

Как организована удаленная работа

в России и странах СНГ

Ключевые результаты исследования

В апреле мы провели анонимный опрос среди специалистов ИТ и ИБ. Цель исследования — узнать, как организована удаленная работа в компаниях в России и странах СНГ. Эта информация нужна нам как вендору, чтобы понять, какие угрозы сейчас наиболее актуальны и выбрать приоритеты для разработки способов их обнаружения.

Опрос проводился с 7 по 14 апреля 2020 года. Мы разместили его на официальном сайте Positive Technologies, интернет-порталах, посвященных ИБ, социальных сетях, в тематических чатах и каналах в Телеграме. Мы получили 776 заполненных анкет.

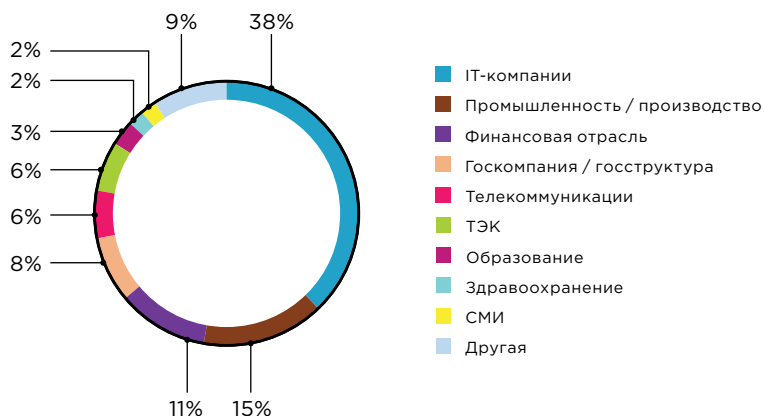
Результаты:

- Только 11% респондентов отметили, что в их компании удаленный доступ организовали в связи с карантином.
- 80% респондентов рассказали, что в их компаниях часть сотрудников или все из них используют для работы домашние компьютеры или ноутбуки.
- OpenVPN, Cisco VPN и Remote Desktop Gateway — самые популярные способы организации удаленной работы среди всех компаний. В большинстве популярных систем для организации удаленного доступа есть критически опасные уязвимости.
- В крупных компаниях чаще всего используют Cisco VPN, OpenVPN и Check Point VPN.
- 57% респондентов отметили, что не планируют менять способы организации удаленного доступа в ближайшее время.
- Каждая пятая компания вывела на периметр корпоративные порталы.

Профиль респондентов

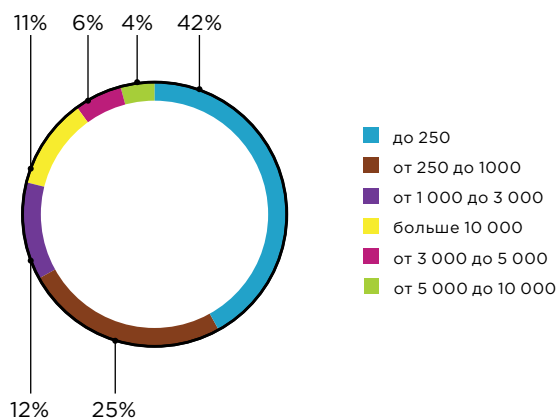
Отрасль

В опросе участвовали в основном специалисты по ИБ и ИТ из сферы информационных технологий, промышленности, финансов и госсектора. Вероятно, ИТ-сектор лидирует потому, что больше всего на вопросы отвечали представители компаний-интеграторов.



Размер компании

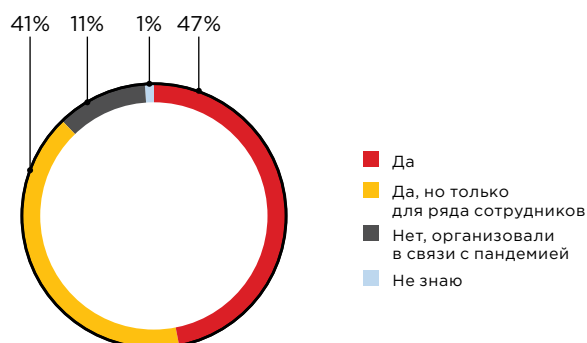
Больше половины респондентов представляют крупный бизнес, остальные 42% — малый и средний бизнес (до 250 работников).



Как организован удаленный доступ сотрудников к локальной сети

Удаленка была до карантина

Оказалось, что полный или частичный удаленный доступ был организован в большинстве компаний еще до карантина. Однако более чем половина респондентов отметила, что его пришлось экстренно организовывать с нуля (11%) или масштабировать на большее количество сотрудников (41%).



