

Рассмотрено:  
на заседании  
педагогического совета  
МБДОУ Высокогорский детский сад «Бэлэкэч»  
Протокол № 1 от «\_\_\_» \_\_\_\_\_ 2018

Утверждено:  
заведующий МБДОУ  
Высокогорский детский сад  
«Бэлэкэч»  
Хайрутдинова И.Ф. \_\_\_\_\_  
Приказ № \_\_\_ от «\_\_» \_\_\_\_\_ 2018

## **Положение об информационной безопасности**

муниципального бюджетного дошкольного образовательного учреждения  
«Высокогорский детский сад «Бэлэкэч» комбинированного вида»  
Высокогорского муниципального района Республики Татарстан»

### **1. Общие положения**

- 1.1. Настоящее Положение об информационной безопасности (далее по тексту Положение) муниципального бюджетного дошкольного образовательного учреждения Высокогорского детского сада «Бэлэкэч» 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:
  - 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 на сервере ЛВС.
  - 2.1.4. Ответственные за информационную безопасность выполняют следующие основные функции:
    - 2.1.5. Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.
    - 2.1.6. Обучение персонала и пользователей ПК правилам безопасной обработки информации и правилам работы со средствами защиты информации.
    - 2.1.7. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДОУ.
    - 2.1.8. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации.
    - 2.1.9. Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём.

- 2.1.10. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК.
- 2.1.11. Контроль пользования Интернетом.

### **3. Обязанности ответственных за информационную безопасность**

- 3.1. Обеспечение функционирования и поддержание работоспособности средств и систем защиты информации в пределах возложенных на них обязанностей. Срочное информирование заведующего Учреждения о выявленных нарушениях и несанкционированных действиях пользователей и сотрудников, а также принятие необходимых мер по устранению нарушений.
- 3.2. Совместно с 2 программистами принятие мер по восстановлению работоспособности средств и систем защиты информации.
- 3.3. Проведение инструктажа сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.
- 3.4. Создание и удаление учетных записей пользователей.
- 3.5. Администрирование работы сервера ЛВС, размещение и классифицирование информации на сервере ЛВС.
- 3.6. Установление по согласованию с заведующим Учреждения критериев доступа пользователей на сервер ЛВС.
- 3.7. Формирование и представление паролей для новых пользователей, администрирование прав пользователей.
- 3.8. Отслеживание работы антивирусных программ, проведение полной проверки компьютеров на наличие вирусов один раз в неделю.
- 3.9. Регулярное выполнение резервного копирования данных на сервере, при необходимости восстанавливать потерянные или поврежденные данные.
- 3.10. Ежемесячно подавать заведующему Учреждения статистическую информацию по пользованию Интернетом.
- 3.11. Ведение учета пользователей «точки доступа к Интернету». В случае необходимости лимитирования времени работы пользователя в Интернете и объем скачиваемой информации.
- 3.12. Незамедлительное сообщение заведующему Учреждением о выявлении случаев несанкционированного доступа в Интернет.

### **4. Права ответственных за информационную безопасность**

- 4.1. Требование 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. Подготовка предложений 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.