базовыми компьютерными навыками, в 2014–2018 гг.
Источник: МСЭ.



Число атак вредоносного ПО на IoT-устройства в 2018–2019 гг., млн. Источник: SonicWall.

9,5 млрд устройств составляли интернет вещей на конец 2019 г.[9]

кунду с задержкой до 4 миллисекунд[10] (для сравнения: LTE/4G поддерживала до 1000 мегабит в секунду при задержке до 20 миллисекунд).

Вместе с тем сети нового типа менее централизованы и в меньшей степени базируются на физическом оборудовании. Это затрудняет защиту от атак и реагирование на инциденты.[11]

Биометрические данные все чаще используют для аутентификации: в отличие от паролей, они не требуют от пользователя запоминания, гарантированно уникальны для каждого человека, и их не так просто взломать методом перебора, как многие популярные пароли.

При этом системы распознавания биометрических данных можно обмануть, а если информация скомпрометирована, заменить ее для конкретного пользователя будет очень трудно.[13]

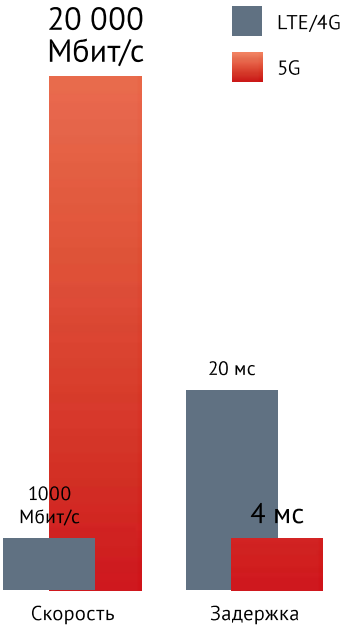
Искусственный интеллект (ИИ) полезен практически в любой сфере, а в кибербезопасности особенно. Он позволяет автоматизировать и ускорить многие рутинные задачи: отсеивание спама, распознавание простых уязвимостей в периметре, сбор и обработку больших данных о предыдущих угрозах.

В то же время ИИ помогает злоумышленникам создавать более продвинутое вредоносное ПО и правдоподобные фишинговые рассылки.[14]

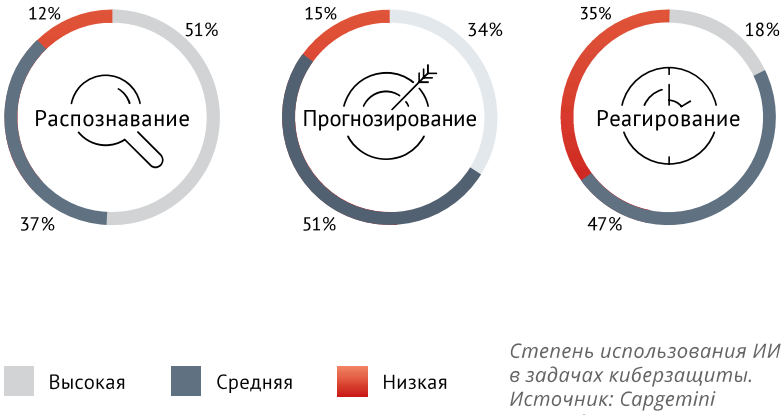
2,7 млрд устройств будет подключено к 5G к 2025 г.[12]

59% компаний утверждают, что внедрение ИИ в кибербезопасность повышает эффективность защиты[15]

10. Minimum requirements related to technical performance for IMT-2020 radio interface (s) // ITU.
11. Why 5G requires new approaches to cybersecurity // Brookings.
12. Market forecast: 5G connections, worldwide, 2018-2025, August 2018 update // CCS Insight.
13. Biometric identification: the good and the bad // UM DCIE Cybersecurity.
14. Adversarial artificial intelligence: winning the cyber security battle // Information Age.
15. The value of artificial intelligence in cybersecurity // Ponemon Institute.



