Требования по защите информации при осуществлении дистанционной работы

Начальник управления ФСТЭК России
Шевцов Дмитрий Николаевич

ПЕРЕХОД НА ДИСТАНЦИОННУЮ РАБОТУ ГОСУДАРСТВЕННЫХ ОРГАНОВ

Поручение Председателя Правительства Российской Федерации от 16 марта 2020 г. № ММ-П9-1861

Поручение Заместителя Председателя Правительства Российской Федерации от 18 марта 2020 г. № ДГ-П17-1987

В целях принятия мер по противодействию коронавирусной инфекции **предусмотрен перевод работников на дистанционный режим** исполнения должностных обязанностей, обеспечивающий бесперебойное функционирование федеральных органов исполнительной власти и подведомственных организаций

Рабочая группа по организации удаленного рабочего места государственного служащего в рамках федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика»

Минцифры России

ФСТЭК России

ФСБ России

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ ДИСТАНЦИОННОЙ РАБОТЫ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Исходящее письмо ФСТЭК России
от 20 марта 2020 г. № 240/22/1204

Рекомендации по применению дополнительных мер защиты информации в связи с переходом государственных служащих на дистанционный режим работы

- Определение перечня СВТ, которые будут предоставлены работникам для дистанционной работы. Для удаленного доступа запрещается использовать личные СВТ
- Идентификация удаленных СВТ по физическим (MAC-адресам)
- Выделение в отдельный домен работников и присвоение каждому удаленному СВТ сетевого (доменного) имени
- Обеспечение двухфакторной аутентификации работников удаленных АРМ
- Организация защищенного удаленного доступа с удаленного СВТ с применением сертифицированных средств криптографической защиты информации (VPN-клиент)
- Установка на удаленные СВТ сертифицированных средств антивирусной защиты информации
- Исключение возможности установки работником программного обеспечения на удаленный СВТ

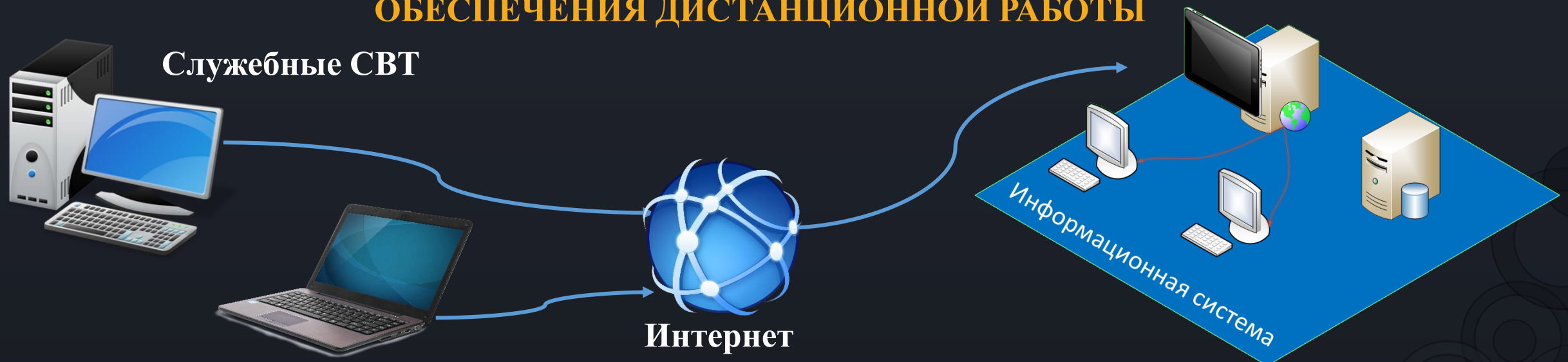
Исходящее письмо ФСТЭК России
от 30 марта 2020 г. № 240/22/1379

Рекомендации по применению технологии LiveUSB для обеспечения дистанционной работы государственных служащих

- Определение перечня информации и информационных ресурсов, к которым будет предоставляться удаленный доступ
- Обеспечение мониторинга действий работников удаленных СВТ и ведения журналов регистрации их действий
- Обеспечение возможности оперативного реагирования и принятия мер защиты информации при возникновении компьютерных инцидентов

В случае невозможности применения специально предназначенных для удаленного доступа средств вычислительной техники допускается применение личных средств вычислительной техники при условии реализации технологии загрузки и работы по удаленному доступу к информационной системе государственного органа (организации) с **защищенного съемного машинного носителя информации по технологии LiveUSB**

ПРИМЕНЕНИЕ СЛУЖЕБНЫХ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ДЛЯ ОБЕСПЕЧЕНИЯ ДИСТАНЦИОННОЙ РАБОТЫ



Дополнительные угрозы

- Перехват информации по каналам передачи данных, передаваемых между служебными СВТ и информационной системой
- Утечка защищаемой информации, обрабатываемой на служебном СВТ, при его утрате (кража, потеря)
- Подмена доверенного пользователя служебного СВТ
- Внедрение на служебное СВТ вредоносного программного обеспечения

Меры защиты

- Сертифицированное средство доверенной загрузки
- Сертифицированная операционная система
- Сертифицированное средство антивирусной защиты
- Сертифицированное средство двухфакторной аутентификации пользователей, авторизация личных СВТ
- Сертифицированные СКЗИ (VPN, шифрование информации)
- Удаленный доступ к системе через технологии RDP, VDI

ДЕЙСТВУЮЩИЕ ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ДИСТАНЦИОННОЙ РАБОТЫ

