УТВЕРЖДАЮ
Директор ГБУ
«Сормовский дом-интернат»
_____ Т.Ю. Фадеева
21 февраля 2018 г.

ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ГБУ «СОРМОВСКИЙ ДОМ-ИНТЕРНАТ»

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1.Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных ГБУ «Пансионат ветеранов войны и труда».
1.2.Администратор безопасности информационных систем персональных данных является сотрудником Учреждения.
1.3 .Администратор безопасности обладает правами доступа к любым программным и аппаратным ресурсам Учреждения.
1.4.Целью защиты информации является:
1.4.1.Предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности.
1.4.2.Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в Учреждении.
1.4.3.Сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации.
1.4.4.Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.
1.5.Основными видами угроз безопасности информационных систем являются:
1.5.1. Противоправные действия третьих лиц.
1.5.2.Ошибочные действия пользователей.
1.5.3.Отказы и сбои технических средств, приводящие к её модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

II. ОБЩИЕ ОБЯЗАННОСТИ

Администратор безопасности ИСПДн обязан:
2.1. Знать перечень сведений, составляющих персональные данные и условия обработки персональных данных в Учреждении.
2.2. Знать перечень установленных в отделах Учреждения технических средств.
2.3. Определять полномочия пользователей.
2.4. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

2.5. Реагировать на попытки несанкционированного доступа к информации.
2.6. Осуществлять контроль за установкой и осуществлением настройки средств защиты информации в рамках компетенции.
2.7. Периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных.
2.8. Проводить работу по выявлению возможных каналов утечки персональных данных, изучать текущие тенденции в области защиты персональных данных.
2.9. Вносить свои предложения по совершенствованию мер защиты персональных данных, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.
2.10.Осуществлять контроль за обслуживанием установленных средств криптографической защиты информации (в том числе персональных данных).
2.11.Знать законодательство РФ о защите персональных данных, следить за его изменениями.

III. ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

3.1. К использованию в Учреждении допускаются только лицензионные средства антивирусной защиты.
3.2.Установка средств антивирусного контроля на компьютерах и серверах осуществляется под контролем администратором безопасности.
3.3.Антивирусный контроль должен быть настроен в режиме постоянной антивирусной защиты.
3.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после её приёма. При передаче файлов, запакованных в архивы, без их распаковки, должна вручную инициироваться антивирусная проверка этих архивов.

IV. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

4.1. Опечатанные конверты с паролями сотрудников должны храниться в сейфе. Для опечатывания конвертов применяется гербовая печать Учреждения. Все конверты с паролями в обязательном порядке фиксируются в «Журнале учёта паролей пользователей информационной системы персональных данных».
4.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учётной записи сразу после окончания последнего сеанса работы данного
пользователя с системой.
4.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственных за организацию обработки персональных данных, администраторов информационной системы и других сотрудников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.
4.4. Администратор безопасности ведёт «Журнал учета паролей пользователя информационной системы персональных данных», в котором он отмечает причины внеплановой смены паролей пользователей.

V.ПРАВА

Администратор безопасности имеет право:

5.1.Требовать от пользователей выполнения инструкций в части работы с программными, аппаратными средствами и персональными данными.
5.2.Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

VI. ОТВЕТСТВЕННОСТЬ

6.1. Администратор несёт персональную ответственность за
соблюдение требований настоящей Инструкции.
6.2. Администратор при нарушении норм, регулирующих
получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.