Утверждаю
Ректор
_____ Л.Н.Горбатова
«26» 05 2021 г.

ИНСТРУКЦИЯ

пользователя информационной системы персональных данных в федеральном государственном бюджетном образовательном учреждении высшего образования «Северный государственный медицинский университет» Министерства здравоохранения Российской Федерации

Версия 2.0

Дата введения: 26.05.2021.

Архангельск
2021

	Должность	Фамилия/подпись	Дата
Разработал	Директор информационно-интеллектуального центра	Трифонов И.А.	02.04.2021.
Проверил	Начальник управления правового и кадрового обеспечения	Котлов И.А.	02.04.2021.
Согласовал	Первый проректор, проректор по учебно-воспитательной работе	Оправин А.С.	02.04.2021.
	Проректор по цифровой трансформации и инфраструктурному развитию	Халезин А.С.	02.04.2021.

1. Рассмотрено на заседании Ученого совета, протокол № 12 от «14» 04 2021 г.
2. Утверждено и введено в действие приказом Ректора, № 146 от «26» 05 2021 г.
3. Соответствует требованиям СГМУ.
4. Введено в действие взамен Инструкция пользователя информационной системы персональных данных – версия 1.0.

СОДЕРЖАНИЕ

1.ОБЛАСТЬ ПРИМЕНЕНИЯ 4

2.ДОПУСК ПОЛЬЗОВАТЕЛЕЙ К РАБОТЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ 5

3.ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИСПДн 5

4.ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ ПРИ РАБОТЕ В ИСПДн 7

5.ТЕХНОЛОГИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ 8

6.ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИСПДн 9

7.УТВЕРЖДЕНИЕ И ИЗМЕНЕНИЕ ПОЛОЖЕНИЯ 10

1.ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Данная Инструкция определяет основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации в информационных системах персональных данных ФГБОУ ВО СГМУ (г.Архангельск) Минздрава России (далее - Университет).

1.2 Пользователь должен быть допущен к обработке соответствующих категорий персональных данных и иметь навыки работы на ПЭВМ.

1.3 Положения Инструкции обязательны для исполнения всеми пользователями информационных систем Университета. Пользователь ИСПДн должен быть ознакомлен под расписку с данной Инструкцией и предупрежден о возможной ответственности за ее нарушение.

1.4 Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность персональных данных, обрабатываемых и хранимых в ПЭВМ, и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

1.5 Каждый работник Университета, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и информационным активам Университета, несет персональную ответственность за свои действия.

2.ДОПУСК ПОЛЬЗОВАТЕЛЕЙ К РАБОТЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Допуск пользователей для работы в информационной системе персональных данных (далее - ИСПДн) осуществляется в соответствии со списком лиц, утвержденным руководителем Университета. 2.3. Присвоение пользователю прав доступа к ресурсам ИСПДн и определение возможного времени работы пользователя АС осуществляется администратором информационной системы персональных данных при первичной регистрации учетной записи пользователя на ПЭВМ.

2.2. При этом администратор ИСПДн производит необходимые записи в списке постоянных пользователей системы, указывая в примечании регистрационный номер и дату служебной записки, Ф.И.О. и должность лица, её утвердившую.

2.3. Учет работы пользователей ИСПДн производится средствами защиты информации (далее - СЗИ) от несанкционированного доступа (далее - НСД), установленных на ПЭВМ, в системном журнале.

3. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ ИСПДн

Пользователь информационной системы персональных данных Университета обязан:

3.1. Выполнять только те процедуры, которые определены для него в Разрешительной системе доступа к информационным активам ИСПДн.

3.2. Знать и соблюдать установленные требования по защите персональных данных, учету, хранению и пересылке носителей информации, а также руководящих и организационно-распорядительных документов Университета.

3.3. Пользователь перед началом обработки данных, хранящихся на съемных носителях информации, должен осуществить проверку файлов на наличие компьютерных вирусов. Антивирусный контроль ИСПДн должен осуществляться пользователем не реже одного раза в неделю.

3.4. Экран монитора располагать во время работы таким образом, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами, жалюзи должны быть закрыты.

3.5. Соблюдать установленный режим разграничения доступа к информационным ресурсам - получать у Администратора ИСПДн пароль, надежно его запоминать и хранить в тайне.