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 11 февраля 2013 г. № 17

ТРЕБОВАНИЯ О ЗАЩИТЕ ИНФОРМАЦИИ, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, СОДЕРЖАЩЕЙСЯ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

УТВЕРЖДЕНЫ
приказом ФСТЭК России
от 18 февраля 2013 г. № 21

СОСТАВ И СОДЕРЖАНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

Утвержден ФСТЭК России
11 февраля 2014 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Удаленный доступ: процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ

- Многофакторная (двухфакторная) аутентификация для удаленного доступа в систему (ИАФ.1)
- Установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа (УПД.13)
- Обеспечение доверенного канала связи при удаленном доступе к системе (ЗИС.4)
- Регистрация попыток удаленного доступа (РСБ.1)
- Контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) (УПД.13)
- В информационной системе обеспечивается управление удаленным запуском компонентов программного обеспечения (ОПС.1)
- Мониторинг и контроль удаленного доступа (УПД.13)
- Очистка информации в мобильном техническом средстве после завершения сеанса удаленного доступа (ЗИС.30)

ПРИМЕНЕНИЕ ЛИЧНЫХ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ПО ТЕХНОЛОГИИ LIVE USB ДЛЯ ОБЕСПЕЧЕНИЯ ДИСТАНЦИОННОЙ РАБОТЫ

Дополнительные угрозы

- Перехват информации по каналам передачи данных, передаваемых между LiveUSB и информационной системой
- Подмена доверенного пользователя LiveUSB
- Внедрение на LiveUSB вредоносного кода через личное СВТ
- Запуск LiveUSB с неавторизованного СВТ
- Несанкционированное копирование защищаемой информации с Live USB на носители личного СВТ
- Утечка защищаемой информации за счет подключения сторонних периферийных устройств к личному СВТ при работе на LiveUSB

Меры защиты

- Сертифицированное средство доверенной загрузки
- Сертифицированная операционная система
- Средство двухфакторной аутентификации
- Сертифицированные СКЗИ для защиты канала передачи данных и шифрования защищаемой информации на Live USB
- Дистанционный доступ к системе через технологии RDP, VDI
- Централизованное управление Live USB и удаленное администрирование

РАЗРАБОТКА ТРЕБОВАНИЙ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ К СРЕДСТВАМ ДИСТАНЦИОННОЙ РАБОТЫ

Протокол заседания Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности от 26 октября 2020 г. № 3

ФСТЭК России поручено разработать и утвердить **Требования к средствам обеспечения безопасной дистанционной работы**

Проект

Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах

Проходит оценку регулирующего воздействия

Проходит экспертное обсуждение

Подготовка к утверждению и направление в Минюст России на государственную регистрацию

СОДЕРЖАНИЕ ТРЕБОВАНИЙ К СРЕДСТВАМ ДИСТАНЦИОННОЙ РАБОТЫ

Требования применяются к программно-техническим средствам защиты информации, обеспечивающим безопасную дистанционную работу в информационной (автоматизированной) системе с использованием средств вычислительной техники, не входящих в состав указанной информационной (автоматизированной) системы

Средство дистанционной работы применяется в ГИС до 1 класса защищенности включительно, в значимых объектах КИИ до 1 категории включительно, в АСУТП до 1 класса защищенности включительно, в ИСПДН до 1 уровня защищенности включительно, в ИСОП II класса

№	Требования по безопасности информации
1	К составу средства дистанционной работы
2	К конструкции защищенного носителя
3	К среде функционирования средства дистанционной работы
4	К уровню доверия средства дистанционной работы – **не ниже 4 уровня доверия**
5	К средству доверенной загрузки средства дистанционной работы – **не ниже 4 класса защиты**
6	К операционной системе средства дистанционной работы – **тип «А» не ниже 4 класса защиты**
7	К идентификации и аутентификации пользователей
8	К идентификации и авторизации средств вычислительной техники
9	К управлению доступом в средстве дистанционной работы
10	К администрированию и централизованному управлению средством дистанционной работы
11	К контролю целостности средства дистанционной работы
12	К регистрации и учету событий безопасности в средстве дистанционной работы

СОСТАВ СРЕДСТВА ДИСТАНЦИОННОЙ РАБОТЫ

Защищенный носитель

Интернет

Личные СВТ пользователей

Программное средство администрирования и централизованного управления

АРМ администратора безопасности

Программное средство двухфакторной аутентификации пользователей

Служебные СВТ пользователей

Микроконтроллер

- Средства управления периферийными устройствами и компонентами
- Встроенный энергозависимый модуль памяти
- Оперативное запоминающее устройство

Энергозависимый модуль памяти

- Защищенный раздел для хранения информации
- Сертифицированные СЗИ
- Системный раздел

СОВЕРШЕНСТВОВАНИЕ ТРЕБОВАНИЙ О ЗАЩИТЕ ИНФОРМАЦИИ

Проект

Изменения в Требования О защите информации, не составляющей государственную т содержащейся в государственн информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. № 17

Проект

ИЗМЕНЕНИЯ В МЕТОДИЧЕСКИЙ ДОКУМЕНТ

«МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ»

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационной системы		
		3	2	1
I. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)				
ЗИС.31	Защита информационной системы при применении средств, обеспечивающих безопасную дистанционную работу в информационной системе с использованием средств вычислительной техники, не входящих в её состав	+	+	+

- Вопросы по реализации требований по защите информации при дистанционной работе

- Телефоны: +7 (499) 263-2765
  +7 (499) 263-2775

- Почта: otd22@fstec.ru

Спасибо за внимание!

Начальник управления ФСТЭК России
Шевцов Дмитрий Николаевич