В вашей компании был организован удаленный доступ до карантина?

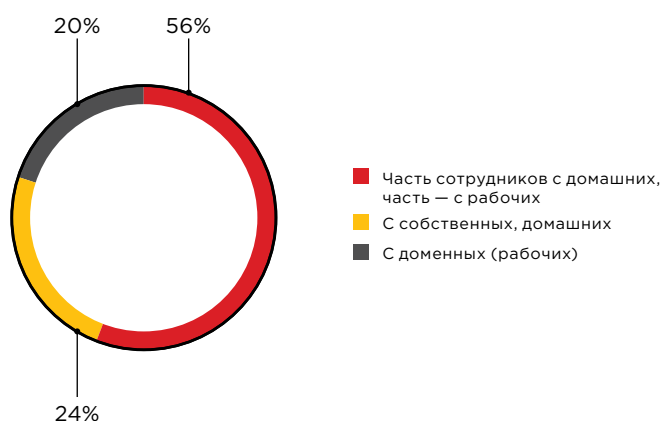
IT-компании — лидер среди отраслей по готовности к переходу на удаленку: в 63% компаний удаленный режим работы был организован еще до карантина. Для сравнения в телекоммуникационной сфере доля таких компаний составляет 54%, в финансовой — 46%, в промышленности — 32%, в ТЭК — 26%, в госструктурах — 24%.

Один из рисков безопасности при быстром переходе на удаленный режим работы — это увеличение нагрузки на ИТ-мощности и отсутствие внимательного мониторинга обновленной инфраструктуры. Желательно, чтобы сотрудники работали с доменных устройств, настроенных по всем стандартам безопасности. На них как минимум должны быть установлены антивирусные средства защиты и все актуальные обновления для ПО и ОС.

Работа с домашних устройств

Однако корпоративные ноутбуки выдали далеко не всем. Сотрудники 20% компаний работают с рабочих устройств, в остальных 80% организаций часть или все сотрудники используют домашние компьютеры или ноутбуки.

С каких компьютеров
(ноутбуков) ваши сотрудники
работают удаленно?



Наиболее безопасный вариант работы на удаленке — использовать выделенные рабочие устройства. Самая большая доля компаний, где все сотрудники работают с доменных устройств, в ИТ-отрасли — 26%. Немного отстает финансовая отрасль — это число составляет 23%. Самый низкий показатель — в промышленности (11%).

Если в вашей компании сотрудники работают с домашних устройств, мы рекомендуем распространить на их девайсы средства антивирусной защиты. Это можно сделать так:

1. Организовать доступ к серверу управления корпоративными антивирусами на конечных узлах через интернет.
2. Настоять, чтобы сотрудники установили у себя корпоративный антивирус и подключились к серверу управления.

Это может потребовать больше лицензий, но позволит проще распространить корпоративную политику безопасности на домашние устройства. Также это позволит сравнивать доменные адреса и проще выявлять нарушителей и подозрительную активность.

Если в вашей компании удаленная работа организована с помощью VPN (как показал опрос, VPN пользуется популярностью), запретите раздельное туннелирование (split tunneling): заверните весь пользовательский трафик во внутрь инфраструктуры через периметровые средства защиты, например прокси и NGFW. Иначе, если устройство сотрудника взломано и контролируется через интернет, службе ИБ будет сложно это выявить.

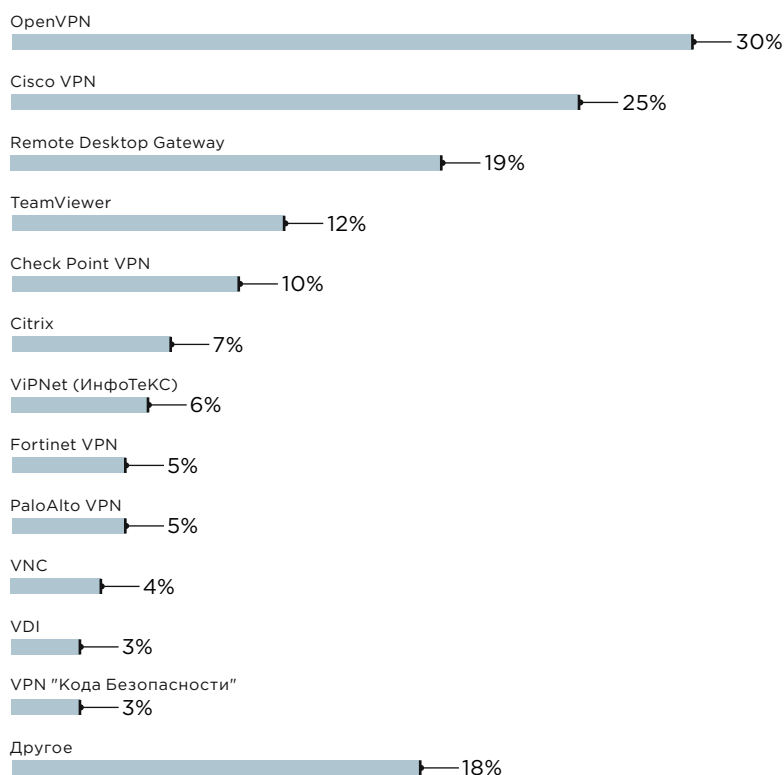
Пропускать трафик всех пользователей через периметр вряд ли получится — это большая нагрузка на каналы. Поэтому мы рекомендуем сегментировать сети и доступ к ним, а через запрет раздельного туннелирования обязательно пропускать трафик сотрудников, которые работают с конфиденциальными данными.

