



Приложение № 1

к приказу № 79 от 03.03.2025г.

**Положение**

**Об информационной безопасности воспитанников и сотрудников Муниципального бюджетного дошкольного образовательного учреждения «Детский сад № 3 «Сказка» общеразвивающего вида второй категории**

1. **Общие положения** 
   1. Настоящее Положение об информационной безопасности воспитанников и сотрудников (далее - Положение) Муниципального бюджетного дошкольного образовательного учреждения «Детский сад № 3 «Сказка» общеразвивающего вида второй категории (далее - ДОУ) разработано в соответствии с Федеральным законом от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 года №152-ФЗ «О персональных данных» (в редакции от 28.06.2010 года), Указом президента РФ от 17.03.2008 года № 351 (в редакции от 22.05.2015 года) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Федеральным законом «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 года № 436-ФЗ, Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства РФ от 2 декабря 2015 года № 2471-р.
   2. Настоящее Положение определяет задачи, функции, обязанности, ответственность и права должностных лиц, ответственных за информационную безопасность, имеющих доступ к электронным базам данных, официальному сайту ДОУ, адресам электронной почты ДОУ.
   3. Должностные лица, ответственные за информационную безопасность, назначаются приказом заведующего ДОУ.
   4. Должностные лица, ответственные за информационную безопасность, подчиняются заведующему ДОУ.
   5. Должностные лица, ответственные за информационную безопасность, в своей работе руководствуются настоящим Положением.
   6. Должностные лица, ответственные за информационную безопасность, в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой при помощи всех информационных средств в ДОУ.
   7. К информационным средствам ДОУ относятся электронные базы данных, содержащие информацию административно-хозяйственного содержания, финансовые документы, персональные данные сотрудников и воспитанников ДОУ, организационно-правовую информацию, материалы, регламентирующие организацию образовательного процесса в ДОУ; официальный сайт ДОУ; официальная электронная почта ДОУ.
2. **Основные задачи и функции должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников** 
   1. Основными задачами должностных лиц, ответственных за информационную безопасность, являются:
      1. Организация эффективной эксплуатации технических и программных средств защиты информации;
      2. Текущий контроль работы средств и систем защиты информации;
      3. Организация и контроль резервного копирования информации.
   2. Должностные лица, ответственные за информационную безопасность, выполняют следующие основные функции:
      1. Соблюдение инструкций по информационной безопасности: инструкции по организации антивирусной защиты, инструкции по безопасной работе в системе Интернет;
      2. При наличии производственной необходимости обучение персонала и пользователей навыкам работы с персональным компьютером (далее - ПК), правилам безопасной обработки информации и правилам работы со средствами защиты информации;
      3. Организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в ДОУ;
      4. Текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации;
      5. Контроль целостности эксплуатируемого ПК программного обеспечения с целью выявления несанкционированных изменений в нём;
      6. Контроль за санкционированным изменением программного обеспечения, заменой и ремонтом ПК;
      7. Контроль пользования сетью Интернет;
      8. Контроль доступа к официальному сайту ДОУ, к официальной электронной почте ДОУ, к электронным базам данных.
3. **Обязанности должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников** 
   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.
   2. Совместно с инженером-программистом принимать меры по восстановлению работоспособности средств и систем защиты информации.
   3. Проводить инструктаж сотрудников и пользователей ПК по правилам работы с используемыми средствами и системами защиты информации.
   4. Создавать и удалять учетные записи пользователей.
   5. Администрировать работу официального сайта ДОУ (далее - сайт), размещать и классифицировать информацию на сайте.
   6. Устанавливать по согласованию с заведующим ДОУ критерии доступа пользователей на сайт, к электронным базам официальных документов ДОУ, к официальной электронной почте ДОУ.
   7. При наличии производственной необходимости формировать и предоставлять пароли для новых пользователей, администрировать права пользователей сайта, электронных баз официальных документов ДОУ, электронной почты ДОУ.
   8. Отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку ПК на наличие вирусов.
   9. Регулярно выполнять резервное копирование данных на сайте, в электронных базах официальных документов ДОУ, при необходимости восстанавливать потерянные или поврежденные данные.
   10. Систематически проверять информацию, поступающую по официальной электронной почте ДОУ, через официальный сайт ДОУ.
   11. Вести учет пользователей сетью Интернет. В случае необходимости лимитировать время работы пользователей в сети Интернет и объём скачиваемой информации.
   12. Сообщать незамедлительно заведующему ДОУ о выявлении случаев несанкционированного доступа в сеть Интернет, к электронным базам официальных документов ДОУ, на официальный сайт ДОУ, в официальную электронную почту ДОУ.
4. **Права должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников** 
   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, персональные данные сотрудников и воспитанников и т.д.
   2. Вносить предложения по совершенствованию используемых систем защиты информации и отдельных их компонентов, по организации и контролю доступа в сеть Интернет, к электронным базам официальных документов ДОУ, на официальный сайт ДОУ, в официальную электронную почту ДОУ.
5. **Ответственность должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников** 
   1. На должностных лиц, ответственных за информационную безопасность воспитанников и сотрудников, возлагается персональная ответственность в соответствии с действующим законодательством РФ:

