УТВЕРЖДЕНА

распоряжением

Администрации Тазовского района

от 24 апреля 2020 года № 94-р

**Инструкция**

**по информационной безопасности при осуществлении удаленной работы сотрудниками Администрации Тазовского района**

1. Общие положения
2. Настоящая инструкция разработана в соответствии с Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными документами по безопасности информации.
3. Инструкция определяет требования к обеспечению защиты информации при организации удаленного доступа к автоматизированным рабочим местам (далее - АРМ) и государственным информационным системам работников Администрации Тазовского района, а также устанавливает ответственность администраторов безопасности информации и пользователей, за выполнение указанных требований.
4. Удаленный доступ к АРМ и государственным информационным системам осуществляется исключительно с использованием технологий построения виртуальной частной сети (далее - VPN) и терминального доступа, определяемых работниками отдела информационных технологий управления делами Администрации Тазовского района (далее - отдел информационных технологий).
5. Координацию организации удаленного доступа к АРМ и государственным информационным системам осуществляет отдел информационных технологий.
6. Предоставление учетной записи или ключей шифрования (далее - ключевой набор) для удаленного доступа к АРМ работника осуществляется работниками отдела информационных технологий на основании служебной записки начальника отдела или подразделения Администрации Тазовского района на имя первого заместителя главы Администрации Тазовского района по внутренней политике.
7. Учетные записи для VPN или ключевые наборы могут быть предоставлены:

- для использования на мобильном рабочем месте (служебный планшетный компьютер);

- для использования на служебном ноутбуке;

- для использования на личном стационарном компьютере или ноутбуке под управлением операционных систем Microsoft Windows 7, 8, 10, MacOS Х.

1. Использование удаленного доступа для работы, предполагающей обработку конфиденциальной информации с пометкой для служебного пользования, сведений составляющих государственную тайну запрещено.
2. Ознакомление сотрудников Администрации Тазовского района с настоящей инструкцией производится с использованием региональной межведомственной системы электронного документооборота и делопроизводства автономного округа.
3. Обязанности администратора информационной безопасности
4. Администратор информационной безопасности (работник отдела информационных технологий) до предоставления удаленного доступа выполняет:
5. проверку АРМ сотрудника, переводимого на удаленную работу, на наличие сертифицированных средств защиты информации:

- средств антивирусной защиты (Kaspersky Endpoint Security для рабочих станций);

- средства защиты информации от несанкционированного доступа (Dallas Lock 8.ОС, 8.ОК);

- средства криптографической защиты информации и межсетевого экранирования уровня узла (ViPNet Client 4);

- средства электронной подписи (КриптоПро CSP 4) при необходимости подписания документов электронной подписью.

1. проверку настройки антивируса, невозможность отключения компонентов защиты пользователем, актуальность антивирусных баз.
2. проверку настройки средства защиты информации от несанкционированного доступа. Вход в операционную систему должен быть разрешен только одной доменной учетной записи работника, закрепленного за данным АРМ, заблокированы подключаемые съемные носители информации и мобильные устройства, установлены требования к сложности пароля и ограничения на возможность неверного ввода пароля не более 5 раз.
3. Проверку настройки средства криптографической защиты информации и межсетевого экранирования уровня узла. В сетевых фильтрах открытой сети должны быть заблокированы все входящие подключения за исключением протоколов: RDP, ICMP, DHCP, NetBIOS, IGMP. Убедиться, что пользователь не может отключать защиту сетевого трафика и менять настройки сетевых пакетных фильтров.
4. Проверку на отсутствие установленного программного обеспечения (далее - ПО) не входящего в перечень разрешенного к установке. (Перечень разрешенного ПО указан в аттестате соответствия требованиям защиты информации).
5. Осуществляет информирование пользователей АРМ о появлении актуальных угрозах безопасности информации, о правилах безопасной эксплуатации государственных информационных систем, находящихся в использовании.
6. Инструктирует сотрудников, получающих удаленный доступ, по требованиям к защите информации, а также доводит положения организационно-распорядительных документов по защите информации с учетом внесенных в них изменений.
7. Оказывает помощь сотруднику, получающему удаленный доступ, по установке ПО, реализующего технологию VPN, а также при необходимости подписания документов электронной подписью, драйвера для ключевых носителей (Рутокен, JaCarta и т.п.).
8. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов, администратор безопасности выполняет действия для приостановления (блокирования) удаленного доступа.
9. Обязанности пользователя удаленного доступа
10. Обеспечить установку актуальных обновлений операционной системы на используемом для удаленной работы стационарном компьютере или ноутбуке (далее - компьютер)
11. Для входа в учетную запись компьютера необходимо установить надежный пароль, содержащий не менее 12 знаков.
12. Обеспечить наличие на компьютер под управлением операционных систем Microsoft Windows 7, 8, 10 лицензионного антивирусного ПО, с настроенным автоматическим обновлением антивирусных баз.
13. Обеспечить использование учетных данных или ключевых наборов для авторизации в ПО для VPN только в служебных целях. Исключить их передачу посторонним лица, коллегам, членам семьи.
14. На время использования личного компьютера для удаленного доступа к АРМ необходимо ограничить доступ к компьютеру со стороны членов семьи. Каждый раз покидая свое удаленное рабочее место необходимо блокировать экран компьютера (используя «горячие клавиши» Windows: WIN + L, MacOS: Ctrl+Cmd+Q). Исключить передачу компьютера с установленным ПО для VPN посторонним лицам, в том числе для ремонта или обслуживания.
15. При необходимости подписания документов электронной подписью выполнять подключение ключевого носителя (Рутокен, JaCarta и т.п.) к компьютеру. После завершения работы принять меры по исключению использования служебной электронной подписи посторонними лицами, членами семьи.
16. Исключить использование публичных точек доступа к сети Интернет (кинотеатры, кафе и т.п.), сторонних прокси-серверов и VРN­ сервисов, позволяющих обходить блокировки посещения интернет-сайтов запрещенных в Российской Федерации.
17. Исключить использование личной электронной почты, облачных файловых хранилищ (Dropbox, Яндекс.Диск, GoogleDocs/Disk, MS OneDrive, Mega и т.д.) для передачи служебных х документов.
18. Не допускать копирование на личный компьютер любых файлов с АРМ и обратно.
19. В случае подозрения на заражение компьютера или АРМ вредоносным программным обеспечением (появилось уведомление от антивируса об обнаружении вредоносного ПО, в интернет-браузере начали появляться всплывающие баннеры с рекламой даже на официальных сайтах государственных органов, курсор мыши начал самостоятельно передвигаться) необходимо незамедлительно обратиться в отдел информационных технологий.
20. По окончанию рабочего времени обеспечить отключение от удаленного рабочего стола АРМ и завершение VPN сессии. Использование служебного VPN вне рабочего времени не допускается.
21. При использовании для к домашней сети Wi-Fi­poyтepa, обеспечить заблаговременную смену пароля доступа на устойчивый к подбору (не менее 12 символов, содержащих буквы, цифры и специальные символы:@,?,%,$).
22. Ответственность
23. Администратор информационной безопасности несет персональную ответственность за выполнение требований, предусмотренных пунктом 2 настоящей инструкции.
24. Сотрудники Администрации Тазовского района, которым предоставлен удаленный доступ к АРМ, несут персональную ответственность, предусмотренную трудовым, административным, уголовным законодательством Российской Федерации за нарушения требований информационной безопасности.
25. Ответственность за своевременно реагирование на инциденты информационной безопасности и своевременное прекращение доступа удаленным пользователям в результате выявления вредоносной активности возлагается на работников отдела информационных технологий.