Повышение скорости от LTE/4G к 5G: от 1000 Мбит/с с задержкой в 20 мс до 20 000 Мбит/с с задержкой в 4 мс.



Степень использования ИИ в задачах киберзащиты. Источник: Capgemini Research Institute.

65,9 млрд $
ожидаемый объём мирового рынка биометрии к 2024 г.[16]

500 тыс
организаций наняли специалистов по защите персональных данных после вступления в силу GDPR[21]

8-10 трлн $
прогнозируемый ущерб мировой экономики от кибератак в 2022 г.[2]

7 место
занимают кибератаки в рейтинге наиболее вероятных глобальных угроз, который составил Всемирный экономический форум[2]

Законодательство

Закон «О безопасности критической информационной инфраструктуры», действующий в России с начала 2018 г., стал важным шагом к повышению кибербезопасности в ключевых отраслях экономики, в том числе в банковской сфере.

Теперь на основе этого закона создаются регулятивные документы для отдельных индустрий. Так, в августе прошлого года вступил в силу приказ Министерства энергетики РФ об утверждении требований к информационной безопасности при создании систем удалённого мониторинга энергообслуживания[17]. Помимо прочего, в документе регламентирован порядок безопасного сбора и хранения информации в этих системах, определены необходимые мероприятия, виды уязвимостей и нарушения при построении моделей угроз[18].

Проблема, однако, стоит шире. Сохранности критических инфраструктур недостаточно, чтобы создать по-настоящему безопасное киберпространство. В глобализированном мире атака в одной отрасли может привести к инцидентам в других. Поэтому требования к безопасности в ключевых сферах нужно дополнять аналогичными регламентами, но уже для всех областей – на национальном уровне. В зарубежном законодательстве, связанном с кибербезопасностью, между тем продолжает доминировать тема защиты персональных данных.

С 1 января 2020 г. вступил в действие Закон о приватности потребителей в Калифорнии (California Consumer Privacy Act, CCPA). Этот документ во многом аналогичен GDPR – регламенту работы с персональными данными, который применяется в Евросоюзе с мая 2018 г. CCPA обязывает компании, работающие с персональными данными калифорнийцев, подробно информировать пользователей о сборе сведений, а также предоставить им возможность запрашивать информацию о себе и запрещать ее продажу третьим лицам[19].

Специалисты по кибербезопасности в США полагают, что появление таких же законов в других штатах – вопрос времени.[20]

Ответы и решения

Цель исследования – рассказать всем заинтересованным сторонам об актуальных киберугрозах и методах защиты от них, показать, что в одиночку, не объединяя усилия, противостоять общему врагу сегодня невозможно.

Киберпреступность по определению игнорирует границы, а значит, связанные с ней кризисы непременно будут иметь глобальный характер. Однако тесная взаимосвязь между компаниями, отраслями и странами создает не только уникальные проблемы, но и исключительные возможности. Кибербезопасность, как и киберпреступность, способна перешагнуть любые границы – препятствует лишь человеческий фактор: сложные взаимоотношения, конкуренция, бюрократия.

Чтобы преодолеть человеческий фактор, каждый руководитель должен осознать: если к киберкризису не готова одна страна или даже одна организация, он настигнет всех – даже тех, кто принял меры. Для защиты от катаклизмов необходимо налаживать эффективную коммуникацию на всех уровнях, открыто и бескорыстно обмениваться данными об инцидентах и сообща прорабатывать встречные меры.[22]

О компании

BI. ZONE помогает компаниям по всему миру сохранять высокий уровень кибербезопасности, поддерживать темпы развития бизнеса и соответствовать ожиданиям клиентов.

- Технологичные продукты для защиты IT-инфраструктур и приложений.
- Услуги от оценки киберустойчивости до расследования инцидентов.
- Решения по аутсорсингу кибербезопасности для бизнеса любого масштаба.

