**Муниципальное казенное дошкольное образовательное учреждение детский сад «Солнышко»**
*(Новосибирская область, село Убинское, улица Янкова № 5, тел. 21 – 649)*
E-mail: ubinskoesolnishko1@rambler.ru

Приложение № 5
к приказу от 01.02.2020 г

СОГЛАСОВАНО:
педагогическим советом
протокол
« 01» февраля 20 19 г.

УТВЕРЖДАЮ:
заведующая МКДОУ детского
сада «Солнышко» Убинского
района Новосибирской области
_____ Е.С. Платова
« 01» февраля 20 19 г.
М.П.

**Согласовано:**
председатель профкома МКДОУ
детского сада «Солнышко»
_____ Е. М. Шурыгина

# Положение
# об информационной безопасности
## в МКДОУ детском саду «Солнышко»

**1.Общие положения**

1.1. Настоящее Положение об информационной безопасности (далее по тексту Положение) муниципального казенного дошкольного образовательного учреждения детского сада «Солнышко» Убинского района Новосибирской области (далее ДОУ) разработано в соответствии с НОРМАТИВНО-ПРАВОВОЙ БАЗОЙ:

- Федеральный закон РФ от 28.12.2010 г. № 390 — ФЗ «О безопасности»
  Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 29.07.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию»
- Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»
- Федеральный закон от 24.07.1998 N 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»
- Распоряжение Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей»
- Приказ Минкомсвязи России от 27.02.2018 N 88 «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018 - 2020 годы»
- <Письмо> Минобрнауки России от 14.05.2018 N 08-1184 «О направлении информации» (вместе с «Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети «Интернет»)
- Письмо Минобрнауки от 28.04.2014 №ДЛ-115/03
- Письмо Минобрнауки от 14.05.2018 №08-1184

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. 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.
3.5. Администрировать работу сервера ЛВС, размещать и классифицировать информацию на сервере ЛВС.
3.6. Устанавливать по согласованию с заведующим ДОУ критерии доступа пользователей на сервер ЛВС.
3.7. Формировать и представлять пароли для новых пользователей, администрировать права пользователей.

3.8. Отслеживать работу антивирусных программ и проводить 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 ДОУ статистическую информацию по пользованию 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 ДОУ 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.

**.ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ.**

*Информационная безопасность* – защищенность информации и соответствующей инфраструктуры случайных или преднамеренных воздействий сопровождающихся нанесением ущерба владельцам и пользователям информации.
*Информационная безопасность* – обеспечение конфиденциальности, целостности и доступнос информации.
*Цель защиты информации* – минимизация потерь, вызванных нарушением целостности и конфиденциальности данных, а также их недоступности для потребителей.

**УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.**

*Основные типы угроз информационной безопасности:*

1. Угрозы конфиденциальности – несанкционированный доступ к данным.
2. Угрозы целостности – несанкционированная модификация, дополнение или уничтожение данны
3. Угрозы доступности – ограничение или блокирование доступа к данным.

*Источники угроз:*

1. Внутренние:
а) ошибки пользователей и сисадминов;
б) ошибки в работе ПО;
в) сбои в работе компьютерного оборудования;
г) нарушение сотрудниками компании регламентов по работе с информацией.
2. Внешние угрозы:
а) несанкционированный доступ к информации со стороны заинтересованных организаций и отдельных лица;
б) компьютерные вирусы и иные вредоносные программы;
в) стихийные бедствия и техногенные катастрофы.

**МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.**

*Методы обеспечения безопасности информации в ИС:*

Препятствие — физическое преграждение пути злоумышленнику к защищаемой информации .

Управление доступом – регулирование использования информации и доступа к ней за счет системы идентификации пользователей, их опознавания, проверки полномочий и т.д.

Криптография – шифрование информации с помощью специальных алгоритмов.

Противодействие атакам вредоносных программ – предполагает использование внешних накопителей информации только от проверенных источников, антивирусных программ, брандмауэров, регулярное выполнение резервного копирования важных данных и т.д. (*вредоносных программ очень много и они делятся на ряд классов: вирусы, эксплойты, логические бомбы, трояны, сетевые черви и т.п.*).

Регламентация – создание условий по обработке, передаче и хранению информации, в наибольшей степени обеспечивающих ее защиту (*специальные нормы и стандарты для персонала по работе с информацией, например, предписывающие в определенные числа делать резервную копию электронной документации, запрещающие использование собственных флеш-накопителей и т.д.*).

Принуждение – установление правил по работе с информацией, нарушение которых карается материальной, административной или даже уголовной ответственностью (*штрафы, закон «О коммерческой тайне» и т.п.*).

Побуждение – призыв к персоналу не нарушать установленные порядки по работе с информацией, т.к. это противоречит сложившимся моральным и этическим нормам.

*Средства защиты информации:*

Технические (аппаратные) средства – сигнализация, решетки на окнах, генераторы помех воспрепятствования передаче данных по радиоканалам, электронные ключи и т.д.

Программные средства – программы-шифровальщики данных, антивирусы, системы аутентификации пользователей и т.п.

Смешанные средства – комбинация аппаратных и программных средств.

Организационные средства – правила работы, регламенты, законодательные акты в сфере защиты информации, подготовка помещений с компьютерной техникой и прокладка сетевых кабелей с учетом требований по ограничению доступа к информации и пр.

**Прошнуровано и пронумеровано:**
**4 (четыре) страницы**
**Заведующая МКДОУ детский сад**
**«Солнышко»:**
**_____ Е.С. Платова**