Приложение № 11
к приказу «Об обеспечении безопасности персональных данных в информационных системах персональных данных ФГБУЗ ММЦ им. Н.И. Пирогова ФМБА России»
№ 01-147 от 12.07.2022

Инструкция пользователя информационной системы персональных данных Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства.

1. Общие положения

1.1. Пользователь информационной системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных (далее – ИСПДн). Пользователем является каждый сотрудник Федерального государственного бюджетного учреждения здравоохранения «Мурманский многопрофильный центр имени Н.И. Пирогова Федерального медико-биологического агентства» (далее – Учреждение и Сотрудник), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.2. Пользователь несет персональную ответственность за свои действия.

1.3. Пользователь в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими обеспечение безопасности персональных данных в информационных системах персональных данных Учреждения документами .

1.4. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов в области обработки и защиты ПДн.

2.4. Соблюдать требования Инструкции по организации парольной защиты.

2.5. Соблюдать правила работы в сетях общего доступа и (или) международного обмена.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к администратору информационной безопасности.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

- Разглашать защищаемую информацию третьим лицам.

- Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

- Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

- Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

- Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

- Отключать (блокировать) средства защиты информации.

- Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

- Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

- Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl> + <Alt> + <Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных на него функций.

3. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

- Осуществлять работу при отключенных средствах защиты (антивирус и других).
- Передавать по Сети защищаемую информацию без использования средств защиты каналов связи.
- Запрещается скачивать из Сети программное обеспечение и другие файлы.
- Запрещается посещение сайтов сомнительной репутации (сайты содержащие нелегально распространяемое ПО и другие).
- Запрещается нецелевое использование подключения к сети.
