АДМИНИСТРАЦИЯ ПРАВИТЕЛЬСТВА КУЗБАССА

Советский проспект, д.62, г. Кемерово, 650064
Тел. (3842) 36-34-09, факс 58-31-56
e-mail: postmaster@ako.ru
http://www.ako.ru

_____ № _____

на № _____от_____

О соблюдении требований по информационной безопасности при использовании удаленного доступа

Руководителям исполнительных органов государственной власти Кемеровской области - Кузбасса

Главам городских округов, муниципальных округов и районов Кемеровской области - Кузбасса

Уважаемые коллеги!

По состоянию эпидемиологической обстановки руководителями органов исполнительной власти субъектов Российской Федерации могут быть приняты решения о переводе работников на дистанционный режим работы с использованием удаленного доступа к информационным ресурсам. Для минимизации рисков возникновения дополнительных угроз безопасности информации при переходе на дистанционный формат работы, Министерством цифрового развития и связи Кузбасса (далее – Министерство), по рекомендации ФСТЭК России, разработаны соответствующие меры защиты информации при обеспечении дистанционного режима исполнения должностных обязанностей работниками органов государственной власти субъектов Российской Федерации, органов местного самоуправления:

1. Определение и утверждение перечня информации и информационных ресурсов (программ, томов, каталогов, файлов), расположенных на серверах информационных систем государственных органов (организаций), к которым будет предоставляться удаленный доступ.

2. Определение и утверждение 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).

3. Идентификация удаленных СВТ по физическим адресам (MAC - адресам) на серверах информационных систем государственных органов (организаций), к которым будет предоставляться удаленный доступ.

4. Выделение сотрудников в отдельный домен, управление которого должно осуществляться с серверов информационных систем

государственных органов (организаций), и присвоение каждому удаленному СВТ сетевого (доменного) имени.

5. Обеспечение двухфакторной аутентификации работников удаленных АРМ, где один из факторов обеспечивается устройством, отделенным от информационной системы, к которой осуществляется доступ.

6. Организация защищенного удаленного доступа с удаленного СВТ к серверам информационных систем государственных органов (организаций) с применением сертифицированных средств криптографической защиты информации (VPN-клиент).

7. Установка на удаленные СВТ сертифицированных средств антивирусной защиты информации. Обеспечение мониторинга действий работников удаленных СВТ и ведение журналов регистрации их действий.

8. Исключение возможности установки работником программного обеспечения на удаленный СВТ, за исключением программного обеспечения, установка и эксплуатация которого определена служебной необходимостью, реализуемое штатными средствами операционной системы удаленного СВТ или сертифицированными средствами защиты информации от несанкционированного доступа.

9. Обеспечение мониторинга действий работников удаленных СВТ и ведение журналов регистрации их действий.

10. Обеспечение возможности оперативного реагирования и принятия мер защиты информации при возникновении компьютерных инцидентов.

11. Запрещается использование несертифицированных средств удаленного доступа (TeamViewer, anydesk, ammyy admin и т.д.).

12. В случае невозможности применения портативных служебных средств вычислительной техники (ноутбуков, планшетных компьютеров, мобильных устройств), с которых работникам будет предоставлен удаленный доступ к информационным системам государственных органов (организаций), Министерство считает возможным применение личных средств вычислительной техники работников при соблюдении следующих требований:

12.1. Реализовать технологию загрузки и работы по удаленному доступу к информационным системам государственных органов (организаций) с защищенных съемных машинных носителей информации по технологии Live USB.

12.2. На защищенном съемном машинном носителе информации должно быть предустановлено следующее программное обеспечение:

сертифицированная по требованиям безопасности информации операционная система или операционная система с установленным сертифицированным средством защиты информации от несанкционированного доступа;

сертифицированное по требованиям безопасности информации средство антивирусной защиты;

сертифицированное по требованиям безопасности информации средство криптографической защиты информации (VPN-клиент).

12.3. На защищенные съемные машинные носители информации должно быть установлено только программное обеспечение, предназначенное для выполнения служебных обязанностей и организации защищенного удаленного доступа.

12.4. В государственных органах (организациях) должны быть подготовлены инструкции по безопасной эксплуатации защищенных съемных машинных носителей информации, которые будут передаваться работникам совместно с указанными защищенными носителями информации.

12.5. Инструкция по безопасной эксплуатации, как минимум, должна содержать:

порядок подключения и запуска защищенных съемных машинных носителей информации через настройку базовой системы (BIOS/UEFI) личного средства вычислительной техники, обеспечивающую загрузку операционной системы с указанных защищенных носителей информации;

порядок настройки операционной системы с защищенного съемного машинного носителя информации;

правила эксплуатации работниками средств защиты информации, установленных на защищенный съемный машинный носитель информации;

ограничения по работе при использовании личного средства вычислительной техники на период удаленной работы;

запрет на подключение личных съемных машинных носителей информации при удаленной работе.

Сотрудникам исполнительных органов государственной власти Кемеровской области – Кузбасса, работающих непосредственно в локальной вычислительной сети Администрации Правительства Кузбасса, за консультацией по возникающим вопросам обращаться в отдел данных и информационной безопасности Министерства (384-2) 58-38-57.

С уважением,

заместитель Губернатора
Кемеровской области – Кузбасса
(по экономическому развитию) К. Г. Венгер

Беломытцев Роман Борисович
тел. 58-38-57 (3-47)