УТВЕРЖДЕНО
Приказом руководителя
МУ ДО «СШ № 1»
от «28» декабря 2024 г. № 134-ОД

Инструкция администратора информационной безопасности Муниципального бюджетного учреждения дополнительного образования Петрозаводского городского округа «Спортивная школа № 1» (МУ ДО «СШ № 1»)

1. Общие положения

1.1. Инструкция администратора информационной безопасности регламентирует вопросы обеспечения конфиденциальности при проведении работ с использованием персональных данных.

1.2. Администратор информационной безопасности назначается на должность и освобождается от должности на основании распорядительного акта руководителя МУ ДО «СШ № 1» (далее соответственно - администратор информационной системы, организация).

2. Основные функции администратора информационной безопасности

2.1.Контроль за исполнением установленного комплекса мероприятий по обеспечению безопасности персональных данных в информационных системах персональных данных (далее - ИСПДн).

2.2. Организация доступа пользователей ИСПДн к защищаемым информационным ресурсам ИСПДн.

2.3. Обеспечение целостности данных в защищаемом сегменте компьютерной сети.

2.4. Обеспечение резервного копирования данных защищаемого сегмента компьютерной сети.

2.5. Установка, настройка и сопровождение средств защиты информации.

2.6. Выполнение регламентных работ по обслуживанию средств защиты информации в соответствии с руководствами по эксплуатации.

2.7. Анализ событий информационной безопасности, получаемых от средств защиты информации, а также обеспечение необходимых мер по устранению нарушения информационной безопасности (оперативное реагирование на поступающие сигналы о нарушениях установленных правил доступа, анализ журналов регистрации событий безопасности и т.п.).

2.8. Организация мероприятий по предотвращению несанкционированных модификаций программного обеспечения, добавления новых функций, несанкционированного доступа к информации, аппаратуре и другим ресурсам защищаемой ИСПДн.

2.9. Периодическое тестирование функций установленных средств защиты информации при изменении программной среды и/или полномочий пользователей.

2.10. Восстановление настроек средств защиты информации после сбоев.

2.11 . Контроль за появлением новых версий программного обеспечения средств защиты.

2.12. Выполнение требований по парольной защите ИСПДн в соответствии с Инструкцией по организации парольной защиты.

2.13. Введение журналов, необходимых для учета процессов при функционировании защищаемого сегмента компьютерной сети.

2.14. Проведение инструктажа пользователей ИСПДн по внедряемым программным и (или) техническим средствам защиты.

2.14. Контроль актуальности сертификатов ФСТЭК России и ФСБ России для средств защиты информации.

2.15. Участие в разработке исходных данных и постановке задач на модернизацию защищаемого сегмента компьютерной сети.

2.16. Документирование изменений в конфигурации ИСПДн.

3. Порядок парольной защиты в ИСПДн

3.1. Администратор информационной безопасности осуществляет организационно-техническое обеспечение процессов установки и смены действия паролей пользователей ИСПДн.

3.2. Личные пароли пользователей ИСПДн должны генерироваться и распределяться в соответствии с пунктом 3 раздела 5 настоящей инструкции.

3.3. Внеплановая смена пароля пользователя ИСПДн должна производиться в случае прекращения полномочий работника организации (увольнение, переход на другую должность и другие обстоятельства) в соответствии с пунктом 3 раздела 5 настоящей инструкции.

3.4. В случае компрометации пароля пользователя ИСПДн администратор информационной безопасности выясняет обстоятельства потери и информирует о произошедшем руководство организации в соответствии с пунктом 1 раздела 5 настоящей инструкции.

3.5. Хранение значений паролей осуществляется в соответствии с пунктом 3 раздела 5 настоящей инструкции.

4. Порядок программно-технического обслуживания ИСПДн

4.1. Администратор информационной безопасности осуществляет контроль за целостностью печатей (пломб) на технических средствах ИСПДн (при наличии таковых), а также за соответствием установленного в ИСПДн программного обеспечения и технических средств, заявленных в техническом паспорте на ИСПДн.

4.2. Все работы по внесению изменений в аппаратно-программную конфигурацию ИСПДн проводятся администраторами ИСПДн, определенными документом «Матрица доступа к защищаемым информационным ресурсам ИСПДн», по согласованию с администратором информационной безопасности.

Произведенные изменения заносятся в технический паспорт на ИСПДн.

4.3. Отправка технических средств, входящих в состав ИСПДн, в ремонт или замена на новые производятся по согласованию с органом, выдавшим «Аттестат соответствия требованиям по безопасности информации» на ИСПДн.

5. Права администратора информационной безопасности

5.1. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследовании фактов несанкционированного доступа и иных инцидентов ИБ.

5.2. Требовать от работников, обрабатывающих конфиденциальную информацию, соблюдения правил обеспечения безопасности информации и выполнения требований локальных нормативных актов, регламентирующих вопросы обеспечения безопасности информации.

5.3. Требовать прекращения обработки конфиденциальной информации в случае нарушения установленных правил, порядка работ или нарушения функционирования средств защиты информации.

5.4. Запрашивать и получать необходимые материалы и документы, относящиеся к вопросам деятельности ответственного за защиту информации.

6. Перечень локальных нормативных актов, ознакомление с которыми рекомендуется в целях соблюдения требований настоящей инструкции

1. Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций.
2. Разрешительная система доступа к ПДн.
3. Инструкция по организации парольной защиты.
4. Инструкция по архивации информационных ресурсов системы.