Если запретить раздельное туннелирование не получается, то для обеспечения безопасности внутренней сети пригодится поведенческий анализ. Например, можно настроить уведомления на случаи подключения сотрудника с IP-адресов из других стран или в нерабочее время. Такие случаи можно покрыть с помощью SIEM-систем — данные в них обогащаются из дополнительных источников: GeoIP-сервиса и системы анализа трафика (NTA).

Популярные ПО для организации удаленного доступа

Самые популярные способы организации удаленной работы: OpenVPN, Cisco VPN и Remote Desktop Gateway. 40% пользователей OpenVPN — компании малого и среднего бизнеса.

Какими способами
организована удаленная
работа в вашей компании?

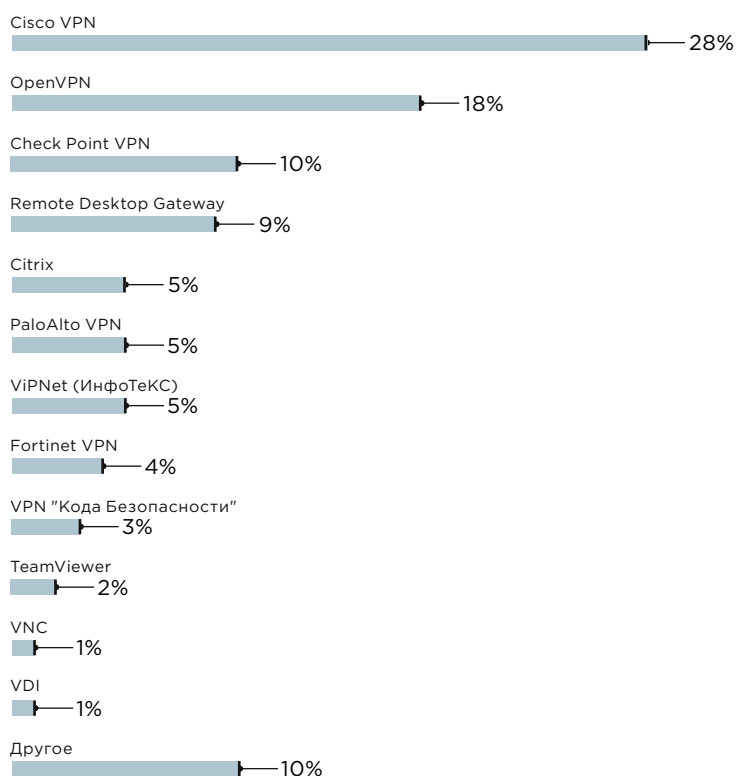


Картина меняется, если смотреть на ответы компаний с количеством сотрудников свыше 250 человек: в тройку лидеров врывается Check Point. А вот OpenVPN, RDG, TeamViewer значительно меньше популярны среди крупного бизнеса.



MaxPatrol SIEM выявляет сетевые аномалии с использованием OpenVPN, Cisco ASA, RDG и межсетевого экрана Check Point. Для этого в продукт добавлен пакет экспертизы, разработанный специально под удаленную работу.

Какими способами
организована удаленная
работа в компаниях
размером 250+ сотрудников



В отраслях список лидеров практически не меняется. Единственное заметное отличие — в ПО, которое используют государственные компании и структуры: среди них появились отечественные игроки. В тройку лидеров вошел VPN «Кода Безопасности» (15%) вместе с Cisco (20%) и OpenVPN (12%). Это можно объяснить требованиями регуляторов и переходом на отечественное ПО.

Мы проверили базу NIST: OpenVPN, Check Point и RDG содержат критически опасные уязвимости. Рекомендуем обязательно проверить версии используемых систем и обновиться до самых новых, а также установить обновления.