* за качество проводимых ими работ по обеспечению защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением;
* за разглашение информации административно-хозяйственного содержания и финансовых документов без согласования с заведующим ДОУ среди лиц, не имеющих производственной принадлежности к ООА Матвеево-Курганского района, проверяющих и контролирующих органов;
* за сохранность персональных данных воспитанников и сотрудников ДОУ.

**6. Компетенции должностных лиц, ответственных за информационную**

**безопасность воспитанников и сотрудников**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Должность** | **Доступ**  **к информационным средствам** | **Доступ к информации** |
| **1** | **Заведующий ДОУ** | * электронные базы официальных документов ДОУ; * официальный сайт ДОУ; * официальная электронная почта ДОУ; * сеть Интернет посредством официального провайдера ДОУ | * информация административно-   хозяйственного содержания;   * финансовые документы; - персональные данные сотрудников и воспитанников ДОУ; - организационно- правовая   информация; - материалы, регламентирующие организацию образовательного процесса в  ДОУ |
| **2** | **Заведующий**  **хозяйством**  **ДОУ** | * электронные базы официальных документов ДОУ;   - официальный сайт ДОУ;  - официальная электронная почта ДОУ;   * сеть Интернет посредством   официального провайдера ДОУ | * информация административно-   хозяйственного содержания; - финансовые документы персональные данные сотрудников и воспитанников ДОУ;   * организационно- правовая |

|  |  |  |  |
| --- | --- | --- | --- |
| 3 | **Секретарь** | * электронные базы официальных документов ДОУ; * официальный сайт ДОУ; * официальная электронная почта ДОУ; * сеть Интернет посредством официального провайдера ДОУ | -информация административно-  хозяйственного содержания; - финансовые документы персональные данные сотрудников и воспитанников ДОУ; - организационно – правовая информация |
| 4 | **Администратор официального**  **сайта ДОУ**  **(старший воспитатель)** | * электронные базы официальных документов ДОУ; * официальный сайт ДОУ; * официальная электронная почта ДОУ; * сеть Интернет посредством официального провайдера ДОУ | - информация административно-  хозяйственного содержания; - персональные данные сотрудников и воспитанников ДОУ;  - организационно-правовая информация;  материалы, образовательного процесса в ДОУ регламентирующие организацию |

\

Приложение № 2

к приказу № 79 от 03.03.2025г.

**ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ**

**ответственного за информационную безопасность и внедрение системы контентной фильтрации в МБДОУ «Д/с № 3 «Сказка»**

1. **Общие положения**

1.1. Настоящий документ определяет основные обязанности, права и ответственность лица за информационную безопасность Муниципального бюджетного дошкольного образовательного учреждения «Детский сад № 3 «Сказка» общеразвивающего вида второй категории (далее - Учреждение).

1.2. Ответственный за информационную безопасность назначается приказом руководителя Учреждения.

* 1. Ответственный за информационную безопасность осуществляет свою деятельность в интересах Учреждения в информационной сфере путем обеспечения защиты информации и поддержания достигнутого уровня защиты автоматизированных информационных систем (АИС) и ее ресурсов на всех этапах создания, модернизации и эксплуатации АИС.
  2. Мероприятия по защите информации являются составной частью управленческой, научной и производственной деятельности Учреждения. Защита информации представляет собой комплекс организационных и технических мероприятий, направленных на исключение или существенное затруднение противоправных деяний в отношении технических и программных средств Учреждения и информации, циркулирующей в них.
  3. Ответственный за информационную безопасность несет ответственность за реализацию принятой в Учреждение политики безопасности, закрепленной в Концепции информационной безопасности Учреждения.
  4. Инструкция регулирует отношения между ответственным за информационную безопасность, пользователями АИС, сторонними организациями, возникающие при:

- эксплуатации и развитии АИС;

- формировании и использовании данных, сообщений, баз данных, информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления пользователю документированной информации;

- при создании, внедрении и эксплуатации новых информационных технологий.

* 1. Ответственный за информационную безопасность обладает правами доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты.
  2. Требования ответственного за информационную безопасность, связанные с выполнением ими своих функций, обязательны для исполнения всеми пользователями АИС.

