ФЕДЕРАЛЬНАЯ СЛУЖБА ПО
ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)
ЗАМЕСТИТЕЛЬ ДИРЕКТОРА

Старая Басманная, д. 17, Москва, 105066
Тел., факс (495) 696-49-04
E-mail: postin@fstec.ru

КО. 03.2020 № 240/ 14
На № _____

Субъектам критической
информационной
инфраструктуры
Российской Федерации

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 удаленный доступ работников к объектам критической информационной инфраструктуры, что создает дополнительные угрозы безопасности информации, связанные с несанкционированным доступом и воздействием на такие объекты.

В дистанционном режиме не допускается предоставлять удаленный 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 удаленного доступа работников на период угрозы распространения новой коронавирусной инфекции рекомендуется принятие следующих мер:

1. Проведение инструктажа работников субъектов критической информационной инфраструктуры, осуществляющих удаленный доступ к объектам критической информационной инфраструктуры, о правилах безопасного удаленного 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 удаленной работы (далее — удаленное СВТ). Для удаленного 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 удаленный доступ.

4. Назначение минимально необходимых прав и привилегий пользователям при удаленной работе.

5. Идентификация удаленных СВТ по физическим адресам (MAC-адресам) на серверах объектов критической информационной инфраструктуры, к которым будет предоставляться удаленный доступ, предоставление им доступа к информационным ресурсам объектов критической информационной инфраструктуры методом «белого списка».

6. Исключение возможности эксплуатации удаленных СВТ посторонними лицами.

7. Выделение в отдельный домен работников, управление которым должно осуществляться с серверов субъекта критической информационной инфраструктуры, и присвоение каждому удаленному СВТ сетевого (доменного) имени.

8. Обеспечение двухфакторной аутентификации работников удаленных СВТ, при этом один из факторов обеспечивается устройством, отделенным от объекта критической информационной инфраструктуры, к которому осуществляется доступ.

9. Организация защищенного доступа с удаленного СВТ к серверам объектов критической информационной инфраструктуры с применением средств криптографической защиты информации (VPN клиент).

10. Применение на удаленных СВТ средств антивирусной защиты информации, обеспечение актуальности баз данных признаков вредоносных компьютерных программ (вирусов) на удаленных СВТ путём их ежедневного обновления.

11. Исключение возможности установки работником программного обеспечения на удаленное СВТ, кроме программного обеспечения, установка и эксплуатация которого определена служебной необходимостью, реализуемое штатными средствами операционной системы удаленного СВТ или средствами защиты информации от несанкционированного доступа.

12. Обеспечение мониторинга безопасности объектов критической информационной инфраструктуры, в том числе ведения журналов регистрации действий работников удаленных СВТ и их анализа.

13. Блокирование сеанса удаленного 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 размещенными 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 удаленного доступа их работников направлены в федеральные органы исполнительной власти в установленном порядке (исх. от 20 марта 2020 г. № 240/22/1204дсп).