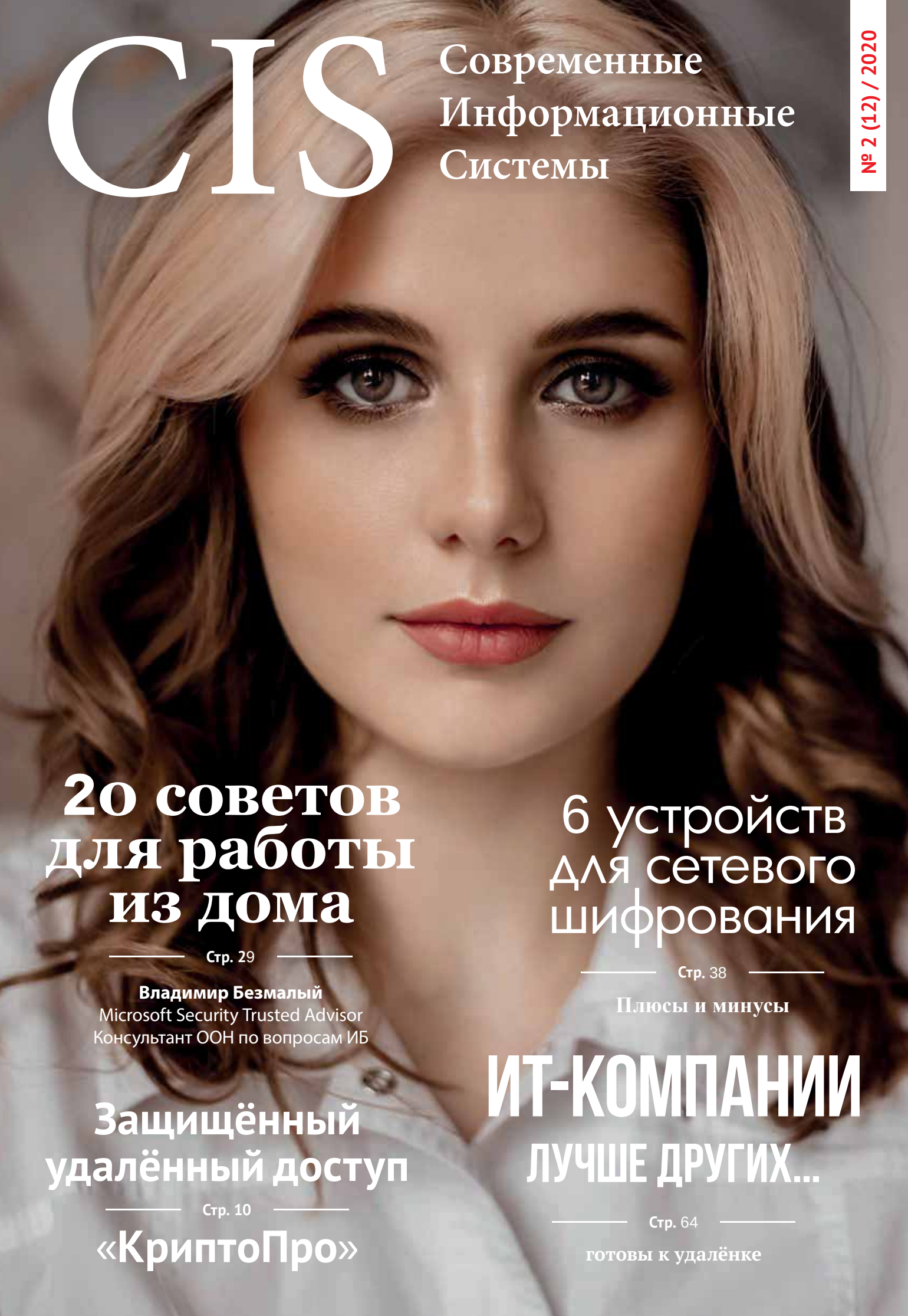
CIS
Современные Информационные Системы
№ 2 (12) / 2020



20 советов для работы из дома

Стр. 29

Владимир Безмалый
Microsoft Security Trusted Advisor
Консультант ООН по вопросам ИБ

6 устройств для сетевого шифрования

Стр. 38

Плюсы и минусы

ИТ-КОМПАНИИ ЛУЧШЕ ДРУГИХ...

Стр. 64

готовы к удалёнке

Защищённый удалённый доступ

Стр. 10

«КриптоПро»

ПРЕДИСЛОВИЕ

РЕШЕНИЯ

ТЕХНОЛОГИИ

ОПЫТ

ПРОДУКТЫ

АНАЛИТИКА

FASHION-IT

КОМИКСЫ

КАЛЕНДАРЬ

КРОССВОРД

От редактора

Распространение нового заболевания в мировых масштабах – пандемии, повлияло на все сферы и отрасли без исключения не только отрицательно, но, как ни странно, и положительно. Ведь всем нам известно, что если где-то что-то убыло, то где-то что-то прибыть должно непременно.

ИТ-компании достаточно быстро начали реагировать на ситуацию и стали подстраиваться. Перед ними встала беспрецедентная по своей сложности и масштабам задача позаботиться не только о здоровье сотрудников и обеспечении своей финансовой стабильности, но и стать полезным в поставке клиентам решений и продуктов, помогающим им достичь того же.

Ситуация также кардинально изменилась и по отношению к сфере информационных технологии: если раньше для большей части отраслей и государства ИТ играли чаще вспомогательную роль и использовались скорее опционально, то сейчас они становятся жизненной необходимостью.

С некоторыми решениями компаний мы предлагаем вам ознакомиться на страницах нашего журнала.

Мы также расскажем, как в нынешней ситуации справляются российские компании, какие принимаются меры и как быстро они реагируют.

Вследствие самоизоляции весной этого года все мероприятия были переведены в онлайн-режим. В частности, наша благотворительная ИТ-конференция CISummIT Digital Hearts в поддержку Фонда Константина Хабенского тоже прошла удалённо.

Однако мы понимаем, что ничто не заменит живого человеческого общения, поэтому надеемся, что на следующем нашем мероприятии – конкурсе красоты «Beauty & DigITal», которое пройдёт осенью, мы встретимся с вами в приятной дружеской обстановке.

В заключение желаем вам и вашим близким здоровья, и пусть все невзгоды обойдут стороной.

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: Мария Калягина.

Тираж 5000 экз. (отпечатанный тираж).

Журнал предназначен для лиц старше 16 лет.

Мария Калягина
Медицинская сестра-анестезист
Московского клинического
центра инфекционных
болезней «Вороновское»

Герои нашего времени

Во всём мире продолжается непрерывная непримиримая борьба с коварным, ранее неизвестным врагом — коронавирусной инфекцией.

Первыми, кто встал на пути опасной пандемии и принял удар на себя, стали медицинские работники, которые сражаются с болезнью на передовой, и теперь абсолютно заслуженно приравниваются к супергероям.

Они — герои нашего времени!

К сожалению, есть между ними одно весомое различие. Если выдуманные супергерои в той или иной степени неуязвимы, то медицинские работники, каждый раз переступая порог больницы, рискуют собственным здоровьем, а порой и жизнью.

Именно поэтому сегодня каждому человеку важно знать и понимать, через какие трудности проходят медицинские работники — врачи, медсёстры, водители скорой помощи. Они ежедневно и самоотверженно заботятся о здоровье людей, занимаются профилактикой, лечением и диагностикой коронавирусной инфекции, чтобы сдержать рост заболеваемости в России и предотвратить развитие мировой пандемии.

В эти дни, недели, месяцы, пока мы находимся в безопасности в своих тёплых и уютных квартирах, большинство медиков работают на износ гораздо дольше обычных 40 часов в неделю. Им приходится работать многие часы без перерыва на обед, в две-три смены подряд. Некоторые медики находятся в разлуке со своими родными, семьями, так как их коллеги не выдерживают напряжённой борьбы, заболевают и временно выбывают из строя. И это ещё одно подтверждение того, что клятва Гиппократа — это не просто речь, считанная с листка. Для таких людей медицина больше чем профессия. Это призвание, потребность помогать, спасать жизни… Когда не можешь оставаться равнодушным.

Глобально мы уже вряд ли сможем изменить сложившееся положение. Но, возможно, эта информация позволит кому-то взглянуть на сегодняшнюю ситуацию под другим углом, заставит быть чуть более осознанным и нести ответственность за свои действия.

Чтобы прекратить распространение коронавирусной инфекции и дать врачам шанс справиться с огромным наплывом пациентов, прежде всего следует соблюдать меры самоизоляции. Это самое простое, что мы можем сделать для всеобщего блага уже сейчас. И, конечно же, не стоит пренебрегать правилами личной гигиены. Только так — вместе, единым фронтом мы сможем справиться с глобальной проблемой, нависшей над всем миром. От ответственности, самодисциплины каждого из нас зависит то, как скоро прекратится карантин, эпидемия пойдёт на спад, и наша жизнь вернётся в прежнее русло.

Можно ли выразить благодарность за свою спасённую жизнь или жизнь родного человека словами? Уверены, для этого не хватит и тысячи слов, но мы попробуем.

Редакция ИТ-журнала CIS — Современные Информационные Системы выражает огромную благодарность, поддержку всем медицинским работникам без исключения: врачам, фельдшерам, водителям скорой помощи, медсёстрам, в частности Марии Калягиной — медицинской сестре-анестезисту Московского клинического центра инфекционных болезней «Вороновское» за круглосуточную работу, невероятную самоотдачу в период пандемии коронавируса.

В это непростое время ваша и без того тяжёлая работа стала намного сложнее и опаснее. Спасая нас, вы рискуете своим здоровьем и жизнью. Спасибо вам за этот титанический труд, за заботу о нас и наших близких! Низкий поклон всем медикам, которые трудятся сейчас на линии «огня» и сохраняют верность своей благородной профессии! Бесконечная благодарность за ваш труд, мужество и самоотверженность! Пока есть такие люди, как вы, наша планета будет продолжать процветать!

CIS Современные Информационные Системы

CIS (Современные Информационные Системы) — *ИТ-журнал об информационных технологиях в России.*

info@sovinfosystems.ru

www.cis.ru

Как использовать «Личное хранилище» OneDrive для защиты ваших файлов

30 сентября 2019 года компания Microsoft представила по всему миру «Личное хранилище» для ваших конфиденциальных файлов. Оно входит в состав облачной службы хранения OneDrive. Эти файлы зашифрованы и защищены с помощью двухэтапной аутентификации, даже если они синхронизируются с вашим ПК под управлением ОС Windows 10. Работает «Личное хранилище» на базе ОС Windows 10, Android, iPhone, iPad и непосредственно в Интернет.

Что такое «Личное хранилище» в OneDrive?

«Личное хранилище» (Personal Vault) – это сверхзащищённая область хранения ваших файлов в OneDrive. Например, если вы собираетесь хранить конфиденциальные финансовые документы или копии своего паспорта в OneDrive, вы, вероятно, захотите поместить их в личное хранилище для дополнительной безопасности.

Стоит отметить, что ваше личное хранилище потребует дополнительной аутентификации для получения доступа к вложенным файлам. Каждый раз при получении доступа к вложенным файлам, вы должны использовать двухфакторную аутентификацию: PIN-код, отпечаток пальца или аутентификацию по лицу. В Windows 10 можно использовать для аутентификации Windows Hello. Хранилище блокируется после 20 минут бездействия, после чего вам необходимо снова пройти аутентификацию, прежде чем снова получите доступ. Если же вы обращаетесь к защищённым данным через веб-сайт OneDrive, они не будут кэшироваться вашим браузером. Вместе с тем необходимо отметить, что время бездействия, после которого личное хранилище будет заблокировано, на iPhone составляет 3 минуты.

При организации личного хранилища на iPhone вам будет предложено ввести PIN-код для его разблокирования и пользоваться Touch ID либо Face ID.

Personal Vault шифрует файлы внутри него. В Windows 10 Personal Vault сохраняет эти файлы в зашифрованной области BitLocker на жёстком диске. Это работает, даже если у вас Windows 10 Home и вы не используете BitLocker ни для чего другого. Microsoft говорит, что ваши файлы также хранятся в зашифрованном виде на серверах Microsoft.

Вы не можете передать файлы, хранящиеся в Personal Vault кому-либо ещё. Даже если вы предоставите общий доступ к файлу, а затем переместите его в Personal Vault, общий доступ к этому файлу будет отключён. Следовательно, вы не можете случайно поделиться чувствительным файлом, если он хранится здесь.

Стоит отметить, что с приложением OneDrive на смартфоне вы можете сканировать документы и делать фотографии прямо из Personal Vault, сохраняя их в безопасном пространстве и не размещая ранее в другом месте вашего телефона.

Вместе с тем необходимо учесть, что ваша учётная запись (Microsoft Account) для двухфакторной аутентификации может использовать один номер телефона, а Personal Vault вы сможете настроить на другой номер. Более того, для двухфакторной аутентификации в Personal Vault вы можете настроить использование аппаратного токена, поддерживающего FIDO2. Вместе с тем стоит указать, что для почтового сервиса Outlook.com или сервиса OneDrive аппаратный ключ сегодня использовать можно только в американской версии Windows 10. В любой другой, увы, нельзя.

Другие крупные облачные сервисы хранения данных – Dropbox, Google Drive и Apple iCloud Drive – пока не предлагают подобную функцию.

Хотя стоит учесть, что уже существуют приложения с подобными функциями, например Kaspersky Password Manager.

Лучше всего работает с Office 365

Бесплатная версия OneDrive и план на 100 ГБ ограничивают вас максимум тремя файлами в вашем Personal Vault. Но вы можете добавить несколько файлов в архив (например, ZIP-файл) и сохранить его как один файл в вашем хранилище. При этом помните, что вы должны ограничиться тремя файлами (рис. 1).

Благодаря платному тарифному плану Office 365 Personal или Office 365 Home вы можете хранить в личном хранилище столько файлов, сколько хотите, вплоть до лимита хранилища OneDrive, который, вероятно, составит 1 ТБ или более.

Какие платформы поддерживаются?

Личное хранилище (Personal Vault) работает в OneDrive на Windows 10, Android, iPhone, iPad и в Интернете по адресу onedrive.live.com.

Данное хранилище недоступно в OneDrive для macOS, Windows 7, Windows 8.1, Windows Phone, Xbox, HoloLens, Surface Hub или Windows 10 S.

Персональное хранилище также доступно только в OneDrive Personal и не доступно в OneDrive Business.

Как использовать персональное хранилище

Чтобы использовать личное хранилище, просто откройте папку OneDrive и нажмите/коснитесь ярлыка Personal Vault (в русской версии – «Личное хранилище»). Вы можете сделать это на ПК с Windows 10 через веб-сайт или с помощью приложения для смартфона, то есть любым удобным способом (рис. 2).

Поместите все файлы, которые вы хотите защитить в личное хранилище.

Если вы не совершаете активные действия, то на компьютере ваше хранилище останется разблокированным в течение двадцати минут. Вы также можете сразу заблокировать его, щёлкнув правой кнопкой мыши в папке Personal Vault и выбрав «Заблокировать» (рис. 3).

Когда вы пытаетесь получить доступ к персональному хранилищу, пока оно заблокировано, вам будет предложено ввести дополнительную аутентификацию.

Например, если вы настроили двухфакторную аутентификацию для своей учётной записи Microsoft, вам будет предложено ввести код аутентификации. Он работает так же, как

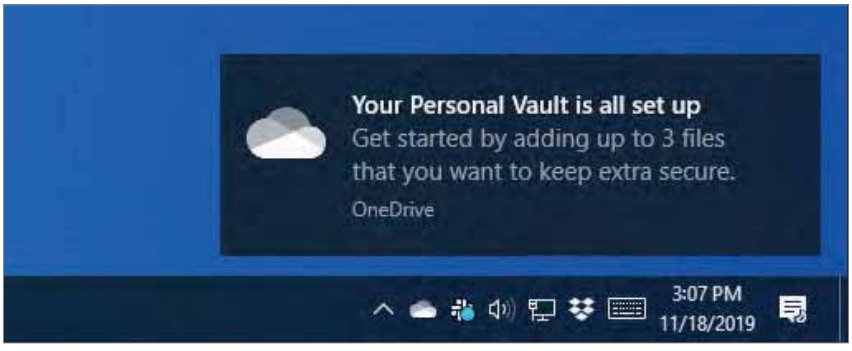


Рисунок 1.

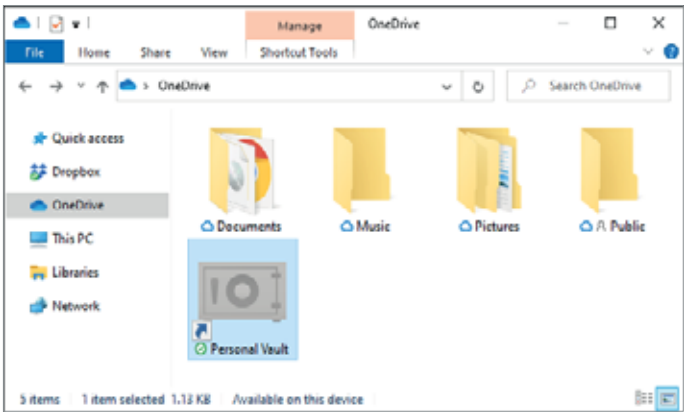


Рисунок 2.

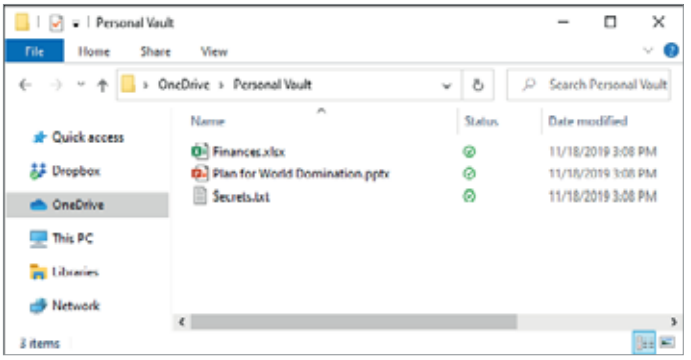


Рисунок 3.

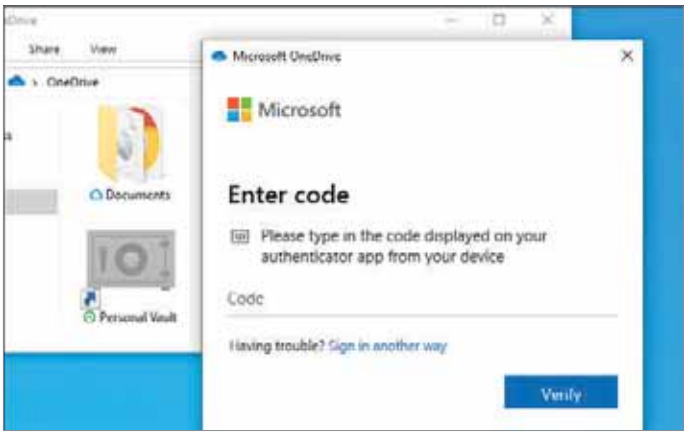


Рисунок 4.

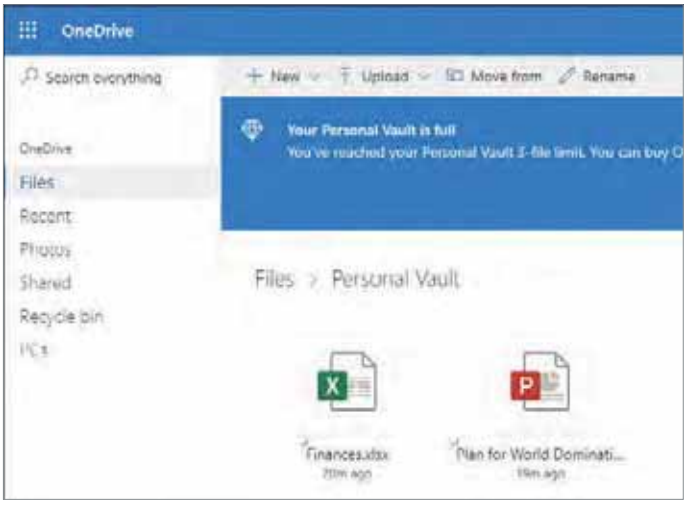


Рисунок 5

если бы вы впервые входили в свою учётную запись Microsoft с нового устройства (рис. 4).

Вы найдёте Personal Vault в главной папке вашей учётной записи OneDrive на всех поддерживаемых платформах: от Windows 10 до веб-сайта и приложений для смартфонов. Просто откройте его, чтобы разблокировать и получить доступ к файлам внутри (рис. 5).

Следует ли вам использовать личное хранилище OneDrive?

Personal Vault – полезная функция, доступная на большинстве современных платформ, за исключением Mac. Если он поддерживает используемые вами устройства, это более безопасный способ хранения конфиденциальных файлов, чем просто выгрузка их в обычную папку OneDrive.

Необходимо отметить, что Personal Vault также шифрует файлы в вашей системе Windows 10. Я считаю, что на компьютере под управлением Windows 10 необходимо использовать полное шифрование BitLocker всего жёсткого диска, но если вы по каким-то причинам этого не делаете, то шифрование личного хранилища это лучше, чем ничего.

Если вы всё же боитесь хранить конфиденциальные файлы в OneDrive, вы можете не использовать личное хранилище, а использовать другое решение, например хранение конфиденциальных документов вместе с данными для входа на веб-сайт в хранилище менеджера паролей. Этот вариант может быть более безопасным. Они будут зашифрованы мастер-паролем вашего менеджера паролей.

В документации Microsoft [1] отмечается, что «Personal Vault в Windows 10 не защищает имена и хеши файлов в вашем Personal Vault, когда Vault заблокирован». Если хотите обеспечить максимальную конфиденциальность ваших файлов, то, вероятно, лучше использовать другое решение. Microsoft обещает, что «намерена расширить защиту этих атрибутов в будущем обновлении».

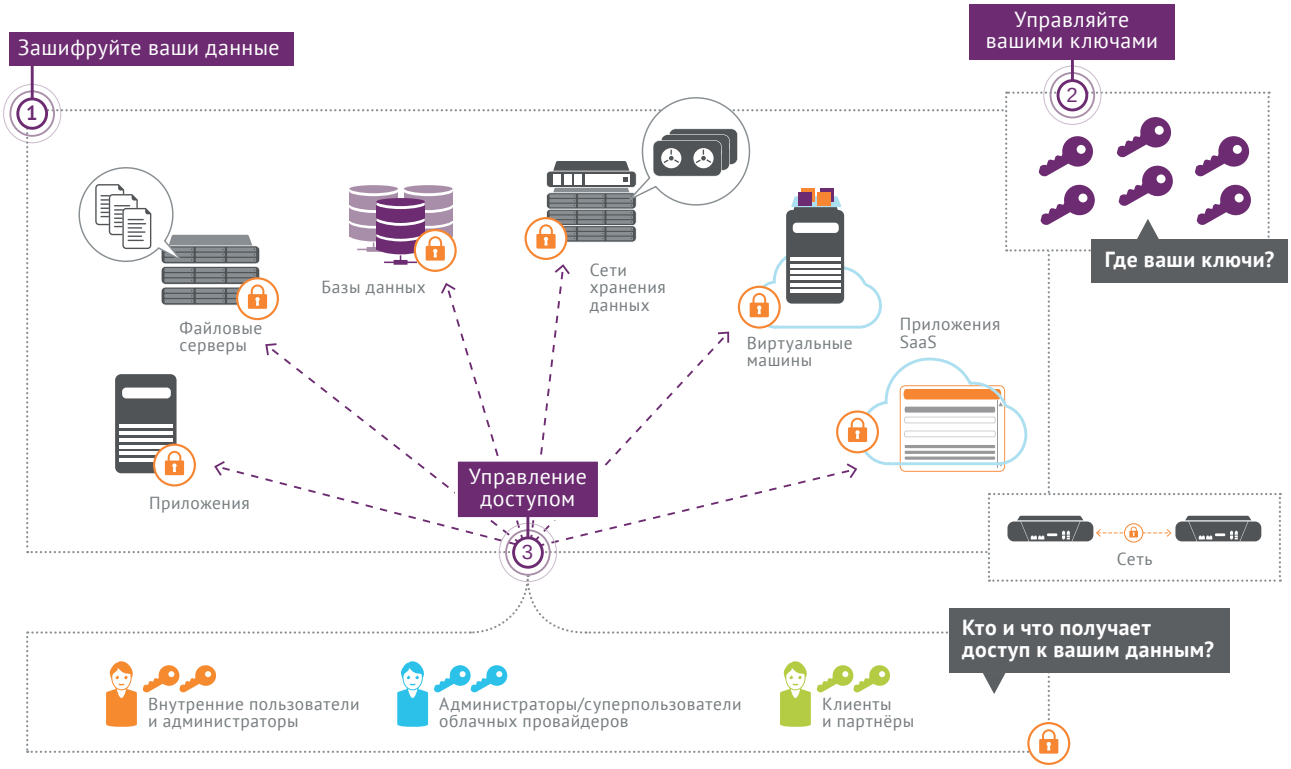
Владимир Безмалый
Microsoft Security Trusted Advisor
Microsoft MVP
Kaspersky Certified Trainer
Консультант ООН по информационной безопасности

TESSIS

TECHNOLOGIES SYSTEMS AND SOLUTIONS FOR INFORMATION SECURITY

Защищая вас и ваши данные

Уязвимые данные повсюду. А в сложном и постоянно развивающемся климате совершенствующихся угроз, виртуализации, нормативных документов и мобильности организации выбирают подход, фокусирующийся на данных, чтобы защитить и контролировать конфиденциальную информацию.



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

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

Thales Accelerate Partner Network DISTRIBUTOR

+ 7 (495) 228-02-08

info@tessis.ru

tessis.ru

CIS / № 2 (12) / 2020 / www.cis.ru

Защищённый удалённый доступ

Компания «КриптоПро» – разработчик средств криптографической защиты информации и электронной подписи – предлагает вашему вниманию пакет инструментов «Защищённый удалённый доступ» для организации удалённого доступа к внутренним ресурсам организаций с учётом требований законодательства РФ по информационной безопасности в условиях удалённого режима работы. Все инструменты пакета доступны для бесплатного использования в течение трёх и более месяцев.

В состав пакета входят следующие компоненты, которые могут быть использованы как совместно, так и отдельно друг от друга:

- **Сертифицированный ФСБ России шлюз удалённого доступа КриптоПро NGate** в виртуальном исполнении (есть также аппаратное исполнение), включающий в себя бесплатную трёхмесячную лицензию на 50 одновременных подключений и реализующий защищённый удалённый доступ к произвольным ресурсам с применением российских криптографических алгоритмов в соответствии с требованиями законодательства РФ по информационной безопасности. В качестве клиентского компонента может использоваться любой браузер, поддерживающий ГОСТ (для подключения к веб-ресурсам), либо нелицензируемый VPN-клиент КриптоПро NGate Client (для подключения к произвольным ресурсам, в том числе с мобильных устройств). По запросу возможно увеличение количества одновременных подключений и/или срока временной лицензии. Скачать ISO-образ дистрибутива Крипто Про NGate для установки в виртуальной среде и документацию на КриптоПро NGate можно здесь → Решение поддерживает различные методы аутентификации, в том числе двухфакторную аутентификацию, имеет клиентов под все популярные платформы, в том числе мобильные, обеспечивает высокую скорость, масштабируемость и отказоустойчивость (поддерживает до 32 узлов в кластере) (рис. 1).

- **Сертификат аутентификации сервера** (необходим для функционирования шлюза КриптоПро NGate), предоставляемый бесплатно и удалённо на три месяца. По запросу сертификат может быть выдан на более длительный срок. Подробности получения сертификата шлюза можно прочитать здесь →

- **Сертифицированный ФСБ России криптопровайдер КриптоПро CSP 4.0/5.0**, включа-

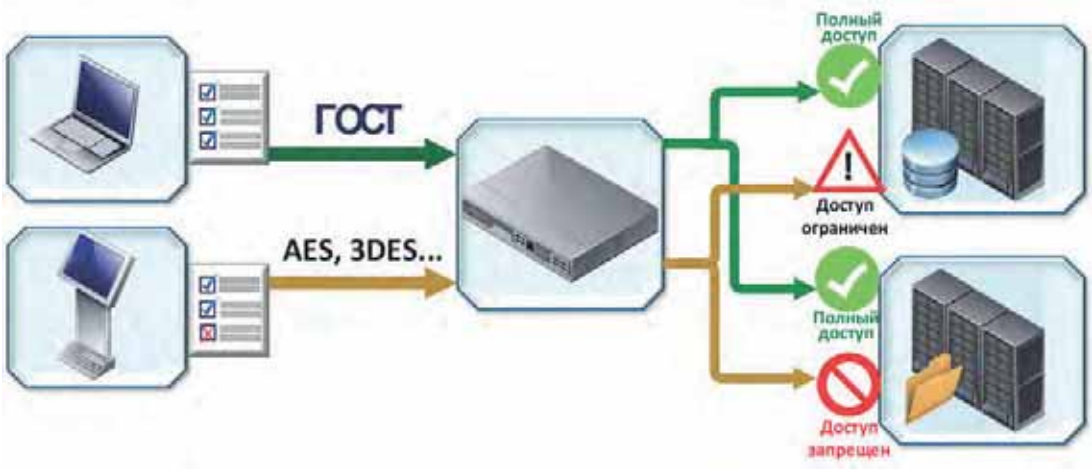


Рисунок 1.

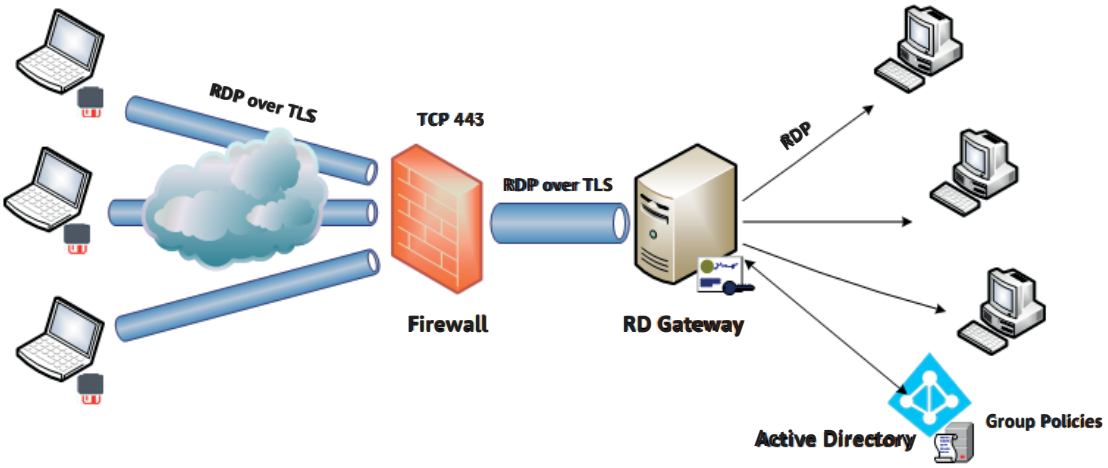


Рисунок 2.

ющий в себя бесплатную трёхмесячную лицензию. Совместное использование данного криптопровайдера со службой Microsoft RDG (Remote Desktop Gateway), входящей в состав современных серверных ОС Windows, способно обеспечить защищённый доступ к удалённому рабочему столу ОС Windows по протоколу RDP с применением российских криптографических алгоритмов. В качестве клиентского компонента для подключения к удалённому рабочему столу используется входящая в состав ОСWindows команда MSTSC. Скачать дистрибутив и документацию на КриптоПро CSP 4.0/5.0 можно здесь →

Предлагаемые для удалённого доступа компоненты нетребовательны к системным и аппаратным ресурсам и могут быть оперативно развёрнуты специалистами организации по документации. В случае необходимости в дальнейшем возможно проведение бесшовной миграции шлюза КриптоПро NGate с виртуального исполнения на более производительное и отказоустойчивое аппаратное с сохранением настроек и политик безопасности. Подробнее о компонентах, входящих в состав пакета, можно прочитать в нашей статье тут →

Предоставляемый пакет будет особенно полезен организациям, для которых удалённый доступ должен быть защищён в соответствии с требованиями законодательства по ИБ, в том числе:

- государственным органам и подведомственным организациям для организации доступа к государственным информационным системам
- операторам персональных данных для организации доступа к информационным системам персональных данных
- субъектам критической информационной инфраструктуры (КИИ) для организации доступа к значимым объектам КИИ
- финансовым организациям для организации доступа к информационным системам

При организации удалённого доступа советуем воспользоваться соответствующими рекомендациями отечественных регуляторов по мерам обеспечения информационной безопасности на время удалённой работы, представленными на страницах этого журнала.