Компетенции

- Стратегический партнер Интерпола в части расследования киберпреступлений.
- Экспертная организация Центра кибербезопасности Всемирного экономического форума.
- Сертифицированный член международного сообщества по кибербезопасности CREST.
- Компетентная организация при Координационном центре национального домена сети Интернет.
- Корпоративный центр Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
- Провайдер сервисов в области кибербезопасности, рекомендованный SWIFT в 79 странах мира.
- Команда BI. ZONE CERT – полноправный член Ассоциации центров реагирования на инциденты и обеспечения кибербезопасности (FIRST).
- Услуги BI. ZONE соответствуют требованиям международных стандартов ISO 9001 и ISO 27001.

Отраслевая экспертиза

Мы реализуем проекты для финансовых организаций, IT- и телеком-компаний, клиентов из индустрий e-commerce, транспорта, промышленности и медиа.

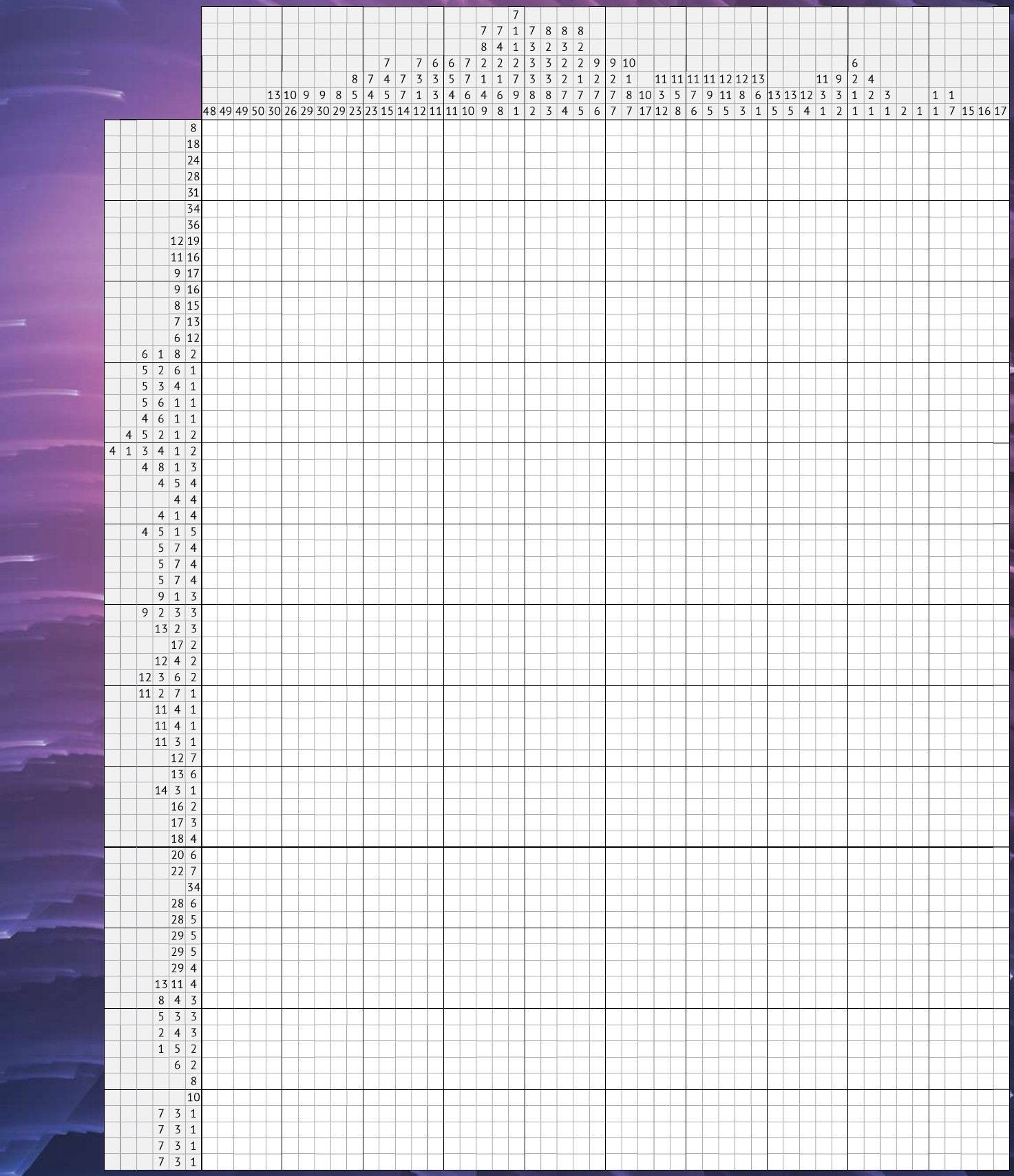
Криминалистика и расследования

Наша команда кибердетективов ежедневно на страже и готова к реагированию на любые хакерские атаки – от фишинга до APT, от DDoS до промышленного шпионажа.

16. Biometric system market: global forecast to 2024 // Markets and Markets.
17. Зарегистрирован Приказ Минэнерго России, утверждающий требования к информационной безопасности систем удаленного мониторинга энергооборудования // Министерство энергетики РФ.
18. Приказ Министерства энергетики Российской Федерации от 06.11.2018 №1015 // Российская газета.
19. AB-375 Privacy: personal information: businesses // California Legislative Information.
20. 5 cybersecurity trends that will dominate 2020, according to experts // TNW.
21. Study: an estimated 500K organizations have registered DPOs across Europe // International Association of Privacy Professionals.
