Dr.WEB®
Сделано в России

ЗАЩИТИ СОЗДАННОЕ

Список задач

для обеспечения
информационной безопасности
при переводе сотрудников
на удаленную работу

Передайте этот документ вашему системному администратору

Список задач для обеспечения ИБ при переводе сотрудников на удаленную работу

До перевода на удаленную работу:

Действие	Отметка о выполнении
Подготовьте список программного обеспечения, рекомендованного для установки на компьютеры сотрудников, и утвердите его приказом по компании. Доведите приказ до каждого удаленного сотрудника.	
Подготовьте дистрибутивы продуктов, рекомендованных для использования сотрудниками, и выложите их в доступном для сотрудников месте вместе с инструкциями по установке, рекомендуемыми настройками и списком плагинов. Убедитесь, что программы скачаны, установлены и настроены должным образом.	
Рекомендуйте сотрудникам использовать надежные пароли, в случае необходимости помогите им выбрать и сменить пароль.	
Рекомендуйте сотрудникам установить обновления безопасности используемой операционной системы и приложений, в случае необходимости помогите им с этим. Проконтролируйте, что задача выполнена.	
Удостоверьтесь, что рабочие сервисы компании доступны извне офиса. Оцените пропускную ширину каналов Интернета и резервных каналов связи – достаточно ли ее для работы ваших сотрудников извне.	
Минимизируйте количество доступных извне сервисов компании. Каждый из них – вероятная цель атаки. По возможности отключите небезопасные бизнес-процессы, от которых можно временно отказаться. Проведите сканирование своих ресурсов на предмет уязвимостей, будьте готовы к DDoS-атакам злоумышленников.	
Если вы сомневаетесь в соблюдении мер безопасности отдельными сотрудниками, для минимизации риска ставьте им задачи, не связанные с работой с важными данными.	
Во избежание приема и отправки зараженных сообщений работать с почтой сотрудники должны через почтовый сервер компании — обеспечьте эту возможность.	
Обеспечьте антивирусную проверку почтовых сообщений на уровне почтового сервера на вредоносные программы и спам.	
Установите на устройства, с которых будет проводиться удаленная работа, средства обеспечения безопасности – антивирус, антиспам, брандмауэр, средство ограничения доступа к небезопасным ресурсам. При невозможности удаленной установки и настройки средств защиты обеспечьте сотрудников дистрибутивами средств безопасности, лицензионными ключами, проинструктируйте о порядке их установки и о рекомендуемых настройках.	
Порекомендуйте сотрудникам обновить прошивку домашнего роутера.	

Настройки антивируса должны исключать возможность намеренного изменения параметров работы программы (например, членами семьи сотрудника). Расскажите сотрудникам, как произвести настройку и проконтролируйте, выполнена ли задача.	
Порекомендуйте сотрудникам работать исключительно с правами пользователя – не администратора. Объясните им риски работы с правами администратора. Рекомендуйте для работы с корпоративными документами использовать отдельную учетную запись.	
Настройте ограничения Офисного контроля для учетной записи, используемой сотрудником для работы, чтобы предотвратить доступ сотрудника к вредоносным ресурсам.	

Если на устройства сотрудников устанавливается антивирусная защита:

Антивирусная защита компьютеров и устройств, которые используются для удаленной работы и к которым могут иметь доступ третьи лица (члены семьи и т. д.), может быть обеспечена как однопользовательскими версиями антивирусных продуктов Dr.Web без централизованного управления, так и системой централизованной антивирусной защиты компании.

Использование централизованно управляемой защиты несет меньше рисков для компании, так как сотрудник и лица, имеющие доступ к его ПК или мобильному, по умолчанию не имеют возможности отключения средств безопасности и изменения их настроек. Это уберегает от возможности взлома сети компании и хищения ее данных.

- Если для защиты удаленных сотрудников используются решения без централизованного управления:

Действие	Отметка о выполнении
Выдайте сотрудникам необходимое количество лицензий или ключевых файлов, обеспечьте их доступ к необходимым дистрибутивам, если установку будут производить сами сотрудники.	
До начала установки антивирусной защиты рекомендуется произвести антивирусную проверку с помощью актуальной версии Dr.Web CureIt!	
Проверьте наличие прав администратора для установки антивируса.	
До начала установки корпоративной антивирусной защиты удалите решения других производителей, если те были установлены.	
Поведите развертывание системы защиты.	
В случае выявления несовместимого с антивирусным агентом Dr.Web Enterprise Security Suite программного обеспечения, потенциально опасного ПО – удалите его.	
Проконтролируйте итоги развертывания защиты и сделанные настройки.	
Проведите антивирусную проверку станций сотрудников.	

