

Министерство здравоохранения Нижегородской области
Государственное автономное учреждение дополнительного профессионального
образования Нижегородской области «Центр повышения квалификации и
профессиональной переподготовки специалистов здравоохранения»
(ГАУ ДПО НО ЦПКПП СЗ)

Утверждаю



Директор ГАУ ДПО НО ЦПКПП СЗ

Л.А. Поклад /Л.А.Поклад/

10.01.2025 год

М.П.

Инструкция пользователя информационной системы персональных данных
учреждения ГАУ ДПО НО ЦПКПП СЗ

Согласовано

Заведующая отдела
комплектования

В.А. Жукова

10.01.2025 год

В.А.Жукова

Ведущий бухгалтер

А.В. Куталина

10.01.2025 год

А.В.Куталина

Специалист по кадрам

Н.В. Кулаковская

10.01.2025 год

Н.В.Кулаковская

Содержание

- 1 Общие положения
- 2 Должностные обязанности
- 3 Организация парольной защиты
- 4 Правила работы в сетях общего доступа и (или) международного обмена

Общие положения

- 1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
- 1.2. Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
- 1.3. Пользователь несет персональную ответственность за свои действия.
- 1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения ГАОУ ДПО НО ЦПК СЗ.
- 1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

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.
- 2.4. Соблюдать требования парольной политики (раздел 3).
- 2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).
- 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.
- 2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за обеспечение защиты персональных данных ГАОУ ДПО НО ЦПК СЗ.
- 2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн ответственному за обеспечение защиты персональных данных ГАОУ ДПО НО ЦПК СЗ.
- 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> 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, в пределах возложенных на него функций.

Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

Пароль должен состоять не менее чем из 8 символов.

В пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от А до Z;

строчные буквы английского алфавита от а до z;

десятичные цифры (от 0 до 9);

символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

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

4.2. При работе в Сети запрещается:

Осуществлять работу при отключенных средствах защиты (антивирус и других).

Передавать по Сети защищаемую информацию без использования средств шифрования.

Запрещается скачивать из Сети программное обеспечение и другие файлы.

Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).

Запрещается нецелевое использование подключения к Сети.