КРИПТОПРО
ключевое слово в защите информации

www.cryptopro.ru

Злоумышленники и COVID-19

Национальный координационный центр по компьютерным инцидентам (НКЦКИ) предупреждает об активном использовании злоумышленниками ситуации вокруг пандемии коронавируса COVID-19 для осуществления широкого спектра вредоносной деятельности и публикует рекомендации по противодействию угрозам компьютерной безопасности, связанным с его распространением.

Специалисты НКЦКИ выделяют два типа вероятных угроз:

1. Мошенничество.
2. Угрозы, связанные с удалённым режимом работы.

Рекомендации по противодействию угрозам компьютерной безопасности:

1. Проявляйте осторожность при обработке электронных сообщений с темой, вложением или гиперссылкой, связанных с COVID-19. Не раскрывайте личную или финансовую информацию в электронном письме и не отвечайте на запросы о предоставлении этой информации.
2. Используйте официальные источники для получения актуальной, основанной на фактах, информации о COVID-19.
3. Для предотвращения кражи персональных данных подключайтесь только к проверенным интернет-платформам для проведения видеоконференций, онлайн-обучения, подписок на онлайн-кинотеатры, мобильных приложений для доставки еды и т. д.
4. Прежде чем делать пожертвования, проверяйте подлинность благотворительных организаций во избежание кражи денежных средств.

Рекомендации по обеспечению информационной безопасности при удалённом режиме работы:

1. Убедитесь, что средства антивирусной защиты и межсетевого экранирования надлежащим образом настроены и функционируют на всех узлах системы.
2. Проверьте обновление всех сервисов и оборудования, которые используются для удалённого доступа (VPN, устройства сетевой инфраструктуры).
3. Используйте удалённый доступ в сеть организации строго с двухфакторной авторизацией.
4. Запретите использовать доступ в корпоративную сеть с помощью сторонних сервисов, которые подключаются через промежуточные сервера и самостоятельно проводят авторизацию и аутентификацию.
5. Организуйте контроль за подключением внешних устройств, в том числе USB-носителей информации, к устройству, предназначенному для удалённого доступа.
6. Задайте ограничение скорости VPN-соединений для приоритизации пользователей, которым потребуется более высокая пропускная способность.
7. Осуществите сегментирование сети и разделите права доступа.
8. Используйте не прямой, а терминальный удалённый доступ в сеть к виртуальному рабочему месту со всеми установленными средствами защиты информации.
9. Проверьте, что электронная почта защищена двухфакторной авторизацией. Необходимо обеспечить анализ электронной почты антивирусными средствами.
10. Используйте стойкий пароль к управляющей панели роутера и WPA2-шифрование при подключении к сети Интернет с применением Wi-Fi.
11. Проверьте наличие и срок ведения журналов удалённых действий пользователей, а также наличие тайм-аута неактивного удалённого подключения с требованием повторной аутентификации.
12. Обновите пароли всех пользователей в соответствии с парольной политикой.
13. Осуществляйте мониторинг безопасности систем с повышенной бдительностью.
14. Приведите в актуальное состояние имеющиеся в организации планы, инструкции и руководства по реагированию на компьютерные инциденты с учётом изменений в инфраструктуре.
15. Акцентируйте внимание сотрудников на фишинговых атаках, связанных с тематикой COVID-19.
16. Проинформируйте сотрудников о необходимости ограничения доступа к удалённому рабочему месту детей, родственников и посторонних лиц, а в случае невозможности – ограничения прав их учётных записей.

Кредитным организациям, некредитным финансовым организациям

Информационное письмо о мерах по обеспечению киберустойчивости и информационной безопасности в условиях распространения новой коронавирусной инфекции (COVID-19)

В связи с комплексом мер, направленных на предотвращение распространения на территории Российской Федерации новой коронавирусной инфекции (COVID-19), и распространением практики дистанционной работы Банк России рекомендует реализовать следующие меры в части обеспечения киберустойчивости и информационной безопасности кредитных организаций, некредитных финансовых организаций (далее при совместном упоминании – финансовые организации).

1. В случае организации финансовыми организациями удаленного доступа в отношении тех операций, которые технически возможно организовать и осуществлять в условиях удаленного доступа, и перевода части работников, осуществляющих указанные операции, на дистанционную работу Банк России считает необходимым рекомендовать следующее.

В целях реализации удаленного логического доступа с использованием мобильных устройств (далее – удаленный мобильный доступ) финансовым организациям рекомендуется обеспечить:

- применение технологий виртуальных частных сетей;
- применение многофакторной аутентификации;
- применение терминального доступа (по возможности);
- мониторинг и контроль действий пользователей удаленного мобильного доступа.

Организационные и технические меры, необходимые для реализации указанных рекомендаций при осуществлении удаленного мобильного

доступа, содержатся в национальном стандарте Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденном приказом Федерального агентства по техническому регулированию и метрологии от 08.08.2017 № 822-ст.

2. Кредитным организациям рекомендуется обеспечить бесперебойное осуществление, в первую очередь, следующих операций: перевод денежных средств, в том числе через платежную систему Банка России, открытие и ведение банковских счетов физических и юридических лиц, а также наличие денежных средств в банкоматах.

В этой связи кредитным организациям рекомендуется идентифицировать работников (включая администраторов систем), задействованных в обеспечении осуществления и осуществлении вышеуказанных операций, и организовать режим работы, обеспечивающий минимизацию рисков нарушения бесперебойности осуществления указанных операций.

В случае если для обеспечения бесперебойного осуществления указанных выше операций перевод работников на дистанционную работу невозможен, рекомендуется выделить группы работников:

- поддерживающих бесперебойное обеспечение осуществления указанных операций на объектах информационной инфраструктуры кредитных организаций;
- ожидающих привлечения к бесперебойному обеспечению осуществления указанных операций на объектах информационной инфраструктуры кредитных организаций.

3. В связи с рисками нарушения информационной безопасности при осуществлении финансовыми организациями операций при организации дистанционной

работы своих работников обращаем внимание на необходимость оперативного информационного взаимодействия с Банком России посредством автоматизированной системы обработки инцидентов Центра мониторинга и реагирования на компьютерные атаки в кредитно- финансовой сфере Департамента информационной безопасности Банка России (АСОИ ФинЦЕРТ) в соответствии с требованиями, предусмотренными нормативными актами Банка России.

4. В условиях сохранения опасности распространения новой коронавирусной инфекции (COVID-19) Банк России считает целесообразным воздержаться от применения мер, предусмотренных статьями 74, 76.5

Федерального закона от 10.07.2002 № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в отношении финансовых организаций, допустивших нарушение требований нормативных актов Банка России в области обеспечения защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента, обеспечения защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций, при организации дистанционной работы работников финансовых организаций.

Настоящее информационное письмо подлежит размещению на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

Д.Г. Скобелкин
Заместитель Председателя Банка России

ФСТЭК России. Документы по обеспечению безопасности критической информационной инфраструктуры

Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры

В связи со сложившейся обстановкой в целях противодействия распространению новой коронавирусной инфекции субъектами критической информационной инфраструктуры может быть принято решение о переводе своих работников на дистанционный режим исполнения должностных обязанностей.

Для обеспечения дистанционного режима исполнения должностных обязанностей может потребоваться удалённый доступ работников к объектам критической информационной инфраструктуры, что создаёт дополнительные угрозы безопасности информации, связанные с несанкционированным доступом и воздействием на такие объекты.

В дистанционном режиме не допускается предоставлять удалённый доступ для управления (в том числе путём передачи управляющих команд и (или) сигналов, изменения параметров управляемых процессов и осуществления иных управляющих воздействий) режимами функционирования промышленного (технологического) оборудования (устройств) автоматизированных систем управления производственными (технологическими) процессами, являющихся значимыми объектами критической информационной инфраструктуры.

В целях минимизации рисков возникновения дополнительных угроз безопасности информации в объектах критической информационной инфраструктуры при осуществлении удалённого доступа работников на период угрозы распространения новой коронавирусной инфекции рекомендуется принятие следующих мер:

1. Проведение инструктажа работников субъектов критической информационной инфраструктуры, осуществляющих удалённый доступ к объектам критической информационной инфраструктуры, о правилах безопасного удалённого взаимодействия с такими объектами.
2. Определение перечня средств вычислительной техники, в том числе портативных мобильных средств вычислительной техники (ноутбуков, планшетных компьютеров, мобильных устройств), которые будут предоставлены работникам для удалённой работы (далее – удалённое СВТ). Для удалённого доступа не рекомендуется использование личных средств вычислительной техники, в том числе портативных мобильных средств вычислительной техники.
3. Определение перечня информации и информационных ресурсов (программ, томов, каталогов, файлов), расположенных на серверах объектов критической информационной инфраструктуры, к которым будет предоставляться удалённый доступ.
4. Назначение минимально необходимых прав и привилегий пользователям при удалённой работе.
5. Идентификация удалённых СВТ по физическим адресам (MAC-адресам) на серверах объектов критической информационной инфраструктуры, к которым будет предоставляться удалённый доступ, предоставление им доступа к информационным ресурсам объектов критической информационной инфраструктуры методом «белого списка».
6. Исключение возможности эксплуатации удалённых СВТ посторонними лицами.
7. Выделение в отдельный домен работников, управление которым должно осуществляться с серверов субъекта критической информационной инфраструктуры, и присвоение каждому удалённому СВТ сетевого (доменного) имени.
8. Обеспечение двухфакторной аутентификации работников удалённых СВТ, при этом один из факторов обеспечивается устройством, отделённым от объекта критической информационной инфраструктуры, к которому осуществляется доступ.
9. Организация защищённого доступа с удалённого СВТ к серверам объектов критической информационной инфраструктуры с применением средств криптографической защиты информации (VPN-клиент).
10. Применение на удалённых СВТ средств антивирусной защиты информации, обеспечение актуальности баз данных признаков вредоносных компьютерных программ (вирусов) на удалённых СВТ путём их ежедневного обновления.
11. Исключение возможности установки работником программного обеспечения на удалённое СВТ, кроме программного обеспечения, установка и эксплуатация которого определена служебной необходимостью, реализуемое штатными средствами операционной системы удалённого СВТ или средствами защиты информации от несанкционированного доступа.
12. Обеспечение мониторинга безопасности объектов критической информационной инфраструктуры, в том числе ведение журналов регистрации действий работников удалённых СВТ и их анализ.
13. Блокирование сеанса удалённого доступа пользователя при неактивности более установленного субъектом критической информационной инфраструктуры времени.
14. Обеспечение возможности оперативного реагирования и принятия мер защиты информации при возникновении компьютерных инцидентов.

Кроме того, субъектам критической информационной инфраструктуры рекомендуется руководствоваться рекомендациями Национального координационного центра по компьютерным инцидентам и центров мониторинга информационной безопасности, имеющих соответствующие лицензии ФСТЭК России, по вопросам компьютерных атак в условиях распространения новой коронавирусной инфекции, в том числе размещёнными на веб-ресурсе www.safe-surf.ru.

Рекомендации о мерах защиты информации, принимаемых в информационных системах федеральных органов исполнительной власти и подведомственных организаций, в целях минимизации рисков возникновения дополнительных угроз безопасности информации при осуществлении удалённого доступа их работников направлены в федеральные органы исполнительной власти в установленном порядке (исх. от 20 марта 2020 г. № 240/22/1204дсп).

В. Лютиков

GMCS развивает BI-систему для DB Schenker в России

Москва, 05 марта 2020 года. GMCS нарастила функционал BI-системы на базе QlikView для российского офиса компании DB Schenker, ведущего международного провайдера логистических услуг.

DB Schenker является одной из старейших компаний на мировом рынке логистических услуг. В России региональная сеть DB Schenker представлена офисами в 26 городах. Компания активно развивает мультимодальные перевозки по всем направлениям, а некоторые из предлагаемых логистических услуг не имеют аналогов на рынке.

DB Schenker в России использует платформу QlikView с 2004 года. За это время в системе накопился большой объём данных, количество интеграций выросло, а используемых отчётов стало недостаточно для обеспечения потребностей бизнеса.

Обновлённая силами специалистов GMCS система Business Intelligence позволяет анализировать деятельность логистической компании более чем по 60-ти показателям, таким как продажи, доходы, расходы, грузоперевозки, тарифы и т.д.

Для анализа доходов настроен дашборд из 35 показателей, а объём поступающих в QlikView данных составляет несколько миллионов строк. Специалисты GMCS обеспечили возможность проведения глубокого анализа цепочки от создания до оплаты заказа, включая отслеживание денежных транзакций до уровня разноски сумм по счетам. На отдельном дашборде пользователи могут анализировать зависимость расходов и резервов, отслеживать количество заведённых заказов по весовым параметрам и видам упаковки, влияющих на стоимость перевозки грузов.

«Наша компания является прогрессивным и опытным пользователем бизнес-аналитики. Амбициозные планы по усилению присутствия компании на рынке транспортно-логистических услуг, а также запуск новой TMS CIEL, в которой регистрируются заказы на мультимодальные перевозки, потребовали модификации и наращивания возможностей BI-системы. Мы довольны результатами. Качество данных улучшилось, повысилась скорость построения отчётов, появились новые инструменты визуализации, что позволяет специалистам работать более эффективно», – **рассказывает Айварс Тауриньш, генеральный директор DB Schenker кластера Россия/Евразия**.

С учётом специфики транспортной отрасли в BI-системе настроена разнообразная аналитическая отчётность, которая необходима компании DB Schenker для обеспечения высочайшего качества предоставляемых услуг. Например, с помощью группы отчётов по контролю качества DB Schenker в режиме реального времени отслеживает соблюдение сроков получения, доставки и обработки заказов на терминале. Данные отчёты также консолидируют информацию из нескольких подсистем, проверяя их корректность, позволяя значительно сократить время распознавания и реакции на проблемы.

Усовершенствованные отчёты для работы с тарифами и финансовой информацией позволяют DB Schenker централизованно анализировать данные, внесённые разными подразделениями. С помощью этих отчётов эффективно выполняется анализ плановых и фактических показателей, производится контроль целостности и достоверности данных.

«Российский офис DB Schenker поставил перед нами задачу оперативно доработать используемые отчёты, обогатив их новыми показателями и аналитиками, а также разработать новые отчёты, которые потребовались в связи с выверкой данных для запуска системы TMS CIEL. Команда GMCS продолжает развивать систему отчётности, а также планирует создание новых аналитических панелей совместно с заказчиком», – отмечает **Ирина Володькина, руководитель направления, департамент аналитических решений компании GMCS.**

DB SCHENKER *– логистическое подразделение компании Deutche Bahn (немецкие железные дороги). Основные направления деятельности: грузовые перевозки по всему миру с оптимальными сроками доставки и без ограничения по весу или размеру груза; международные и внутрироссийские перевозки грузов всеми видами транспорта (автомобильные, ж/д, авиационные, морские, контейнерные), включая перевозки сборных грузов и кросс-докинг; таможенное оформление; контрактная логистика (склад). А также специальные услуги: логистика спортивных мероприятий и выставок; перевозка тяжеловесных и негабаритных грузов; организация чартерных рейсов; онлайн-отслеживание; страхование грузов; управление цепями поставок.*

Компания гарантирует одинаково высокое качество услуг как в России, так и в любом другом офисе мира. DB Schenker использует большой опыт и экспертные знания глобальной сети подразделений для решения самых сложных логистических задач и предлагает своим клиентам лучшее обслуживание в отрасли.

www.dbschenker.com

GMCS *– один из лидеров в России в ИТ-сфере по внедрению бизнес-решений и разработке ПО. С октября 2018 года компания входит в группу Совкомбанка, являющегося одним из крупнейших частных банков России. Проекты GMCS направлены на повышение эффективности бизнеса заказчиков. GMCS основана в 1997 г., компания имеет значительный опыт работы с крупнейшими предприятиями различных секторов экономики стран мира. GMCS является разработчиком «Платформы ВерЭкс» – комплекса собственных решений для автоматизации бизнес-процессов (www.verex.ru). «Платформа ВерЭкс» входит в реестр отечественного ПО. Головной офис компании расположен в Москве, филиалы в Санкт-Петербурге, Пензе, Перми и Казани.*

www.gmcs.ru

МТС увеличила скорость облачных вычислений в 2,5 раза

Москва, РФ. ПАО «МТС» (NYSE: MBT, MOEX: MTSS) — крупнейший российский телекоммуникационный оператор и провайдер цифровых услуг — сообщает о технологическом развитии облачной платформы #CloudMTS. Провайдер расширил объём облачного хранилища в 1,5 раза, скорость вычислений выросла в 2,5 раза. Улучшение характеристик облака позволит компаниям в разы ускорить решение задач в области искусственного интеллекта и машинного обучения, повысить скорость работы клиентских приложений.

Провайдер увеличил производительность облака благодаря новому высокопроизводительному оборудованию с мощностью процессоров до 3,1 ГГц. Минимум на 25% выросла скорость работы корпоративных ИТ-систем и приложений в облаке на всей территории страны. В Дальневосточном и Сибирском округах дополнительные ресурсы расширили возможности облака для размещения систем, обладающих особыми требованиями к частоте процессоров. Например, бухгалтерских программ 1С и решений на основе SAP.

«Российский бизнес активно цифровизируется: перестраиваются бизнес-модели, внедряются новые цифровые решения, продажи уходят в онлайн. Растут объёмы хранимых и обрабатываемых данных в облаке. Для расширения спектра и оказания облачных услуг на самом высоком уровне мы совершенствуем нашу облачную платформу. Компании могут размещать в облаке МТС виртуальные сервера с большим объёмом оперативной памяти и информационные системы с высокими требованиями к тактовой частоте процессоров», — отметил директор облачного бизнеса МТС Олег Мотовилов.

Увеличение производительности и расширение облачной платформы реализовано за счёт дополнительных инсталляций оборудования на ключевых площадках в Москве, Владивостоке и Новосибирске. В дальнейшем планируется подключение к программе модернизации облачных площадок в других городах.

Подробнее о развитии облачной платформы

Усовершенствование ресурсов облачной платформы реализовано на основе высокопроизводительного оборудования на базе процессоров Intel Cascade Lake: Intel Xeon Gold 6254 с частотой 3,1 Ггц и оперативной памятью 1,5 ТБ, а также Intel Xeon Gold 6240 с частотой 2,6 ГГц и оперативной памятью 512 ТБ. Дополнительные облачные ресурсы предназначены для размещения любых информационных систем и бизнес-критичных приложений. Например, интернет-магазинов, CRM-систем, баз данных, решений на основе 1С и SAP, а также корпоративных сервисов для общения сотрудников.

Об облачной экосистеме МТС

Облачная экосистема МТС включает в себя инфраструктурные решения в формате частных, публичных и гибридных облаков, комплекс консалтинговых и профессиональных услуг, услуги дата-центров и телеком-сервисы. В облачное направление бизнеса МТС входит собственный провайдер #CloudMTS[1], один из крупнейших российских провайдеров «ИТ-ГРАД», ориентированная на стартапы, малый и средний бизнес платформа 1cloud и дата-центр «Авантаж»[2]. Экосистеме доверяют свыше 1,5 тысячи представителей крупного бизнеса. Среди клиентов экосистемы ABBYY, Belka Car, S7, OTIS, Tutu.ru, Газпромбанк и другие международные и отечественные компании.

Алексей Меркутов
Пресс-секретарь Группы МТС

Наталья Маткова
Руководитель направления внешних коммуникаций провайдера #CloudMTS

1. cloud.mts.ru
2. cloud.mts.ru/data-center

МТС Быть лучше каждый день

Публичное акционерное общество «Мобильные ТелеСистемы» *(ПАО «МТС») — ведущая компания в России и странах СНГ по предоставлению услуг мобильной и фиксированной связи, передачи данных и доступа в интернет, кабельного и спутникового ТВ-вещания, цифровых сервисов и мобильных приложений, финансовых услуг и сервисов электронной коммерции, ИТ-решений в области системной интеграции, интернета вещей, мониторинга, обработки данных, облачных вычислений и электронного документооборота. В России, Беларуси и Армении услугами мобильной связи Группы МТС пользуются 86,8 миллионов абонентов. На российском рынке мобильного бизнеса МТС занимает лидирующие позиции, обслуживая крупнейшую 78,8-миллионую абонентскую базу. Фиксированными услугами МТС — телефонией, доступом в интернет и ТВ-вещанием — охвачено свыше девяти миллионов российских домохозяйств. Компания располагает в России розничной сетью из 5 800 салонов связи по обслуживанию клиентов, продаже мобильных устройств и финансовых услуг. МТС лидирует в сегменте межмашинных соединений (M2M) в России с наибольшей 42%-ной долей рынка по числу SIM-карт. МТС — традиционный лидер на телекоммуникационном рынке России по величине выручки и OIBDA. Крупнейшим акционером МТС является АФК «Система». С 2000 года акции МТС котируются на Нью-Йоркской фондовой бирже под кодом MBT, с 2003 года — на Московской бирже под кодом MTSS.*

mts.ru

Некоторые заявления в данном пресс-релизе могут содержать проекты или прогнозы в отношении предстоящих событий или будущих финансовых результатов Компании в соответствии с положениями Законодательного акта США о ценных бумагах от 1995 года. Такие утверждения содержат слова «ожидается», «оценивается», «намеревается», «будет», «мог бы» или другие подобные выражения. Мы бы хотели предупредить, что эти заявления являются только предположениями и реальный ход событий или результаты могут отличаться от заявленного. Мы не обязуемся и не намерены пересматривать эти заявления с целью соотнесения их с реальными результатами. Мы адресуем вас к документам, которые компания отправляет Комиссии США по ценным бумагам и биржам, включая форму 20-F. Эти документы содержат и описывают важные факторы, включая те, которые указаны в разделе «Факторы риска» формы 20-F. Эти факторы могут быть причиной расхождения реальных результатов от проектов и прогнозов. Они включают в себя следующее: тяжесть и продолжительность текущего состояния экономики, включая высокую волатильность учётных ставок и курсов обмена валют, цен на товары и акции и стоимости финансовых активов, воздействие государственных программ России, США и других стран по восстановлению ликвидности и стимулированию национальной и мировой экономики, нашу возможность поддерживать текущий кредитный рейтинг и воздействие на стоимость финансирования и конкурентное положение, в случае снижения такового, стратегическая деятельность, включая приобретения и отчуждения и успешность интеграции приобретённых бизнесов, возможные изменения по квартальным результатам, условия конкуренции, зависимость от развития новых услуг и тарифных структур, быстрые изменения технологических процессов и положения на рынке, стратегию; риск, связанный с инфраструктурой телекоммуникаций, государственным регулированием индустрии телекоммуникаций и иные риски, связанные с работой в России и СНГ, колебания котировок акций; риск, связанный с финансовым управлением, а также появление других факторов риска

«Техносерв» и Winnum запустили сервис «IIoT из облака»

Москва, 21 апреля 2020 года. Группа компаний «Техносерв» – один из крупнейших российских системных интеграторов – объявляет о разработке и выводе на рынок услуги «Промышленный интернет вещей из облака», которая предназначена для облачного мониторинга разнопланового оборудования и технологических процессов.

Промышленный интернет вещей (IIoT) – это платформа, которая обеспечивает обмен данными между физическими машинами и цифровыми устройствами с последующей интеллектуальной обработкой этих данных. Компании используют IIoT-платформы для удалённого мониторинга, контроля на производстве, анализа изменений и внедрения изменений в производство на основе полученных данных.

Услуга «Промышленный интернет вещей из облака»[1] предоставляется из собственного облака «Техносерва» – облачной платформы «Техносерв Cloud». Она ориентирована на потребности предприятий различных секторов промышленности, энергетики, нефтедобычи и сельского хозяйства.

Сервис позволяет организовать автоматизированный сбор данных от устройств или производственного оборудования и их последующую обработку на облачной платформе. При этом спектр решаемых задач очень широк и зависит от выбора заказчика: мониторинг действий персонала или загруженности производства с выявлением его узких мест, дистанционная диагностика технического состояния оборудования и его ошибок, отслеживание фактического количества произведённой продукции, анализ технологического процесса и выявление необходимости его оптимизации, цифровой двойник производства.

Качество и объективность получаемых данных (сигналов с оборудования) обеспечивается отсутствием оператора и человеческого фактора, а также возможностью принимать любые сигналы и применять в их обработке очень широкий спектр алгоритмов. Дополнительными преимуществами являются возможности диагностики и анализа через создание алгоритмов проверки и запуск диагностических программ.

Сервис «Промышленный интернет вещей из облака» организован на базе универсальной программной платформы Winnum. Она обеспечивает интеллектуальную среду для создания и последующей отладки приложений: модули для подключения устройств, защищённое облако, платформу для подключения пользователей, а также готовые

1. ts-cloud.ru/service/promyshlennyy-internet-veshchey-iz-oblaka-iiot

к использованию отраслевые решения и библиотеки разработчика (SDK).

«Платформа Winnum позволяет компании самостоятельно, даже без привлечения программистов, создавать собственные уникальные решения под свои потребности и выходить на уровень «умного производства», обеспечивая уникальные сроки возврата инвестиций – в 2018 г. средний срок окупаемости составил 2 месяца. Также существенно упрощает процедуру подключения поддержка платформой всех известных контроллеров (Siemens, Heidenhain, Fanuc, Haas, Mazak, Mitsubishi, Балт-Систем, Schneider Electric, Shimaden, Omron и др.) и основных промышленных протоколов. При этом оборудование, неоснащённое собственными контроллерами, может быть подключено с использованием коммуникационного модуля Winnum Hardware OE, а для редких систем при вводе в эксплуатацию мы обеспечим индивидуальную поддержку», – рассказал **Александр Московченко, директор по развитию Winnum.**

Для подключения к облачной платформе предприятию необходимо развернуть на своих мощностях сервер Winnum Connector, обеспечивающий механизм «туманных вычислений», и выполнить физическое подключение к нему оборудования по технологической сети по протоколу Ethernet. При этом подключиться можно как через доступные интерфейсы RS-232/485, MPI/PROFIBUS с использованием специального Ethernet-шлюза, так и промышленных протоколов (ModBus RTU/ASCII/TCP, OPC DA/UA). Сервер Winnum Connector должен быть сконфигурирован для доступа к облачной платформе через сеть Internet. Для защиты этого Интернет-соединения может быть использован один из встроенных алгоритмов шифрования, в том числе и ГОСТ.

Каждый пользователь имеет личный кабинет, в котором может на основе готовых модулей формировать необходимое ему решение самостоятельно или с привлечением эксперта компании «Техносерв». Простота и качество платформы гарантируют эффективность удалённых коммуникаций между специалистами заказчика и облачной платформой Техносерв Cloud при организации подключения.

«Благодаря нашему новому облачному сервису любое предприятие сможет быстро организовать у себя IIoT-сеть. По нашим оценкам, в среднем потребуется примерно 5 дней на подключение одного цеха. Дополнительным преимуществом использования SaaS-решения из облака станет защищённость, упрощение финансирования проекта благодаря переводу CAPEX-затрат в OPEX и возможность отказаться от использования сервиса в любой момент без существенных финансовых потерь, – отметил **Михаил Блинов, руководитель облачного провайдера «Техносерв Cloud».** – Отправив запрос через форму на сайте, вы сможете ознакомиться с возможностями программной платформы Winnum, получить консультацию специалиста в подборе оптимальной конфигурации под ваши задачи, профессиональную помощь при развёртывании и настройке решения, а также поддержку во время проведения опытно-промышленной эксплуатации».

«IoT – очень перспективное направление: по оценкам аналитиков количество подключений к IoT вырастет к 2025 г. до 25-41 млрд в мире. Российский рынок уже по итогам прошлого года показал прирост на 8,3%, по данным IDC, а к следующему году его рост прогнозируется ещё более существенными темпами[2], учитывая заинтересованность крупнейших игроков. Наш опыт это подтверждает: по сравнению с прошлым годом, интерес наших клиентов к решениям IIoT вырос более чем на 12%, – прокомментировал событие **Андрей Шуравин, директор центра отраслевой экспертизы ГК «Техносерв».** – При подготовке решения к эксплуатации важнейшей задачей для нас было обеспечить его универсальность и возможность подключения предприятий различных отраслей, то есть предоставить нашим клиентам мощный и современный инструмент для цифровизации их производственных процессов. Поэтому в качестве основы мы выбрали решение своего технологического партнёра Winnum[3]».

Для справки:

Winnum – передовая российская платформа для промышленного Интернета Вещей. Она позволяет осуществлять мониторинг и диагностику оборудования, оптимизировать технологические процессы, следить за ходом производства, тестировать новые алгоритмы и решения на реальных данных. Решение сокращает сроки, расходы и риски, связанные с внедрением новых бизнес-моделей, за счёт использования интеллектуальной среды, включающей защищённое облако, работающее с большими данными, модули для подключения любых устройств и изделий и платформу для запуска Web-приложений. Ключевыми особенностями платформы являются высокая производительность, простота подключения устройств и безопасность работы с полученными большими данными, выбор взаимодействия любого уровня: от мониторинга до создания специализированных систем для автоматизированной оптимизации производственных процессов, гибкое управление изменениями, а также наличие набора готовых решений для различных отраслей и областей применения.

2. По прогнозам аналитического центра TAdviser и госкорпорации «Ростех», российский рынок интернета вещей к 2021 году достигнет 270 млрд рублей. Для сравнения, в 2018 году его объём составил 93 млрд рублей.

3. technoserv.com/about/company/press/news/tekhnoserv-predstavlyaet-novyy-reliz-iiot-platformy-svoego-tekhnologicheskogo-partnera-winnum

ТЕХНОСЕРВ

«Техносерв» – один из крупнейших российских системных интеграторов, работающий в России, странах СНГ и Европе. Он основан в 1992 году. В 2019 финансовом году оборот ГК «Техносерв» составил 26,5 млрд руб. Головной офис «Техносерва» расположен в Москве, региональные подразделения – в Волгограде, Ижевске, Краснодаре, а дочерние предприятия – в Алматы, Баку, Ереване, Минске и Ташкенте. Численность сотрудников – более 2600 человек.

«Техносерв» имеет значительный опыт в реализации крупных проектов по внедрению, развитию и аутсорсингу инфокоммуникационной инфраструктуры, систем информационной безопасности, энергетических и инженерных систем, прикладных платформ масштаба крупного предприятия и отрасли. В компетенцию также входит ИТ-консалтинг, BI-системы, услуги сервиса и аутсорсинга. Группа компаний «Техносерв» внедряет и развивает инфокоммуникационные и инженерные системы на основе собственных технологических разработок, а также решений ИТ-лидеров: APC by Schneider Electric, Avaya, Cisco Systems, Dell Technologies, Hitachi Vantara, HP Enterprise, Lenovo, Huawei, IBM, Juniper Networks, Oracle, VMware, Red Hat, Yadro и др.

Заказчики «Техносерва» – государственные структуры и крупнейшие предприятия ключевых отраслей экономики: телекоммуникации, ТЭК, промышленные, транспортные, торговые и финансовые предприятия. Интегратор занимает первые места в ИТ-рейтингах аналитических агентств РБК, «Эксперт» и CNews Analytics.

www.technoserv.com

ГК «Техносерв»
e-mail: pr@technoserv.com
тел.: +7 (495) 648-0808

Winnum
e-mail: marketing@winnum.io

CIS / № 2 (12) / 2020 / www.cis.ru

Тенденции будущего. Преступления

Каждый раз в начале года эксперты в различных областях пытаются дать свои прогнозы: а что же нам готовит следующий день? Чаще всего эти прогнозы не сбываются или сбываются совсем иначе. Решил и я попробовать себя в нелёгкой роли прогнозиста. Сегодня мы с вами поговорим о том, а всегда ли новые технологии готовят нам только благо? В статье речь пойдёт о новых, вполне возможных, если не сегодня, то завтра, преступлениях, основанных на технологиях, уже существующих сейчас. Ведь не секрет, что первыми новые технологии осваивают военные и преступники.

С появлением новых технологий всё чаще появляются и новые преступления. Ещё не так давно мы с вами даже представить не могли, что потребуется специальное законодательство в области защиты персональных данных. Более того, прибыль интернет-злоумышленников сегодня намного превышает доходы офлайн злоумышленников. Но преступления в будущем потребуют ещё более высокого уровня сложности. По мере развития технологий мир взрывается вокруг нас.

Это уже происходит в области киберпреступности, но вскоре новые технологии освоят практически каждый уровень «традиционной» организованной преступности, включая всё: от дизайнерских наркотиков до обхода законов об иммиграции и крупномасштабной подделки торговых марок. Давайте попробуем заглянуть в страшное завтра и рассмотрим ряд будущих преступлений и новых технологий, которые будут использоваться для их выполнения.

