

# Как обеспечить безопасность удаленного рабочего места



**GFI**<sup>TM</sup>

Aurea SMB Solutions

## Содержание

	Введение	3
---	----------	---

---

### Проблемы безопасности при удаленной работе, которые следует учитывать системным администраторам

	Значительное увеличение онлайн-коммуникации	6
---	---	---


---

	Сканирование и обновление программного обеспечения на удаленных устройствах	8
---	---	---

---

	Обеспечение безопасности домашней сети	11
---	--	----

---

	Использование зашифрованных резервных копий для резервного копирования всех данных	12
---	--	----

---

	Насколько сложно обеспечить безопасность удаленного рабочего места?	13
---	---	----

---

	Защитите свой бизнес с помощью Unlimited   Network Security	13
---	---	----



## Введение

Ваш малый бизнес изменился самым неожиданным образом. Даже если вы не работаете в учреждении, где действуют распоряжения об обязательной самоизоляции, вы хотите обеспечить безопасность своих сотрудников.

Вследствие этого ваш бизнес мог частично или полностью переместиться в удаленный формат.

Это усложняет необходимость обеспечивать безопасность всех файлов и коммуникаций. Компьютеры, управляющие вашим бизнесом, больше не могут находиться исключительно в ваших офисах.

Куда же вам деваться? Ваш бюджет ограничен. В вашей команде нет ИТ-специалистов по организации удаленной работы. Ваш бизнес-план, скорее всего, не предусматривал обеспечения интернет-безопасности на случай форс-мажорного события, при котором все сотрудники должны оставаться дома.

Многие виды бизнеса начали привлекать удаленных сотрудников еще до пандемии COVID-19. Для других это означает наличие зарекомендовавших себя передовых методов и экономичного программного обеспечения, которые облегчат жизнь, обеспечат безопасность компании,

## Проблемы безопасности при удаленной работе, которые следует учитывать системным администраторам

### **Значительное увеличение онлайн-коммуникации**

Теперь, после перехода столь многих взаимодействий и коммуникаций в интернет-формат, вам необходимо обеспечить надежную защиту электронной почты и коммуникации в целом.

И если обеспечение безопасности в видеочате обычно сводится к выбору наиболее пригодного для сохранения конфиденциальности программного обеспечения исходя из ваших потребностей, то выбор электронной почты имеет больше нюансов. Электронная почта должна быть защищена от множества угроз, включая несанкционированный доступ или потерю данных.

Несанкционированные проникновения посредством электронной почты могут быть фишинговыми атаками, спамом или вредоносным ПО с ложными темами, содержимым, вложениями или ссылками, заманивающими пользователей. Вы нуждаетесь в комплексной службе защиты от спама в сочетании с разъяснением сотрудникам природы и внешних признаков этих атак.

Количество фишинговых атак, направленных на работающих из дома сотрудников, вероятно, будет расти, поскольку злоумышленники будут знать об увеличении числа людей, выступающих в этой новой и потенциально менее защищенной роли.

Существует множество видов атак, в том числе направленных на работающих из дома сотрудников. Эти атаки могут лишить людей денег, поставить под угрозу жизненно важную информацию и открыть вашу компанию для других атак. Можно распознать потенциальные попытки несанкционированного доступа, если знать, на что обращать внимание. Предложите сотрудникам пройти курс повышения квалификации, чтобы ознакомить их с современными видами мошенничества по электронной почте и фишинговыми атаками.

Злоумышленники всё также могут использовать незащищенную электронную почту в качестве точки входа для доступа к вашей сети. Чтобы предотвратить



это, убедитесь, что у всех есть надежный пароль и включена многофакторная аутентификация (МФА).

Вашей компании также следует рассмотреть в качестве передового метода автоматизированное решение для шифрования электронной почты, которое анализирует трафик исходящих сообщений для распознавания и шифрования конфиденциальных материалов.

Если вы пользуетесь большой почтовой программой на базе браузера, такой как Gmail, каждое ваше письмо уже шифруется протоколом безопасности транспортного уровня (TLS). Этот тип шифрования не так безопасен, как сквозное шифрование, поэтому вам все равно нужно пользоваться и другим сервисом для передачи конфиденциальных данных. Если все сотрудники вашей компании следуют перечисленным выше советам: обеспечивают безопасность своих учетных записей, избегают ссылок на вредоносные программы и распознают фишинговые схемы — ваши коммуникации безопасны для удаленной работы.

