

## **ПОЛОЖЕНИЕ**

### **Об информационной безопасности**

муниципального автономного дошкольного образовательного учреждения  
«Центр развития ребенка-детский сад № 377» городского округа Самара

#### **Общие положения**

- 1.1. Настоящее Положение об информационной безопасности (Положение) в муниципальном автономном дошкольном образовательном учреждении «Центр развития ребенка-детский сад № 377» городского округа Самара (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).
- 1.2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность.
- 1.3. Ответственные за информационную безопасность назначаются приказом заведующего ДОУ.
- 1.4. Ответственные за информационную безопасность подчиняются заведующему ДОУ.
- 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 ДОУ.

## **2. Основные задачи и функции, ответственных за информационную безопасность**

2.1. Основными задачами ответственных за информационную безопасность являются: организация эксплуатации технических и программных средств защиты информации; текущий контроль работы средств и систем защиты информации.

2.2. 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 ДОУ;

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**

3.1. Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей.

Немедленно докладывать заведующему ДОУ 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.
- 3.7. Формировать и представлять пароли для новых пользователей, администрировать права пользователей.
- 3.8. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.
- 3.9. Выполнять регулярно резервное копирование данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.
- 3.10. Ежемесячно подавать заведующему ДОО статистическую информацию по использованию Интернетом.
- 3.11. Вести учет пользователей «точки доступа к Интернету». В случае необходимости лимитировать время работы пользователя в Интернете и объем скачиваемой информации.
- 3.12. Сообщать незамедлительно заведующему ДОО 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 н