Будущие преступления, которых сегодня ещё нет. Что день грядущий нам готовит?

В будущем с преступными целями будет использоваться 3D-печать для создания собственных пистолетов, не обнаруживаемых сегодняшними металлодетекторами, и, например, беспилотников. Вы мне возразите: создание 3D-печатного оружия – уже реальность. Да. Всё верно. Это уже реальность. К счастью, пока не массовая. Пока!

Всё чаще будут использоваться глушилки мобильной связи, шпионское ПО, оборудование для генной инженерии. Практически каждая новая технология, создаваемая с лучшими намерениями, в будущем может и будет использоваться против нас. Ведь заказчиками чаще всего выступают военные, силовые структуры и преступность!

Достаточно сказать, что преступные умы непрерывно работают, чтобы сфабриковать новые возможности использования каждой из этих новых областей.

Преступления и беспилотники

Сегодня законы о применении беспилотников чаще всего находятся в стадии разработки. Вот те области преступлений, в которых беспилотники будут использоваться в ближайшем будущем:

1. **Перевозка незаконных веществ** – бомбы, яды, наркотики, человеческие органы и т.д.
2. **Оружие** – оборудование дронов пушками, пулемётами, лазерами, тазерами, огнемётами и многим другим.
3. **Вуайеризм** – шпионаж за людьми в их резиденциях или в пределах личного пространства.
4. **Подрывной маркетинг** – приёмы, которые удивляют и буквально переворачивают с ног на голову наше сознание. Он достигает одной, самой главной цели: товар или торговая марка надолго врезается в память, потому что делает что-то не так, как все.
5. **Незаконная стрельба или уничтожение беспилотных летательных аппаратов.** Число обладателей анти-дрон оружия растёт непрерывно. Более того, если несколько лет назад появление такого оружия считалось чем-то из области фантастики, то сегодня это реальность. Дрессированные хищники, направленные ручные глушилки, стационарные системы для перехвата управления (пока военные, но ведь всё было пока...).
6. **Шум.** Будущие беспилотники с динамиками и прикреплёнными системами звукоусиления (думаю, летающие концертные акустические системы) могут быть превращены в разрушительное оружие. Вспо мните опыты с инфразвуком. А если учесть возможность миниатюризации?
7. **Летающие фальшивые мобильные станции** для перехвата или глушения мобильных разговоров. Не так давно подобные станции, правда размещённые на небольших самолётах (вертолётах), применяла полиция Калифорнии. Кто следующий?
8. **Drone издевательства** – акты запугивания, угрозы или отображение постыдных фотографий.
9. **Дроны-истребители других беспилотных летательных аппаратов** – дроны, специально предназначенные для захвата или уничтожения других беспилотных летательных аппаратов.

Смешанная реальность

Представьте смешанную реальность. Игры, показывающие мир, в котором мы живём, только с визуальными накладками, которые делают людей вокруг нас невольными игроками и пешками. Нет такого? Разве? Вспомните Pokemon Go.

10. **Сбор толпы для совершения теракта.** Запускаем игру (тот же Pokemon Go) и собираем игроков в заранее определённом месте. Затем взрыв. На массовых мероприятиях место заранее проверяется полицией, проверяются и приходящие люди. В данном случае никто никого не проверяет. Да и люди приходят туда абсолютно произвольно – в ходе игры.
11. **Смешение реальности и игры, предназначенное для набора баллов путём нанесения различных повреждений другим игрокам.** Пользователи набирают очки, нанося физические ушибы, словесные оскорбления, используя публичные осуждения и даже физическое отключение или убийство.
12. **Целенаправленное искажение реальности для получения выгоды за счёт других.**

История. Атаки на подмену памяти о прошлом

Мы сегодня всё чаще и чаще видим подобное. Пока с помощью телевидения, фильмов, атак через интернет. Что можем этому противопоставить? Практически ничего. Народ ищет зрелища!

13. **Наглый обман и перевирание прошлого.** Сбор фрагментов из жизни человека может заставить выглядеть его дураком. Мы все имеем свои скелеты в шкафу. У всех бывают ошибки, и здравый смысл отказывает нам в тот или иной момент.

14. **Явный ревизионизм**. Для некоторых создание ложной реальности, ложных выводов и переосмысление событий прошлого станет новой формой уголовного искусства. Вспомните сегодняшние заявления в некоторых изданиях, что концлагерь Освенцим (Аушвиц) освобождала американская армия. А ведь этому уже верят!

15. **Ложные мемы** – продолжатели ложных исследований и опросов. Здесь тоже можно привести массу примеров ложных исследований. Вспомните заявление США о наличии в Ираке оружия массового поражения. Оружие не нашли, но страна разгромлена. Можно вспоминать и вспоминать.

16. **Поддельные выводы** – изобразительное искусство достижения ложных выводов.

Социальные шантажисты

Во многом таким же образом, как персонализированная система маркетинга компании Google обеспечивает целевую рекламу, запугивание может быть создано с единственной целью – доставка высокорелевантных угроз. Как только обостряется киберпреступность, мы рискуем иметь наши социальные структуры перерождающимися в невидимые сообщества мафиозного типа шантажистов. В то время как большинство из них будет делать это за деньги, другие – из-за мести, немногие, если таковые найдутся, будут способны понять происходящие истинные закулисные разборки.

17. **Шантаж путём угрозы детям.** С социальными медиа всё чаще будет легко запугать угрозой причинения вреда ребёнку, другу или любимому человеку. Тем более что дети и наши пожилые родственники атакуются гораздо проще. Вспомните телефонные звонки: «Ваш сын попал в милицию...»

18. **Угроза изоляции.** Мы все по своей природе социальные существа и угроза отчуждения (и тем самым изоляции нас от друзей) может быть хуже смерти.

Угрозы ИИ

Очень легко будет полагаться на искусственный интеллект, который будет помогать нам принимать многие решения: куда идти, с кем встретиться, какую музыку слушать и даже как развлечь наших детей. Но что происходит, когда наш ИИ используется злоумышленниками?

19. **Дорожно-транспортные происшествия.** Так как умные автомобили без водителя и беспилотные летательные аппараты будут управляться ИИ, то программное обеспечение, скомпрометированное злоумышленниками, может нарушить всю транспортную сетку через ряд аварий, несчастных случаев и массовых пробок. Вспомните опыт, в ходе которого автомобиль с ИИ заставили свернуть с дороги, просто нарисовав неверную дорожную разметку. А сколько таких ошибок возможны ещё?

20. **Потеря данных** – потеря информации, изменения и целенаправленные искажения информации.

21. **Отключение электропитания, других коммунальных услуг** – отрезать некоторые компании или людей от коммунальных услуг и другой помощи, в которых они нуждаются. Уже сегодня это реальность, достаточно вспомнить массовое отключение электроэнергии в США или нечто подобное на Украине, произошедшие в результате вирусной атаки.

22. **Паралич линий связи.** ИИ скоро станет важной частью наших повседневных процессов принятия решений, но перезагрузка ИИ, эквивалентная «отказу в обслуживании» вызовет огромные проблемы.

Пересмотр прошлого

Мало что в жизни более тревожно, чем уничтожение наследия людей после смерти. Увы, но изменить память проще, фактически убив мёртвых и начав перевоспитывать детей, которые в данном случае являются первичными субъектами этого вида атак. Мы уже сегодня наблюдаем это на примере вопросов о второй мировой войне, где уже основными победителями называются армии США и Великобритании.

23. **Ложные мотивы, ложные намерения.** Если человека уже нет в живых, чтобы он мог оправдать свои действия, то относительно просто исказить его мотивацию. Всё чаще так происходит с прошлым. Пока историческим прошлым, но ведь это пока!..

24. **Последствия выдуманных поражений.** Наш круг тесно связан с друзьями и знакомыми. Этот круг расширяется в геометрической прогрессии, так что его относительно легко взломать. В данном случае взламывать будут не вас, а ваших друзей. Но вам-то от этого вряд ли будет легче.

25. **Изменение мышления.** Изменяющиеся причинно-следственные связи стали обычным инструментом, используемым в политических кругах, чтобы изменить

мышление людей, заставить их сделать неправильный вывод. Примеров здесь, уверен, можно привести массу. Причём вы это сделаете, может быть, даже лучше меня.

26. **Переписывание выводов, используя неверные оценки воздействия.** Большинство злоумышленников (и не только они) имеют большой набор инструментов, в том числе и способности превратить любое, самое маленькое событие в жизни в гигантское, весьма важное, переврав при этом само событие. Примеров тоже можно привести массу. Вспомните атаки химического оружия в Сирии. Было или не было – доказать сложно, но вот нагнать страху…
27. **Возможность вогнать финансовые системы стран в каменный век.** Сегодня, а тем более завтра это сделать будет куда проще.
28. **Пандемии.** Смертельные инфекции и вирусные заражения будут появляться гораздо чаще и быстрее, чем когда-либо, в изготовлении, распространении и заражении в течение ближайших десятилетий. Думаю, что биологическое оружие никто не отменяет, увы. Пример того, что может произойти, у нас перед глазами.
29. **Паралич из-за отключений связи.** Так как мы стали больше полагаться на данные связи, голосовые сообщения, то наши ключевые точки уязвимости становятся всё более очевидными.
30. **Один тщательно направленный взрыв может вызвать неизмеримый ущерб,** причём это может быть как реальный, так и информационный взрыв.

Преступления руками роботов

С помощью растущего дисбаланса между супербогатыми и супербедными вероятным сценарием будет расширение масштабов техно-стелс войны подпольного типа с технологиями хакеров, используемыми для разрушения наших систем, промышленности и правительства новыми и необычными способами.

31. **Беспилотники, роботы, беспилотные автомобили и манипуляторы данных злоумышленников.** Увы, это скоро станет общей частью словаря каждого будущего преступника. Уже сегодня известно о смерти человека от «рук» робота. Неверное, программирование. А где гарантии, что это не случится специально?
32. **Атаки на медицинские системы.** Атака на инсулиновые помпы, на прочее медицинское оборудование, результатом которых стала смерть пациента. Это сегодня. А завтра?
33. **Управление психо-ботами.** Один слегка ненормальный психо-бот может быть в тысячу раз более разрушительным, чем один террорист-смертник сегодня.

Криптовалюта

Криптовалюты стали идеальным инструментом для сокрытия сделок.

34. **Тайные операции.** Криптовалюты открывают дверь для действительно секретных коммуникаций и денежных переводов.
35. **Хранение богатства с помощью криптовалют** становится невозможным для сдерживания преступной деятельности, нет никакого способа, чтобы понять, как делаются операции и как эти деньги хранятся.

Генная инженерия

Генная инженерия уже давно обещала препараты для лечения заболеваний и общего улучшения состояния человека. В то же время манипуляция генами представляет собой инструмент, который может быть использован в преступных целях.

36. **Создание деструктивных новых форм жизни.** Мы не имеем ни малейшего представления о том, какие вредные новые формы жизни могут быть и будут созданы. Где гарантия, что в этот момент не создаются новые штаммы вирусов? Их нет!
37. **Создание суперзаразных новых болезней** будет включать в себя всё, что ставит под угрозу здоровье, безопасность или жизнеспособность людей.
38. **«Редактирование» человека.** Без сдержек и противовесов учёные могут попытаться реализовать рискованные схемы мутации человека. Уже сегодня в Китае созданы два ребёнка с искусственно подправленными генами. А что будет завтра?
39. **Создание суперребёнка.** Люди, желающие сделать себе имя, могут проверить экстремальные теории проектирования младенцев.

Взлом мозга человека

Нам нравится думать о собственном мозге, как о безопасном убежище для наших мыслей, но что, если это не так? Что произойдёт, когда наше серое вещество постараются взломать?

40. **Имплантация ложных воспоминаний.** Понимание человеческого мозга улучшится, при этом возможен взлом воспоминаний или вызов провалов в памяти. Это может стать обычным явлением.
41. **Слитые воспоминания.** Без нашего ведома мозг может быть взломан, а воспоминания «слиты» на другой носитель.
42. **Использование ложных директив вытеснит свободную волю.** Мы высоко ценим свободу воли. А так ли уж она свободна? Мы можем быть вынуждены совершать

преступления, даже если физически сопротивляемся. Увы, под воздействием определённых препаратов и гипноза это возможно уже сегодня.

43. **Внедрение доминирующих личностей.** Для властных преступников вложенная доминирующая личность будет отклонять возражения пассивной личности и заставит её соответствовать.

Время преступления

44. **Временные законы.** Напрасно тратить наше время скоро станет преступлением.

45. **Штрафы за потерянное время.** Поскольку время является дефицитным товаром, мы скоро увидим штрафы за потерянное время.

Террористы и умные транспортные средства

Впереди нас ожидает небольшая потребность в смертниках, так как взлом умных транспортных средств откроет дверь в совершенно новый набор опасностей.

46. **Фанатики.** Умные транспортные средства, оснащённые бомбами, перевозящие опасных животных, химическое оружие, боевые отравляющие вещества и т. д.

47. **Похищение детей/похищение людей:** друзей, родственников, детей, путешествующих без сопровождения из школы или после школы.

48. **Глушение связи.** Глушилки связи будущего могут быть практически необнаруживаемы с их способностью блокировать все формы света, тепла, звука.

49. **Самоуничтожающиеся генераторы страха.** Мобильные наземные мины, предназначенные для запугивания людей.

Мегапроект манипуляторы

50. **Ложные утверждения о рабочих местах.** Большинство стран будут активно вкладываться в соответствие их использования людьми, так что большинство предложений будут приходить с фиктивными претензиями на работу.

51. **Обманчивые экономические выгоды.** Претензии крупномасштабной экономической выгоды всегда привлекательны для политиков, но благие намерения не делают жизнеспособными бизнес-операции.

52. **Придуманные потребности.** Инфраструктуру, как правило, легко продать, особенно если существующая не устраивает, но жулики будут эксплуатировать гигантский проект фиктивной «потребности».

53. **Фиктивный учёт.** Мир мегапроектов всё чаще будет притягивать злоумышленников.

Промышленный геноцид

54. **Манипулирование глобальным спросом.** Когда покупатели вынуждены уйти, отрасль просто перестанет существовать.

55. **Прекращение финансовой поддержки** – финансисты могут манипулировать, отступая от сделки.

56. **Манипуляция частями или материалами, вызывающая резкий рост расходов.** Наиболее успешные продукты образуются вокруг важных компонентов, которые часто трудно сделать и трудно получить. Умышленное создание нехватки может стать преградой в цепочке поставок завода-изготовителя.

57. **Причинение вреда с помощью слухов.** Хорошо разработанная дезинформация, направленная на создание разнообразных слухов, может легко заставить упасть даже лучшие акции. В будущем этот процесс не займёт много времени, чтобы заставить акции падать всё ниже и ниже.

Проблемы, которые находятся за пределами наших возможностей

Увы, с каждым годом DarkNet становится всё «темнее».

58. **Уничтожение экономики целой страны.** Это уже происходит на определённых уровнях. С помощью нескольких новых инструментов это будет только легче и быстрее.

59. **Массовые стихийные бедствия.** В будущем наша способность контролировать ураганы, землетрясения, град или саранчу будет в пределах досягаемости.

60. **Принуждение АЭС к саморазрушению.** Каждая новая технология даёт злоумышленникам дополнительные возможности.

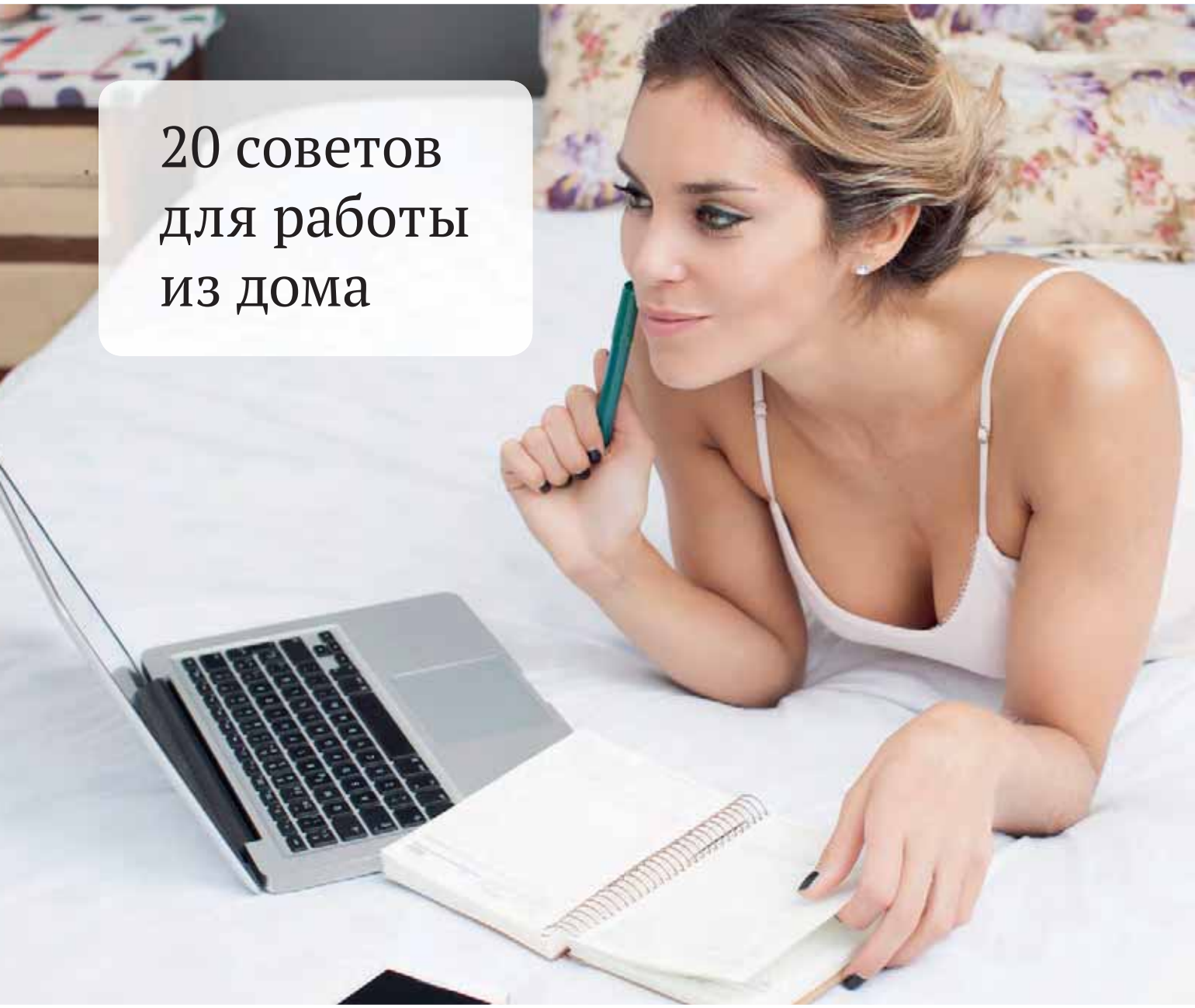
Заключение

Как ни странно, в будущем преступления станут всё более и более изощрёнными. С одной стороны, человек получает всё больше и больше власти, с другой – гонка вооружений в области ИТ толкает преступность на новый уровень.

С одной стороны, хорошо, если удаётся поймать злоумышленников, с другой – плохо, ведь правительство постоянно заглядывает нам через плечо.

Бизнес-модель «преступление-как-сервис» будет развиваться в сложные бизнес-операции буквально с тысячами невольных людей, занимающихся на разных уровнях, но мало кто будет знать точный характер плана.

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



20 советов для работы из дома

Вспышка коронавируса заденет большинство людей, работающих дома. Если вы новичок в удалённой работе, эти советы, надеюсь, помогут вам оставаться продуктивным и поддерживать баланс.

Глобальное распространение COVID-19 – нового коронавируса – держит людей дома. Уже отменены крупные конференции, включая Mobile World Congress и Google I/O, чтобы снизить риск заражения. Некоторые работодатели перевели своих сотрудников на работу из дома на неопределённый срок. Если вы до этого не работали в подобном режиме, то придётся изменить некоторые из ваших привычек и процедур, чтобы достичь успеха в такой работе.

Каждый, кто работает удалённо, должен выяснить: когда работать, где работать и как создать границы между работой и личной жизнью. А как насчёт офисного оборудования, карьерного роста, возможностей для обучения и построения отношений с коллегами? Работа удалённо, особенно из дома большую часть времени, означает выяснение ответов на эти и другие вопросы. Вот 20 советов для ведения лучшей и более продуктивной удалённой работы.

1 Поддерживайте регулярные часы

Установите график и придерживайтесь его большую часть времени. Наличие чётких руководящих принципов, для того чтобы понимать, когда работать и когда отдыхать, помогает многим удалённым работникам поддерживать баланс между работой и личной жизнью. Тем не менее одним из преимуществ удалённой работы является

гибкость, ведь иногда вам нужно продлить рабочий день или начать его ранее обычного, чтобы попасть в другой часовой пояс. Когда вы это сделаете, не забудьте закончить раньше, чем обычно, или поспать немного на следующее утро, чтобы компенсировать усталость.

Автоматические приложения для отслеживания времени, такие как RescueTime (www.rescuetime.com), позволяют проверить, придерживаетесь ли вы своего расписания. Они также могут помочь выяснить, в какое время суток вы наиболее продуктивны. Вы можете использовать эту информацию в своих интересах, резервируя такие часы для наиболее важных задач.

2 Создавайте утреннюю рутину

Решить, что вы сядете за стол и начнёте работу в определённое время, – это одно. Ежедневные привычки, которые направляют вас в кресло, – это другое. Что в утренней рутине указывает на то, что вы собираетесь начать работу? Это может быть чашка кофе. Возможно, привычная одежда. Привычки могут быть более важным средством, чем часы, помогая вам комфортно начать каждый день.

Я говорю «утро», но не все, кто работает из дома, следуют графику с 09:00 до 17:00. Ваш рабочий режим может быть в другое время суток.

3 Устанавливайте правила отношений с людьми

Будет правильнее, если вы объявите детям и остальным домочадцам о расписании и согласуете свою доступность и совместные активности, например: просмотр фильмов, помощь с домашними делами, проверка учёбы у детей и т. д. Кроме того, только потому что вы дома, – это не означает, что другие члены семьи должны предположить, что вы всегда будете им помогать в своё рабочее время.

4 Перерывы в расписании

Если вы самостоятельно заняты, дайте себе достаточно времени в течение дня, чтобы уйти от экрана компьютера и телефона.

5 Перерывы в их полноте

Не изменяйте себе во время перерывов, особенно в обеденный. Вы можете использовать приложение, например TimeOut для Mac и Smart Break для Windows (inchwest.com/smartbreak),чтобы заблокировать компьютер на 60 минут, либо просто запустить простые часы или таймер на экране, когда берёте перерыв. Если вы вернётесь к своему столу только через 40 минут, уходите ещё на 20.

6 Оставьте дома

Старайтесь регулярно покидать своё рабочее место. Тот же совет относится и к людям, которые работают в традиционных условиях офиса. Ваше тело должно двигаться. Кроме того, свежий воздух и естественный свет принесёт пользу.

7 Не стесняйтесь запросить, что вам нужно для работы

Если вы работаете в компании или организации, которая поддерживает работу из дома, перейдя на удалённый режим, сразу запросите нужное оборудование или в течение одного – двух дней, когда поймёте, что вам нужно что-то другое.

Если работаете из дома неожиданно, например из-за коронавируса, просите, что вам необходимо в пределах разумного.

8 Сохраняйте выделенное офисное пространство

В идеальном мире удалённые сотрудники будут иметь не только специальный офис, но и два компьютера: один – для работы и другой – для личного пользования. Это более безопасно для работодателя.

9 Поддерживайте отдельный номер телефона

Настройка номера телефона, который используется только для звонков коллегам и клиентам. Это не должен быть стационарный, второй мобильный или даже другая SIM-карта. Его могут заменить бесплатный VoIP-сервис, такой как Google Voice или Skype. Как и некоторые другие советы, наличие отдельного номера телефона поможет вам управлять балансом между работой и личной жизнью.

10 Используйте VPN

Используйте VPN всякий раз, когда вы подключены к сети, которую не контролируете. Это включает в себя Wi-Fi в коворкингах, кафе, библиотеках и аэропортах. Некоторые организации имеют свои собственные VPN. Вам также нужно будет использовать VPN дома. В любом случае это хорошая идея, чтобы выработать привычку оставлять VPN подключённым как можно чаще, потому что это всегда безопаснее.

11 Общайтесь с коллегами

Одиночество, отключение и изоляция являются общими проблемами в удалённой трудовой жизни, особенно для экстравертов. Компании с культурой удалённой работы обычно предлагают способы общения. Например, у них существуют каналы чата, где сотрудники могут говорить об общих интересах, встречаться онлайн с людьми в одном и том же регионе. Важно выяснить, сколько вам нужно взаимодействия, чтобы чувствовать себя связанным с коллективом и включённым в общее дело. Даже если вы очень замкнуты и не любите общаться, попробуйте сделать это.

Сошлюсь на опыт своих коллег из компании Citrix. Среди своих инженеров, которые раз-

бросаны по огромному региону – Африка, Ближний Восток, Восточная Европа, Россия, Греция, Турция и Израиль, – они завели в день две «необязательные» для посещения встречи на GoToMeeting – «кофе-паузы». Определённой программы нет, но менеджер (утром – один, а вечером – другой) приглашает всех подключиться и просто «поболтать», обсудить всё, что угодно, за виртуальной чашкой чая или кофе, пригласить своих детей к конф-колу, поделиться позитивными новостями. Обычно приходит 5-8 человек, кто сейчас в этот момент не занят.

12 «Присутствуйте» на собраниях и будьте услышаны

Конечно, вы будете принимать участие в видеоконференциях и конференц-звонках. Полезная идея состоит в том, чтобы иногда проявлять это присутствие, даже если вам практически нечего сказать. Проявите уверенность: говорите во время встречи, чтобы все знали, что вы на вызове. Простое «Спасибо, всем. Пока!» в конце встречи позволит ненавязчиво заявить о своём присутствии.

13 Возьмите больничный

Если вам нехорошо, вызовите врача и берите больничный. Имейте в виду, что иногда лучше отдохнуть, чтобы быть наиболее продуктивным в долгосрочной перспективе.

14 Не забывайте о рабочем графике

Исследования, проведённые в США и Европе, доказывают, что удалённая работа существенно удлиняет рабочий день. Это правда, но в тоже время это позволяет днём выделить необходимые родным ресурсы на общение, на помощь им в домашних делах. Таким образом, «всё неоднозначно». Да, человек, например, дома работает больше, но и делает больше перерывов, может больше времени уделить детям и родным.

15 Ищите возможности для обучения

Когда вы не находитесь в офисе с другими сотрудниками, то можете пропустить обучение и курсы по развитию навыков, которые преподаются лично. Компания может даже забыть добавить вас в свои онлайн-курсы обучения. Это заманчиво рассматривать с точки зрения как бы «увернулся», но вы упустите возможность узнать что-то полезное. Убедитесь, что о вас не забыли.

Все крупные конференции сейчас перевели в онлайн и сделали бесплатными: Nvidia, RedHat, AWS, Citrix, etc. Таким образом, вы получите обучение и время для общения с коллегами.

16 Звонки «не вовремя»

Работа удалённо часто перегружена звонками и активной перепиской по определённой задаче. Расскажите всем, кто должен знать о вашем графике доступности, а когда закончите проект или важную задачу, сообщите об этом.

17 Будьте позитивными

Мне нравятся краткие и чёткие сообщения, но знаю, что, чем меньше времени я физически контактирую с людьми, тем меньше они понимают, как интерпретировать мой тон в письменной форме. Когда вы работаете удалённо полный рабочий день, то должны быть «положительными», вежливыми до такой степени, чтобы собеседник чувствовал, какой вы позитивный. В противном случае, вы рискуете «звучать» агрессивно, нервозно или равнодушно. Это прискорбно, но правда.

18 Воспользуйтесь преимуществами ваших привилегий

Приготовление утреннего кофе давно вошло в привычку. Почему? Потому что я работаю из дома и могу. К тому же, мне это нравится. В работе удалённо есть уникальные преимущества. Воспользуйтесь ими. Вы этого заслуживаете!

19 Не будьте слишком жёстки к себе

Самые успешные удалённые сотрудники имеют репутацию чрезвычайно дисциплинированных. В конце концов, требуется серьёзное внимание, чтобы из нетрадиционного пространства сделать любой рабочий день офисной работы полноценным. Тем не менее каждый позволяет себе иногда отвлечься.

20 Завершите свой день рутиной

Так же, как вы должны начать свой день с рутины, создайте привычку, которая сигнализирует вам о том, что рабочий день закончился. Это может быть вечерняя прогулка с собакой или что-то другое. Что-то такое же простое, как выключение компьютера и включение любимого фильма. Что бы вы ни выбрали, делайте это, чтобы отметить окончание рабочего времени.

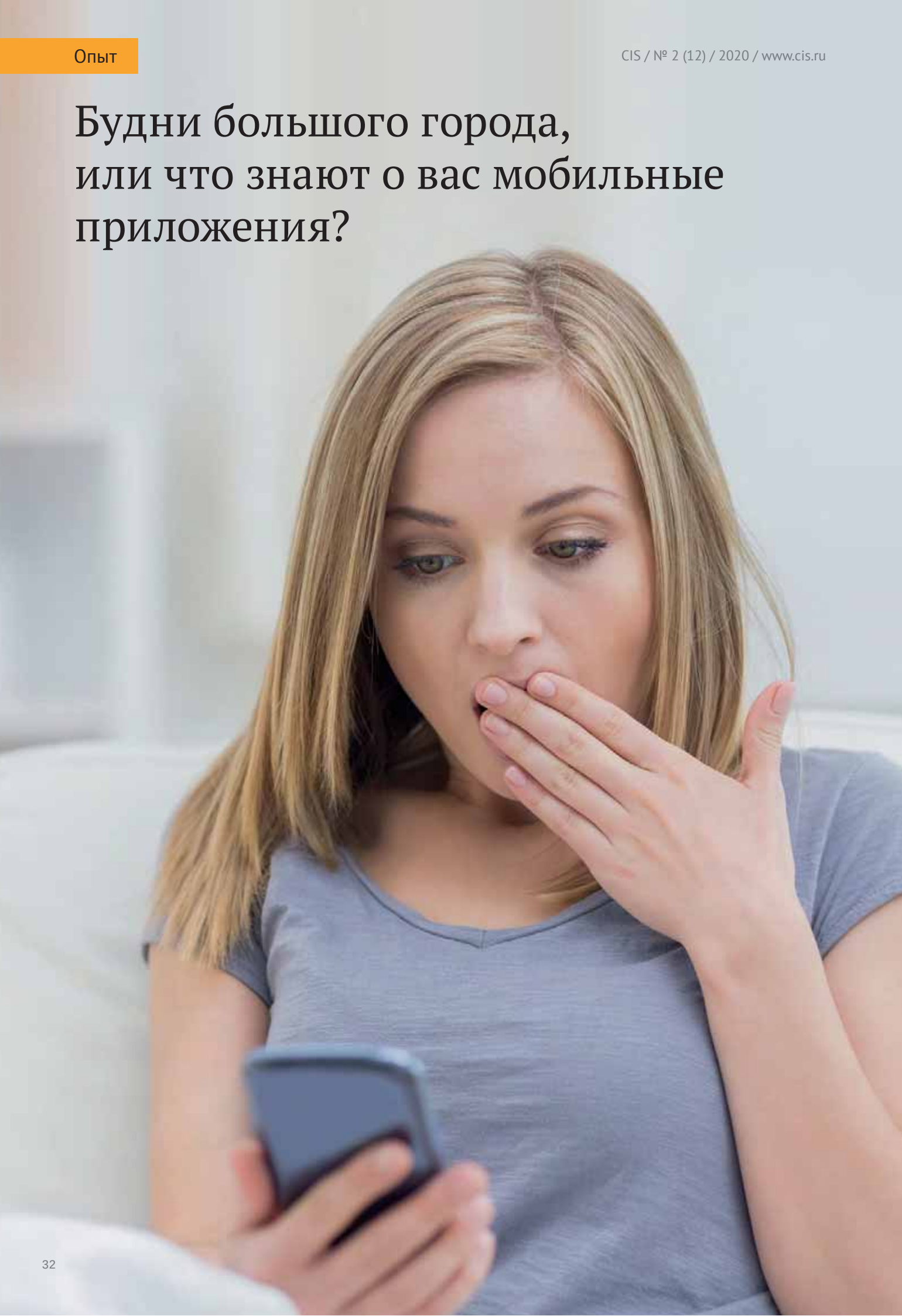
Заключение

Прежде всего выясните, что лучше для вас. Иногда ответ очевиден, но иногда может понадобиться некоторое вдохновение от других людей, которые находятся в том же положении.