22. The global risks report 2020 // World Economic Forum.

Японский кроссворд

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



CIS / № 3 (13) / 2020 / www.cis.ru

ИБЭШНИКИ: ХОЛОДИЛЬНИК ДЛЯ ЛИЗЗИ

А вы задумывались что к умным вещам ещё и хозяева умные должны прикладываться? Жаль, что у хозяев нет кнопки «Сменить прошивку». А вы готовы к умным вещам? Точно?

Автор:
Владимир Безмалый

Календарь мероприятий

1 сентября – 31 августа
Москва • Курс
Стажировка в IT-направлении ВТБ Капитал

1 сентября – 31 октября
Онлайн-трансляция • Курс
Бесплатный Интенсив по Android-разработке на Kotlin

4 сентября
Москва • Онлайн-трансляция • Курс
Стажировка для IT-направлений, ВТБ Юниор

5 сентября
Москва • Онлайн-трансляция • Форум
KaiCode – Open Source Summit

5 сентября
Санкт-Петербург • Турнир
Велотурнир «IT Bike Fest St. Petersburg 2020»

8 сентября
Нижний Новгород • Конференция
Пандемия не пройдёт: семинар TrueConf про видеоконференцсвязь и удалённую работу в Нижнем Новгороде

8-10 сентября
Онлайн-трансляция • Конференция
MOBILE Z-DAYS

9-11 сентября
Москва • Курс
Администрирование кластера Kafka

9 сентября
Онлайн-трансляция • Конференция
SEO без воды 2

10 сентября
Москва • Форум
IT Management Forum 2020

10 сентября
Казань • Конференция
Пандемия не пройдёт: семинар TrueConf про видеоконференцсвязь и удалённую работу в Казани

14-18 сентября
Онлайн-трансляция • Конференция
Russian Python Week

14-16 сентября
Москва • Курс
BDAM: Большие данные Big Data для руководителей

15-17 сентября
Москва • Онлайн-трансляция • Конференция
TestCon Moscow 2020 – международная конференция по тестированию и обеспечению качества ПО

15 сентября – 15 декабря
Москва • Курс
Оплачиваемые программы развития для IT-специалистов в ВТБ

16-18 сентября
Краков • Конференция
ACE!