### **Инструменты, необходимые для решения этой проблемы безопасности**

- ✓ Антивирус со встроенным сканированием электронной почты
- ✓ Инструменты защиты от фишинга и интернет-безопасности (обычно встроены в браузер)

### **Передовые методы**

- Обучайте своих сотрудников распознавать все распространенные фишинговые и спам-атаки
- Будьте чрезвычайно внимательны ко всем ссылкам и вложениям, получаемым по электронной почте, особенно от неизвестных отправителей
- Обеспечивайте соблюдение надлежащих правил пользования паролями
- Обеспечивайте использование двухфакторной аутентификации
- Пользуйтесь более безопасными методами сквозного шифрования при передаче конфиденциальных данных



## Сканирование и обновление программного обеспечения на удаленных устройствах

В обычных обстоятельствах ваша команда ИТ-специалистов следует графику и сложившейся практике, немедленно проводя важные обновления и планируя маловажные на ночное или нерабочее время, чтобы не мешать работе сотрудников. А теперь в вашей сети есть компьютеры, больше не находящиеся в офисе.

Чтобы обеспечить безопасность всех рабочих мест при удаленной работе, вам необходимо программное обеспечение, сканирующее и устанавливающее обновления на всех удаленных устройствах. **Каждая третья утечка данных** вызвана нескорректированными с помощью обновлений уязвимостями программного обеспечения. Эти нарушения в системе безопасности можно было бы предотвратить, просто убедившись, что все уязвимости программ исправлены.

При переходе на удаленную работу это осуществить сложнее, но вполне возможно. Есть программные опции, созданные именно для этой цели. Ваша команда ИТ-специалистов может следовать своему локальному плану обеспечения безопасности с небольшими изменениями. Программное обеспечение на устройствах ваших сотрудников может постоянно обновляться и быть защищенным, даже при удаленной работе.

### Инструменты, необходимые для решения этой проблемы безопасности

- ✓ Сетевой монитор
- ✓ Программное обеспечение для дистанционного управления

### Передовые методы

- Оценивайте свою сеть и проводите полную инвентаризацию. Регулярно сканируйте свою сеть для выявления отсутствующих
- Убеждайтесь, что все операционные системы в вашей сети защищены (например, нечто, о чем вам не приходится беспокоиться, если вы не работаете удаленно, если на каждом компьютере в вашем офисе работает только Windows)

- Планируйте время для запуска обновлений, не забывая при этом о важных обновлениях, которые необходимо производить немедленно
- Тестируйте обновления после установки и будьте готовы к возврату ПО в предыдущее состояние после вызывающих проблемы обновлений до тех пор, пока не будет найдено решение или не будет выпущено новое обновление
- Выявляйте все уязвимости с помощью удаленного сканирования, даже те, которые не связаны с отсутствием обновлений





## Обеспечение безопасности домашней сети

Еще один важный шаг к защите рабочих мест удаленных сотрудников — обеспечение готовности и надежности системы безопасности их домашней сети.

### Шифрование данных при передаче

При работе из дома важно шифрование данных ваших сотрудников. Для сохранения конфиденциальности материалов все сотрудники вашей компании должны дома пользоваться сетью VPN для доступа к конфиденциальной информации.

Сеть VPN предоставляет зашифрованный туннель, защищающий ваш веб-трафик, и отвязывает вас от вашего конкретного IP-адреса. Это дает больше конфиденциальности вашей компании и сотрудникам.

В зависимости от вашей сети VPN сотрудники могут увеличить риск для вашей сети из-за подключения к потенциально незащищенным устройствам. Убедитесь, что сотрудники знают об этом риске и пользуются сетью VPN только для доступа к рабочим данным.

### Зашифрованный Wi-Fi

Хотя безопасность личного Wi-Fi нарушается редко, однако, если это происходит, злоумышленник может перехватить все, что вы отправляете или вводите в Интернете: банковскую информацию, учетные записи электронной почты, учетные данные корпоративного доступа и многое другое.

Убедитесь, что ваша сеть правильно настроена и вы зашифровали свое соединение. WPA2 или в настоящее время WPA3 обычно считается лучшим вариантом для шифрования Wi-Fi, и ваш пароль для доступа к Wi-Fi должен быть надежным.



## Изменения данных маршрутизатора

Вам необходимо изменить логин и пароль вашего маршрутизатора. Они могут быть стандартными (например, admin) и ненадежными или легко угадываемыми. Злоумышленники пользуются этим, чтобы захватить маршрутизатор, превратив его в бота или позволив взломщикам шпионить за вами, поскольку ваша онлайн-информация пересылается через маршрутизатор. Убедитесь, что обновления прошивки устанавливаются автоматически для устранения уязвимостей системы безопасности.

В зависимости от уровня безопасности, который требуется вашему бизнесу, вы также можете предпринять дополнительные шаги: ограничить входящий и исходящий трафик сотрудников, выбрать шифрование с самым высоким уровнем безопасности, установленным в настройках их маршрутизаторов, и отключить точки беспроводного доступа. Эти шаги создают неудобства для пользователя, поэтому прибегайте к ним только в случае крайней необходимости.

## Настройки брандмауэра

Дважды проверьте настройки брандмауэра, чтобы усилить безопасность домашней сети. Брандмауэры создают барьер для предотвращения попыток проникновения в вашу систему. Это помогает двумя способами: защищает вашу сеть от проникновения вредоносных программ и предотвращает утечку данных с ваших домашних устройств.