Работать из дома можно, главное, делать это максимально комфортно для себя.

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

Будни большого города, или что знают о вас мобильные приложения?



– Где служишь?
– Я работаю в СБ.
– Расскажи что-нибудь интересное...
– О тебе или о себе?

Боб никогда не думал, что станет полицейским детективом. Он окончил престижный технический университет и рассчитывал на престижную работу в банке или другой крупной корпорации. Однако последние летние каникулы резко изменили его судьбу. Что произошло?

Смена работы и судьбы

Боб давно пытался ухаживать за красавицей Лиззи, но после школы их судьбы разошлись. Он уехал в один университет, она – в другой, где каждый занимался своим любимым делом. Боб – компьютерами, а Лиззи – филологией. Прошло 4 года.

– Боб! Привет! Говорят, ты стал крутым компьютерщиком?
– Да нет, просто пытаюсь стать инженером, а что?
– Да проблема у меня... Представляешь, с моей карты пропали деньги. Банк обещает разобраться, но говорит, что я сама виновата, ведь даже SMS-банкинг меня не спас! Я же каждую свою транзакцию в интернете подтверждала с помощью SMS-кода!
– Погоди, а всё остальное нормально?
– Да нет! У меня чёрная полоса. И деньги с телефона пропали.
– А что сказал твой провайдер?
– Говорит, что я сама отправила SMS на платный номер. И не одну. Хорошо, что я ввела лимит на оплату мобильного.
– Ты что, привязала к мобильному счёту основную карту?! Лиззи, мне кажется, что придётся повозиться с твоим телефоном.
– Я только «за». Сможешь сегодня?
– Смогу. Приноси смартфон. Только подумай, это может быть не один час.
– Ничего.

Вечером Лиззи принесла смартфон, однако работа над ним затянулась на всю ночь. Ведь как бы быстро мы с вами не стремились найти и победить зловред, на практике всё оказывается куда медленнее и сложнее.

Утром уставший и небритый Боб, тихо ругаясь, отдавал смартфон.

– Итак, Лиззи, ты понимаешь, что ты устанавливаешь? У тебя здесь масса приложений для выбора причёски, макияжа, игры какие-то.
– И что такого? Я же девушка.

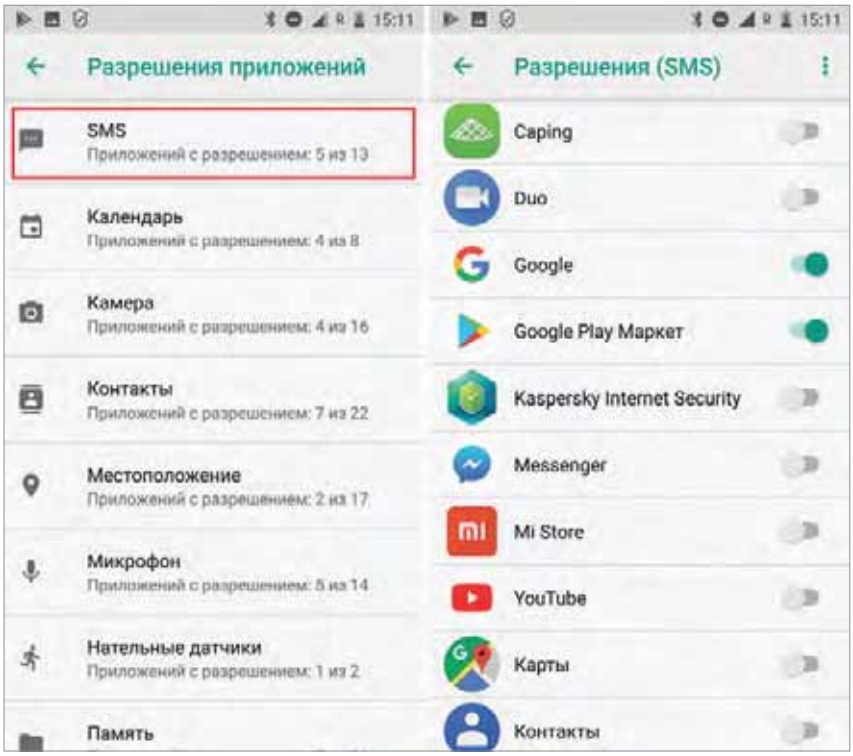


Рисунок 1. Разрешение SMS

– А то, что минимум четыре из них просят доступ к SMS.
– И что?
– Проблема в том, что они могут не только читать SMS со смартфона, но и отправлять SMS, MMS. А раз так, то какое-то из приложений прочло твою SMS из банка и подтвердило платёж от твоего имени. Кстати, похожее случилось и с твоим мобильным счётом. Просто отправлялись SMS на платные номера, пока у тебя не закончились деньги! Думать желательно до, а не после. Милая, будь аккуратнее и старайся не давать такие разрешения, хорошо? На самом деле опасных разрешений много, гораздо больше, чем я сказал.

Так Боб сделал свой первый шаг в выборе профессии.

Разрешение SMS

- **Что это:** Разрешение на отправку и приём SMS, MMS и WAP push-сообщений, а также на просмотр сообщений в памяти смартфона.
- **Чем опасно:** Приложение с этими правами сможет читать/писать SMS, включая сообщения из банков с одноразовыми кодами для входа в интернет-банк и подтверждения транзакций.
- **Где настроить:** *Настройки → Приложения и уведомления → Разрешения приложений → SMS (рис. 1).*

Однако ключевой стала совсем другая история. Произошло это буквально через неделю.

Фальшивый звонок

В тот год в их городок пришла большая беда. Тропические штормы и ураганы в городке бывали регулярно. Но такого ещё не было никогда. Казалось, что летающими крышами никого не удивить, но в этот раз была разрушена практически половина городка.

Поздно вечером в доме матери Боба раздался звонок.

– Мэм, вас беспокоят из городского полицейского участка. Ваш сын, Боб, находится в городском госпитале, и ему срочно нужна операция. Вы могли бы приехать? От вас потребуется найти его страховое свидетельство, а так как лечение не покрывается страховкой, то внести денежный платёж на сумму...
– Да, конечно! Говорите куда.

После разговора мать Боба решила к нему дозвониться.

– Боб? Как здоровье? Ты в госпитале?
– Мама, я через 5 минут буду дома. Какой госпиталь? Тебя просто обманули!
– Погоди, но звонил шериф, Питер Уайт! Мы знакомы с детства, и я знаю его голос.

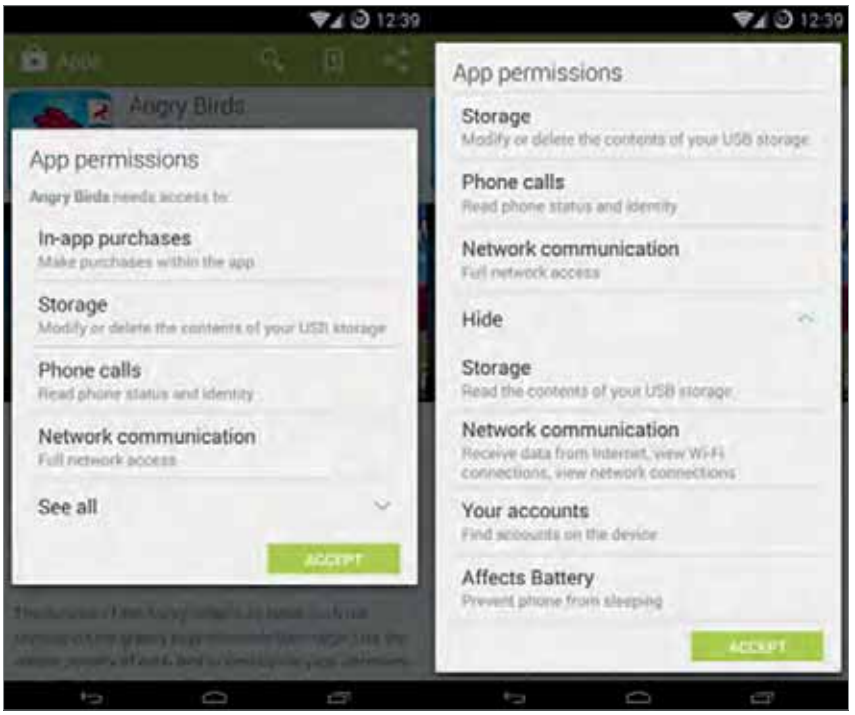


Рисунок 2. Разрешение Телефон (Phone)

– Мама, успокойся! Я сейчас при тебе перезвоню шерифу и всё выясню.
– Шериф, вы звонили моей матери 10 минут назад?
– Я? Боб, мне сейчас некогда. Нет, не звонил.
– Интересно, а кто же тогда звонил ей от вашего имени и вашим голосом? Да и номер определился как ваш.
– Самому интересно. Завтра будем разбираться!

На следующее утро мобильный оператор дал неутешительную информацию. Звонили действительно с карты шерифа, а говорили его голосом с помощью специальной программы подделки голоса. Как?

На смартфоне шерифа была обнаружена программа с доступом к разрешениям класса «Телефон».

После этого Боб окончательно понял, что количество подобных преступлений будет только расти. А ведь к этому нужно добавить то, что пользователи, да и сами сотрудники правоохранительных органов, имеют весьма слабые представления о подобных преступлениях. А значит, ему просто необходимо поступать на должность кибердетектива. Ведь если не он, то кто?

Разрешение Телефон (Phone)

- **Что это:** Разрешение на чтение и изменение истории звонков; считывание вашего телефонного номера, данных сотовой сети и статуса исходящих звонков; добавление голосовой почты; доступ к IP-телефонии; просмотр номера, на который вы в данный момент звоните, с возможностью завершить звонок или переадресовать его на другой номер; ну и, конечно же, исходящие звонки на любые номера.
- **Чем опасно:** По сути, обладая этим разрешением, приложение может делать всё, что угодно, если это касается голосовой связи.
- **Где настроить:** *Настройки → Приложения и уведомления → Разрешения приложений → Телефон (рис. 2).*

Прошло полгода.

Незаконная съёмка

– Боб, у нас странное дело.
– В чём проблема?
– К нам пришла госпожа М. Она пожаловалась, что кто-то разместил в Интернете её снимки, мягко говоря, в почти обнажённом виде.
– Вы разобрались, где сняты эти фотографии?
– Да. Они сняты в доме госпожи М. Но у неё нет скрытых фото- и видеокамер и не видно, чтобы они устанавливались. Более того, судя по всему, фотографии были сняты на её же смартфон.
– Вы уверены?
– Да. Они удалены со смартфона, но мы сумели их восстановить.
– Что дала проверка смартфона?
– На смартфоне была установлена новая игрушка.
– Бесплатная?
– Нет, в том-то и дело. Дешёвая, но не бесплатная. Она требовала доступ к «Камере». Официально, чтобы фотографировать пользователя во время игры. А потом должен был проводиться конкурс на самую забавную фотографию. Призовой фонд около 10000.
– И пользователи решили устанавливать?
– Ну да.
– Интересно, а когда они поймут, что, однажды получив это разрешение, приложение сможет в любой момент сделать фото или записать видео, не предупреждая их об этом? Такой компромат злоумышленники могут использовать с самыми разными целями.

Камера (Camera)

- **Что это:** Разрешение на доступ к камере, чтобы приложение могло делать фотографии и записывать видео.
- **Чем опасно:** Однажды получив это разрешение, приложение сможет в любой момент сделать фото или записать видео, не предупреждая вас об этом.
- **Где настроить:** *Настройки → Приложения и уведомления → Разрешения приложений → Камера (рис. 3).*

Слежка

Утро начиналось, как обычно. Боб успел сварить кофе и даже выпить его на кухне, и тут зазвонил телефон.

– Боб? Ты ещё дома?
– Да. Я успеваю на службу, ещё почти 45 минут, а мне тут пешком минут 15, не более!
– На сборы тебе 3 минуты. Сейчас к тебе приедет патрульная машина. Вопросов не задавай, всё равно ребята ничего не знают. Их задача тебя отвезти. Всё расскажут потом на месте.
– Понял, выхожу. А можно хоть намекнуть, шеф?
– Да сам не знаю. Приказ сверху.
– Понял.

Ещё никогда Боба не везли с такой скоростью по городу. Машина летела, как на пожар. Вдруг они выехали за город и свернули куда-то в лес.

– Мы куда?
– Куда приказано!
– Кем приказано?

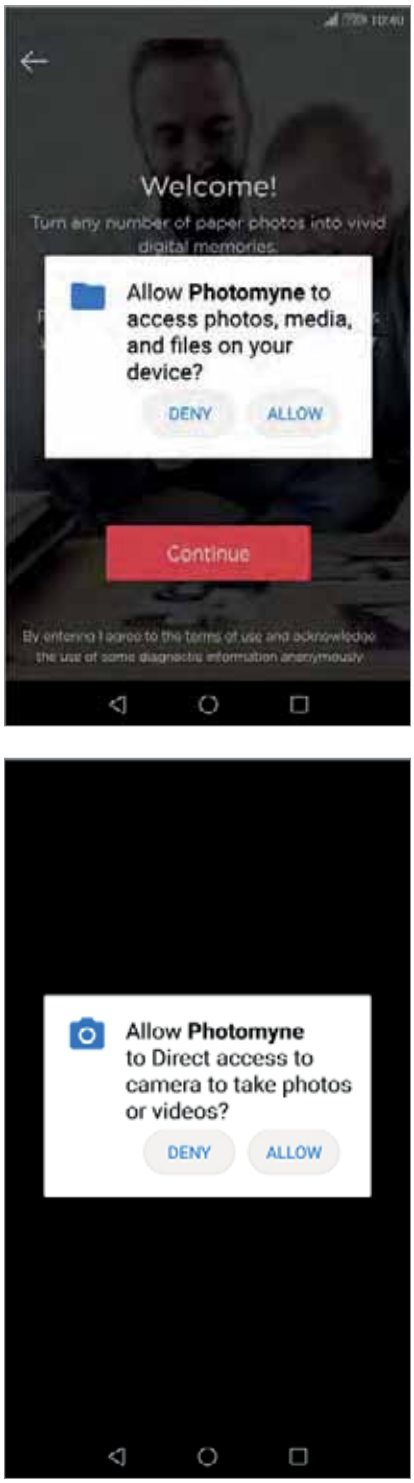


Рисунок 3. Разрешение Камера

– Кем надо! Все ответы на вопросы узнаешь сам. Моё дело – дорога. И вообще, уже приехали.

Машина въехала в коттеджный посёлок. Боб заметил, что охрана в посёлке вооружена автоматическим оружием.

– Всё! Приехали. Заходите в дом.
– Добрый день, Боб! Присаживайтесь! Кофе будете? Насколько я знаю, позавтракать вы не успели? Предлагаю совместить приятное с полезным.
– Где я?
– У друзей. Большего вам пока знать ни к чему. Нам нужна ваша помощь. С вашим руководством всё согласовано. Не волнуйтесь! Итак, у нас есть мистер, назовём его А. Нам нужно проследить его маршруты. Но сделать это нужно без его ведома. Увы, установить слежку мы не можем.
– Что вы знаете о нём?
– Любит скачки, американский футбол, покер. Использует смартфон от компании G. Активно играет в спортивный тотализатор с него.
– Вы сможете мне добыть его смартфон на полчаса? Или просто узнать, в каком приложении он играет?
– Приложение я вам скажу. Это Sport от компании X. А зачем нам это?
– Дело в том, что это приложение каждые 5 минут отсылает данные о местоположении клиента на сервер. А сама компания X принадлежит бывшему сотруднику службы безопасности. Вам не составит труда убедить его делиться этими данными, верно? Вот и всё. А вы сможете не только узнать маршруты его передвижения, но и сопоставить эту информацию с маршрутами общественного транспорта.

Местоположение (Location)

- **Что это:** Доступ к вашему местоположению как примерному (на основе данных о базовых станциях мобильной сети и точках доступа Wi-Fi), так и более точному (на основе данных GPS и ГЛОНАСС).
- **Чем опасно:** Позволяет приложению шпионить за всеми вашими перемещениями в пространстве.
- **Где настроить:** *Настройки → Приложения и уведомления → Разрешения приложений → Местоположение (рис. 4, рис. 5).*

Вечер у моря

Славный вечер! Наконец-то можно отдохнуть от службы после сумасшедшего дня и тихонько прилечь на диване перед телевизором с банкой пива. Тем более сегодня играет его любимая университетская команда. Пиво, пицца, телевизор…

В такую жару приехавший из столицы инспектор заставил их сдавать физподготовку. Идиот!!! Неудивительно, что теперь с дивана даже за пивом вставать лень…

Но, увы, счастье было так близко… Зазвонил телефон.

Рисунок 4. Местоположение.

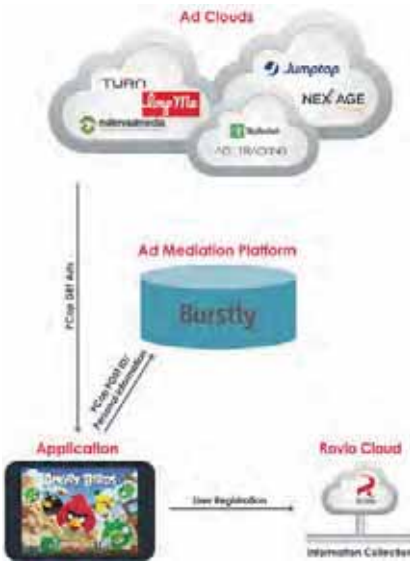


Рисунок 5. Местоположения. Сторонние приложения.

– Кого чёрт принёс? Я отдыхаю!
– Боб, это твой капитан. Извини, есть идея. Приезжай ко мне на побережье. У нас тут чудесное барбекю. Я понимаю, что ты решил расслабиться с банкой пива, а может, и не одной. Но ты мне нужен! Прямо сейчас. Пиво и не только – с меня! Я тебя жду.

Боб со стоном сполз с дивана, умылся и поехал к шефу. Интересно, что же там случилось.

– Шеф, привет! Только не говорите, что вы рады меня видеть после того, как целый день гоняли по жаре, как бешеного кролика.
– И не буду. У меня проблема. Внук взял поиграть мой смартфон. Результат? Мой телефон виснет с идиотской надписью после 10 минут работы.
– Что он пишет?
– Заплатите 10 долларов, и игра будет продолжена…
– Понятно. Зовите вашего оболтуса. Нужно узнать, что он загружал.
– Джонни! Что ты устанавливал на смартфон?
– Игрушку, у нас все в неё играют.
– А что она спрашивала во время установки?

– Вы думаете, я читал? Я быстро отвечал «Да», ведь хотелось поиграть.
– Ну что ж... Сейчас сделаю. Но все ваши сегодняшние добавления в список контактов будут утеряны, как и звонки, и СМС.
– Не страшно. Но что это было?
– Это? Обычный блокировщик экрана. Скорее всего, ваш внук ответил «Да» на предложение «Поверх других окон».
– А что ты будешь делать?
– Сброшу всё, верну заводские установки. Ваш телефон сам делает резервную копию, как только вы подключитесь к Wi-Fi. А сейчас мы его восстановим. И всё. Но не давайте больше телефон ребёнку!

Поверх других приложений (Display over other apps)

- **Что это:** Это разрешение позволяет приложению выводить изображение поверх других приложений.
- **Чем опасно:** Вредоносные приложения могут скрывать от пользователя какие-то важные предупреждения, а также подсовывать ему фальшивые формы ввода номера кредитной карты или пароля поверх окон легитимных приложений.
- **Где настроить:** *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Доступ к функции «Поверх других приложений» (рис. 6).*

Рисунок 6. Поверх других приложений

Ограбление

«Неужели уже прошло три года, как я начал работать в полиции? – подумал Боб. – Сколько времени прошло, сколько раскрыто дел. Но сколько ещё предстоит... Вот и сегодня шеф задал задачу. У мистера Д. с карты украли деньги. Двухфакторная аутентификация включена. Банк клянётся, что SMS-подтверждение пришло... Что произошло? Кажется, придётся лететь к друзьям за помощью».

– Боб, так что с банком? Выяснил?
– Выяснил, да только проблема стала ещё непонятнее. Шеф, я проверил логи банковского сервера. Всё верно. Пароль введён правильно, SMS-подтверждение банком отправлено и получено. А на телефоне клиента нет ничего. И провайдер клянётся, что SMS не могло быть доставлено, так как доставку отклонил сам клиент. Кто же тогда?
– Ну... Боюсь, я тебе не помогу. Увы. Ты у нас самый умный. Думай.
– Шеф, я посоветуюсь с полицией штата. Я такого ещё не видел.
– Звони, кто тебе мешает...

Прошло полчаса.

– Привет, Мигель!
– Привет, Боб! Что случилось? Ты всегда звонишь только в случае больших неприятностей.
– Увы, так и есть. Не понимаю. У клиента увели деньги с карты. Причём банк отправил SMS и получил подтверждение. Но клиент клянётся, что ничего не получал. Более того, провайдер заявляет, что SMS отклонена смартфоном клиента.
– А ты проверил смартфон клиента?
– Да. Там всё по работе и какое-то приложение для покупки билетов.
– Проверь функцию «Не беспокоить», она есть в новейших функциях Android. Ты же помнишь? Она фактически позволяет полностью отключить звук всех входящих сообщений. А если у твоего билетного приложения есть это право?
– Ты прав, этого я ещё не видел. У меня нет такого в смартфоне.
– Не болтай! Проверь!
– О! Ты был прав. Действительно, у него стоит «Не беспокоить» в период с 12 дня до 15. Вернее стоял. По состоянию на позавчера. Сейчас он выключен. А доступ к этому режиму есть только у приложения «Покупка билетов».
– Ну, вот и разгадка. Вредоносное приложение в нужный момент включило режим «Не беспокоить», чтобы владелец телефона пропустил какие-то важные звонки или сообщения. Например, звонок от службы безопасности банка в момент совершения подозрительной транзакции. Или SMS-оповещение.

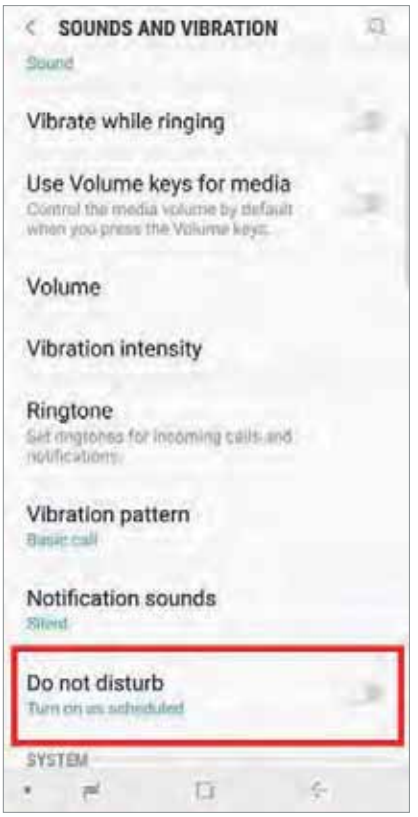


Рисунок 7. Не беспокоить.

Доступ к функции «Не беспокоить» (Do Not Disturb access)

- **Что это:** В новейших версиях Android есть функция «Не беспокоить» с массой настроек. Она позволяет полностью отключить звук голосовых звонков и сообщений, скрывать всплывающие уведомления.
- **Чем опасно:** Вредоносное приложение может в нужный момент включить режим «Не беспокоить», чтобы владелец телефона пропустил какие-то важные звонки или сообщения.
- **Где настроить:** *Настройки → Приложения и уведомления → Расширенные настройки → Специальный доступ → Доступ к функции «Не беспокоить» (рис. 7).*

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

В 2019 году 60% кибератак имели целенаправленный характер

Эксперты Positive Technologies проанализировали актуальные киберугрозы 2019 года. Анализ показал, что доля целевых атак существенно превысила долю массовых, а наиболее атакуемыми отраслями оказались госучреждения, промышленность, медицина, сфера образования и финансовая отрасль.

По данным исследования, количество уникальных кибератак выросло на 19%, а доля целенаправленных атак составила 60%, что на 5 п. п. больше, чем в 2018 году. При этом эксперты компании фиксировали поквартальный рост числа атак, и если в I квартале целевыми были менее половины атак (47%), то в конце года их доля составила уже 67%.

«Рост доли целенаправленных атак обусловлен рядом причин, – говорит **Алексей Новиков, директор экспертного центра безопасности Positive Technologies (PT Expert Security Center).** – Ежегодно появляются новые группы злоумышленников, специализирующиеся на атаках класса APT (advanced persistent threat). В течение года мы отслеживали APT-атаки 27 групп, среди которых есть как широко известные (Cobalt, Silence, APT28), так и относительно новые, малоизученные. Однако более пристальное внимание организаций к кибербезопасности, внедрение и использование специализированных средств защиты, нацеленных на выявление и противодействие сложным атакам (в частности, внедрение решений anti-APT), позволяет более качественно детектировать активность злоумышленников, существенно сокращать время их присутствия в организациях. В итоге в публичном поле оказываются данные об инцидентах, а главное – информация о тактиках и инструментарий APT-группировок, что позволяет повысить эффективность противодействия в целом».

По мнению экспертов, сегодня компании должны сместить фокус внимания с защиты периметра на возможность своевременно выявить развитие атаки внутри сети, регулярно проверять, не были ли они атакованы ранее. Учитывая рост целенаправленных атак, постоянно меняющиеся подходы преступников и усложнение ВПО, ключевыми факторами в обеспечении защиты в ближайшие годы станут непрерывный мониторинг инцидентов ИБ, глубокий анализ сетевого трафика и ретроспективный анализ событий в сети.

Наиболее часто кибератакам подвергались госучреждения, промышленность, медицина, сфера науки и образования, финансовая отрасль. При этом доля атак на промышленные компании выросла до 10% против 4% в 2018 году.

Значительные изменения коснулись мотивации злоумышленников в атаках против частных лиц: как показал анализ киберугроз в 2019 году, более половины атак осуществлялись с целью хищения данных, в то время как в 2018 году аналогичный показатель составлял 30%. В целом кража информации стала главным мотивом атак и для частных (57%), и для юридических лиц (60%). Наибольший интерес для злоумышленников в 2019 году представляли персональные данные, учётные записи и данные банковских карт.

Как показал анализ, трояны-шифровальщики стали одной из наиболее актуальных киберугроз для юридических лиц по всему миру. В 2019 году на их долю пришлось 31% заражений, а средняя сумма выплат злоумышленникам достигла нескольких сотен тысяч долларов США. В конце года эксперты Positive Technologies отметили новый тренд: операторы шифровальщиков в случаях отказа платить выкуп начали шантажировать жертв публикацией данных, которые они скопировали перед тем, как зашифровать их. По данным исследования, на конец 2019 года такие кампании проводили операторы шифровальщиков Maze и Sodinokibi. Информация о том, что преступникам удалось заработать на выкупах позволяет предположить, что в 2020 году нас ожидает новая волна атак шифровальщиков, а возникшая в конце года тенденция к публикации файлов жертв, отказавшихся платить выкуп, получит развитие.

Актуальные киберугрозы: итоги 2019 года

POSITIVE TECHNOLOGIES

***Компания Positive Technologies** за 15 лет существования завоевала лидирующие позиции на отечественном и европейском рынке систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений.*

www.ptsecurity.com

CIS / № 2 (12) / 2020 / www.cis.ru

6 устройств для сетевого шифрования: плюсы и минусы

В обзоре представлены пять из доступных сейчас на российском рынке линеек (семейств) устройств сетевого шифрования (шифрования трафика, шифрования каналов) для сетей Ethernet, причём от разных производителей и принадлежащих к разным классам. Проанализированы архитектурные особенности, эксплуатационные характеристики, сценарии применения. Приведены их плюсы и минусы.

Все рассматриваемые устройства представляют собой программно-аппаратные комплексы, которые состоят из оборудования (платформы) и среды функцио нирования СКЗИ. Последняя, в свою очередь, включает в себя базовую ОС и криптомодуль, который и выполняет криптографические функции: шифрование, расшифровку, формирование и проверку кода аутентификации сообщения.

Нужно сразу оговориться, что в фокусе этого обзора функция межсайтового шифрования. Дело в том, что 4 из 6 устройств в этом обзоре – это конвергентные (многоцелевые) устройства, которые, кроме собственно шифрования трафика, выполняют много других функций. Можно долго спорить о том, что лучше: специализированные средства для решения отдельных задач или «швейцарский нож», который решает сразу несколько задач, пусть даже и ценой каких-то компромиссов. Набор этих функций может быть разным, и чтобы не ограничивать себя только одним классом устройств, а, наоборот, идти от задач, в этом обзоре все остальные функции, не относящиеся к межсайтовому шифрованию, как бы «вынесены за скобки». При желании их можно оценить и учесть отдельно.

В этом обзоре по возможности используются общепринятые (официальные или разговорные) термины и сокращения, а не те, которые придуманы самими производителями: так будет проще понять, о чём идёт речь.

C-Терра Шлюз и Шлюз 10G

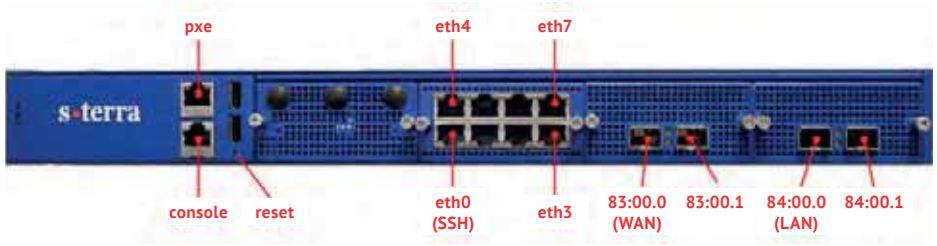


Рисунок 1. Шлюз / Шлюз 10G. Источник: «С-Терра СиЭсПи».

Линейка «Шлюз» компании «С-Терра СиЭсПи» обозначается как программно-аппаратный комплекс для обеспечения безопасности сети, по сути же представляет собой классический шлюз безопасности (криптошлюз, криптомаршрутизатор). Как и большинство других конвергентных устройств, устройства компании «С-Терра СиЭсПи», помимо функции сетевого шифрования, обеспечивают поддержку межсайтовых VPN, межсетевого экранирования и доступа VPN-клиентов. Модель 10G, хотя и обладает общими характеристиками с остальной линейкой, но имеет другое назначение: она предназначена для защиты отдельных высокоскоростных каналов связи на L2 в линейном режиме («точка-точка») (рис. 1).

Устройства состоят из аппаратной платформы (здесь есть довольно широкий выбор как по производительности, так и по конструктивному исполнению, в том числе с поддержкой сторонних АПМДЗ для исполнений, сертифицированных по классам КС2 и КС3) с предустановленным ПО и набора лицензий на криптомодуль, средства управления и поддержку. В качестве программного обеспечения аппаратных средств используется ОС Debian Linux с криптомодулем, поддерживающим набор алгоритмов ГОСТ, в том числе блочные шифры из ГОСТ Р 34.12-2015 – «Магма» и «Кузнечик».

Подобно другим шлюзам безопасности, устройства поддерживают большой набор сетевых функций и функций обеспечения безопасности. Реализован по существу весь стек протоколов IPsec, в частности для межсайтового шифрования L3 и L2 в серии «Шлюз» используется протокол IPsec ESP в транспортном или туннельном режиме, причём большое внимание уделяется строгому следованию RFC и российским ГОСТам (рис. 2).

Шлюз 10G захватывает кадры из доверенной локальной сети, инкапсулирует их в IP, который потом шифруется тем же IPsec (рис. 3).

Серия «Шлюз» отличается умеренной на сегодняшний день производительностью. Максимальная пропускная способность у верхней в линейке модели около 3 Гбит/с на больших пакетах, на IMIX она составляет около 2 Гбит/с. В общем, работой на скорости линии в 10-гигабитном канале Ethernet эти устройства похвастаться не могут. Так как известны и протоколы, и режимы их работы, можно довольно точно рассчитать накладные расходы пропускной способности: для небольших пакетов они могут превышать 50%. В режиме L2 они ещё больше: кадры инкапсулируются в UDP-заголовки, к которым потом добавляются новые (транспортные) IP- и MAC-заголовки.

