Областное государственное общеобразовательное бюджетное учреждение
«Специальная (коррекционная) школа-интернат»

УТВЕРЖДАЮ
Директор школы
А.В. Белова
«_01 »сентября 2022 г.

Инструкция
администратора безопасности информации ИСПДн
в ОГОБУ СКШИ с. Ленинское

1. **Общие положения.**

Настоящая инструкция определяет функции, права и обязанности администратора безопасности информации ИСПДн по вопросам обеспечения информационной безопасности при работе с персональными данными в ИСПДн 3 класса.

Администратор безопасности информации назначается из числа сотрудников ОГОБУ СКШИ с.Ленинское и обеспечивает правильность использования и нормальное функционирование установленных систем защиты информации от НСД, резервное копирование персональных данных, обновление антивирусных баз, периодический анализ защищённости.

Настоящая инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных, и не исключает обязательного выполнения их требований.

2. **Основные функции администратора безопасности информации.**

2.1 Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения защиты персональных данных при их обработке в ИСПДн.

2.2 Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в ИСПДн:

¨ реализация полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам и т.д.);

¨ ввод описаний пользователей автоматизированной системы (АС) в информационную базу установленного на АС, СЗИ от несанкционированного доступа (НСД);

¨ своевременное удаление описаний пользователей из базы данных СЗИ от НСД при изменении списка допущенных к работе на АС лиц.

2.3 Контроль доступа лиц в помещения, где установлены АС в соответствии со списком сотрудников, допущенных к работе на АС.

2.4 Контроль за ежемесячным проведением смены паролей для доступа к АС пользователями соответствующих АС.

2.5 Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

¨ введение в базу данных установленных на АС, СЗИ от НСД;

¨ своевременное информирование ответственного о несанкционированных действиях персонала и проведение расследования попыток НСД.

Сопровождение подсистемы обеспечения целостности информации в ИСПДн:

1. периодическое тестирование функций установленных на АС СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;
2. восстановление программной среды, программных средств и настроек СЗИ при сбоях;
3. ведение двух копий программных средств СЗИ от НСД и контроль их работоспособности;

4. поддержание установленного порядка и правил антивирусной защиты информации в ИСПДн;
5. периодическое обновление антивирусных средств (баз данных), установленных на АС, контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования АС;
6. периодически проводить анализ защищённости ИСПДн с помощью специальной программы;
7. периодически производить резервное копирование персональных данных на отчуждаемый носитель информации (flash-накопитель);
8. периодический анализ защищённости ИСПДн с помощью специальной программы.

Сопровождение подсистемы антивирусной защиты в ИСПДн:

Регулярно производить обновление антивирусных баз антивирусного средства (Антивирус VIPNET CLIENT, SECUPITY 9, NOD 32)

- в случае обнаружение вредоносной программы или ПМВ в ИСПДн предпринимать действия для их устранения.

3. Администратор безопасности информации имеет право:

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;
- требовать прекращения обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4. Администратор безопасности информации обязан:

- обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;
- проводить инструктаж пользователей по правилам работы на АС с установленными СЗИ от НСД;
- в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- докладывать ответственному о неправомерных действиях пользователей, приводящих к нарушению требований по защите персональных данных;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.