Список актуальных уязвимостей для популярного ПО

OpenVPN

В OpenVPN Access Server версии 2.8.0 есть критически опасная уязвимость: возможен обход LDAP-аутентификации, за исключением случаев, когда пользователь использует двухфакторную аутентификацию ([CVE-2020-8953](#)).

Еще одна уязвимость, актуальная для OpenVPN, позволяет атакующему похищать активные VPN-подключения ([CVE-2019-14899](#)).

Cisco

Уязвимость в компоненте установщика Cisco AnyConnect Secure Mobility Client для Windows может позволить аутентифицированному злоумышленнику копировать предоставленные пользователем файлы в каталоги системного уровня с привилегиями системного уровня ([CVE-2020-3153](#)).

Уязвимость в межсервисном взаимодействии Cisco AnyConnect Secure Mobility Client для Android может позволить злоумышленнику, не прошедшему аутентификацию, получить контроль над сервисом или вызвать отказ в обслуживании (DoS) ([CVE-2019-16007](#)).

Remote Desktop Gateway

Уязвимости с высоким уровнем опасности: возможность удаленного выполнения кода из-за уязвимостей в клиенте удаленного рабочего стола, когда пользователь подключается к вредоносному серверу ([CVE-2020-0817](#), [CVE-2020-0734](#), [CVE-2020-0681](#), [CVE-2020-0611](#), [CVE-2019-1333](#), [CVE-2019-1291](#), [CVE-2019-1290](#), [CVE-2019-0788](#), [CVE-2019-0787](#)).

В службах удаленных рабочих столов, ранее известных как службы терминалов, есть опасная уязвимость удаленного выполнения кода: злоумышленник, прошедший аутентификацию, злоупотребляет перенаправлением буфера обмена ([CVE-2020-0655](#)).

Критически опасные уязвимости удаленного выполнения кода есть в шлюзе удаленных рабочих столов Windows (RD Gateway): злоумышленник, не прошедший аутентификацию, подключается к целевой системе с помощью RDP и отправляет специально созданные запросы ([CVE-2020-0610](#), [CVE-2020-0609](#)).

Check Point

Check Point IKEv2 IPsec VPN версий ниже R80.30 может позволить злоумышленнику со знанием внутренней конфигурации успешно подключиться к VPN-серверу «сайт—сайт» ([CVE-2019-8456](#)).

Критически опасная уязвимость есть в клиенте Check Point Endpoint Security для Windows версии E80.83 с блейдом VPN. Он запускает процесс без использования кавычек в пути. Это может вызвать загрузку ранее размещенного исполняемого файла с именем, похожим на части пути, вместо намеченного ([CVE-2019-8459](#)).

Еще одна уязвимость клиента Check Point Endpoint Security под Windows, но уже для версий ниже E81.30. Он пытается загрузить отсутствующий файл DLL из разных каталогов переменной окружения %PATH%. Атакующие могут использовать это для повышения привилегий, используя специально созданную библиотеку DLL, расположенную в любом месте %PATH%, доступном для пользователя с правами на запись ([CVE-2019-8461](#)).

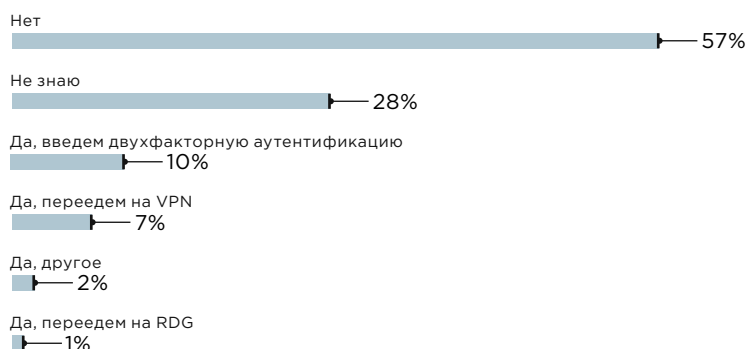
TeamViewer

Опасная уязвимость обнаружена в TeamViewer 14.2.2558. Она позволяет перехватывать учетные данные в открытом виде из памяти процессов ([CVE-2019-11769](#)). Еще одна уязвимость позволяет не только расшифровать пароль пользователя, но и повысить привилегии до системных ([CVE-2019-18988](#)).

Что изменится в ближайшее время

Больше половины компаний не планируют менять способы организации удаленки в ближайшие месяцы. Вероятно, их все устраивает, либо они надеются, что удаленная работа скоро закончится, и поэтому не готовы вкладываться в организацию безопасного удаленного доступа. Только каждая десятая организация будет вводить двухфакторную аутентификацию.