У модели 10G пропускная способность выше: до 12 Гбит/с на больших пакетах и 10 Гбит/с на IMIX. Правда, как сообщает сама компания, речь идёт о суммарной пропускной способности шифрования, то есть для симметричного полнодуплексного трафика эти цифры, видимо, нужно делить пополам, то есть и эта

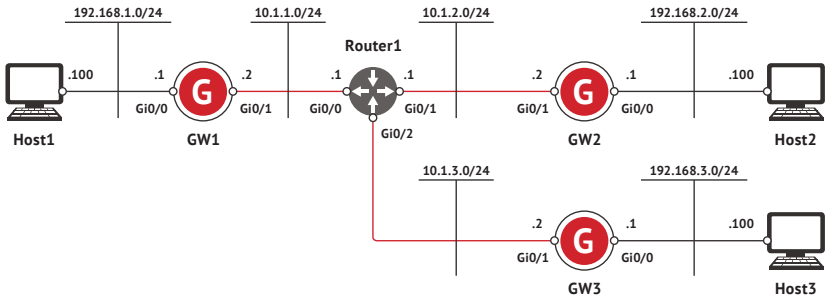


Рисунок 2. Одна из схем подключения Шлюз. Источник: «С-Терра СиПиЭн».

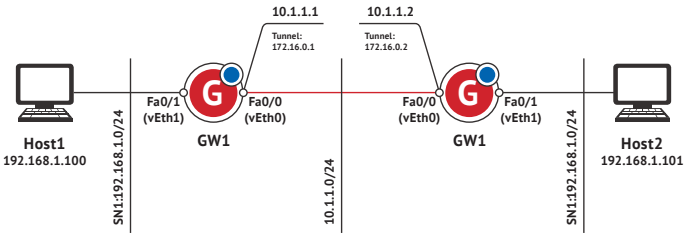


Рисунок 3. Схема подключения Шлюз 10G. Источник: «С-Терра СиПиЭн»

модель не может работать на полной скорости 10-гигабитной линии. Что касается накладных расходов, то, хотя применяемый здесь протокол инкапсуляции EtherIP отличается компактным 4-октетным заголовком, это всё же туннельный режим, и накладные расходы составляют десятки байтов на пакет. Вносимая задержка при полной нагрузке (когда устройство ещё не начало терять пакеты) составляет около 1 мс. Для увеличения пропускной способности модели обеих серий могут объединяться в фермы агрегирования.

Шлюз и Шлюз 10G могут работать в сетях любых размеров, не накладывая своих ограничений на масштаб сети. Серия «Шлюз» отличается отменной гибкостью, причём как в сетевых возможностях, так и в криптографических алгоритмах. Поскольку используются стандартные протоколы шифрования, то Шлюз может работать в паре с шлюзами безопасности ГОСТ других производителей (такими, где тоже реализован «честный» IPsec). Кстати, помимо прочих, в устройстве поддерживается и набор алгоритмов для AES, что позволяет связывать Шлюз с зарубежными устройствами IPsec. А вот Шлюз со Шлюзом 10G связать не получится: режим L2 в этих сериях реализован по-разному.

Что касается совместимости, то разработчики пошли по пути явной полной поддержки большого количества протоколов, особенно на L3. То есть шлюз безопасности «на равных» взаимодействует с другими устройствами в сети. Обратная сторона такого подхода – риск нарушения работы сети из-за неправильных настроек или тонких отличий в реализации одних и тех же протоколов разными производителями.

Для обеих серий предусмотрены разнообразные средства управления, включающие в себя интерфейс командной строки, веб-интерфейс и фирменную систему управления, которая состоит из сервера управления и клиента управления (станции администратора). Управление через сеть возможно во внеполосном (через отдельный сетевой порт устройства) и внутриполосном (через общий туннель IPsec) режимах. Интерфейс командной строки интересен тем, что содержит, кроме оболочки Linux, ещё и специальную консоль с синтаксисом команд Cisco. Вообще система ориентирована на специалистов с хорошим знанием сетевых технологий. В руководстве пользователя честно написано, что «желательно обладать знаниями на уровне сертификата CCNA или аналогичного»! В частности, достаточно трудоёмким процессом будет настройка соединений IPsec (правда, мастер настройки и возможность применения конфигурационных файлов облегчают его). Начальная настройка шлюзов включает в себя разумное количество ручных операций, в частности ввод номеров лицензий и инициализация датчика случайных чисел (нажатиями на клавиши или использованием внешней гаммы). Управление ключами централизованное автоматическое с аутентификацией на базе PKI (для этого при начальной настройке нужно сгенерировать и установить на каждый шлюз безопасности сертификат). В качестве внутреннего удостоверяющего центра используется Microsoft CA, внешние тоже поддерживаются.

Отказоустойчивость обеспечивается как резервированием компонентов (блоков питания и дисков), так и разнообразными средствами резервирования самих устройств, портов и каналов.

Модели серии «Шлюз» в зависимости от состава оборудования и набора лицензий будет стоить до 1,3 млн рублей, Шлюз 10G – примерно 3,6 млн рублей.

Подводя итог, к плюсам можно причислить:

- хорошую интероперабельность
- криптографическую гибкость
- гибкость в настройке и совместимость в сетях L3
- мощные и гибкие средства управления
- большой набор средств обеспечения отказоустойчивости
- автоматическое управление ключами
- удобную документацию
- невысокую цену

К минусам:

- слабую производительность: большая задержка, низкая пропускная способность, большие накладные расходы
- сложное управление: обилие настроек, ручное управление зашифрованными соединениями, высокие требования к квалификации персонала, сложность разграничения задач между ИБ и ИТ
- ограниченную гибкость в сценариях подключения модели «Шлюз 10G»
- ограниченную совместимость с сетями L2

ViPNet Coordinator HW

Рисунок 4. ViPNet Coordinator HW5000. Источник: «ИнфоТеКС».

Это семейство устройств, разработанных компанией «ИнфоТеКС». Производитель называет их шлюзами безопасности. Устройства являются частью фирменной архитектуры сетевой безопасности ViPNet. Выполняют функции VPN-шлюза сетевого (L2) и канального (L2) уровней. Кроме того, они обеспечивают фильтрацию трафика (являясь межсетевыми экранами) и поддерживают большой набор сетевых функций L3 и L2. В общем, их тоже можно отнести к той же категории конвергентных устройств российского производства. Текущее поколение продукта – четвёртое.

Продукт состоит из специализированной сетевой платформы (до 8 гигабитных и 10-гигабитных портов в зависимости от модели) и криптомодуля, разработанного «ИнфоТеКС». В качестве базовой ОС используется Linux (рис. 4).

В устройствах применяется фирменный протокол сетевого шифрования (разработчик иногда называет его IPlir). Одно время «ИнфоТеКС» даже предпринимал попытки стандартизовать его в рамках комитета ТК26. Протокол использует инкапсуляцию зашифрованных блоков данных в нестандартный протокол с номером 241 в заголовке IP. Этот протокол используется, когда смежные шлюзы находятся в одном широковещательном домене и могут без проблем найти друг друга, в этом случае обнаружение и поддержание связи между шлюзами происходит автоматически. Если же устройства находятся в разных подсетях, в том числе за NAT, то блок данных инкапсулируется в UDP или (если связи по этому протоколу нет) в TCP (рис. 5).

При организации связи на L2 используется обычный подход L2overIP с захватом кадров из локального сегмента, их инкапсуляцией в IP-пакеты и отправкой этих пакетов другому шлюзу в нужный сегмент на другой стороне сети. Устройство обрабатывает и передаёт все широковещательные и все однонаправленные кадры с известными (заученными) адресами, а кадры с неизвестными либо передаёт во все порты, либо сбрасывает. При этом не должно быть альтернативных маршрутов на любом из уровней сети в сегменты L2, иначе, как об этом предупреждают в руководстве, «это может парализовать работу всей сети»! Количество подключаемых сегментов L2 (портов виртуального коммутатора) не может превышать 31, кроме того, в этом режиме рекомендуется придерживаться (по соображениям производительности) максимального количества 252 IP-адресов.

В целом такой подход годится для построения виртуальной частной сети L2 (в том числе через сеть L3) для некоторых сценариев, но не обеспечивает интеграции защищённых сегментов с опорной сетью L2 для построения масштабных сетей L2 (рис. 6).

Интересно, что в качестве криптографического алгоритма используется старый ГОСТ 28147-89 в режиме гаммирования (CTR) или гаммирования с обратной связью по шифротексту (CFB), а не разработанный при участии «ИнфоТеКСа» «Кузнечик».

Согласно опубликованным данным, производительность шифрования на старших моделях достигает 6,8 Гбит/с, то есть на скорости 10-гигабитной линии и эти устройства работать не могут. Правда, «ИнфоТеКС» заявляет, что использует свою методику тестирования, так что неясно, к трафику какого профиля относятся эти цифры. В режиме L2 производительность падает примерно на 15-20%. Накладные расходы при использовании инкапсуляции в IP должны быть невелики (хотя открытых данных с форматами пакетов нет), но при инкапсуляции в UDP они неизбежно возрастают и будут сравнимы с накладными расходами IPsec в туннельном режиме. Для повышения пропускной способности можно агрегировать порты на самом устройстве, а также (в режиме L2) объединять устройства в фермы внутри агрегированного канала.

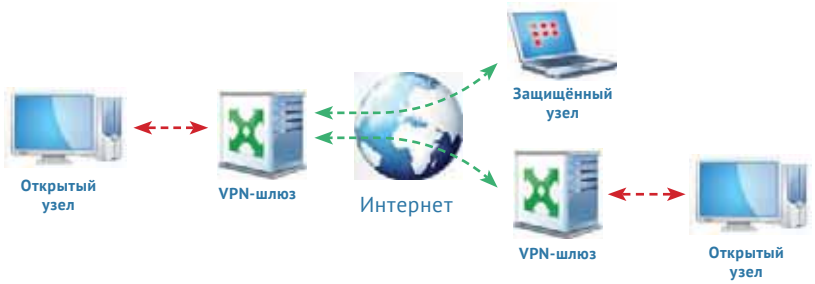


Рисунок 5. Схема подключения ViPNet Coordinator HW. Источник: «ИнфоТеКС».

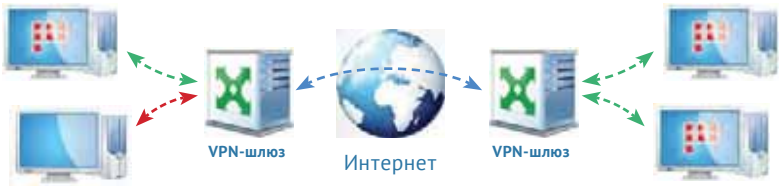


Рисунок 6. Схема подключения ViPNet Coordinator HW на L2. Источник: «ИнфоТеКС».

Архитектура ViPNet вместо простых туннелей «точка-точка» позволяет создавать виртуальные частные сети с замысловатой структурой, сложными правилами адресации и маршрутизации, резервированием, приоритизацией и так далее. Благодаря этому поддерживается большое разнообразие сценариев межсайтового шифрования, в том числе федерация разных защищённых сетей ViPNet. Так как всё это работает поверх обычной IP-сети, где тоже есть свои настройки, понятно, что простоты в эксплуатации это не добавляет. Фактически появляется отдельная самостоятельная задача по планированию, развёртыванию и сопровождению защищённой сети, требующая хороших знаний сетевых технологий, и вопрос в том, на кого эту задачу возложить.

Для управления отдельными шлюзами безопасности можно использовать интерфейс командной строки (через последовательный или сетевой порт) со своей оригинальной системой команд, а также веб-интерфейс (правда, с ограниченным набором функций). Режим подключения внутриполосный. Но помимо этого нужна ещё и среда для управления всей защищённой сетью, а также ключами и сертификатами. Именно в этой среде создаётся структура защищённой сети, генерируются ключи и сертификаты, рассылается по сети конфигурация и ключи. Начальная настройка устройств заключается в переносе на них файлов с ключами и конфигурацией. В дальнейшем конфигурация и ключи передаются на шлюзы через защищённую сеть. Документация довольно качественная и полезная.

У шлюзов нет резервирования важнейших узлов (таких, как блоки питания), заявленное время наработки на отказ – 50 тыс. часов. Для защиты от отказов можно использовать кластер «активный-пассивный» с быстрым (порядка нескольких секунд) переключением, а также агрегацию портов на устройстве и резервирование внешних каналов.

Цена старшей модели составляет 2 млн. рублей.

Плюсы серии:

- гибкость в конфигурации защищённой сети
- средства обеспечения отказоустойчивости и наращивания производительности
- небольшие накладные расходы в L3

Минусы:

- низкая производительность: пропускная способность не дотягивает до 10 Гбит/с, работа на скорости линии не поддерживается
- ограниченная функциональность, производительность и масштабируемость L2
- сложное управление структурой и настройками защищённой сети
- ручная настройка сегментов L2
- ручное управление ключами
- ограниченная защита от физического вскрытия

АПКШ «Континент»

Рисунок 7. АПКШ «Континент» IPC-3000FC. Источник: «Код безопасности»

Это семейство продуктов, разработанное компанией «Код безопасности», позиционируется как «централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ». Это конвергентное устройство с набором алгоритмов ГОСТ и обычным набором функций, включая межсайтовое шифрование (оно нас интересует прежде всего) в сочетании с VPN, шлюз доступа VPN-клиентов, межсетевой экран и систему обнаружения вторжений. Текущая версия продукта – 3.9 (именно её и будем рассматривать в обзоре), но поставляется и предыдущая – 3.7, и уже представлена (но пока не сертифицирована в ФСБ и не поставляется) следующая – 4.

Итак, семейство построено на базе сетевых платформ x86 (как обычно, в компактных и стоечных корпусах) под управлением ОС FreeBSD. Производительность шифрования, а также некоторые функциональные возможности определяются выбранной моделью платформы в сочетании с набором лицензий. В зависимости от модели есть от 3 до 16 сетевых интерфейсов, что позволяет реализовывать разнообразные конфигурации (подключение к одному шлюзу нескольких защищённых сегментов, подключение к нескольким внешним каналам, агрегация каналов и прочее). Платформы оснащены датчиками вскрытия и АПМДЗ. В одной из моделей используется криптоускоритель на FPGA (рис. 7).

Для межсайтового шифрования используется ГОСТ 28147-89 в режиме гаммирования с обратной связью (CFB) с имитозащитой по тому же ГОСТу. Межсайтовое шифрование L3 работает в сочетании с VPN и фильтрацией пакетов. Используется фирменный протокол L3 туннельного режима (инкапсуляция IP-пакетов в UDP). Редкая функция – это сжатие IP-пакетов по алгоритму Deflate (причём можно устанавливать минимальную длину шифруемых пакетов), она должна компенсировать накладные расходы.

В режиме L3 поддерживаются несколько внутренних и внешних интерфейсов, поэтому к одному шлюзу можно напрямую (то есть без промежуточных маршрутизаторов или коммутаторов) подключить несколько внешних каналов и защищённых сегментов. Несколько внешних интерфейсов можно использовать для резервирования каналов (через переключение маршрутов, статическую или динамическую маршрутизацию), поддерживается также агрегация интерфейсов. Можно реализовать выборочное (по диапазонам адресов) шифрование,

устройство также может пропускать (оставлять незашифрованными) отдельные протоколы.

Ещё одна редко встречающаяся особенность – это внешнее подключение через телефонный модем (с дозвоном по требованию, как у теперь забытых дозванивающихся маршрутизаторов из 90-х годов!) и USB-модем 3G (разумеется, скорости у таких каналов соответствующие и не все функции через них работают). Есть механизм QoS (на базе поля ToS протокола IP в режимах IPP и DSCP) с классификацией и приоритизацией трафика (правда, не для интерфейсов 10 Гбит/с) (рис. 8).

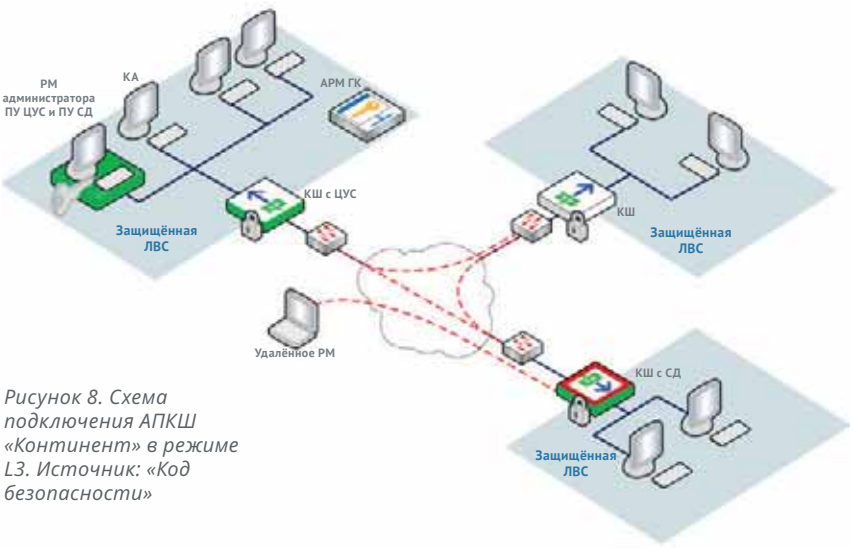


Рисунок 8. Схема подключения АПКШ «Континент» в режиме L3. Источник: «Код безопасности»

В режиме шифрования L2 защищённые сегменты, подключённые к внутренним портам устройств, как бы «сшиваются» в виртуальный коммутатор с помощью туннелей между парами АПКШ. Кадры инкапсулируются в UDP и маршрутизируются через IP-сеть. По заявлению производителя, поддерживаются любые протоколы и форматы кадров Ethernet, в том числе jumbo frames. Поддерживается пропуск или сброс кадров отдельных служебных протоколов L2. Для маршрутизации кадров через виртуальный коммутатор используются таблицы с динамическими (заученными) и статическими MAC-адресами.

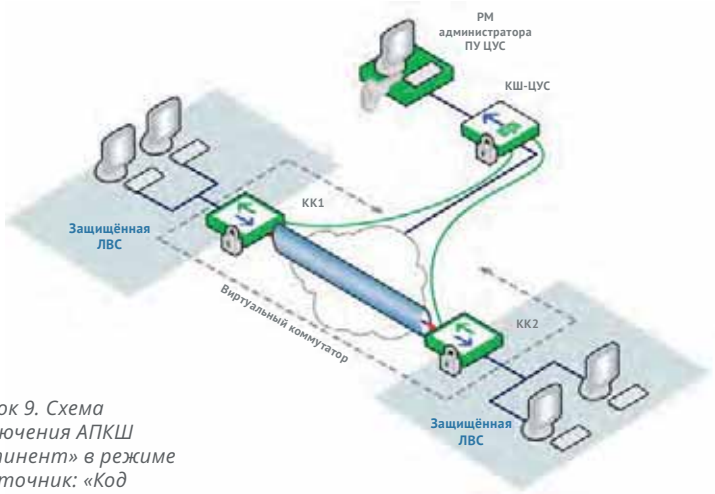


Рисунок 9. Схема подключения АПКШ «Континент» в режиме L2. Источник: «Код безопасности»

Так как компания «Код безопасности» применяет свою собственную методику измерения производительности, то с опубликованными цифрами нужно работать с осторожностью. Но, как следует из опубликованных компанией материалов, даже модель с криптоускорителем, которая работает только в режиме L2, не обеспечивает работу на скорости линии во всем диапазоне длин пакетов. Для остальных моделей с «программным» шифрованием суммарная пропускная способность зависит от модели платформы и для старшей модели составляет 6,4 Гбит/с. Фирменный протокол шифрования из-за длинного криптографического заголовка и инкапсуляции в UDP отличается довольно высокими накладными расходами (свыше 50 байт на пакет в L3, свыше 70 в L2). Что касается вносимой задержки, то для модели с криптоускорителем она не превышает 60 мкс – очень хороший результат, достигнутый благодаря использованию FPGA. Для остальных моделей задержка существенно (в разы) больше. Для наращивания пропускной способности можно использовать фермы устройств (в качестве балансировщика может выступать либо «Континент», либо стороннее устройство) и агрегацию портов устройства.

С ограничениями по масштабированию можно столкнуться, пожалуй, только в режиме L2, где есть «потолок» по суммарному количеству портов виртуального коммутатора (впрочем, оно довольно велико). Заметно ограничивает гибкость то, что IPv6 можно использовать исключительно на внешних интерфейсах, причём без динамического назначения адресов. В «Континенте» есть явная поддержка некоторых сервисов L3 и L2, а с помощью механизма выборочного шифрования можно обеспечить прозрачность для некоторых других (но не всех) протоколов.

Так как используется проприетарный протокол шифрования, интероперабельности с другими производителями нет. Совместимость между текущей (3.9) и предыдущей (3.7) версиями, в общем, поддерживается, но с некоторыми ограничениями и неудобствами.

Управление комплексом обеспечивается с помощью фирменной трёхзвенной среды управления (станция управления на ПК под Windows – АПКШ с сервером управления – управляемые устройства). Сервер управления может работать на выделенном или одном из рабочих шлюзов, в выделенном или одном из рабочих сегментов сети. С помощью этой среды происходит выработка ключей, установка VPN-туннелей, и вообще вся архитектура комплекса сильно «завязана» на сервер управления и без него не работает. Поэтому для сохранения работоспособности при отказе сервера управления предусмотрено резервное копирование его БД, а также «горячее» резервирование самого сервера.

Кроме управления через фирменную среду управления, есть так называемое локальное управление с помощью текстовых меню: либо локально (монитор, клавиатура), либо по сети через SSH. В этом режиме доступен ограниченный набор функций. Командной строки и веб-интерфейса нет. Поддерживается мониторинг через SNMP.

Для инициализации (ввода в эксплуатацию) любого из устройств требуются клавиатура и монитор. При инициализации сервера управления нужно выполнить около десятка ручных операций, зато для инициализации прочих устройств сначала через среду управления создаются соответствующие им логические объекты, а уже потом конфигурация и начальный набор ключей выгружаются на внешний носитель. При первом запуске нового устройства эта конфигурация копируется и применяется к нему (в духе централизованной идеологии управления «Континентом»). Установка туннелей L3 выполняется вручную, а вот связи между портами виртуального коммутатора L2 настраиваются автоматически.

Заявленное среднее время наработки на отказ для всех аппаратных платформ – 50 тыс. часов. Отказоустойчивость защищённой сети обеспечивается следующим: во-первых, с помощью резервирования отдельных аппаратных узлов (только в старших моделях) и агрегации портов, во-вторых, средствами кластера «активный-пассивный» со временем переключения порядка секунд (настройка кластера имеет свои особенности, но в целом не превосходит по трудоёмкости добавление пары обычных шлюзов), в-третьих, путём объединения устройств в фермы. Устройства также могут обеспечивать резервирование внешних каналов.

Для управления ключами «Континента» используется централизованная система генерации и распределения ключей. Есть ключи нескольких типов: для шифрования трафика, для шифрования данных в устройстве и для защиты канала связи с сервером управления. Ключи последних двух типов генерируются, выгружаются на внешний носитель, передаются через сеть, устанавливаются, отзываются и так далее вручную. Смена заранее сгенерированных ключей, а также выработка и установка ключей для защиты туннелей происходит автоматически. При так называемой усиленной схеме для генерации ключей и случайных чисел используется выделенное офлайновое (изолированное от сети) устройство (платформа начального уровня) с АПМДЗ.

Также есть возможность объединения разных криптографических сетей (федерация) с помощью межсетевого ключа (он, в свою очередь, распределяется с помощью собственного, встроенного в сервер управления удостоверяющего центра).

Цена старшей модели (с криптоускорителем) составляет почти 4 млн. рублей.

В плюсах:
- низкая задержка и высокая пропускная способность у модели с криптоускорителем
- функция сжатия трафика
- гибкость в топологиях L3
- автоматическая настройка туннелей L2

В минусах:
- высокие накладные расходы при передаче трафика
- нет работы на скорости линии
- ручное конфигурирование сети, в том числе установка туннелей L3
- ручное управление ключами
- полная зависимость от сервера управления
- нет управления через веб-интерфейс и командную строку
- нет эффективных механизмов разделения ролей между ИТ и ИБ

Diamond VPN/FW

Серия многофункциональных комплексов сетевой защиты (МКСЗ), разработанных компанией TSS, предлагается в качестве единого средства защиты от сетевых угроз и сочетает в себе межсетевой экран, средства построения зашифрованных виртуальных частных сетей и систему обнаружения вторжений. То есть это тоже типичное конвергентное устройство, напрямую конкурирующее с тремя описанными выше.

Точно так же оно состоит из ПО на основе Linux и аппаратной платформы. Поддерживается довольно разнообразный набор оборудования, но, как и упомянутые ранее производители, TSS отдаёт предпочтение платформам Lanner, специально предназначенным для сетевых устройств различного назначения.

Для шифрования и построения VPN используется протокол DTLS – датаграммная, основанная на UDP разновидность TLS. По своим основным характеристикам (в частности, накладным расходам на установку туннелей и передачу данных) этот протокол примерно соответствует IPsec, отличаясь, правда, гораздо меньшей гибкостью. То есть шифрование происходит на L4, но за счёт использования режимов L2 over VPN и L3 over VPN (очевидно, инкапсуляции) можно связывать сегменты на 2-м и 3-м уровнях сетевой модели соответственно (рис. 10).

В качестве алгоритма шифрования используется ГОСТ 28147-89 с учётом рекомендаций ГОСТ Р34.12-2015, то есть фактически это «Магма». В полнодуплексном режиме старшие модели достигают пропускной способности 16 Гбит/с, но, как следует из опубликованного TSS графика производительности, она быстро падает с уменьшением размера пакета, причём это падение нельзя объяснить только накладными расходами: очевидно, устройство начинает терять пакеты. Что касается накладных расходов, то их можно оценить как средние – несколько десятков байт на пакет. Сетевая задержка, согласно опубликованным данным, не превышает 1,5 мс – довольно большой даже для «программного» шифрования показатель.

В довольно формальной и неудобной документации никакие ограничения на масштаб сети не указаны. Реализована явная поддержка некоторых сетевых технологий L3 (например, динамическая маршрутизация) и L2 (в частности, LACP и STP). Интероперабельность устройств на базе TLS и особенно менее популярного пока DTLS довольно слабая, так что рассчитывать на возможность взаимодействия с оборудованием других производителей не стоит.

Для управления устройствами используется обычный набор технологий: интерфейс командной строки через консольный порт или ssh, веб-интерфейс

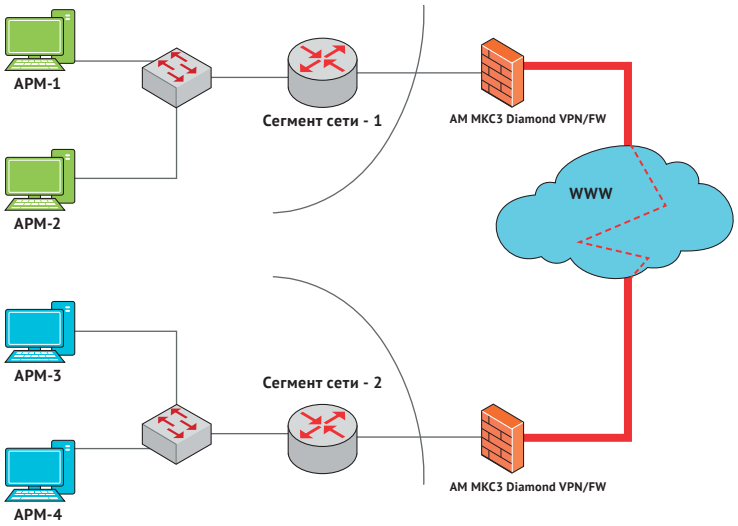


Рисунок 10. Схема подключения Diamond VPN/FW. Источник: TSS

(с ограниченной функциональностью) и фирменная среда управления. Как и в описанных выше устройствах, общая идеология управления ориентирована скорее на «сетевиков», чем на «безопасников», хотя среда управления позволяет создавать собственные роли, комбинируя разные права. Управление идёт через одно из устройств, которое становится ведущим – для него потребуется приобрести лицензию на управление. Начальная настройка, как и везде, идёт через консоль. Автоматической установки туннелей нет, их нужно конфигурировать вручную (одно из устройств становится сервером, другое/другие – клиентом VPN). Поддерживаются АПМДЗ и дополнительные модули (платы) для внеполосного управления. Для централизованного управления ключами применяется PKI, причём используются либо встроенные в среду управления – внутренние, либо сторонние УЦ.

В модельном ряду есть устройства с резервированием блоков питания, плюс поддерживаются кластеры «активный-пассивный», агрегация портов и резервирование туннелей VPN (список из нескольких серверов, которые может перебирать клиент).

К плюсам решения можно отнести:
- высокую пропускную способность на длинных пакетах
- автоматическое управление ключами

А к минусам:
- большую вносимую задержку
- падение производительности на коротких пакетах
- ручную настройку туннелей
- неудобную документацию

Недавно компания TSS объявила о подготовке к выпуску устройства шифрования нового поколения под условным пока названием Dcrypt XG. Для этого устройства заявлена:
- высокая пропускная способность (до 100 Гбит/с)
- низкие задержки (20 микросекунд)
- алгоритм ГОСТ «Магма»
- аппаратные модули шифрования (криптоускорители)

Так как официальная спецификация на этот продукт отсутствует, он пока оставлен за рамками обзора (были выбраны только уже поставляемые, присутствующие на рынке модели). Согласно плану развития Dcrypt XG, его доведение до полной функциональности запланировано на август 2020 года.

«Квазар»

Рисунок 11. «Квазар» H-172A. Источник: «ИнфоТеКС»

Интересная серия устройств, разработанных компанией «СПБ» (сейчас она входит в группу компаний «ИнфоТеКС»). Это единственное на сегодняшний день решение с ГОСТ для шифрования L1 в синхронных оптических сетях. Устройства называются модулями шифрования и встроены в транспондеры и мукспондеры (мультиплексирующие/агрегирующие транспондеры) для сетей OTN. Хотя OTN относится к другому, нежели Ethernet, стеку технологий, в качестве одного из клиентских (подключаемых со стороны локальной сети) интерфейсов можно использовать Ethernet, поверх которого можно пустить любые протоколы верхних уровней. То есть такой защищённый оптический канал (или даже оптическую сеть) можно использовать в качестве одного из сегментов опорной сети Ethernet L2 или L3. Вот почему мы рассматриваем здесь это устройство наравне с другими, принимая во внимание все его плюсы и минусы (рис. 11).

Итак, этот комплекс предназначен для криптографической защиты магистральных каналов связи на базе OTN. Он помещает протокольные блоки данных (то есть кадры целиком) клиентских протоколов L2 в кадры (своеобразные конверты) синхронной сети и потом шифрует их. Далее эти кадры доставляются через оптическую сеть и распаковываются модулем шифрования на другом её конце. Сами модули выполнены либо как телекоммуникационные устройства высотой 1U и с 48-вольтным питанием, либо как модуль для шасси «Волга» компании «Т8». Для обработки потока данных и шифрования применяется ПЛИС. Устройства имеют 2 контроллера, подключённых к ПЛИС: один для управления потоком данных и мониторинга, другой для управления ключевой информацией (аутентификация администратора, ввод ключей, контроль, стирание) (рис. 12).

На операторской стороне модули используют сигнал OTU2 с битовой скоростью примерно 10 Гбит/с, что

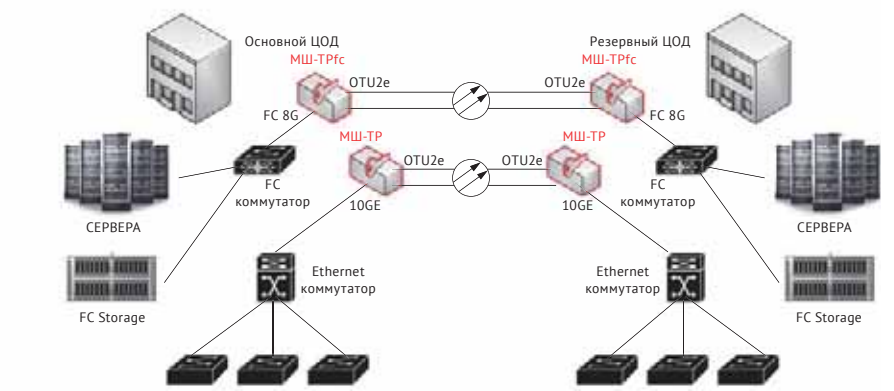


Рисунок 12. Схема подключения «Квазар». Источник: «СПБ»

соответствует скорости клиентского интерфейса (то есть полосе пропускания Ethernet) чуть меньшей, чем 10 Гбит/с, что вынуждает использовать отдельную разновидность физического уровня Ethernet – WAN PHY. Шифрование идёт на полной скорости линии. Используется проверенный алгоритм ГОСТ «Магма» в режиме гаммирования. Что касается накладных расходов, то они здесь нулевые: вся избыточная информация помещается за пределами кадра Ethernet. Сетевая задержка тоже невелика и составляет примерно 50 микросекунд.

