ПРИНЯТО
Общим собранием работников
протокол №3 от 12.03.2020

УТВЕРЖДЕНО
Заведующей МБДОУ
«Детский сад №1» п.г.т. Уруссу
_____ Р.А. Игнатова
Приказ № 44 от 13.03.2020

С учетом мнения родителей
протокол № 2 от 11.03. 2020

Муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад №1» комбинированного вида п.г.т. Уруссу
Ютазинского муниципального района Республики Татарстан

МБДОУ «Детский сад №1» п.г.т. Уруссу

ПОЛОЖЕНИЕ
ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

п.г.т. Уруссу

1.Общие положения

1.1. Настоящее Положение об информационной безопасности (далее по тексту Положение) МБДОУ «Детский сад №1» комбинированного вида п.г.т. Уруссу Ютазинского муниципального района Республики Татарстан, 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».

1.2. Настоящее Положение определяет основные понятия и объекты информационной безопасности, а также задачи, функции, обязанности, ответственность и права ответственных за информационную безопасность.

1.3. Ответственные за информационную безопасность назначаются приказом заведующего ДОУ, подчиняются Заведующему ДОУ.

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

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

2. Основные понятия и объекты информационной безопасности

2.1. В МБДОУ «Детский сад №1» п.г.т. Уруссу Ютазинского муниципального района Республики Татарстан развернута локально-вычислительная сеть с выходом в интернет, подлежащая информационной защите. Под безопасностью локально вычислительной сети понимается ее защищенность от случайного или преднамеренного вмешательства в нормальный процесс функционирования, а также от попыток хищения, модификации или разрушения ее компонентов. Безопасность системы достигается обеспечением конфиденциальности обрабатываемой ею информации, а также целостности и доступности компонентов и ресурсов системы.

2.2. Безопасность системы обеспечивается комплексом технологических и административных мер. применяемых в отношении аппаратных средств, программ, данных и служб с целью обеспечения доступности, целостности и конфиденциальности связанных с компьютерами ресурсов; сюда же относятся и процедуры проверки выполнения системой определенных функций в строгом соответствии с их запланированным порядком работы.

2.3. Система обеспечения безопасности включает в себя следующие подсистемы:

- компьютерную безопасность;
- безопасность данных;
- безопасное программное обеспечение;
- безопасность коммуникаций.

2.3.1. Компьютерная безопасность обеспечивается комплексом технологических и административных мер, применяемых в отношении аппаратных средств компьютера с целью обеспечения доступности, целостности и конфиденциальности связанных с ним ресурсов.

2.3.2. Безопасность данных достигается защитой данных от неавторизованных, случайных, умышленных или возникших по халатности модификаций, разрушений или разглашения.

2.3.3. Безопасное программное обеспечение представляет собой общецелевые и прикладные программы и средства, осуществляющие безопасную обработку данных в системе и безопасно использующие ресурсы системы.

2.3.4.Безопасность коммуникаций обеспечивается посредством аутентификации телекоммуникаций за счет принятия мер по предотвращению предоставления неавторизованным лицам критичной информации, которая может быть выдана системой в ответ на телекоммуникационный запрос.

2.4. К объектам информационной безопасности относятся: информационные ресурсы, содержащие конфиденциальную информацию, представленную в виде документированных информационных массивов и баз данных; средства и системы информатизации — средства вычислительной и организационной техники, локальной сети, общесистемное и прикладное программное обеспечение, автоматизированные системы управления рабочими местами, системы связи и передачи данных, технические средства сбора, регистрации, передачи, обработки и отображения информации.

3. Основные задачи и функции, ответственных за информационную безопасность

3.1. Основными задачами ответственных за информационную безопасность являются:

3.1.1. Организация эксплуатации технических и программных средств защиты информации.

3.1.2 Текущий контроль работы средств и систем защиты информации.

3.1.3 Организация и контроль резервного копирования информации на сервере ЛВС.

3.2 Ответственные за информационную безопасность выполняют следующие основные функции:

3.2.1. Разработка инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете.

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

3.2.3.Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДОУ.

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

3.2.5.Контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нѐм.

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

3.2.7. Контроль пользования Интернетом.

4. Обязанности ответственных за информационную безопасность

4.1. 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.

4.2. Принимать меры по восстановлению работоспособности средств и систем защиты информации.

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

4.4. Создавать и удалять учетные записи пользователей.

4.5. Администрировать работу сервера ЛВС. размещать и классифицировать информацию на сервере ЛВС.

4.6. Устанавливать по согласованию с заведующим ДОУ критерии доступа пользователей на сервер ЛВС.

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

4.8. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов.

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

4.10. Ежемесячно подавать заведующему ДОУ статистическую информацию по пользованию Интернетом.

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

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

5. Права ответственных за информационную безопасность.

5.1. 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.

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

6. Ответственность ответственных лиц за информационную безопасность.

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