СОГЛАСОВАНО:
Представитель трудового коллектива:
Председатель профсоюзной организации государственного бюджетного учреждения Вышневолоцкого дома – интерната для престарелых и инвалидов
_____ М.С. Кувшинова
«___» _____ 20___ год

УТВЕРЖДАЮ
Приложение № 2 к приказу директора государственного бюджетного учреждения Вышневолоцкого дома-интерната для престарелых и инвалидов
№ 19/3 от «18» апреля 2017 года
Директор _____ С.В. Богданова

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных государственного бюджетного учреждения Вышневолоцкого дома-интерната для престарелых и инвалидов

1. Общие положения

1.1 Инструкция пользователя информационных систем персональных данных государственного бюджетного учреждения Вышневолоцкого дома-интерната для престарелых и инвалидов (далее – Инструкция) определяет общие правила работы сотрудников в информационных системах персональных данных учреждения.
1.2 Персональные данные (далее - ПДн) относятся к категории информации ограниченного доступа.
1.3 Основные понятия и термины, используемые в настоящей Инструкции, применяются в значениях, определенных статьей 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон).
1.4 Руководители структурного подразделения, отделов, ответственные за эксплуатацию информационной системы персональных данных (далее - ИСПДн), под роспись ознакамливают пользователей ИСПДн с настоящей Инструкцией.

2. Обязанности пользователя ИСПДн

2.1 Знать и выполнять требования законодательных актов Российской Федерации, иных нормативных актов Правительства Российской Федерации, нормативно-методических документов федеральных органов исполнительной власти в области защиты персональных данных, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

2.2 Выполнять на автоматизированном рабочем месте (персональный компьютер или терминал) только те процедуры обработки персональных данных, которые определены для него должностной инструкцией.
2.3 Знать и соблюдать установленные требования по режиму обработки персональных данных, обеспечению безопасности персональных данных при их автоматизированной обработке.
2.4 Соблюдать требования парольной политики.
2.5 Соблюдать правила работы в сетях общего доступа и (или) международного обмена.
2.6 Не разглашать персональные данные, которые доверены или стали известны пользователю ИСПДн в ходе рабочего процесса во время выполнения должностных обязанностей.
2.7 Не сообщать устно или письменно, не передавать в каком-либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.
2.8 Немедленно ставить в известность руководителя структурного подразделения, отдела, администратора безопасности ИСПДн:
- при подозрении на компрометацию личных ключей и паролей;
- при обнаружении нарушения целостности пломб (наклеек) на аппаратных средствах АРМ или иных фактов совершения попыток несанкционированного доступа (далее - НСД) к ресурсам государственного бюджетного учреждения Вышневолоцкого дома-интерната для престарелых и инвалидов (далее - Учреждение);
- при несанкционированных (произведенных с нарушением установленного порядка) изменениях в конфигурации программных или аппаратных средств ИСПДн;
- при обнаружении фактов и попыток НСД и случаев нарушения установленного порядка обработки защищаемой информации.
2.9 Использовать информационные ресурсы и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.
2.10 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, в том числе через оконные проемы.
2.11 Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных в ИСПДн необходимо сообщать администратору безопасности Учреждения и непосредственному руководителю.
2.12 В случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или

периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения необходимо обращаться к администратору ИСПДн.
2.13 Ставить в известность Администратора безопасности при:
- необходимости обновления антивирусных баз;
- обновлении программного обеспечения;
- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;
- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;
- некорректном функционировании установленных средств защиты информации.
2.14 Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.
2.15 Вынос средств вычислительной техники, на которых проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п., без разрешения руководителя структурного подразделения, отдела и согласования с администратором безопасности ИСПДн запрещен. При принятии решения о выносе средств вычислительной техники, носители информации должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения, отдела Учреждения.
2.16 Пользователю ИСПДн запрещается:
- разглашать защищаемую информацию третьим лицам;
- использовать персональные данные при подготовке открытых публикаций, докладов, научных работ и т.д.;
- оставлять не запертыми и не опечатанными после окончания работы помещения и хранилища, в которых находятся ИСПДн;
- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АРМ и средств защиты информации или устанавливать на АРМ программные и аппаратные средства без согласования с администратором безопасности ИСПДн и администратором ИСПДн.
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- копировать и хранить персональные данные на неучтенных носителях информации;
- оставлять включенной без присмотра рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к утечке персональных данных;
- подключать к автоматизированному рабочему месту личные внешние носители информации и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- сообщать (передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям 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 6 символов;
- 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 уч□том регистра, в котором пароль был;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).
3.5 Правила хранение 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 безопасности ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

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

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 персональных данных (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 (сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

5. Ответственность

5.1 Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации. За нарушение требований настоящей инструкции, порядка работы с документами и машинными носителями, содержащими ПДн, должностные лица могут быть привлечены к дисциплинарной или иной, предусмотренной законодательством ответственности.