- Если устройства и компьютеры сотрудников включаются в систему централизованного управления безопасности:

Действие	Отметка о выполнении
Проверьте наличие прав администратора для установки антивируса.	
Установите необходимые обновления безопасности на устройства и компьютеры.	
До установки антивирусного агента Dr.Web Enterprise Security Suite рекомендуется произвести антивирусную проверку с помощью актуальной версии Dr.Web CureIt!	
До начала установки корпоративной антивирусной защиты удалите решения других производителей, если те были установлены.	
Настройте антивирусный сервер Dr.Web, если сотрудники будут подключаться непосредственно к нему, или установите антивирусный прокси-сервер.	
Создайте в Антивирусной сети Центра управления Dr.Web отдельные группы для защищаемых станций сотрудников.	
Выполните необходимые действия по настройке созданных групп. Так, если в ходе установки необходимо будет указывать параметры доступа к антивирусному серверу или антивирусному прокси, разрешите соответствующие действия в Центре управления.	
Добавьте в Центр управления Dr.Web ключевой файл или файлы, обеспечивающие защиту необходимого числа сотрудников.	
Создайте необходимое число новых станций и раздайте сотрудникам дистрибутивы антивирусных агентов в соответствии с выбранной схемой развертывания.	
Проконтролируйте итоги развертывания защиты и созданные настройки.	
В случае выявления несовместимого с антивирусным агентом Dr.Web Enterprise Security Suite программного обеспечения, потенциально опасного ПО – удалите его.	
Проведите антивирусную проверку станций сотрудников.	
Используйте функционал Центра управления Dr.Web для контроля списка установленных обновлений и устанавливаемого сотрудниками ПО. В случае выявления потенциально опасного ПО формируйте запрещающие его использование правила с помощью модуля Контроль приложений Dr.Web.	

Подробная инструкция об удаленной защите средствами Dr.Web Enterprise Security Suite работающих вне офиса сотрудниках

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Все права на технологии Dr.Web принадлежат компании «Доктор Веб». «Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ, имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки, которые расположены в России.

Компания «Доктор Веб» — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации. Свой выбор в пользу продуктов Dr.Web сделали Государственная Дума Федерального Собрания РФ, ЦИК России, Минобороны России, Верховный Суд РФ, Совет Федерации Федерального Собрания РФ, Центральный банк Российской Федерации, многие другие государственные учреждения и крупнейшие компании.

Вот только некоторые клиенты Dr.Web: https://customers.drweb.com.

Dr.Web внесен в «Единый реестр российских программ для электронных вычислительных машин и баз данных» **Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации.**

Использование отечественного антивирусного ПО Dr.Web обеспечивает нашим клиентам защиту от рисков, связанных с изменением международной обстановки, таких как отказ в использовании, продлении, поставке или получении обновлений, а также от угроз, созданных для целенаправленных атак на предприятия и граждан России.

Со знаком качества

- «Доктор Веб» имеет сертификаты, позволяющие использовать ПО Dr.Web в организациях с повышенными требованиями к уровню безопасности.
- Dr.Web сертифицирован на отсутствие недекларированных возможностей – по 2 уровню контроля, на соответствие требованиям документа «Требования к средствам антивирусной защиты», утв. приказом ФСТЭК России № 28 от 20.03.2012 г., на соответствие требованиям ФСБ России к антивирусным средствам.
- Продукты Dr.Web применяются для защиты информации, содержащейся в различных информационных системах, в том числе информации ограниченного доступа (государственная тайна, персональные данные и т. д.).
- Его использование позволяет обеспечить надлежащее выполнение требований норм законодательства РФ о применении мер для защиты:

  – информации с ограниченным доступом (государственная тайна, персональные данные и т. д.);

  – отдельных категорий граждан от информации, причиняющей вред.

Сертификаты ФСТЭК России	**Сертификаты Минобороны России**	**Сертификаты ФСБ России**	**Все сертификаты и товарные знаки**

Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп. 12а
Тел.: +7 495 789–45–87 (многоканальный)
Факс: +7 495 789–45–97
https://антивирус.рф | https://www.drweb.ru | https://curenet.drweb.ru | https://free.drweb.ru