На масштабируемость сети, построенной с элементами технологий OTN, модули шифрования никак не влияют. Разумеется, гибкость решения шифрования диктуется особенностями стандарта OTN. В качестве транспортной технологии может использоваться либо «тёмное» (без активного оборудования) оптоволокно, либо канал с аппаратурой частотного разделения (DWDM), либо опорная сеть оператора, использующая OTN. Так как все заголовки L2 и выше шифруются, то возможно только позвенное шифрование (в том числе в кольцевых сетях OTN). Это вынуждает использовать большое количество таких шифраторов. Зато обеспечивается доставка кадров не только Ethernet, но и Fibre Channel, поэтому нет необходимости упаковывать трафик FC в Ethernet или IP. В сочетании с низкой задержкой это делает такие устройства привлекательным решением для сетей хранения данных (SAN), в частности для синхронной репликации баз данных.

Поскольку, как уже упоминалось выше, стандартов шифрования в OTN пока нет, поэтому интероперабельности с устройствами других производителей тоже нет. В сочетании с большим «расходом» шифраторов при позвенном шифровании и высокой ценой одного модуля (4,6 млн рублей) это делает порог входа в такие решения весьма высоким.

Устройство ориентировано на необслуживаемый удалённый от администраторов режим работы. Поддерживаются полноценные функции защиты от физического вскрытия, в частности стирание всей ключевой информации при потере питания, вскрытии корпуса или нажатии на кнопку экстренного сброса. Управление обеспечивается через выделенные сетевые порты, причём как локальное, так и удалённое (внутриполосное и внеполосное). Сами средства управления разделены на сетевые/коммуникационные и криптографические – удобное решение. Огорчает только отсутствие централизованного управления ключами: весь ключевой материал (ключ администратора и ключи шифрования данных) должен генерироваться на отдельной станции, записываться на смарт-карты, физически доставляться к модулям шифрования и записываться на них. Конечно, это неудобно.

Отказоустойчивость обеспечивается с помощью дублирования операторских (WAN) портов и технологии автоматического выключения лазера (ALS) – аналога LLF в Carrier Ethernet.

Итак, плюсы:
- низкие (нулевые) накладные расходы пропускной способности, работа на скорости линии, низкая задержка
- поддержка других протоколов L2 (мультисервисность)
- защита от физического вскрытия
- разделение функций управления
- резервирование линий

Минусы:
- ограниченный выбор топологий
- ограничения в выборе среды передачи
- только позвенное шифрование
- ручное управление ключами

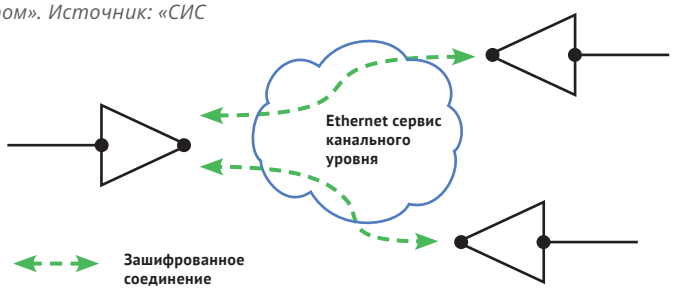
«Палиндром»

Рисунок 13. ВСШ «Палиндром-6140». Источник: «СИС Крипто».

Завершает обзор семейство высокоскоростных шифраторов (ВСШ) Ethernet серии «Палиндром». Их выпускает российская компания «СИС Крипто». Это пока единственные на российском рынке шифраторы Ethernet L2 с поддержкой алгоритмов шифрования ГОСТ. Семейство состоит из двух серий: 4000-й в двух вариантах (с портами RJ45 или гнёздами SFP) и скоростью 1 Гбит/с и 6000-й с гнёздами SFP+ и скоростью 10 Гбит/с.

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 (рис. 13).

Рисунок 14. Многоточечное соединение ВСШ «Палиндром». Источник: «СИС Крипто».



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 всём 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 (14).

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.

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, а администратор получает уведомление о взломе.

Подводим итог. Плюсы:

- высокая производительность: работа на скорости линии, низкие накладные расходы, рекордная задержка
- гибкость в поддержке технологий Ethernet
- автоматическое управление ключами
- автоматическая настройка туннелей
- разделение задач управления сетью и ИБ
- защищённое от вскрытия оборудование

Минусы:

- нет управления через веб-интерфейс
- нет встроенных средств построения VPN L3
- для реализации отказоустойчивости и масштабирования нужно внешнее сетевое оборудование

Иван Макаров

Калачева Светлана
Начальник департамента
веб-разработки ВШП г. Краснодар

Карьера в ИБ. От простого к сложному

Приветствую вас, дорогие друзья, на благотворительной ИТ-конференции по информационной безопасности. Ежегодное мероприятие журнала CIS в поддержку фонда Константина Хабенского Digital Hearts.

Так как наша тема связана с информационной безопасностью, мы решили от неё не отступать и посвятить этот семинар будущим безопасникам: коротко и по существу рассказать, с чего начать, на какую карьеру можно рассчитывать.

Эксперт

Хороший эксперт по кибербезопасности – практик, который знает, как примерно мыслит злоумышленник и какими инструментами оперирует. С 80% атак безопасники справляются с помощью уже существующих методик, а 20% – это уязвимости нулевого дня, вновь изобретённые методы взлома и т.п. Профессионал должен быть всегда начеку, для того чтобы вовремя среагировать.

Что должен знать и уметь специалист – разнится от профиля. Знать нужно много:

Архитектуру компьютера и программного обеспечения, протоколы и стандарты, несколько языков программирования, используемых в той или иной области, хорошо понимать, как устроена операционная система.

Всё это – основные принципы, без знания которых сложно будет развиваться не только в информационной безопасности, но и в ИТ в целом.

Образование

Нужно иметь техническое образование. Лучше всего – специальность, в которой есть слова «автоматизация», «безопасность», «программирование» или «математика». На сегодняшний день в каждом техническом вузе есть соответствующее направление. Вот перечень этих направлений:

- Криптография
- Компьютерная безопасность
- Организация и технология защиты информации
- Комплексная защита объектов информатизации
- Информационная безопасность телекоммуникационных систем
- Противодействие техническим разведкам
- Информационная безопасность
- Комплексное обеспечение информационной безопасности автоматизированных систем

Но необходимо помнить о том, что вузы дают мало практики, зачастую теория даётся устаревшая на сегодняшний день, а упор делается на те направления, которые с реальной работой в ИБ связаны очень отдалённо.

Инфраструктура образования активно развивается, сегодня существуют различные учебные центры, которые позволяют изучить профессию с нуля, пройти профессиональную переподготовку или повысить квалификацию. Конечно, нужно учитывать, что временные затраты при этом будут разные. Скажем, если вы системный администратор или программист, то времени, для того чтобы углубиться в новую отрасль, у вас уйдёт меньше.

Чем раньше, тем лучше. Этот тезис подходит и к началу стажировки, и к началу образования. Мир значительно меняется, ни для кого не секрет, что востребованы будут технические, инженерные специальности. Поэтому считаю разумно развивать детей именно в направлении ИТ-технологий в целом.

Оптимально проходить практику уже на старших курсах обучения.

Важно помнить, что базу знаний надо не только набрать, но и постоянно пополнять. Если человек достигший определённых высот, начинает думать, что он всё знает, происходит стагнация, и в скором времени находится тот, кто не останавливался в развитии и, разумеется, достигнет большего. Саморазвитие – один из важных процессов профессионального самосовершенствования.

Очень важен наставник-ментор – это, скорее всего, старший специалист или руководитель, который будет вводить в курс дела, рассказывать о практических особенностях и объяснять, какие ошибки вы можете допустить.

Наиболее важные специальности в ИБ?

Здесь много возможных вариантов ответа, поскольку специальности можно делить на разные типы и разновидности. Кроме того, можно долго спорить, какие направления в ИБ главнее. Поэтому сделаем субъективное выделение трёх важных направлений работы:

Пентестер

Без навыков системного администратора, программиста в области пентестера делать нечего.

Мы живём в мире приложений, они везде: в смартфоне, ноутбуке, на стационаре и даже в холодильнике. К сожалению, далеко не все разработчики ПО имеют более или менее продвинутые навыки в информационной безопасности. А если и так, то уязвимость может возникнуть при взаимодействии, например фронтенда приложения с бэкендом. Ошибки могут быть и в написанном коде. Эксперт, который может подсказать, как защитить приложение или сервис от взлома, – весьма ценный специалист.

Специалист по безопасной разработке приложений

Такой эксперт уже не просто ищет потенциальные уязвимости, используя готовые инструменты или тулзы

собственной разработки. Он способен разобраться в коде проектов, написанных на разных языках программирования, определить типовые ошибки кода и указать разработчикам на их наличие. В своей работе специалист использует различные инструменты, использует статический и динамический анализ кода, знает разные инструменты и способен выступать в качестве эксперта для команды разработки. Он может указать разработчикам на потенциально уязвимые части кода, которые необходимо переписать.

Специалист по ИБ широкого профиля

Здесь речь о профессионалах, которые могут быть экспертами в 2-3 направлениях информационной безопасности и хорошо разбираться ещё в 4-5 смежных. Такие профессионалы могут погружаться в экспертизу и выступать в качестве консультантов или архитекторов сложных высоконагруженных проектов.

Это три наиболее крупных ответвления в сфере ИБ, но не забываем, что первая ступень в любой профессии – должность стажёра!

Сертификация

В сфере информационной безопасности среди атрибутов, позволяющих другим причислять вас к серьёзным специалистам, являются такие статусы, как:

- Сертифицированный специалист по ИБ
- Сертифицированный ИТ аудитор
- Сертифицированный Менеджер по ИБ и др.

Для получения сертификата специалистам необходимо успешно сдать экзамен. Допуск к экзамену получают специалисты, у которых опыт работы в соответствующей сфере минимум 5 лет. Экзамены длятся порядка 4-6 часов, за это время специалисту будет задано около 150-250 вопросов, стоимость таких экзаменов примерно 600-750 $.

Для кого сертификат?

CISSP

Обладатель CISSP должен прекрасно ориентироваться в актуальных течениях информационной безопасности в области менеджмента ИБ. Опыт администрирования средств защиты информации или этичного взлома компьютерных сетей будет, бесспорно, полезен, но на экзамене никто не потребует вспомнить какую-то определённую настройку или команду какой-либо системы, так как сертификация не зависит от какого-либо вендора. Так же специалист должен понимать, какие используются алгоритмы шифрования, хэширования и т. п.

CISA

Обладатель CISA должен не только хорошо ориентироваться в области информационной безопасности, но и в ИТ-менеджменте, жизненном цикле информационных систем и в том, как это всё проверять на соответствие лучшим мировым практикам. В идеале соискателю данного сертификата надо пройти жизненную школу в крупной компании, в которой есть полноценная группа или отдел ИТ-аудита.

CISM

Если обладателем CISSP может быть недавний выпускник вуза, работающий с «железом» и софтом, то CISM уже для людей, занимающихся менеджментом в области ИБ не первый год. Доменов в CISM меньше, чем в CISSP, и сдать его человеку, уже сдавшему CISSP, проблем не составит.

Все сертификаты, полученные специалистом, говорят о его опыте в определённой сфере ИБ.

Работа

Без сотрудников по информационной безопасности сегодня не могут обойтись ни коммерческие структуры, ни ведомственные организации, такие как:

- Внутренняя ИБ (государственная и коммерческая организация)
- Консалтинг/Интегратор
- Производители СЗИ
- Дистрибьютор СЗИ
- SOC
- Стартап
- Учебный центр
- Регулятор
- Правоохранительные органы

Рынок труда

Спрос на специалистов по ИБ есть, и к этому спросу необходимо создать хорошее предложение.

Нужно понимать в целом нюансы прохождения собеседования.

На должность безопасника преимуществом будет:

- наличие сертификатов
- высшее образование
- знание основных методик классификаций и международных практик
- навыки выявления угроз ИБ на основе сведений об уязвимостях
- знание нормативной базы в части защиты информации: законов и иных нормативных правовых актов РФ, регулирующих отношения, связанных с защитой информации ограниченного доступа (не относящейся к гостайне), руководящих документов ФСТЭК, ФСБ, в том числе по защите банковской тайны, коммерческой тайны
- наличие лидерских качеств, умение добиваться поставленных целей, инициативность, активность, навыки самоорганизации, ответственность
- умение программировать на одном или нескольких скриптовых языках
- экспертные знания профильного ПО
- экспертные знания в узкоспециализированных системах
- опыт разработки собственных средств/утилит/методик
- опыт разработки технической и аналитической документации
- опыт проведения статистических исследований
- опыт расследования инцидентов безопасности, сбор доказательной базы
- владение английским языком будет плюсом

Заключение

Защита информации для участников рынка становится одной из приоритетных задач. Обеспечить такую защиту только автоматизированными средствами практически невозможно. Востребованность специалистов в сфере ИБ растёт с той же скоростью, с которой развиваются и сами информационные технологии. Информационная безопасность изобретена не напрасно, и на этой ноте я закончу свой доклад.

Калачева Светлана

начальник департамента веб-разработки ВШП г. Краснодар

www.it-proger.com

Кейс «Как адаптироваться к изменениям рынка ЭП с выгодой для бизнеса»

Компания: представитель МСП, лицензиат ФСБ.
Цель компании: получение прибыли за счёт укрепления позиций организации на рынке ЭП и превентивной адаптации к законодательным изменениям.
Способы достижения цели: модернизация бизнес-процессов и присоединение к партнёрской сети удостоверяющего центра «Основание».
Спикер: инженер СКЗИ ООО «ТриНити» Михин Максим, специальность «Прикладная информатика», специализация «Криптография в продуктах 1С».

О компании

ООО «ТриНити» основано в 2002 году, в данный момент штат компании составляет 10 человек, которые занимаются сопровождением информационных систем и программных продуктов, использующих средства криптозащиты информации.

ООО «ТриНити» – лицензиат ФСБ с 2008 года. ОКВЭД 62.09. Деятельность компании связана с использованием вычислительной техники и информационных технологий.

Клиенты ООО «ТриНити», использующие сертификаты удостоверяющего центра «Основание»:

- местное самоуправление Забайкальского края: руководители глав администраций 28 районных центров, 200 глав сельских и городских поселений, руководители комитетов по имуществу;
- представители силового блока: СУ СК, УМВД, УФСИН, УФО Минобороны по Забайкальскому краю, сотрудники Россельхозбанка, Связьбанка;
- коммерческие организации и индивидуальные предприниматели региона.

Ситуация на рынке

Согласно Федеральному закону от 27 декабря 2019 года № 476-ФЗ «О внесении изменений в Федеральный закон «Об электронной подписи» и статью 1 Федерального закона «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля», **рынок электронной подписи ждут кардинальные изменения**. Подробнее о них можно прочитать в 11 номере журнала CIS (стр. 58-60) или на Едином портале Электронной подписи в разделе «Статьи».

Коротко о главном: в связи с предстоящим переносом вступления в силу некоторых положений Федерального закона от 27.12.2019 № 476-ФЗ на более поздний срок коммерческие удостоверяющие центры вправе будут выдавать квалифицированные сертификаты ключа проверки электронной подписи (КСКПЭП) только физическим лицам начиная с 01 января 2022 года.

С 01 июля 2020 года для получения аккредитации по новым правилам УЦ должны соответствовать следующим требованиям:

- минимальный размер собственных средств (капитала) не менее 1 млрд рублей либо 500 млн рублей при наличии не менее чем в трёх четвёртых субъектов РФ одного или более филиала или представительства УЦ;
- наличие финансового обеспечения ответственности в сумме не менее чем 100 млн и 500 тысяч рублей за каждое место осуществления лицензируемого вида деятельности (всего на сумму не более 200 млн рублей).

Введение обязательного соответствия требованиям к деловой репутации руководителя и учредителей (участников) УЦ, а также разделение аккредитации на 2 этапа намечено на 01 января 2021 года.

Цель компании

ООО «ТриНити» поставило перед собой **цель сохранить и развить бизнес, связанный с выпуском КСКПЭП,** в качестве одного из источников доходов компании, для чего требовалось качественно улучшить текущие бизнес-процессы и адаптироваться к ожидаемым законодательным изменениям.

Действия компании

С момента появления первого проекта поправок, затрагивающих Федеральный закон «Об электронной подписи», стало понятно, что для достижения указанной цели необходимо перевести бизнес на новый уровень.

На подготовительном этапе потребовалось:

- расширить список проектов по консультационно-технической поддержке клиентов;
- разработать модель сопровождения 24 часа в сутки.

Инструментами для решения поставленных задач стали внедрённые:

- современная CRM-система для десктоп и мобильных платформ;
- SIP-телефония (англ. Session Initiation Protocol) – технология телефонной связи, организованной через интернет, включающей в себя функции обычной телефонии: определение номера, записи разговоров, переадресация, распределение звонков и другое.

Благодаря принятым мерам время реакции на обращения в техническую поддержку сократилось с нескольких часов до нескольких минут. Это позволило завоевать репутацию компании, оперативно решающей любую поставленную клиентами задачу.

Скорость и качество работы, а также смещение в сторону первичного обучения, консультирования и внедрения ИТ-решений запустило так называемое «сарафанное радио». Клиенты стали обращаться к ООО «ТриНити» по рекомендации людей своего личного или делового круга.

Один из секретов успеха

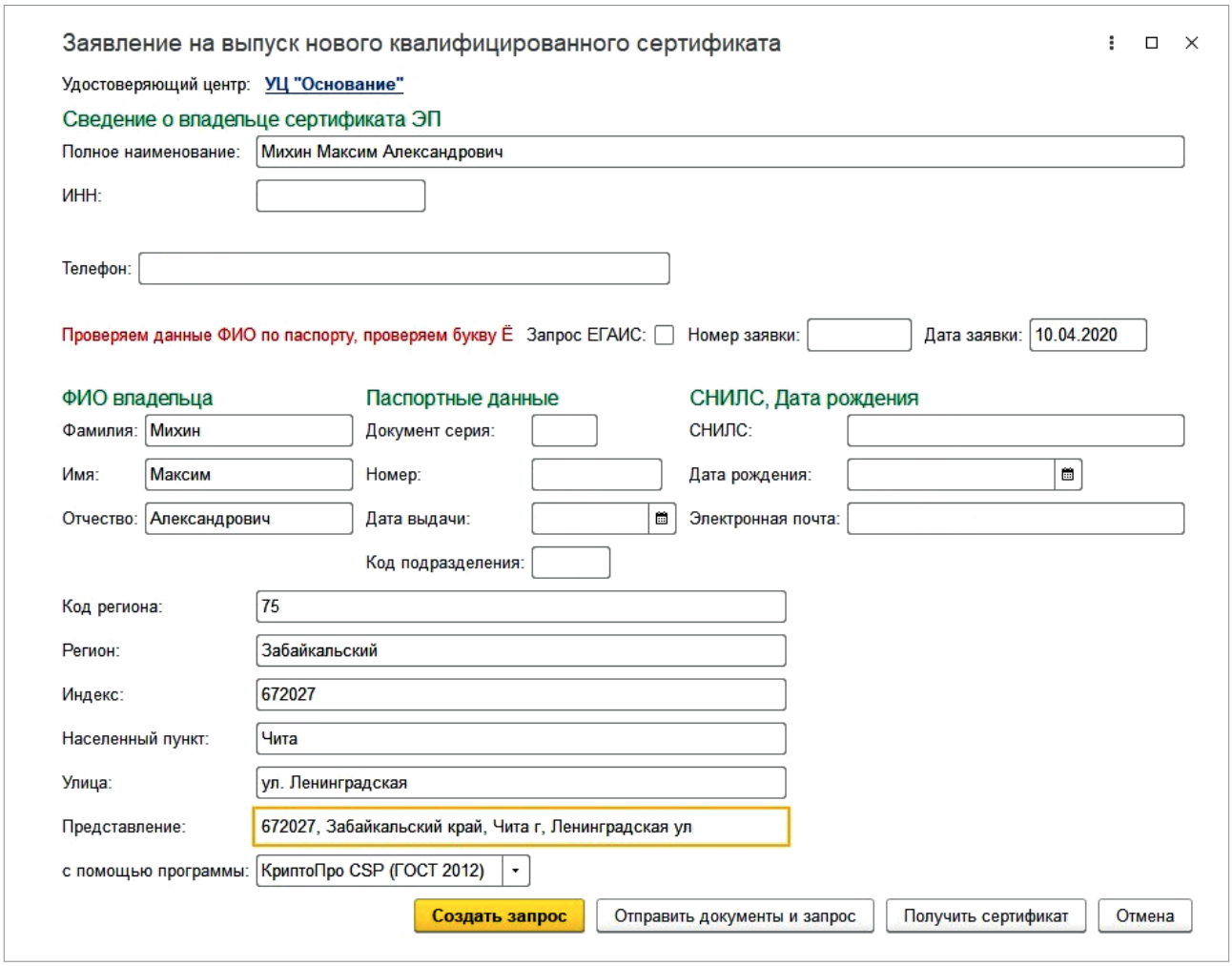
Выстраивание долгосрочных отношений с клиентами за счёт обеспечения различных видов сервиса и дальнейшего обслуживания – более эффективный и надёжный источник прибыли, чем попытка продать продукт по максимальной цене. Подобная деятельность требует и новых партнёрских отношений с теми, кто способен оперативно реагировать на новые изменения и вызовы, предлагать гибкие схемы сотрудничества. Таким партнёром стал удостоверяющий центр «Основание».

Справка:
Удостоверяющий центр «Основание» – УЦ, созданный компанией «РТ-Проектные Технологии» госкорпорации «Ростех» и группой компаний «Селдон». Одна из целей УЦ «Основание» сохранить бизнес добросовестных участников рынка электронной подписи, объединяя их под общим брендом.

Сохранение и развитие бизнеса, связанного с выпуском КСКПЭП

Для сохранения и развития бизнеса на рынке электронных подписей задач, решённых на подготовительном этапе, оказалось недостаточно.

В том числе в связи с законодательными изменениями и высокой конкуренцией на этапе реализации потребовалось:



- присоединиться к партнёрской сети УЦ «Основание»;
- внедрить модуль формирования заявления на выпуск КСКПЭП;
- интегрировать модуль в 1С.

Помощь в решении поставленных задач оказали специалисты УЦ «Основание».

Инженер ООО «ТриНити» Михин Максим: «Моей задачей как инженера была разработка модуля формирования заявления на выпуск КЭП для типовых конфигураций 1С. Сейчас он используется на аттестованном рабочем месте для генерации клиентом ключевой пары и запроса на выпуск сертификата электронной подписи. Запрос передаётся через API в web-интерфейс УЦ «Основание».

Этот модуль можно интегрировать как в учётную систему партнёра УЦ (в нашем случае мы используем «1С: Управление торговлей», версию 11), так и использовать его как внешнюю обработку в учётной программе 1С клиента. В таком случае, клиент уже **со своего рабочего места** может сгенерировать ключевую пару, подписать его своим действующим сертификатом, направить запрос и после проверки документов представителем УЦ получить ответ в виде готового сертификата и его печатной формы.

Внедрение этой системы позволяет экономить время при заполнении полей в форме заявления на выпуск КЭП, так как некоторые общедоступные сведения уже содержатся в базе наших клиентов, при этом отправка документов тоже осуществляется непосредственно из 1С. Эта обработка позволяет всегда видеть заполняемые данные, а не скроллить страницу web-интерфейса и не переключаться между вкладками сайта, как это было до внедрения системы. При этом в своей форме можно настроить проверку правильности заполнения некоторых данных, что уменьшит вероятность допущения ошибки из-за человеческого фактора.

Внедрение разработанной системы оптимизировало работу инженеров и повысило эффективность работы нашей компании».

Преимущества модуля:

- удобство использования;
- экономия времени клиента, УЦ и партнёра УЦ.

Основание
Удостоверяющий центр

*Подробнее о партнёрской программе **УЦ «Основание»** можно узнать:*

- отправив заявку на электронную почту partners@iecp.ru;
- позвонив по телефону 8-800-511-70-50.

Преимущества партнёрской программы УЦ «Основание»:

- *условия направлены на максимизацию прибыли партнёра;*
- *индивидуальный подход, в том числе возможность брендировать онлайн-сервис для работы с КСКПЭП в соответствии с цветовой гаммой и символикой партнёра.*

Ознакомиться с подробным обзором законодательных изменений рынка ЭП, а также с подзаконной нормативной базой, которая будет принята с целью реализации новелл, можно на Едином портале Электронной подписи iEcp.ru.

Ауди Центр Таганка
+7 (495) 755-81-81
Михайловский пр-д, 3
www.audi-taganka.ru

Ауди Центр Варшавка
+7 (495) 755-88-11
Варшавское ш., 91А
www.audi-warshavka.ru

Ауди Центр Восток
+7 (495) 755-82-82
г. Балашиха, ш. Энтузиастов, д. 12Б
www.audi-vostok.ru

Чувство стиля. Не требует доказательств

Безупречные материалы отделки
в сочетании с прогрессивными решениями

Автомобиль, показанный в рекламе, оснащен дополнительным оборудованием, которое устанавливается за отдельную плату. Реклама.

Продукты Thales получили сразу 3 высшие награды 2020 Cybersecurity Excellence Awards

В номинации «Облачная безопасность» золотая награда досталась продукту для управления ключами в мультиоблачных средах **CipherTrust Cloud Key Manager** (CCKM). Миграция конфиденциальных данных в мультиоблачные среды вызвала спрос на решения для шифрования, ведь шифрование в сочетании со средствами управления ключами – это мощный инструмент для обеспечения защиты данных и соответствия нормативам. Средства шифрования, предлагаемые облачными провайдерами, обычно используются по модели «принеси свой ключ» (Bring Your Own Key), благодаря чему заказчики сохраняют контроль над своими данными. Однако по мере роста количества облачных провайдеров и объёма данных в облаках растёт и сложность управления ключами. CipherTrust Cloud Key Manager снижает эту сложность благодаря FIPS-совместимым ключам, автоматизации типичных операций и прозрачным для аудита отчётам. Продукт повышает эффективность работы ИТ-службы, обеспечивая автоматическую ротацию ключей по графику или по их устареванию, централизует управление ключами в мультиоблачных средах, в том числе ключами, созданными в консолях облачных провайдеров, и, храня ключи в их источнике, предотвращает потери данных из-за случайного удаления ключей в консоли.

Продукт **Vormetric Transparent Encryption** (VTE) был отмечен золотом в номинации «Шифрование». Он позволяет обойти проблему выбора между безопасностью и эффективностью хранения данных, которая возникает из-за того, что шифрование нарушает работу технологий сжатия и дедупликации. Благодаря безопасному обмену ключами между Vormetric Transparent Encryption for Efficient Storage (VTE-ES) и внешними системами хранения, зашифрованные данные с компьютеров под управлением VTE могут быть проанализированы, сжаты и дедуплицированы, а затем записаны на диски в зашифрованном виде. Pure Storage FlashArray – это первая совместимая с VTE-ES система хранения данных. В результате заказчики получили первое в отрасли решение, которое сочетает сквозное шифрование с экономичностью хранения Pure Storage.

Наконец, в номинации «Управляемые сервисы безопасности» победила служба **SafeNet Data Protection On Demand** (DPOD). Это облачная платформа с широким набором сервисов безопасности по требованию, доступных через простой онлайн-магазин. С её помощью можно быстро выбрать нужный тип защиты, развернуть сервисы, добавить политики безопасности и собрать отчёты. Облачная служба ориентирована на рынок управляемых услуг безопасности (она позволяет их провайдерам предлагать защиту данных как услугу) и, благодаря поддержке сторонних API, легко встраивается в уже развёрнутые собственные платформы этих провайдеров. Data Protection On Demand не привязана к какой-то одной облачной инфраструктуре, обеспечивает многоуровневое управление с полным разделением обязанностей, в том числе в средах с несколькими уровнями дочерних организаций (виртуальными сервис-провайдерами).

Премия Cybersecurity Excellence Awards – это ежегодный конкурс, награды в котором присуждают профессионалам, продуктам и компаниям, демонстрирующим свои преимущества, инновации и лидерство в области информационной безопасности.

TESSIS
TECHNOLOGIES SYSTEMS AND SOLUTIONS FOR INFORMATION SECURITY

***TESSIS** – официальный дистрибьютор в России.*

www.tessis.ru

CIS / № 2 (12) / 2020 / www.cis.ru

Цифровая система здравоохранения до и после COVID-19

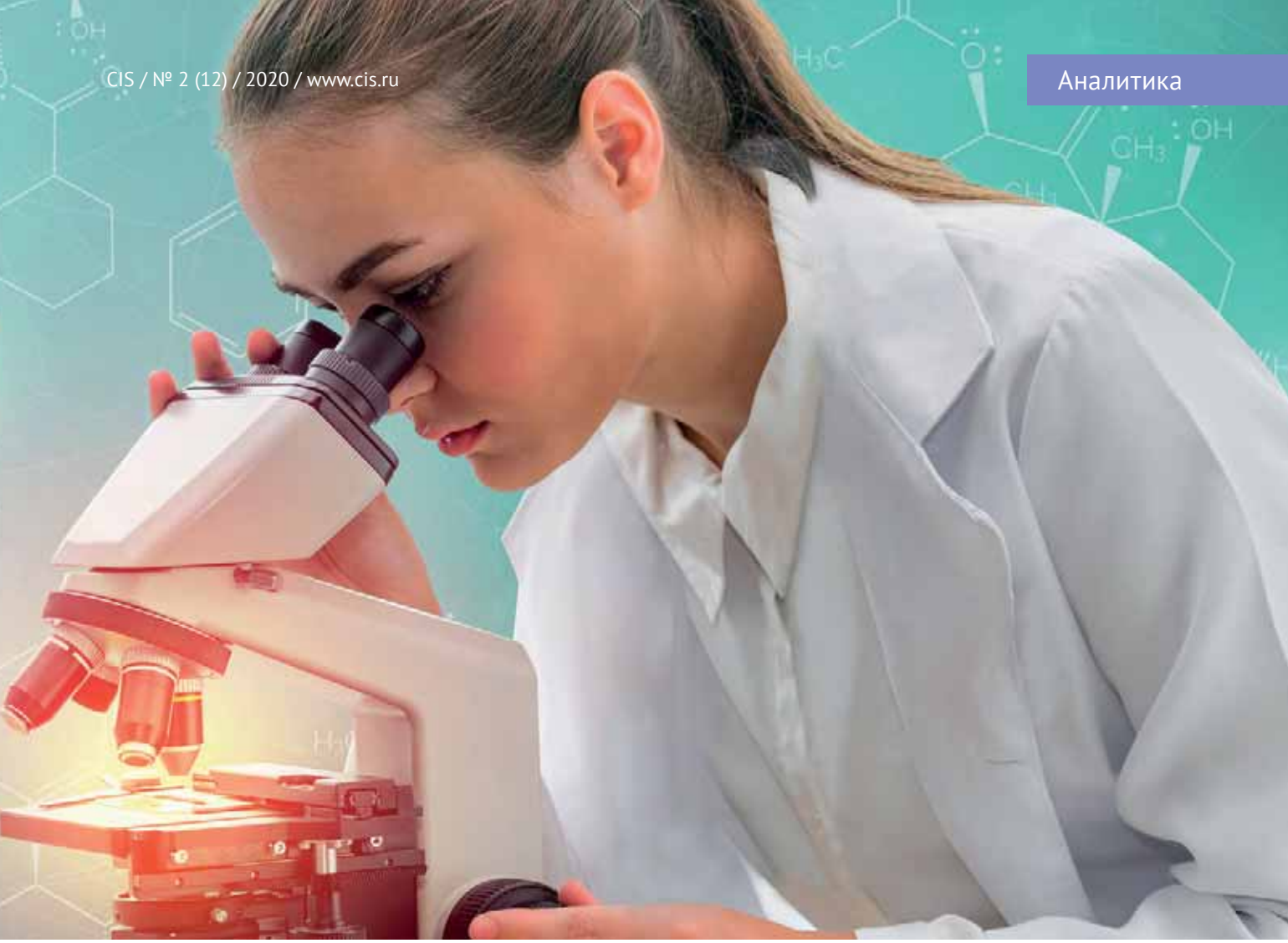
Буквально год назад, а именно в 2019 году, мы все смотрели с оптимизмом на те положительные «цифровые» тенденции, которые отражала современная система здравоохранения Российской Федерации, находящаяся, так сказать, в тренде ускоренного инновационного «цифрового» развития, в котором планировались к применению радикально новые механизмы регулирования системы здравоохранения на уровне государства.