Планируете что-то менять в организации удаленки в ближайшие месяцы?

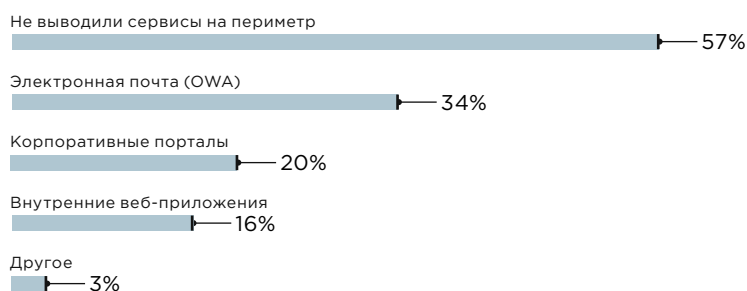


Мы рекомендуем всем компаниям использовать двухфакторную аутентификацию с помощью аппаратных токенов. Это поможет снизить риск компрометации сети компании в случае подбора словарного пароля сотрудника.

Какие сервисы выведены на периметр

43% респондентов отметили, что в их компаниях выведены какие-либо сервисы на периметр. 34% компаний вывели на периметр электронную почту, каждая пятая компания — корпоративные порталы, 16% — внутренние веб-приложения. Вместе с удобством пользования это влечет риски безопасности.

Какие дополнительные сервисы вашей компании выведены на периметр в связи с карантином и удаленной работой?



Зачастую IT-подразделение выводит сервисы на периметр без уведомления службы ИБ: они узнают об этом с помощью сервисов по мониторингу периметра или уже во время расследования инцидента. Если в вашей компании на периметре теперь доступна только почта, то вы можете быть спокойны при условии, что у вас строгая парольная политика и она соблюдается сотрудниками.

Но если вы среди тех, кто вывел корпоративные порталы или внутренние веб-приложения, то обеспечьте их защиту: в среднем на одно веб-приложение приходятся 22 уязвимости, четыре из которых имеют высокий уровень риска. Уязвимое приложение на периметре может стать открытой дверью для злоумышленников.

Чтоб снизить риск возникновения инцидентов:

- используйте WAF — они хорошо справляются с защитой и выявлением атак на опубликованные сервисы под тонкие клиенты;
- следите за соблюдением парольной политики;
- не забывайте про двухфакторную аутентификацию.

Общие рекомендации

Если ранее для компаний более актуальной была защита от внешних угроз, то сейчас сами пользователи систем становятся внешней угрозой. Здесь как с коронавирусом — вышел за дверь, можешь вернуться зараженным и заразить других. Пользователи перестают быть доверенной стороной при подключении к инфраструктуре.

Как сделать бизнес более защищенным при удаленной работе:

- Проверьте версию ПО, через которое в вашей компании организован удаленный доступ. Если она имеет критически опасную уязвимость, срочно обновитесь до последней версии. Регулярно проверять защищенность инфраструктуры помогут [сканеры уязвимостей](#).
- Проверьте, какие сервисы опубликованы на периметре. Найти их можно с помощью сервиса по мониторингу сетевого периметра [Advanced Border Control](#) от PT Expert Security Center. Так вы узнаете, если на узлах сетевого периметра появились новые сервисы и уязвимости, которые могут быть использованы потенциальным нарушителем для проведения атак со стороны сети Интернет.
- Если в вашей компании на периметр выведены корпоративные порталы или внутренние веб-приложения, используйте [web application firewall](#) для защиты их от атак (лучше в режиме «в разрыв») и проверьте их на наличие уязвимостей и ошибок в коде с помощью [анализатора защищенности приложений](#).
- Следите за аномалиями в подключениях и в сетевом трафике. Для этого потребуется [SIEM-система](#) как информационный центр мониторинга, который собирает информацию о происходящем со всех узлов защищаемой сети. В связке с SIEM [решение NTA](#) позволит определять пользователей, которые авторизуются на VPN-сервере, и отслеживать их действия внутри сети. Подробно про выявление сетевых аномалий во время удаленной работы мы рассказали [на вебинаре](#).
- Запретите раздельное туннелирование. Это позволит оперативно выявлять ситуации, когда сотрудники «ловят» на устройство, с которого они подключаются во внутреннюю сеть, вредоносное ПО на просторах интернета.

О других важных рекомендациях по защите IT-инфраструктуры при удаленном режиме работы мы рассказали [в отдельной статье](#).

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «Новости» на сайте ptsecurity.com.