3.6. Немедленно докладывать Администратору ИБ и Ответственному ИСПДн обо всех фактах и попытках несанкционированного доступа к обрабатываемой в ИСПДн информации, об ее исчезновении или искажении.

3.7. Пользователям ИСПДн запрещается:

- записывать и хранить информацию на неучтенных носителях информации;
- оставлять во время работы носители информации (далее - НИ) без присмотра, передавать их другим лицам и выносить за пределы помещения, в котором разрешена обработка информации;
- отключать или блокировать средства защиты информации, предусмотренные организационно-распорядительными документами Университета;
- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ;
- сообщать или передавать посторонним лицам личные атрибуты доступа к ресурсам ИСПДн;
- производить копирование отдельных файлов с учтенных НИ на неучтенные НИ, в том числе для временного хранения информации;
- работать в ИСПДн при обнаружении каких-либо неисправностей;
- хранить НИ вблизи сильных источников электромагнитных излучений и прямых солнечных лучей;
- хранить на учтенных НИ программы и данные, не относящиеся к рабочей информации;
- привлекать посторонних лиц для ремонта и обслуживания ИСПДн.

4. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ ПРИ РАБОТЕ В ИСПДн

4.1. Личные пароли доступа к объекту информатизации, системе защиты от НСД, выдаются пользователям Ответственным ИСПДн (Администратором ИС), в случае самостоятельного выбора пароля руководствоваться Инструкцией по организации парольной защиты в информационных системах ФГБОУ ВО СГМУ(г.Архангельск) Минздрава России.

4.2. Лица, использующие пароли, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по использованию паролей;
- своевременно сообщать Администратору ИС и Администратору ИБ о всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

4.3. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.

4.4. Полная плановая смена паролей на ИСПДн проводится не реже 1 раза в год.

4.5. Удаление (в том числе, внеплановая смена) личного пароля любого пользователя ИСПДн должна производиться в следующих случаях:

в случае подозрения на дискредитацию пароля; по окончании срока действия;

в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) пользователя после окончания последнего сеанса работы с системой;

по указанию Администратора ИСПДн.

4.6. Для предотвращения доступа к персональным данным, находящейся в ПЭВМ, минуя ввод пароля, пользователь во время перерыва в работе обязан осуществить блокирование системы нажатием комбинации СЫ+ЛИ+Ь или кнопки «Блокировать».

Порядок применения (смены) паролей при работе на ПЭВМ, оборудованных системой защиты от НСД, приведен в эксплуатационной документации на СЗИ.

5.ТЕХНОЛОГИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. При первичном допуске к работе на ИСПДн Пользователь знакомится с требованиями руководящих, нормативно-методических и организационно-распорядительных документов по вопросам автоматизированной обработки информации и защиты персональных данных, изучает инструкцию

пользователя системы защиты СЗИ НСД получает личный текущий пароль у Администратора ИСПДн.

5.2. В процессе работы пользователь производит обработку персональных данных на ИСПДн с применением программного обеспечения, под управлением операционной системы, которые указаны в техническом паспорте на данную ИСПДн.

5.3. При необходимости вывод персональных данных из ИСПДн осуществляется следующим образом:

1. копированием персональных данных на учтенные носители;
2. печать бумажных копий на локальном принтере;
3. передача персональных данных по защищенным каналам связи.

6. ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ ИСПДн

6.1. Пользователь несет ответственность за:

- правильное и своевременное выполнение приказов, распоряжений, указаний руководства Университета по вопросам обеспечения безопасности персональных данных ИСПДн;
- выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;
- качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями.
- согласно действующему законодательству Российской Федерации за разглашениесведений ограниченного распространения, ставших известными ему по родуработы.

7. УТВЕРЖДЕНИЕ И ИЗМЕНЕНИЕ ПОЛОЖЕНИЯ

7.1. Настоящее Положение вводится в действие с момента подписания приказа Ректором.

7.2. Ответственность за соблюдение требований, изложенных в данном Положении, несет Директор ИИЦ.

7.3 Изменения и дополнения в Положение вносятся по инициативе:

- ректора СГМУ;
- первого проректора, проректора по учебно-воспитательной работе;
- проректор по инфраструктурному развитию
- директор ИИЦ;
- начальника управления правового и кадрового обеспечения;