Ещё не так давно ситуация в отрасли здравоохранения была такова, что по всей стране происходила повсеместная автоматизация и информатизация, а именно: внедрение новых медицинских, телемедицинских и информационных технологий, систем электронного документооборота, единой медицинской электронной карты, личного кабинета пациента, рабочего места врача и медицинской сестры, электронных рецептов и больничных листов, электронных информационно-аналитических и обучающих систем, автоматизированных систем контроля качества, системы оценки удовлетворённости граждан качеством работы медицинских организаций и так далее. И это только было хорошим началом бурного процесса трансформации отрасти.

Но! Волей судеб в 2020 году ситуация радикально изменилась не только в России, но и во всём мире. И этому есть много причин, но две из них основные – это COVID-19 (или как мы его все называем «коронавирус») и глобальная перестройка всей мировой экономической системы, в основе которой лежат исключительно интересы мировых элит.

Незадолго до ситуации с COVID-19, ещё в начале 2020 года, российская система здравоохранения планировала в своём развитии сделать акцент на технологии четвёртой промышленной революции и широко использовать технологии обработки больших массивов данных (так называемая Big Data) и искусственный интеллект, например в системах диагностики и помощи в принятии решений. В медицине планировалось широкое применение новых био-, нано-, нейро- и других технологий. Также планировалось широко использовать новые вычислительные технологии, технологии дополненной реальности и применение различных роботизированных систем и нанороботов.

В ближайшие пять лет должны были быть сформированы «цифровые контуры» субъектов Российской Федерации, которые функционировали бы в рамках единого информа-



ционного пространства, или так называемой цифровой экосистемы здравоохранения. Также планировалось широкое применение носимых и имплантируемых устройств мониторинга здоровья, бионические системы, принтеры для печати живых тканей и органов и так далее.

В ближайшие семь лет должна была быть создана платформа «следующего этапа развития» – этапа «медицины сопровождения здоровых».

Но ситуация, как мы все уже с вами знаем, радикально изменилась!

И уже всем очевидно, что все инновации и «цифровые» инициативы, которые напрямую зависят от социально-экономического развития нашего с вами государства буквально растворяются в тумане небытия и призрачных перспектив ближайших десяти – пятнадцати лет…

По оценкам экспертов, ситуация с «самоизоляцией», которая парализовала всю экономику России, остановила работу крупных предприятий, привела к коллапсу тысяч компаний среднего и малого бизнеса и буквально ускорила процесс обнищания нашего населения, в конечном итоге текущая ситуация приведёт к «отскоку» в экономическом развитии нашей страны на 3-5 лет назад, а по совсем пессимистичным прогнозам, мы уже на полной скорости летим в «лихие 90-е»…

Уже сейчас (в апреле 2020-го года) мы с вами видим, что наше государство не способно взять на себя ответственность за принятие трудных решений, введя режим «чрезвычайной ситуации» или «чрезвычайного положения». На сегодняшний день в текущей ситуации оно не способно (или не хочет) обеспечить стабильную социальную и экономическую поддержку, ведь в первом случае гражданам нашей страны нужно будет выплачивать хотя бы минимальные суммы денег, для того чтобы им буквально выжить, а во втором случае направить финансирование на поддержку компаний не только среднего и малого бизнеса, но буквально во все реально нуждающиеся в помощи организации. О чём можно говорить, если наше государство не способно даже обеспечить население бесплатными медицинскими масками и гелями для дезинфекции рук? Когда вся страна находится в «добровольной самоизоляции», а врачи работают как «каторжные», рискуя своими жизнями и борясь с COVID-19, преступная халатность наших чиновников не знает границ: то они закупают тротуарные бордюры на немыслимые миллиарды, то организуют поддержку своих «646 системообразующих организаций экономики РФ».

В столь не простые времена, когда жизнь подкинула нам новое испытание в виде COVID-19, не только мы с вами, но и любая отрасль экономики Российской Федерации проходит «тест» на прочность.

В апреле 2019 года на заседании итоговой коллегии Минздрава Министр Здравоохранения Российской Федерации Вероника Скворцова сообщила, что по итогам работы в 2018 году более 15,5 тысяч медицинских организаций внедрили медицинские информационные системы, автоматизировано около 600 тысяч рабочих мест врачей, 82 субъекта Российской Федерации обеспечили интеграцию с компонентами Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ). К региональным телемедицинским системам подключено уже 6,5 тысяч медицинских организаций, а к центральным архивам медицинских изображений – 5,5 тысяч. Более 4,2 миллиона граждан воспользовались услугами и сервисами личного кабинета пациента «Моё здоровье». Успехи впечатляют, но имея весь этот арсенал, готовы ли мы были к COVID-19 и к новым вызовам?

Какова была Стратегия развития здравоохранения Российской Федерации на период до 2025 года (утверждённой Указом президента РФ от 6 июня 2019 года № 254), а её проекты и программы реализации хорошо проработаны, насколько эффективно они реализовывались и, самое главное, была ли в них заложена хоть доля, относящаяся к ситуации «форс-мажора», подобно текущей, – вот об этом мы и поговорим, с точки зрения процессов «цифровизации».

Сама по себе Стратегия – довольно сложный документ для понимания не только для специалистов в области медицины, но и специалистов в области информационных технологий. На первый взгляд, с точки зрения информационных технологий, под «соусом цифровизации» нам преподносят классическую автоматизацию и информатизацию отрасли, приправив, ничего толком не поясняя, это «блюдо» двумя бессвязными терминами – «цифровая медицина» и «электронное здравоохранение», о которых впоследствии ничего так и не будет подробно написано в Стратегии, а также добавив вишенку сверху в виде желания использовать технологии Big Data и «искусственный интеллект». Возможно, кому-то понравились термины Digital Health, eHealth, mHealth и он, не особо погружаясь в суть, на мой взгляд, самых передовых трендов развития всемирного здравоохранения, просто перевёл их на русский язык и вставил для «красного словца» в стратегию?

Но это на первый взгляд. Давайте всё по порядку подробно проанализируем.

Стратегия представляет из себя крайне интересный документ для любого специалиста в области информационных технологий, как с точки зрения понимания современных трендов развития отрасли «цифрового» здравоохранения, так и с точки зрения перспектив использования новых технологий для создания принципиально новых информационных, аналитических, роботизированных и иных систем.

Для дальнейшего анализа Стратегии развития здравоохранения Российской Федерации на период до 2025 года я убрал из неё всё (дабы не пересказывать её содержание), что не имеет, на мой взгляд, отношения к процессам автоматизации, информатизации, цифровизации и технологиям, чтобы оставить основу, которая позволит нам проникнуть в самую суть «цифровой трансформации» отрасли здравоохранения.

Начнём с того, что сама Стратегия включает в себя несколько основных разделов:

- оценку современного состояния отрасли и угрозы развития системы здравоохранения в Российской Федерации;
- цель, основные задачи, приоритетные направления, механизмы реализации развития здравоохранения;
- результаты и основные этапы её реализации.

Как отмечается в документе, Стратегия направлена на реализацию основных задач и национальных приоритетов Российской Федерации, определённых в документах стратегического планирования, и является основой для организации деятельности и взаимодействия органов государственной власти Российской Федерации, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, государственных и иных структур в сфере здравоохранения, а также она является основой для разработки отраслевых документов стратегического планирования в области обеспечения охраны здоровья граждан Российской Федерации, государственных программ Российской Федерации, государственных программ субъектов Российской Федерации, а также иных документов стратегического планирования. И это важно потому, что Стратегия уже активно используется для формирования региональных стратегий развития здравоохранения, в том числе и в части определения основных направлений для цифровой трансформации отрасли.

На основании положений Стратегии региональные стратегии развития здравоохранения ставят перед собой задачи: к концу 2024 года не менее 90% медицинских организаций должны обеспечить доступ гражданам к юридически значимым электронным медицинским документам посредством Личного кабинета пациента «Моё здоровье» на Едином портале государственных услуг и функций.

Целью Стратегии является создание условий, способствующих обеспечению доступности и качества оказания медицинской помощи населению при условии соблюдения прав граждан в сфере охраны здоровья, реализуемых в том числе в рамках единой цифровой экосистемы, объединяющей все субъекты Российской Федерации.

В качестве механизма достижения указанной цели является создание Национальной пациент-ориентированной системы здравоохранения – системы,

объединяющей все медицинские организации, независимо от формы собственности и ведомственной принадлежности, функционирующей на основе единых правил и норм с учётом особенностей и специфики выполняемых в рамках законодательства Российской Федерации задач.

В соответствии со Стратегией развития здравоохранения Российской Федерации на период до 2025 года к приоритетным направлениям развития «цифрового» здравоохранения можно отнести следующие:

1. Обеспечение доступности медицинской помощи населению.
2. Разработка и внедрение новых медицинских и информационных технологий.
3. Цифровизация здравоохранения.
4. Формирование ответственного отношения граждан к своему здоровью.
5. Развитие центров экспорта высокотехнологичных медицинских услуг.
6. Непрерывное повышение уровня квалификации медицинских работников.
7. Развитие системы управления качеством медицинской помощи.

Остановимся подробнее на разработке и внедрении новых медицинских и информационных технологий и цифровизации здравоохранения.

Разработка и внедрение новых медицинских и информационных технологий в здравоохранении будут реализованы путём:

1. Внедрения телемедицинских консультаций пациентов, врачей и медицинских организаций с ведущими специалистами национальных научно-практических медицинских центров по профилю их деятельности.

Внедрение телемедицинских технологий в здравоохранении сейчас вызывают ожесточённые споры как среди научного и медицинского сообщества, так и среди широкого населения нашей страны, которое является так называемым «потребителем» медицинских услуг.

Телемедицинские технологии – информационные технологии, обеспечивающие дистанционное взаимодействие медицинских работников между собой, с пациентами и (или) их законными представителями.

Вопросов к внедрению телемедицины на сегодняшний день больше, чем ответов. До сих пор не ясно, как врач будет ставить диагноз пациенту дистанционно даже после первичного очного приёма? Сколько это займёт времени? Как пациенту обезопасить себя от неверного диагноза или мошенников? И зачем, вообще, всё это нужно?

Сторонники телемедицины подчёркивают, что она делает врачебную помощь оперативной и при этом позволяет избежать ненужных личных обращений к докторам. А значит, сократить и очереди, и время пребывания в клиниках, а также дополнительные затраты на медицинские услуги. Кроме того, услуги можно будет получать из любой точки мира.

Но! Телемедицина – это не медицина реального времени.

А значит, вопросов остаётся ещё много…

2. Расширения перечня высокотехнологичных методов лечения заболеваний посредством внедрения новых технологий лечения на основе ядерной медицины, персонализированной фармакотерапии, редактирования генома, создания национальной системы биобанков, коллекций биологических материалов.

На этом пункте хочется остановиться хотя бы потому, что в 2011 году я уже сталкивался с задачей создания «цифровой памяти», и в процессе её реализации мы интересовались возможностями оцифровки и анализа ДНК.

Я не буду останавливаться на морально-этических проблемах процесса редактирования генома, но хочу отметить, что на сегодняшний день уже разработана и совершенствуется технология редактирования человеческого генома – «молекулярные ножницы» (CRISPR-Cas9), которая широко применяется учёными России. Даже компания Netflix выпустила на эту тему документальный фильм из четырёх серий под названием «Неестественный отбор» (Unnatural Selection).

3. Предоставления пациентам услуг персонализированной медицины.

Цифровизация здравоохранения будет реализована путём создания, внедрения и развития:

4. Федеральной государственной информационной системы «Единая государственная информационная система в сфере здравоохранения» (ЕГИСЗ) и её ключевых компонентов, функционирующей в рамках Национальной пациент-ориентированной системы здравоохранения с целью обеспечения единого информационного пространства в сфере здравоохранения для реализации информационной поддержки деятельности врачей и медицинских работников, преемственности оказания медицинской помощи, электронных сервисов и суперсервисов для граждан, а также для информационной поддержки деятельности органов управления здравоохранением.
5. Дополнительных подсистем ЕГИСЗ, в том числе системы нормативно-справочной информации и интегральной электронной медицинской карты, внедрение электронного медицинского документооборота, электронных сервисов и суперсервисов для граждан и информационных систем, обеспечивающих поддержку деятельности медицинских работников.
6. Комплексной аналитической системы сбора, хранения, обработки и анализа больших массивов информации (это и есть Big Data) в ЕГИСЗ.

7. Информационных систем поддержки принятия врачебных решений, в том числе с использованием технологий искусственного интеллекта (машинного обучения).

Внедрение искусственного интеллекта в медицине – это один из важнейших современных трендов развития мирового здравоохранения. Технологии искусственного интеллекта в корне меняют мировую систему здравоохранения, позволяя кардинальным образом переработать систему медицинской диагностики, разработку новых лекарственных средств, а также в целом повысить качество услуг здравоохранения при одновременном снижении расходов для медицинских клиник.

Искусственный интеллект применяют для диагностики и прогнозирования заболеваний, выявления групп пациентов с высоким риском заболеваний, организации профилактических мер, автоматизации и оптимизации процессов в больницах, управления ценообразованием, снижения различных рисков для пациентов, адаптации терапии и состава лекарств для каждого отдельного пациента, использования виртуальных ассистентов для построения маршрута пациента в медучреждениях и так далее. Искусственный интеллект также активно применяется и в исследованиях развития методик диагностики рака.

Как отмечают специалисты Microsoft, искусственный интеллект является двигателем четвёртой промышленной революции и сердцем цифрового преобразования, трансформируя государство, общество и бизнес. К 2030 году глобальный рынок искусственного интеллекта будет стоить до 15,7 триллионов долларов США.

На сегодняшний день над разработкой искусственного интеллекта и задачами машинного обучения в системе здравоохранения работают такие мировые ИТ-гиганты, как Microsoft (Microsoft Azure), Google (Google DeepMind Health), IBM (IBM Watson Health), Apple и Amazon.

Систему IBM Watson Health используют для диагностики раковых заболеваний или проблем с сердцем клиники США, Индии и Таиланда. Российская разработка TeleMD создана для диагностики и анализа опасности возникновения раковых заболеваний. Google DeepMind Health работает в британской офтальмологической клинике, выявляет некоторые глазные болезни и рекомендует, как их лечить. Microsoft широко применяет искусственный интеллект в Индии для диагностики рака и так далее.

8. Инновационных методов скрининга и мониторинга состояния здоровья, включая дистанционные и мобильные приложения с целью развития персонализированной медицины, основанной на современных научных достижениях.

Вот оно, господа!

То, что никак в Стратегии фактически не раскрыто.

Встречайте – Медицинская носимая электроника и mHealth.

Медицинская носимая электроника – это носимые или портативные устройства (умные часы или очки, браслеты, фитнес-трекеры, умная одежда и т.д.), применяемые в целях здравоохранения, которые используют датчики для мониторинга, анализа и фиксации изменений в организме. Такие устройства позволяют людям контролировать уровень сахара в крови, температуру тела, артериальное давление, пульс, производить оценку вариабельности сердечного ритма, осуществлять трекинг частоты дыхания, регистрировать состояние организма во время сна, следить за диетой и калорийностью потребляемых продуктов и многое другое.

По данным Global Market Insights, свыше 20% расходов на медицинские носимые гаджеты в 2018 году пришлось на решения для лечения сахарного диабета. Около 43% медицинских носимых устройств в 2018 году были приобретены для занятия спортом и фитнесом.

В 2018 году аналитики IDC насчитали 172,2 миллиона носимых устройств, поставленных на мировой рынок.

mHealth (мобильное здравоохранение) – это ряд мобильных технологий, систем, сервисов и приложений, установленных на мобильных устройствах и использующихся в медицинских целях и для обеспечения здорового образа жизни человека и мотивации людей к здоровому образу жизни и формированию новой «цифровой» культуры здоровья.

Приложения mHealth можно использовать для общего отслеживания состояния здоровья и физической подготовки, удалённого мониторинга пациентов, консультаций, ведения болезней и т.д. Наибольшая польза от таких приложений заключается в совместном использовании с различными носимыми устройствами.

В 2019 году Zion Market Research опубликовала новый отчёт под названием «Рынок приложений mHealth по типу». Согласно отчёту мировой рынок приложений мобильного здравоохранения был оценён примерно в 8 млрд долларов США в 2018 году, и ожидается, что к 2025 году он составит около 111,1 млрд долларов США, при среднегодовом темпе роста около 38,26% между 2019 и 2025 годами.

Как отмечает Zion Market Research все приложения можно разделить на две группы:

- Приложения для здоровья. Приложения для фитнеса и общего здоровья, приложения для управления лекарствами, приложения для учёта личных болезней, приложения для здоровья женщин и др.

- Медицинские приложения. Приложения для непрерывного медицинского образования, приложения для медицинских справок, приложения для консультаций и коммуникаций, а также приложения для мониторинга и управления пациентами.

9. Киберпротезов и человеко-машинных интерфейсов.
10. Геоинформационной системы мониторинга территориальной доступности медицинской помощи населению для выявления зон риска в субъекте Российской Федерации и в каждом населённом пункте.
11. Информационно-аналитической системы медицинских консультаций с применением телемедицинских технологий между медицинскими организациями и специалистами разного профиля.
12. Региональных централизованных информационных систем органов управления здравоохранением субъектов Российской Федерации, обеспечивающих информационное сопровождение процессов организации медицинской помощи и управления в сфере здравоохранения, в том числе межведомственное взаимодействие.

Суммируя всё вышесказанное, хочется ещё раз отметить тот факт, что реализация процесса формирования «цифровых контуров» субъектов Российской Федерации, которые будут функционировать в рамках единого информационного пространства, или так называемой цифровой экосистемы здравоохранения, в связи с COVID-19, скорее всего, растянется на ближайшие десять – пятнадцать лет. Мы должны отдавать себе отчёт в том, что формирование «цифровых контуров» не определяется лишь числом компьютеров, подключённых к ЕГИСЗ.

На сегодняшний день большинство медицинских организаций не только не дооснащены необходимым телекоммуникационным оборудованием, локальными вычислительными сетями, серверным оборудованием, компьютерами и программным обеспечением, необходимых для медицинских работников, но им буквально не хватает медицинского и рабочего персонала, чтобы оказывать услуги на хоть сколь-нибудь приемлемом уровне. Ситуация с COVID-19, как шторм, вынесла на берег все проблемы нашей системы здравоохранения на поверхность. О какой «цифровизации» можно говорить, если в больницах не хватает аппаратов ИВЛ, да, что там аппаратов – буквально нет масок и средств дезинфекции.

Согласно методическим рекомендациям Роспотребнадзора МР 3.1.2.0139-18 о критериях расчёта запаса профилактических и лечебных препаратов, оборудования, индивидуальных средств защиты и дезинфекционных средств для регионов на период пандемии гриппа, утверждённых главным государственным санитарным врачом 10 декабря 2018 года, на 1 млн жителей требуется до 200 аппаратов ИВЛ. Расчёты делались на основании данных о пандемии гриппа A (H1N1) pdm092009 года. На конец марта 2020 года в Москве насчитывалось 6414 аппаратов ИВЛ, что как минимум вдвое меньше необходимого количества.

Также предстоит огромная работа по разработке и совершенствованию самой ЕГИСЗ и её супер-сервисов, созданию инфраструктуры хранения и обработки информации, обеспечению информационной безопасности, подготовке квалифицированных и компетентных кадров и многое другое. Тем не менее все эти задачи вполне решаемы, а самое главное, перспективы использования технологий четвёртой промышленной революции, такие как новые вычислительные технологии в обработке Big Data, искусственный интеллект и робототехника, дополненная реальность, новые материалы и т.д., дают поистине неограниченное поле деятельности для развития цифровой экосистемы здравоохранения в ближайшее десятилетие.

Следующим за этим этапом развития экосистемы станет цифровая трансформация трёхуровневой системы организации оказания медицинской помощи, использующей в своей основе ЕГИСЗ, в новую «сетевую» модель, которая будет работать на новой платформе «следующего этапа развития» – этапа «медицины сопровождения здоровых».

Говоря о цифровой трансформации системы здравоохранения и создании Национальной пациент-ориентированной системы здравоохранения, мы должны отдавать себе отчёт в том, что успешное формирование и развитие цифровой системы здравоохранения Российской Федерации, определяемое Стратегией развития здравоохранения Российской Федерации на период до 2025 года, во многом зависит не только от используемых технологий четвёртой промышленной революции, но и по большей части от общего уровня социально-экономического развития страны в целом, от преодоления проблем «цифрового неравенства», а также от тех процессов, которые определяют развитие «информационного общества» и «цифровой экономики» Российской Федерации.

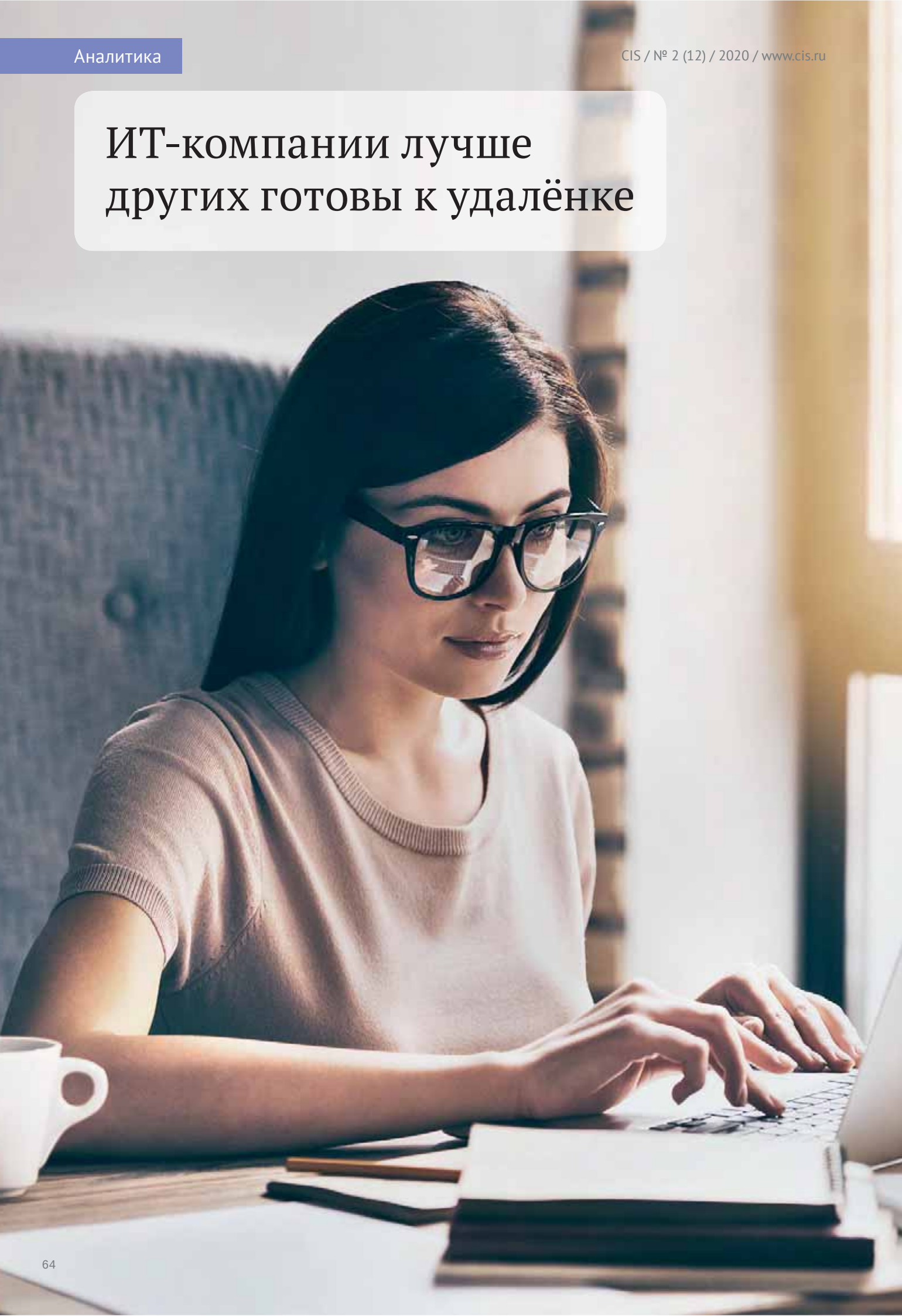
Интересной особенностью данного периода времени является и то, что текущие вызовы показали, насколько эффективно работает ИТ-инфраструктура большинства медицинских и других учреждений в России.

Очевидно, что с окончанием «истории коронавируса» и COVID-19, начнётся другая история для новой цифровой трансформации. Будут разработаны новые отраслевые и корпоративные стратегии. Много «ИТ-мишуры» будет выкинуто на «свалку» и произойдёт повсеместное обновление ИТ-инфраструктур, будут внедряться принципиально новые подходы и ИТ-системы, которые станут основой трансформации всего делового климата в России.

Автор: Александр Чесалов

CIS / № 2 (12) / 2020 / www.cis.ru

ИТ-компании лучше других готовы к удалёнке



Из-за экстренного перехода на удалённую работу на закупку и внедрение решений для защиты от кибератак и кражи данных у предприятий не было времени. Поэтому в зависимости от бюджетов компаний используются различные решения. Тем, чьи сотрудники уже трудились удалённо, перевести персонал на домашнюю работу было проще. Процесс практически безболезненно прошёл и для компаний с достаточными компетенциями в сфере информационных технологий и кибербезопасности: им потребовалось только масштабировать сервис.

Треть персонала покинула рабочие места

По данным мартовского опроса Аналитического агентства «Национального агентства финансовых исследований» (НАФИ), треть компаний перевели персонал на дистанционную работу. 11% смогли наладить «дистанционку» для всех сотрудников. Лучше с задачей справились средние и крупные предприятия.

Согласно результатам апрельского исследования Positive Technologies, проведённого среди ИТ-специалистов и специалистов по информационной безопасности, лидерами по готовности к дистанционному режиму работы оказались ИТ-компании. У 63% таких организаций режим home-office использовался и до введения ограничительных мер. В сфере телекоммуникаций готовность оценена в 54%, в финансовой – 46%, в промышленности – 32%, в ТЭК – 26%, в госструктурах – 24% (рис. 1).

29% респондентов потратили на организацию дистанционных рабочих мест и обеспечение их защиты менее 1 млн руб., 23% – от 1 до 3 млн руб., 11% – от 3 до 5 млн руб., 9% – от 5 до 10 млн руб. и 4% – более 10 млн руб. (рис. 2) Такие цифры приводятся в мартовском исследовании ESET. По оценке компании «Инфосистемы Джет», создание одного виртуального рабочего места (VDI; с хранением данных в ЦОД) обойдётся предприятию от 2 тыс. долларов. Такими средствами располагают банки, страховые компании, индустриальные предприятия.

Дома остаются не все

Компании или владельцы информации сами решают, кого переводить на удалёнку. По мнению экспертов, для собственного спокойствия компаниям лучше, когда сотрудники, работающие с расчётными счетами и системами «клиент-банк», переведены на «домашнюю» работу.

Точно не получится перевести на дистанционную работу персонал, взаимодействующий с системами, аттестованными на соответствие требованиям информационной безопасности, считает **Михаил Смирнов**, директор экспертно-аналитического центра ГК InfoWatch.

К таким, например, относятся государственные ИТ-системы. «В данном случае требования предъявляются не только к защите рабочего места, компьютера и ПО, но и доступа в помещение. В квартире полностью соблюсти эти требования не получится. Кроме того, в соответствии с рекомендациями ФСТЭК России, нельзя предоставлять удалённый доступ для управления режимами функционирования промышленного (технологического) оборудования (устройств) – значимыми объектами критической информационной инфраструктуры», – объяснил он.

Перевести на home-office можно любого работника, уверен **Дмитрий Ковалёв**, руководитель отдела технологической экспертизы управления информационной безопасности Softline. Но от критичности информационных систем и оборудования зависят меры по обеспечению безопасности удалённого рабочего

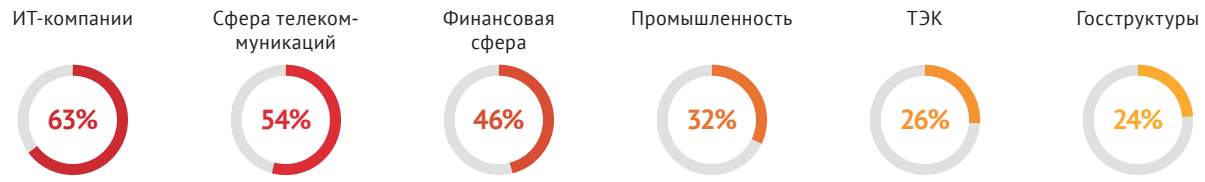


Рис. 1. Готовность к дистанционному режиму согласно результатам апрельского исследования Positive Technologies.

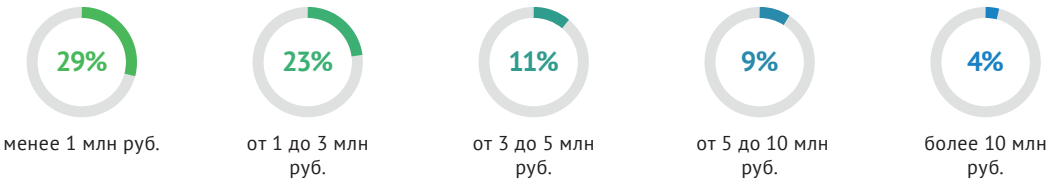


Рис. 2. Потратили на организацию дистанционных рабочих мест и обеспечение их защиты.

места и связанные с этим затраты. «С технической точки зрения возможно удалённо управлять даже производственными линиями. Но одно дело – риск потерять деньги со счета компании, а другое – если из строя выйдет, например, электростанция», – считает эксперт.

Компаниям помогает опыт удалённой работы

В банке «Хоум Кредит» сообщили, что до марта 2020 года активно использовали удалённый режим для ИТ-специалистов. Это помогло распространить опыт ИТ-блока на другие подразделения. Введение ограничений вынудило перевести на дистанционную работу 5 тыс. сотрудников из Москвы, Обнинска, Томска и Волгограда. Среди тех, кто работает дома, – специалисты ИТ-блока и сотрудники горячей телефонной линии. «Некоторым специалистам выдали технику с рабочих мест, монитор побольше и т.д. Для сотрудников контакт-центра банк установил специальное программное обеспечение и выдал гарнитуры. Перестроена схема взаимодействия между сотрудниками и руководителями», – рассказал **Сергей Фёдоров**, директор департамента инфраструктуры и поддержки сервисов банка «Хоум Кредит».

Опыт удалённого сотрудничества помог и Usetech. Процессы компании и ресурсы были готовы задолго до ограничительных мер. «35% сотрудников из городов России работали из дома и коворкингов. Перевести на дистанционную работу не удалось отдел кадров, ведь работа с бумажной документацией необходима всегда», – сообщила **Мария Николаева**, директор по маркетингу в Usetech.

Создание удалённого рабочего места не потребовало инвестиций и для компании PRNEWS. IO, в которой работает 38 сотрудников из Николаева, Киева, городов Эстонии и других стран мира. «Мы изначально строили бизнес как ИТ-компания. Не смогли перевести на «удалёнку» только офис-менеджера. Ему приходится отвечать на многочисленные звонки клиентов и обслуживать сам офис», – пояснил **Александр Нигматулин**, директор по маркетингу в PRNEWS. IO.

Предприятиям доступен зоопарк решений

По результатам исследования Positive Technologies, большинство компаний использует такие инструменты, как OpenVPN (30%), Cisco VPN (25%), Remote Desktop Gateway (19%), TeamViewer (12%) (рис. 3). В зависимости от бюджета предприятия применяют и другие решения.

Например, в Debex процессы оцифрованы и ведутся через CRM, сотрудники продолжают работу со своих ноутбуков. «Встречи с коллегами перешли в виртуальный режим. Сотрудник делает отчёт о проделанной работе за неделю и ставит план задач. Компания использует систему электронного документооборота: информация хранится на собственном хранилище и не потеряется», – объяснил **Александр Данилов**, генеральный директор онлайн-аукциона Debex.

Сервисы с криптозащитой и сквозным шифрованием используют в Enfilade Security. Так, групповые чаты ведутся в Telegram. Сотрудники компании настроили двухфакторную авторизацию в мессенджере, а для изучения важных сведений используют секретные чаты. «К защите внутренних процессов сотрудники подходят щепетильно, даже с ноткой некой паранойи. Внешнее общение происходит через электронную почту. Мы отказались от корпоративной e-mail в пользу ProtonMail. Для важных задач есть VPN, а о работе через приложения с сомнительной безопасностью (Zoom даже упоминать не хочется) речи не идёт», – рассказала **Дарья Логинова**, исполнительный директор Enfilade Security.

