УТВЕРЖДЕНО
директором Центра «Поиск»
О. А. Томилиной
приказ № 514
от «28» декабря 2024 г.

И Н С Т Р У К Ц И Я

администратора информационной безопасности Центра «Поиск»

1. Общие положения

1.1. Инструкция администратора информационной безопасности (далее – Инструкция) разработана в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с Федеральным законом Российской Федерации от 27.06.2006 г. № 152-ФЗ "О персональных данных".

1.2. Настоящая инструкция определяет функции, права и обязанности администратора информационной системы по вопросам обеспечения информационной безопасности при работе с персональными данными в информационной системе Государственного автономного образовательного учреждения дополнительного образования «Центр для одаренных детей «Поиск» (далее – Центр «Поиск»).

1.3. Администратор безопасности информации (далее – Администратор) назначается приказом директора Центра «Поиск» из числа сотрудников.

1.4. Администратор в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Центра «Поиск».

1.5. Администратор обеспечивает правильность использования и бесперебойное функционирование установленных систем защиты информации.

1.6. Методическое руководство работой Администратора осуществляется директором Центра «Поиск».

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

1.8. Нарушение настоящей Инструкции влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

2. Основные функции администратора безопасности

2.1. Обеспечение функционирования и поддержание работоспособности средств и систем защиты информации в пределах возложенных функций:

– установка, настройка и своевременное обновление элементов информационных систем;

– обеспечение работоспособности элементов ИСПДн и локальной вычислительной сети;

– контроль за порядком учета, создания, хранения и использования резервных и архивных копий массивов данных.

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

– реализация полномочий доступа для каждого пользователя к элементам защищаемых информационных ресурсов;

– ввод описаний пользователей информационных систем, используемых в Центре «Поиск», в информационную базу автоматизированной системы;

– своевременное удаление описаний пользователей из информационной базы автоматизированной системы при изменении списка лиц, допущенных к работе с информационными системами.

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

– введение в базу данных автоматизированной системы описания событий, подлежащих регистрации в системном журнале;

– регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

– своевременное информирование руководителя учреждения о несанкционированных действиях персонала и проведение расследования попыток несанкционированного доступа к информации.

2.4. Сопровождение подсистемы обеспечения целостности информации в ИСПДн:

– периодическое тестирование функций установленных средств защиты информации от НСД, особенно при изменении программной среды и полномочий исполнителей;

– проведение комплекса мероприятий по восстановлению работоспособности программной среды, программных средств и настроек средств защиты информации при сбоях;

– поддержание установленного порядка и правил антивирусной защиты информации в ИСПДн;

– периодическое обновление установленных антивирусных средств (баз данных);

– резервное копирование персональных данных на резервный накопитель;

– регулярный анализ защищённости ИСПДн.

3. Обязанности администратора безопасности

3.1. Знание и выполнение требований настоящей инструкции, действующих нормативных и руководящих документов, а также внутренних инструкций, положений по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

3.2. Ведение документации на ИСПДн в соответствии с требованиями нормативных документов.

3.3. Проведение инструктажа пользователей по правилам работы в ИСПДн.

3.4. Присутствие при выполнении технического обслуживания элементов ИСПДн сторонними физическими людьми и организациями.

3.5. Обобщение результатов своей деятельности и подготовка предложений по ее совершенствованию.

3.6. Анализ причин возникновения нарушений и принятие мер по предотвращению подобных нарушений в дальнейшем.

3.7. Своевременное сообщение директору Центра «Поиск» о неправомерных действиях пользователей, приводящих к нарушению требований по защите персональных данных.

3.8. Составление служебной записки на имя директора Центра «Поиск» по факту нарушения информационной безопасности с указанием причин нарушения и принятых мер.

4. Полномочия администратора безопасности

4.1. Требование от пользователей ИСПДн соблюдения установленных технологий обработки информации, выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн.

4.2. Контроль за выполнением работниками Центра «Поиск» требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности и защиты персональных данных при их обработке в ИСПДн.

4.3. Контроль доступа лиц в помещения, где установлены серверы, в соответствии со списком сотрудников, допущенных к осуществлению работ по настройке серверов.

4.4. Контроль за регулярным проведением смены паролей доступа пользователями автоматизированной системы Центра «Поиск».

4.5. Контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования.

4.6. Прекращение обработки персональных данных в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.

4.7. Участие в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4.8. Инициирование проведения служебных проверок по фактам нарушения установленных требований обеспечения безопасности информации, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

4.9. Контроль монтажа оборудования учреждения специалистами сторонних организаций.