

«Согласовано»

Председатель профсоюзного комитета

МБОУ ДО «ЦРТ «Радуга»

Щевелёва Л.В. Щевелёва

Протокол № 41 от 01.09.2025 г.

«Утверждено»

Директор МБОУ ДО «ЦРТ «Радуга»

Щипакина Е.В. Щипакина

Принято общим собранием коллектива

Протокол № 4 от 01.09.2025 г.



Положение

об информационной безопасности

Муниципального бюджетного

образовательного учреждения

дополнительного образования

«Центр развития творчества «Радуга»

городского округа город Уфа

Республики Башкортостан

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

1. Общие положения

1.1. Настоящее Положение об информационной безопасности (далее по тексту Положение) Муниципального бюджетного образовательного учреждения дополнительного образования «Центр развития творчества «Радуга» городского округа город Уфа Республики Башкортостан (далее Учреждения) разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (редакция от 28.06.2010), методическими рекомендациями Минкомсвязи от 16.05.2019г. в целях создания безопасной информационно-образовательной среды, повышения уровня информационной безопасности в части информирования воспитанников, их родителей (законных представителей) и педагогических работников.

1.2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность.

1.3. Ответственные за информационную безопасность назначаются приказом директора Учреждения.

1.4. Ответственные за информационную безопасность подчиняются директору Учреждения.

1.5. Ответственные за информационную безопасность в своей работе руководствуются настоящим Положением.

1.6. Ответственные за информационную безопасность в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи информационных средств в Учреждении.

2. Основные задачи и функции ответственных за информационную безопасность:

2.1. Основными задачами ответственных за информационную безопасность являются:

2.1.1. организация эксплуатации технических и программных средств защиты информации;

2.1.2. текущий контроль работы средств и систем защиты информации;

2.1.3. организация и контроль резервного копирования информации.

2.2. Ответственные за информационную безопасность выполняют следующие основные функции:

2.2.1. разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.

2.3. Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.

2.4. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в Учреждение.

2.5. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.

2.6. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.

2.7. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.

2.8. Контроль пользования Интернетом.

3. Обязанности ответственных за информационную безопасность

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных на них обязанностей. Немедленно докладывать директору Учреждения о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.

3.2. Совместно с программистами принимать меры по восстановлению работоспособности средств и систем защиты информации.

3.3. Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.

3.4. Создавать и удалять учетные записи пользователей.

3.5. Администрировать работу сервера ЛВС, размещать и классифицировать информацию на сервере ЛВС.

3.6. Устанавливать по согласованию с директором Учреждения критерии доступа пользователей на сервер ЛВС.

3.7. Формировать и представлять пароли для новых пользователей, администрировать права пользователей.

3.8. Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.

3.9. Ежемесячно подавать заведующему ДООУ статистическую информацию по пользованию Интернетом.

3.10. Вести учет пользователей «точки доступа к Интернету». В случае необходимости лимитировать время работы пользователя в Интернете и объем скачиваемой информации.

3.11. Сообщать незамедлительно директору Учреждения о выявлении случаев несанкционированного доступа в Интернет.

4. Права ответственных за информационную безопасность

4.1. Требовать от сотрудников и пользователей компьютерной техники безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения и электронных платежей.

4.2. Готовить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов.

5. Ответственность ответственных лиц за информационную безопасность

5.1. На ответственных за информационную безопасность возлагается персональная ответственность за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определенными настоящим Положением.