Обычно брандмауэры уже встроены в ваши устройства. Убедитесь, что они включены в ваших настройках. Представителям малого бизнеса может потребоваться более комплексный план безопасности для усиления брандмауэра, предоставленный сторонним поставщиком.



## Установите локальные антивирусные решения на личные устройства

Хотя на компьютерах, которыми вы пользуетесь в офисе, уже может быть установлена локальная антивирусная защита, многие сотрудники сейчас пользуются личными устройствами, на которых антивируса может и не быть. Даже если они последуют другим советам, плохо защищенные устройства представляют собой значительную угрозу безопасности.

Убедитесь, что на компьютерах, которыми ваши сотрудники пользуются дома, установлены мощные антивирусные решения. Из-за обстоятельств, возможно, придется купить надежное антивирусное решение для устройств ваших сотрудников, по крайней мере, на то время, пока на них должна находиться конфиденциальная информация компании.

Очень важно обеспечить защиту всей информации, имеющей отношение к вашему бизнесу, включая защиту личных устройств и своевременную установку обновлений для этих решений.

## Инструменты, необходимые для решения этой проблемы безопасности

- ✓ Сеть VPN
- ✓ Управление пропускной способностью
- ✓ Инструменты для усиления брандмауэра
- ✓ Антивирусное решение

## Передовые методы

- Всегда используйте сеть VPN при работе с ненадежными сетями
- Помните о возможностях полосы пропускания удаленной сети VPN компании
- Загружайте удаленную сеть VPN вашей компании только на устройства, которыми вы пользуетесь для работы
- Следите за тем, чтобы метод проверки подлинности и шифрование сети VPN были максимально надежными
- Постоянно отслеживайте входящие и исходящие сетевые соединения на предмет подозрительной активности

- Установите надежный пароль к вашей беспроводной сети
- Пользуйтесь личным маршрутизатором, а не тем, который вам предоставил ваш интернет-провайдер, и измените заводские имя пользователя и пароль
- Используйте самые мощные существующие возможности брандмауэра, которые всё же позволяют вам получать доступ к Интернету по желанию
- Внедрите WPA2 или WPA3 в свою беспроводную сеть
- Проводите обновления маршрутизатора
- Своевременно обновляйте антивирусное решение



### **Использование зашифрованных резервных копий для резервного копирования всех данных**

Данные не защищены должным образом без регулярного создания зашифрованных резервных копий. Это верно вне зависимости от удаленного формата работы ваших сотрудников, но приобретает еще большую важность, если они работают из дома.



У вас меньше контроля над устройствами на удаленных рабочих местах, поэтому вы никогда не можете быть достаточно уверены в их полной функциональности и безопасности. Даже такой пустяк, как пролитый на устройство кофе, может означать потерю работы или данных, если для них не будет должным образом создана резервная копия.

Хорошо защищенная система гарантирует, что все данные компании могут быть зашифрованы, выгружены и сохранены в централизованном источнике (часто в облаке, но это не обязательно), поэтому вам не нужно беспокоиться о потере важной информации из-за человеческого фактора или злонамеренных действий.

### **Инструменты, необходимые для решения этой проблемы безопасности**

 Программное обеспечение для хранения с поддержкой шифрования

### **Передовые методы**

- Часто выполняйте резервное копирование надлежащим образом
- Зашифровывайте данные во время хранения
- Решите вопрос продолжительности хранения резервной копии в зависимости от вида вашего бизнеса и нормативных требований к нему
- Рассмотрите возможность хранения наиболее важных данных более чем в одном месте (следите за тем, чтобы они по-прежнему были зашифрованы и должным образом защищены)



### **Насколько сложно обеспечить безопасность удаленного рабочего места?**

Многие из предложенных здесь действий требуют небольших изменений в сложившихся методах, которые вы уже применяли в компании, например, в службе автоматизированного управления обновлениями или регулярном резервном копировании ваших данных.

Некоторым изменениям для начала может потребоваться адаптация, но существует множество продуктов для поддержки компаний, переходящих на частично или полностью удаленный формат работы. Если вы будете следовать некоторым простым передовым методам и дополнительно привлечете несколько необходимых инструментов, ваш бизнес сможет работать безопасно в удаленном формате.



Защитите свой бизнес с помощью пакета решений по обеспечению безопасности от GFI

## Unlimited | Network Security

Многоуровневая защита для предотвращения, обнаружения и устранения угроз в вашей сети

**Secure Network** with **Firewall & Intrusion Prevention**

**Secure Traffic** with **Web & Email Antivirus**

**Secure Endpoints** with **Vulnerability Monitoring & Patching**

[Узнать подробнее](#)



Все упомянутые названия продуктов и компаний могут быть товарными знаками или зарегистрированными товарными знаками соответствующих владельцев. По имеющимся у нас сведениям, вся информация в этом документе действительна на момент его публикации. Информация, содержащаяся в этом документе, может быть изменена без предварительного уведомления.