В банке «Хоум Кредит» дистанционная работа налажена с помощью аудио и видеоконференц связи. Для защиты удалённого доступа используют привычные решения и подходы: двухфакторная аутентификация, защита привилегированного доступа, мониторинг событий информационной безопасности. «Новых угроз для безопасности не возникло. Доступ в критичные сегменты происходит в терминальном режиме, что минимизирует риски информационной безопасности», – сообщил Сергей Фёдоров.

Меры домашней безопасности

Как выяснили в ESET, 22% респондентов сообщили о достаточном уровне инвестиций в усиление защиты и назвали уровень подготовки отличным. 54% опрошенных поставили оценку «хорошо»: меры по защите информации достаточны. Необходимый минимум используется на 23% предприятий (рис. 4). Результаты исследования Positive Technologies показали: в каждом четвёртом случае (24%) для работы используются собственные компьютеры или ноутбуки, а в 56% – в служебных целях используются и домашние ПК, и рабочие (рис. 5).

Чтобы минимизировать риски утечек критичных данных и масштабы инцидентов дома, эксперты советуют использовать совокупность нескольких проверенных решений и подходов.

- **Провести инструктаж или вебинар по цифровой гигиене**

Тех, кто не работал из дома, нужно обучить цифровой гигиене: напомнить о популярных методах фишинга, предупредить, что в спорных вопросах лучше обратиться в ИТ-департамент, а не пытаться решить проблему самостоятельно, считает **Тимурбулат Султангалиев**, директор практики информационной безопасности компании AT Consulting.

Рис. 3. По результатам исследования Positive Technologies, такие инструменты использует большинство компаний.

Рис. 4. Оценка респондентами уровня защиты (по данным ESET).

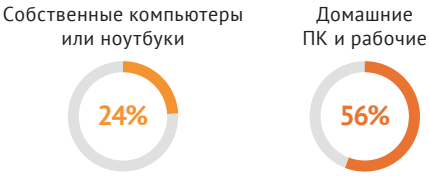


Рис. 5. Какие компьютеры или ноутбуки используются для работы (по результатам исследования Positive Technologies).

• Использовать корпоративные устройства

Как правило, на корпоративных компьютерах уже установлены защитные средства (антивирусы, программные файрволлы, DLP клиенты и прочее), а также используются программы шифрования данных и средства для «ограничения» действий пользователя в системе. «Это минимизирует влияние домашней «инфраструктуры» на рабочий компьютер и обезопасить корпоративные системы от несанкционированного доступа», – полагает **Дмитрий Терехов**, менеджер по ИТ-инфраструктуре и сервису 3M в регионе Россия и СНГ.

Если в компании не готовы предоставить пользователям корпоративные лэптопы, то MDM-системы помогут организовать дополнительный уровень контроля и безопасности для работы с ИТ-системами предприятия.

• Настроить двухфакторную идентификацию

Для доступа к корпоративным сервисам требуется внедрить двухфакторную идентификацию. «Решений для защиты удалённых подключений с личных и рабочих устройств на рынке много. Нужно выбирать продукты в соответствии со спецификой работы и потребностями конкретной организации», – рекомендовал Дмитрий Ковалёв.

• Защитить от утечек с помощью DLP

Для защиты от утечек информации применяются системы класса DLP (Data Leak Prevention), отслеживающие актуальные риски для организации и оперативно реагирующие на них. «Практика Softline показывает: наличие DLP в организации значительно повышает дисциплину персонала в работе с информацией», – замечает **Дмитрий Ковалёв**.

• Использовать виртуальные частные сети

Мало организовать VPN, нужно ещё и мониторить нагрузку на каналы VPN, чтобы подключение к виртуальным частным сетям не стало «бутылочным горлышком» и не остановило или затруднило работу сотрудников компании. «Хорошо, если VPN сервис резервируется, имеет несколько точек подключения. Стоит дополнительно обезопасить подключение, применив двухфакторную аутентификацию», – говорит **Дмитрий Терехов**.

• Настроить виртуальные рабочие столы

Удалённый доступ к рабочим столам через VDI-инфраструктуру – проверенное временем решение. «Инфраструктура виртуальных рабочих столов предполагает, что рабочее место сотрудника (персональный компьютер, ноутбук или тонкий клиент) – лишь транспорт до его рабочего места. Вся информация работников хранится на платформе работодателя, сотруднику доставляется «картинка» рабочего стола. Эта технология обеспечивает достаточный уровень безопасности», – говорит **Денис Шмырев**.

• Отслеживать активность сотрудников

Для контроля дисциплины персонала применяются решения для учёта рабочего времени, анализа работы с бизнес-приложениями, оптимизации нагрузки сотрудников и т.д. Не лишним будет принять превентивные меры для защиты данных. Из-за ограничений снижается выручка бизнеса, оптимизируются зарплаты и численность персонала. Вне стен офиса гораздо проще скопировать чувствительные для компании сведения и при конфликте с работодателем попробовать продать их конкуренту.

Для защиты печатных, графических и электронных копий документов в НИИ СОКБ разработали специальные невидимые человеческому глазу метки. «Такая маркировка определяет источ-

Рис. 6. Готовность сохранить удалённый режим работы после снятия ограничений (по результатам опроса НАФИ).

Рис. 7. Динамика эффективности сотрудников (по оценке работадателей).

Рис. 8. По данным исследования SAP, проведённого в марте-апреле.

ник утечки, так как для каждого пользователя создаётся индивидуальная копия. В итоге источник утечки найдётся даже по фотографиям экрана», – объяснил **Игорь Калайда**, генеральный директор НИИ СОКБ.

Переоценка офисных ценностей

Пока представители бизнеса оценивают достоинства и недостатки удалёнки и расходятся во мнении о целесообразности такого режима. Например, согласно результатам опроса НАФИ, после снятия ограничений только 20% предприятий готовы сохранить частичный и 7% полный удалённые режимы (рис. 6). При этом 82% работодателей заметили снижение, а 14% – повышение эффективности сотрудников (рис. 7).

По данным исследования SAP, проведённого в марте-апреле, 32% самих сотрудников утверждают, что стали продуктивнее работать из дома. 22% — готовы остаться на удалёнке, 25% – ещё не решили, откуда работать и однозначно за офис выступает 53% респондентов (рис. 8).

Частично сотрудников на удалёнке оставят PRNEWS. IO, «Хоум Кредит» и «Эватор».

Треть персонала PRNEWS. IO продолжит работать из дома, поделился Александр Нигматулин: «Выяснилось: рабочий процесс в удалённом режиме также продуктивен и имеет свои неоспоримые плюсы». В банке «Хоум Кредит» не решили, как быть с удалёнщиками. Сейчас, по словам Сергея Фёдорова, обсуждаются возможные форматы работы.

В «Эвоторе» отмечают рост эффективности сотрудников. «Поэтому мы просим команду не работать на выходных, чтобы избежать эмоционального выгорания. Мы используем удалённый формат работы и после окончания карантина для части сотрудников. Наша компания быстро растёт, рабочих мест в офисе не всегда хватает, это была постоянная проблема. Процессы настроены, можно будет не только экономить на аренде, но и нанимать специалистов в регионах», – поделился планами **Андрей Романенко**, генеральный директор ИТ-компании «Эвотор».

Однозначно за удалёнку выступают в руководстве Enfilade Security, чей персонал изначально работает дистанционно. «Количество очных встреч с партнёрами и заказчиками сократилось до нуля. В итоге не надо тратить время на транспорт и лишнее общение. Электронная переписка лаконична и содержит уже фиксированные и необходимые для работы детали. Рабочая жизнь технических специалистов не изменилась вообще. Продуктивность возросла: мы проанализировали опыт других организаций и поменяли множество внутренних процессов», – поделилась опытом **Дарья Логинова**.

Спрос на защиту информации не замедлится

Введённые ограничительные меры подстегнули не только спрос на решения для удалённой работы, такие как защита удалённых подключений, системы класса DLP и ИБ-сервисы, что связано с резким ростом нагрузки на ИТ- и ИБ-департаменты. В тренде услуга по переводу сотрудников на home-office «под ключ». «Большинство таких предложений предполагают меры по защите информации», – отметил **Михаил Смирнов**.

Насколько эффективны решения и подходы для home-office, которыми вооружился бизнес, станет известно нескоро: многие компании не раскрывают сведения. «Инциденты наносят ущерб компании в конкурентной борьбе, сильно бьют по репутации и нередко становятся причиной судебных тяжб и выплат компенсаций пострадавшим», – объяснил **Денис Шмырев**, заместитель директора центра компетенций по информационной безопасности компании «Техносерв».

После снятия карантина бизнес примет первоочередные меры для защиты от внешних проникновений и утечек данных, считают в Softline. Вырастет спрос на образовательные проекты, направленные на улучшение уровня цифровой грамотности и гигиены сотрудников. Многие компании воспользуются аудитом информационной безопасности, проведут тесты на проникновение и проанализируют защищённость инфраструктуры.

Автор: Виталий Мосеев

eToken

Продукты линейки eToken –
основа инфраструктуры информационной
безопасности современного предприятия

etokenstore.ru

Когда дует ветер перемен, нужно строить ветряную мельницу

Павел Клепинин,
Учредитель Клуба IT&Digital директоров «я-ИТ-ы»

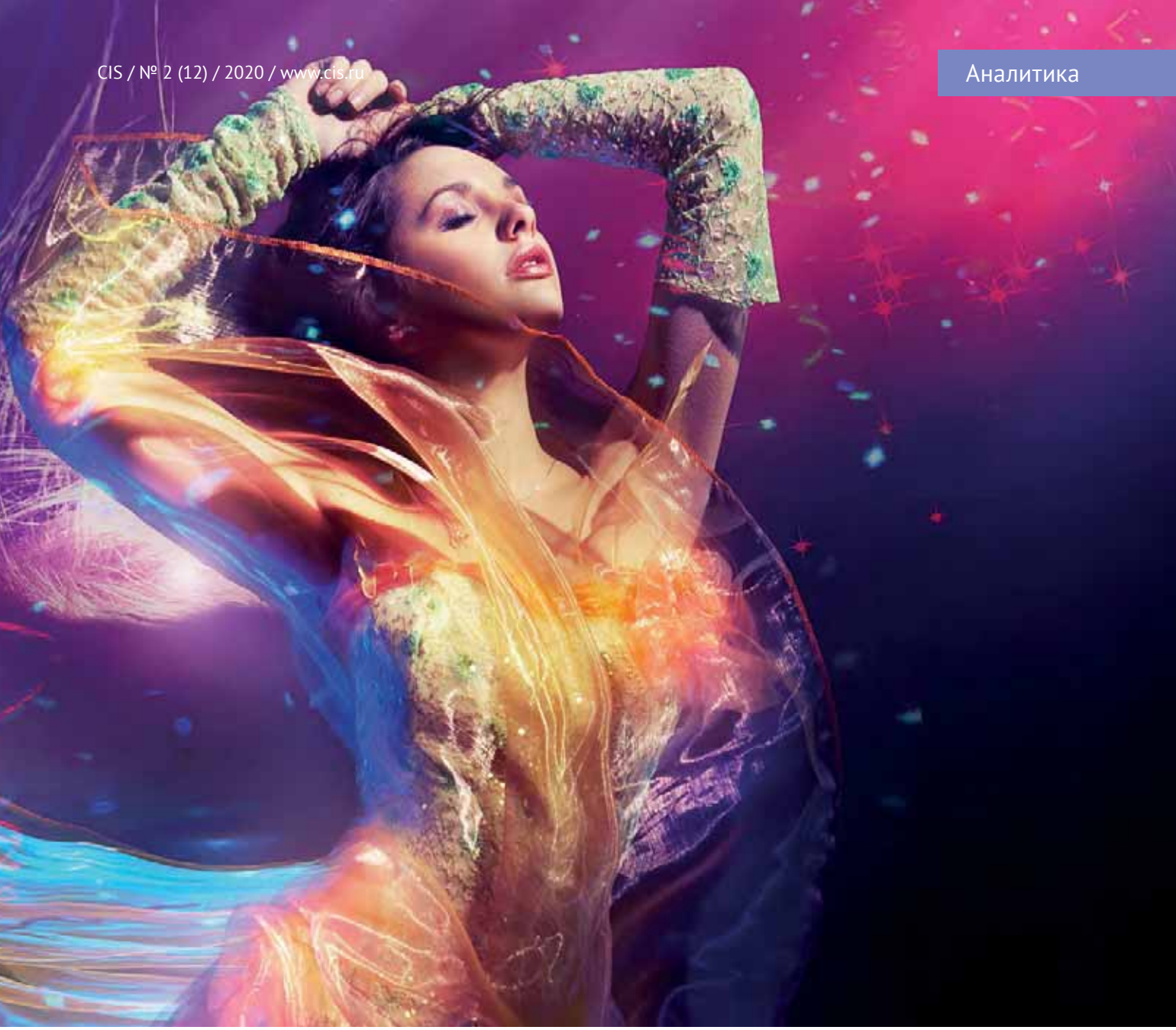
Последствия пандемии «COVID-19» ускорили технологические изменения и не обошли стороной промышленный сектор – его цифровая трансформация стала жизненно необходима. Несмотря на то что работу предприятий лишь частично можно перевести на дистанционный формат, им важно начать менять привычные бизнес-модели и усиливать автоматизацию. Обе задачи весьма непросто решить без грамотных ИТ-специалистов.

О том, как ИТ-сфера адаптируется к новым реалиям и как цифровизация проникает в промышленность, рассказывает учредитель Клуба IT&Digital директоров «я-ИТ-ы».

– Павел, вы основатель Клуба «я-ИТ-ы». Что даёт его членам участие в этой организации?

– Наш клуб был основан в 2012 году. Сейчас он объединяет более 400 директоров по информационным (CIO) и цифровым (CDO) технологиям, а также директоров по цифровой трансформации (CDTO) из различных регионов России.

По факту мы уже стали заметным IT&Digital управленческим офлайн-сообществом, участники которого видятся друг с другом «вживую». За годы деятельности клуба мы посетили больше сотни предприятий и организаций из разных отраслей экономики, детально разбирали ИТ-составляющую каждого из них, изучали лучшие ИТ-практики. На таком временном горизонте прекрасно видно, как члены клуба развиваются по линии ИТ, как приобретают новые управленческие компетенции и навыки. И, конечно, как они растут в карьерном плане.



– Чем сегодня живёт ваше сообщество?

– В период пандемии ИТ-сообщество буквально живёт на работе. В авральном режиме, часто по ночам, специалисты в области информационных технологий помогают организовать работу в новых условиях. Понятно, что компаниям из списка наиболее пострадавших от коронавируса отраслей сейчас особенно непросто, ведь им в короткие сроки приходится запускать совершенно новые бизнесы, например по онлайн-продажам, доставке или дистанционному обучению. Многие к этому не были готовы.

Эти темы плотно обсуждаются в онлайн-каналах коммуникаций клуба. Согласитесь, крайне важно иметь возможность задать вопрос «коллективному разуму», быстро получить ответ, а ещё лучше – узнать о готовой к тиражированию лучшей практике. В этом сила нашего сообщества.

Что касается активностей самого клуба, то на последствия неблагоприятной эпидемиологической обстановки мы отреагировали оперативно. Офлайновые мероприятия марта – апреля сдвинули на вторую половину года, заменив их вебинарами на злободневные темы. 24 апреля успешно провели большую онлайн-конференцию «Пока я-ИТ-ы дома», участниками которой стали более ста ИТ и «цифровых» руководителей со всей России от Камчатки до Калининграда.

Действительно, новые условия стёрли географические границы, и Клуб мгновенно к ним адаптировался. На онлайн-конференции CIO крупных компаний страны рассказали, как меняется их работа, и поделились «боевым» опытом управления корпоративным ИТ в новых реалиях.

Кроме того, мы запускаем несколько новых проектов: YouTube-канал управленческих кейсов #моИТвои, онлайн-конкурс красоты

и ума – Beauty&Digital, арену «я-ИТ-ы» для интеллектуальных сражений.

– Какие подразделения промышленных компаний легче поддаются автоматизации? Где возникает сопротивление?

– Вывел для себя такую формулу: чем дальше подразделение от выручки и распределения ресурсов, тем легче проводить любые организационные изменения, включая внедрение ИТ-решений. Например, это склады или производство.

В любом новом деле всегда есть динамичные и рисковые первопроходцы.

А вот заставить продавца фиксировать результаты переговоров с клиентом в воронке продаж в CRM-системе – поистине высший пилотаж! По статистике, около 50% руководителей российских компаний в различных отраслях сталкиваются с саботажем сотрудников при внедрении CRM. При этом рынок CRM-систем в России довольно перспективен.

Судите сами: доля компаний в России, где компьютерами оборудовано более половины рабочих мест, составляет около 40%. CRM-системами обладают 14% компаний, и это достаточно неплохой показатель для нашей страны. Особый подход нужен к людям творческих профессий: конструкторам, дизайнерам, программистам. Практика показывает, что алгоритмизировать их работу вполне возможно.

– В рамках деятельности Клуба «я-ИТ-ы» вы регулярно посещаете российские промышленные предприятия и можете оценить степень их автоматизации. Что бы вы сказали об уровне их цифровой зрелости?

– Уровень базовой автоматизации оцениваю как довольно высокий. Бухгалтерский учёт, управление финансами, складской и производственный учёт, внутренняя логистика – традиционные лидеры.

Сложная ситуация с автоматизацией планирования производства, особенно в части использования оптимизационных алгоритмов. При создании продуктов инструменты проектирования есть у всех, а вот систем управления жизненным циклом разработки изделий (PLM), используемых на практике, немного. Тем не менее статистика в этом вопросе создаёт весьма позитивное впечатление.

Так, по прогнозам авторов проекта дорожной карты по развитию новых производственных технологий (НПТ), количество высокотехнологичных предприятий, применяющих технологию цифровых двойников, увеличится с трёх в 2019 году до ста в 2024 году, а число реализованных проектов на высокотехнологичных предприятиях из приоритетных отраслей промышленности, для которых была применена технология разработки цифровых двойников, – с трёх до 250. За этот же период сокращение времени разработки высокотехнологичных продуктов составит 25%.

Если же выйти за границы внутрикорпоративной автоматизации, мы ясно увидим, что зоной для развития может стать взаимодействие с контрагентами и партнёрами.

– В какой мере цифровизация ощущается акционерами как насущная необходимость, а в какой – как дань моде?

– Хайп цифровизации в мире свидетельствует о том, что говорить о дани моде вполне уместно. В любом новом деле всегда есть динамичные и рисковые первопроходцы. Есть компании, которые внимательно наблюдают за лидерами и выжидают, после чего тиражируют успешный опыт. Они хотят быть уверены, что эффекты от внедрения новой технологии будут положительными. Есть и те, которые не воспринимают изменения и считают нововведения пустой затеей. Это вопрос толерантности к риску и наличия относительно свободных финансовых ресурсов.

Согласно докладу ООН о цифровой экономике за 2019 год, в 2009 году в рейтинге 20 самых крупных компаний мира ведущие позиции занимали добывающие организации. При этом в список, в который составители доклада включили и цифровые платформы, попали тогда всего три компании из технологического и потребительского секторов. К 2018 году количество бизнесов из последней категории увеличилось до восьми. При этом в двадцатке остались всего две добывающие организации.

Также немаловажен вектор на цифровизацию, заданный руководством нашей страны. Известно, что инвестиции в этой сфере активно поощряются.

– Можно ли утверждать, что функция ИТ в последние годы трансформировалась из сервисной в полноценную бизнес-функцию с прямой экономической отдачей?

– Трансформация CIO в CDO/CDTO требует большего погружения в функционирование бизнеса, масштабности мышления для понимания возможностей расширения и трансформации компании и, естественно, знания новых технологий. «Когда дует ветер перемен, нужно строить ветряную мельницу». Да, теперь у ИТ-функции гораздо больше возможностей превра-

титься из центра затрат в центр прибыли. А у ИТ-директора – повысить свою значимость в корпоративной иерархии.

– Кстати, а как изменилась роль ИТ-директора сейчас, в период пандемии?

– На волне коронавируса роль CIO существенно выросла. В момент бизнес стал критически зависеть от работы ИТ-персонала, его скорости, качества, креативности. Поэтому общение с руководителями первой линейки очень тесное, мессенджеры трещат. Уверен, что многие ИТ-руководители в текущей ситуации наберут очки. Если ты, не жалея себя, спасаешь родную компанию, такое не забывается.

Конечно, есть внутренняя конкуренция: часть обязанностей на себя забирают CDDO и руководители, отвечающие за цифровую трансформацию, или директора инновационных лабораторий. Но всё зависит от конкретной персоны ИТ-директора. Однозначно можно сказать, что если он готов возглавить нетрадиционные для себя направления, то становится одним из важнейших людей в компании.

– Как вы считаете, в каких случаях корпорациям целесообразнее запускать пилотные проекты вместе со стартапами, пробовать, экспериментировать, а в каких – полагаться на собственные профильные подразделения или дочерние структуры?

– В крупных компаниях, которые могут себе это позволить, виден тренд на создание собственных центров разработки. Такие центры, в частности, существуют в Росатоме, Газпроме, СИБУРе.

На волне коронавируса роль CIO существенно выросла. В момент бизнес стал критически зависеть от работы ИТ-персонала.

Представим, что критическую для предприятия функцию или конкурентное преимущество автоматизировала маленькая компания – стартап с 5-10 разработчиками в штате. Понятно, что в любой момент они могут разбежаться, уйти к конкурентам: с ними может случиться всё, что угодно. Для больших компаний в этом заключаются высокие риски потери части бизнеса и дохода. Чтобы их снизить, такой стартап можно купить, причём в идеале с использованием опционной схемы на раннем этапе, пока цена компании невысока. Можно также сразу создать внутреннее подразделение, собирать людей и экспериментировать внутри. И, конечно, важно не забыть сообщить людям, что они теперь не только производственная компания.

– Многие крупные корпорации, в том числе добывающие и обрабатывающие, активно создают инновационные лаборатории, внутренние корпоративные акселераторы. В марте этого года о запуске партнёрской программы по поиску, развитию и поддержке технологических компаний, предлагающих решения для промышленного сектора, сообщили Фонд «Сколково» и компания «Инновационный центр Ай-Теко». Программа даёт компаниям возможность самостоятельно отбирать команды, проекты, продукты для инновационных решений, отвечающие индивидуальным потребностям. Как оцениваете эту практику?

– Повторюсь. Есть технологические лидеры, активно развивающие ИТ, R&D и работающие со стартапами. Есть те, которые только начинают использовать инновационные элементы, а некоторые вообще не задумываются о необходимости их внедрять.

Основная проблема в том, что пока нет достаточной статистики о том, какие именно технологии помогают ускорить развитие компаний, дать ей конкурентные преимущества и возможность больше заработать, поэтому тема поиска и внедрения инновационных решений сейчас – пока больше о вере и венчурных инвестициях, чем о просчитанных и экономически обоснованных решениях.

Как показывает моя практика, один успешный проект может дать эффект, который перекроет затраты десяти неуспешных проектов. Кстати, если посмотреть на западных первопроходцев четвёртой промышленной революции, то легко найти «эпик фейлы», что также подтверждает – лидеры сильно рискуют. При этом ещё три года назад мы смотрели на данные компании как на гуру цифровизации.

Насколько мне известно, с создателями стартапов активно сотрудничают пока не более 50 компаний из списка топ-1000 российского бизнеса. Тем не менее я и не исключаю, что, если стартап сумел предложить бизнесу свежую идею или нестандартное решение, партнёрская кооперация будет крепкой.

– У вас есть профессиональная мечта?

– Скажу так – есть, она тесно связана с нашей страной и клубом. Как и любая сто́ящая мечта, она крайне амбициозна и труднодостижима. Когда добьюсь, тогда о результатах не стыдно будет рассказать моим внукам, а может, и правнукам.

Павел Клепинин

Генеральный директор компании «Цифрум» (ГК «Росатом»)

Основатель «Я-ИТ-ы» Клуб IT&Digital Директоров

Alena Akhmadullina впервые представляет капсулу 3D-одежды

В 2020 году бренд Alena Akhmadullina начинает отмечать 20-летие, в рамках чего представит несколько онлайн и оффлайн проектов. Осенью состоится показ специальной концептуальной коллекции, созданной к этой дате. В качестве тизера бренд создал 3D-капсулу из 5 луков, которые передают эмоцию и идею коллекции, оставляя недосказанность.

Основной концепцией стал образ одежды будущего, осмысленной в разрезе использования русских культурных кодов – в данном случае мотивов дымковской игрушки – в сочетании с высокотехнологичными тканями. Неотъемлемым аксессуаром являются маски-шлемы, необходимые в условиях ухудшения экосистемы Земли и поиска новой на других планетах. 3D-луки из капсулы Alena Akhmadullina представила виртуальная модель Алиона Пол.

В тему 3D-одежды дизайнер Алёна Ахмадуллина глубоко погрузилась во время периода самоизоляции: «Этот вопрос волнует меня давно, но в контексте происходящего ответ стал очевиден, что будущее моды в диджитал. Всё идёт к тому, что мы будем иметь несколько виртуальных воплощений – аватаров – для разных задач и областей нашей жизни. И, конечно, нам нужна будет виртуальная одежда! Причём в онлайн формате мы будем гораздо смелее экспериментировать со своим стилем и образом в целом, чем в реальности. Очевидные плюсы для дизайнеров и для планеты – безграничное пространство для творческих идей и уменьшение перепроизводства одежды».

Alena Akhmadullina одним из первых в сегменте люкс представил проект с 3D-одеждой. Продолжением этого проекта бренд видит продажу диджитал моделей в официальном онлайн-магазине, где клиенты смогут «примерить» их на свои фотографии.

Алиона Пол: «Хочу поблагодарить прекрасную Алёну Ахмадулину за смелость и доверие! Ещё вчера в цифровую моду никто не верил и не воспринимал всерьёз. Сегодня на неё начинают смотреть иначе и строят планы. Развиваются технологии виртуальной примерки, появляется новая плеяда цифровых дизайнеров. Уверена, что будущее цифровой моды и виртуальных моделей будет кибер-светлым!»

ALENA AKHMADULLINA

*Бренд **Alena Akhmadullina** был основан в 2001 году в Санкт-Петербурге. Создавая коллекции в стилистике интеллектуального романтизма, дизайнер Алёна Ахмадуллина опирается на традиции русского костюма и сказочную образность. Направление, в котором работает бренд, называется «артизан». Для него характерно вдохновение предметами искусства, живописью, кинематографом, литературой и большое количество ручной работы. Развивая философию «Жизнь как искусство», дизайнер сочетает её в работе с силуэтами народного костюма и традиционными русскими техниками.*

www.alenaakhmadullina.ru

АЛИОНА ПОЛ – виртуальный человек, модель, блогер. Её придумала загадочная современная художница, а создали нейросети и компьютерная графика. Её имя – это соединение имени Алёна и слова Alien – пришелец, чужой. Фамилия означает простор, размах и просто пол – это её респект цифровой эпохе за то, что гендерные различия уже не имеют большого значения. Алиона родилась 4 сентября 2018 года, и ей всегда 18. Никогда не постареет, если сама этого не захочет. Живёт в Москве, в Киото, на Астероиде Б-12 и одновременно везде. Поддерживает осознанное потребление и экологичную моду.

Instagram: aliona_pole

CIS / № 2 (12) / 2020 / www.cis.ru

ИБЭШНИКИ – МАРШРУТ

Сегодня полиция в процессе расследования различных преступлений всё чаще обращается к базе Sensorvault, принадлежащей Google, чтобы отследить местоположение и перемещение смартфонов.

Sensorvault содержит записи геолокации сотен миллионов мобильных устройств по всему миру. Она собирает соответствующую информацию, которую передают продукты Google, чтобы лучше понимать, какую рекламу отображать пользователям и как эта реклама работает.

Как передаёт The New York Times, за последние шесть месяцев подобные запросы резко увечились в количестве – стало приходить по 180 запросов за одну неделю.

Автор:
Владимир Безмалый

Календарь мероприятий

4 июля
С.-Петербург • Турнир
Турнир по пейнтболу «IT Top Gun St. Petersburg 2020»

6-9 июля
Москва • Курс
Школа распределенных вычислений SPTDC 2020

10 июля
Санкт-Петербург • Конференция
PG Day Russia 2020

10-11 июля
Москва • Онлайн-трансляция • Конференция
Hydra 2020

12-13 июля
Москва • Онлайн-трансляция • Конференция
DevOops 2020 Moscow

14-27 июля
Билярск • Курс
Летний лагерь Сэлэт-Санак

14-15 июля
Москва • Онлайн-трансляция • Конференция
C++ Russia 2020 Moscow

17 июля
Иркутск • Митап
INFOSTART MEETUP Irkutsk

18 июля
Кронштадт • Турнир
Парусная регата «IT Sailing St. Petersburg 2020»

14 августа
Владивосток • Митап
INFOSTART MEETUP Vladivostok

5 сентября
С.-Петербург • Турнир
Велотурнир «IT Bike Fest St. Petersburg 2020»

15-17 сентября
Москва • Онлайн-трансляция • Конференция
TestCon Moscow 2020 – международная конференция по тестированию и обеспечению качества ПО

16-18 сентября
Краков • Конференция
ACE!

19 сентября
Москва • Турнир
Турнир по картингу «IT Race Moscow 2020»

19 сентября
Москва • Мероприятие
ИТ-конкурс красоты «Beauty & DigITal»

21-22 сентября
С.-Петербург • Конференция
Saint HighLoad ++ 2020

23-24 сентября
С.-Петербург • Конференция
Saint TeamLead Conf 2020

26-27 сентября
С.-Петербург • Онлайн-трансляция • Конференция
HR API 2020

17 октября
С.-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 • Онлайн-трансляция • Конференция
Big Data Days 2020

27-29 октября
Москва • Конференция
3-я Международная научно-техническая конференция «Современные сетевые технологии»

30-31 октября
С.-Петербург • Онлайн-трансляция • Конференция
Open Source Tech Conference Piter

5-6 ноября
Москва • Онлайн-трансляция • Конференция
INFOSTART EVENT 2020

21 ноября
Москва • Турнир
Интеллектуальный турнир «IT Brain Battle Moscow 2020»

27 ноября
С.-Петербург • Онлайн-трансляция • Конференция
PiterPy 2020

27 ноября
С.-Петербург • Онлайн-трансляция • Конференция
Golang Piter 2020

5 декабря
С.-Петербург • Турнир
Турнир по кикеру «IT»s KICKER St. Petersburg 2020»

Японский кроссворд

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

							8																																										
				10		8	2														5	5	6	6	6	6	6	7	7	7																			
				2	9	2	3	7	6	5	5	4					4	4	5	5	3	3	3	2	2	1	2	1	1	1	9	11	13	14															
	11	11	11	1	2	5	2	9	8	7	4	3	4	4	4	4	1	4	5	7	3	4	4	3	4	6	7	7	8	6	5	4	3	2	15	15	16	17	18	16	31	30	26	22	19	15	8	2	
15	5	1	2	1	4	2	4	8	9	11	12	14	16	19	16	17	17	19	20	22	23	23	25	27	28	30	30	32	33	33	33	32	32	32	32	32	32	32	31	32	15	12	9	8	8	8	9	6	13

				40
				41
				42
				44
			11	26
			9	23
			9	18
			8	16
			6	16
			5	15
			4	15
			3	15
			2	15
			2	14
			1	13
			1	12
			1	12
		1	9	1
	1	4	8	1
	2	3	6	1
	2	3	6	1
1	5	6	7	1
1	4	8	6	1
1	5	9	7	1
	3	10	7	1
		15	7	1
		13	8	1
8	5	4	9	1
9	1	4	10	2
		4	12	1
		7	13	1
		8	13	1
		9	15	1
2	3	1	17	2
	6	1	18	1
	2	2	21	1
	1	3	23	1
			36	2
			35	2
			36	3
				41
				40
				39
				39
				39
				37
				36
				35
				33
				31
				30
				28
				26
				24
				21
				20
				18
				16
				13
				11
				8
				6
				3

Лучшие в мире решения для информационной безопасности

Дистрибуция

Сертифицированные решения

Мобильные технологии

Канальное шифрование

TESSIS является официальным дистрибутором компаний Gemalto и CYREN, имеет статус Reseller у компании Blackberry и предлагает решения, обеспечивающие комплексную защиту и использующие технологии шифрования для защиты систем коммуникаций, программных разработок и контроля цифровой идентификации, а также решения для корпоративных и частных виртуальных сред.

TESSIS
TECHNOLOGIES, SYSTEMS AND SOLUTIONS FOR INFORMATION SECURITY

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