

Автономное муниципальное дошкольное образовательное учреждение муниципального образования Динской район «Детский сад № 2»

ПРИНЯТО
Педагогическим советом
АМДОУ МО Динской район
«Детский сад №2»

Протокол № 1 от «01» сентября 2022г



ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Общие положения

Настоящее Положение об информационной безопасности (далее по тексту Положение автономного муниципального дошкольного образовательного учреждения МО Динской район «Детский сад № 2») (далее ДОУ 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).

Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность. Ответственные за информационную безопасность назначаются приказом заведующего ДОУ. Ответственные за информационную безопасность подчиняются заведующему ДОУ.

Ответственные за информационную безопасность в своей работе руководствуются настоящим Положением.

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

2. Основные задачи и функции, ответственных за информационную безопасность

Основными задачами ответственных за информационную безопасность являются:

- Организация эксплуатации технических и программных средств защиты информации.
- Текущий контроль работы средств и систем защиты информации.
- Организация и контроль резервного копирования информации на сервере ЛВС.
- Ответственные за информационную безопасность выполняют следующие

основные функции:

- Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.
- Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.
- Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДООУ.
- Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
- Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.
- Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.
- Контроль пользования Интернетом.
-

3. Обязанности ответственных за информационную безопасность

- Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных на них обязанностей.
- Немедленно докладывать заведующему ДООУ о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принимать необходимые меры по устранению нарушений.
- Совместно с программистами принимать меры по восстановлению работоспособности средств и систем защиты информации.
- Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.
- Создавать и удалять учетные записи пользователей.
- Администрировать работу сервера ЛВС, размещать и классифицировать информацию на сервере ЛВС.
- Устанавливать по согласованию с заведующим ДООУ критерии доступа пользователей на сервер ЛВС.
- Формировать и представлять пароли для новых пользователей, администрировать права пользователей.
- Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.
- Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.
- Ежемесячно подавать заведующему ДООУ статистическую информацию по использованию Интернетом.
- Вести учет пользователей «точки доступа к Интернету». В случае необходимости лимитировать время работы пользователя в Интернете и объем скачиваемой информации.

- Сообщать незамедлительно заведующему ДОУ о выявлении случаев несанкционированного доступа в Интернет.

4. Права ответственных за информационную безопасность

- 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.

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

5. Ответственность ответственных лиц за информационную безопасность

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.