17 сентября
Москва • Форум
Российский саммит по цифровой трансформации организаций CDO/CDTO Summit & Award 2020

17 сентября – 11 ноября
Онлайн-трансляция • Курс
Фундаментальный курс по SEO

19 сентября
Москва • Мероприятие
IT-конкурс красоты журнала CIS «Beauty & DigITal»

19 сентября
Москва • Турнир
Турнир по картингу «IT Race Moscow 2020»

19-20 сентября
Санкт-Петербург • Хакатон
Hack Life

21-23 сентября
Москва • Курс
DEVKA1: Kafka Streams для разработчиков

23 сентября – 2 октября
Онлайн-трансляция • Конференция
Frontend Live 2020

23 сентября
Москва • Конференция
Видео+Конференция 2020

24 сентября
Онлайн-трансляция • Вебинар
Управление талантами на платформе 1С: Предприятие: оценка персонала по компетенциям, управление развитием персонала и кадровый резерв

24-25 сентября
Москва • Курс
DEVKA2: Kafka интеграция для разработчиков

26-27 сентября
Новосибирск • Хакатон
Tour. Hack

26-27 сентября
Санкт-Петербург • Онлайн-трансляция • Конференция
HR API 2020

28 сентября – 2 октября
Москва • Курс
HADM: Администрирование кластера Hadoop

29 сентября
Самара • Конференция
Пандемия не пройдёт: семинар TrueConf про видеоконференцсвязь и удалённую работу в Самаре

29 сентября – 7 октября
Онлайн-трансляция • Конференция
DevOps Live 2020

1 октября
Москва • Конференция
RPA 2020: Роботизация бизнес-процессов

1 октября
Санкт-Петербург • Конференция
Пандемия не пройдёт: семинар TrueConf про видеоконференцсвязь и удалённую работу в Санкт-Петербурге

8 октября
Онлайн-трансляция Вебинар
Автоматизация управления по целям и KPI в среднем и крупном бизнесе

14-17 октября
Онлайн-трансляция • Конференция
Golang Live 2020

15 октября
Москва • Конференция
Благотворительная ИТ-конференция журнала CIS «Digital Hearts»

17 октября
Санкт-Петербург • Турнир
Турнир по мини-футболу «IT Goal St. Petersburg 2020»

24 октября
Москва • Турнир
Турнир по волейболу «IT Match Ball Moscow 2020»

27-29 октября
Москва • Конференция
3-я Международная научно-техническая конференция «Современные сетевые технологии»

27-29 октября
Москва • Онлайн-трансляция • Конференция
Big Data Days 2020

29 октября
Онлайн-трансляция • Вебинар
Управление талантами на платформе 1С: Предприятие: оценка персонала по компетенциям, управление развитием персонала и кадровый резерв

30-31 октября
Санкт-Петербург • Онлайн-трансляция • Конференция
Open Source Tech Conference Piter

4-7 ноября
Онлайн-трансляция • Конференция
Heisenbug 2020 Moscow: Большая техническая конференция по тестированию

5-6 ноября
Москва • Онлайн-трансляция • Конференция
INFOSTART EVENT 2020

9-10 ноября
Москва • Конференция
HighLoad ++ 2020

11-14 ноября
Онлайн-трансляция • Конференция
C++ Russia 2020 Piter: Конференция для C++-разработчиков

11-14 ноября
Онлайн-трансляция • Конференция
Mobius 2020 Moscow: Конференция для мобильных разработчиков

17 ноября
Москва • Конференция
PHP Russia

21 ноября
Москва • Турнир
Интеллектуальный турнир «IT Brain Battle Moscow 2020»

CISummIT

Мероприятие журнала CIS

Благотворительная ИТ-конференция Digital Hearts

15 октября, 2020

Площадка «Москва-Сити»

Фонд Хабенского

Мероприятие журнала CIS в поддержку Фонда Константина Хабенского

Заполните регистрационную форму для участия на мероприятии

Ждём вас на благотворительной ИТ-конференции CISummIT Digital Hearts, которая объединит самых активных участников ИТ-рынка, ведущих производителей и экспертов, чтобы собрать средства для помощи детям с заболеваниями головного мозга.

CIS Современные Информационные Системы

www.cisevent.ru
www.cismag.news
www.cis.ru