2. **Обязанности ответственного за информационную безопасность. Ответственный за информационную безопасность обязан:**

* 1. Обеспечить информационную безопасность, защиту конфиденциальной информации, в том числе и на бумажных носителях, от несанкционированного доступа, искажения и уничтожения при ее передаче, обработке и хранении с использованием средств вычислительной техники.
  2. Организовывать доступ пользователей и посторонних лиц в помещения, где размещены средства информатизации и коммуникации, а также хранятся носители информации.
  3. Организовывать, в установленном порядке, передачу информации, составляющей коммерческую тайну Учреждения на сменных магнитных носителях и иными способами.
  4. Организовывать сопровождение работ по категорированию объектов средств вычислительной техники Учреждения.
  5. Знать перечень установленных в подразделениях Учреждения серверов, рабочих станций, средств копировально-множительной техники, устройств и топологию локально вычислительной сети.
  6. Иметь перечень информационных ресурсов Учреждения.
  7. Обеспечить доступ к защищаемой информации пользователям АИС согласно их прав доступа при получении оформленного соответствующим образом разрешения;
  8. Осуществлять оперативный контроль за работой пользователей защищаемых рабочих станций, анализировать содержимое системных журналов всех PC и реагировать на возникающие нештатные ситуации.
  9. Запрещать и немедленно блокировать применение пользователям сети программ, с помощью которых возможны факты несанкционированного доступа к ресурсам АИС.
  10. Не допускать установку, использование, хранение и размножение в АИС программных средств, не связанных с выполнением функциональных задач.

2.11. Не допускать к работе на рабочих станциях и серверах ЛВС посторонних лиц. 2.12. Аппаратными и программными средствами выявлять факты

несанкционированного доступа к информационным ресурсам АИС, а также другие нарушения, которые могут привести к разглашению или утрате конфиденциальной информации, и принимать меры по их пресечению.

* 1. Контролировать физическую сохранность средств и оборудования АИС.
  2. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных рабочих станций и серверов.
  3. Участвовать в приемке новых программных и аппаратных средств;

2.16. Периодически проверять состояние используемых СЗИ НС'Д. осуществлять проверку правильности их настройки.

* 1. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных рабочих станций.
  2. Вести контроль за процессом резервирования и дублирования важных ресурсов АИС.
  3. Вести наблюдение за состоянием антивирусного контроля в организации.
  4. Контролировать информацию, передаваемую по электронной почте, с целью исключения утечки конфиденциальной информации по открытым каналам связи в Учреждении.
  5. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.
  6. Периодически представлять руководству отчет о состоянии защиты и о нештатных ситуациях на объектах АИС и допущенных пользователями нарушениях установленных требований по защите информации.
  7. Вносить предложения для принятия решений о привлечении виновных к ответственности, за грубые нарушения требований нормативных документов по обеспечению сохранности конфиденциальной информации, а также о приостановке работ в случае обнаружения условий для утечки информации или материалов с пометкой для служебного пользования.

1. **Права ответственного за информационную безопасность.**

**Ответственный за информационную безопасность имеет право:**

* 1. Проводить мероприятия по защите конфиденциальной информации от несанкционированного доступа.
  2. Требовать от сотрудников Учреждения соблюдения установленных технологий обработки информации и выполнения инструкций по защите информации.
  3. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АИС.
  4. Обращаться к руководителю Учреждения с требованием прекращения работы в АИС при несоблюдении установленной технологии обработки информации и невыполнении требований по защите информации пользователями.
  5. Отключать от сети пользователей, осуществивших НСД к защищаемым ресурсам ЛВС и БД или нарушивших другие требования по безопасности информации.
  6. Запрещать устанавливать на серверах и рабочих станциях ЛВС нештатное программное и аппаратное обеспечение.

**Ответственность лица, ответственного за информационную безопасность:**

* 1. Ответственный за информационную безопасность несет ответственность за качественное и своевременное выполнение задач, возложенных на него и изложенных в настоящей инструкции, а также определенных в текущих приказах и распоряжениях руководителя ДОУ.
  2. На ответственного за информационную безопасность возлагается персональная ответственность за программно-технические и криптографические средства защиты информации, и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

Приложение № 3

к приказу № 79 от 03.03.2025г.

**План мероприятий**

**по обеспечению информационной безопасности детей и родителей**

**МБДОУ «Д/с № 3 «Сказка» на 2024-2025 учебный год**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование мероприятия | Срок  исполнения | Исполнители, ответственные за реализацию мероприятия | Планируемый результат |
| ***I. Создание организационно-правовых механизмов защиты детей от распространения информации, причиняющей вред их здоровью и развитию*** | | | | |
| 1.1 | Издание приказов, инструкций, положений, направленных на обеспечение информационной безопасности | Август- сентябрь | Заведующий | Создание нормативной базы информационной безопасности в ДОУ |
| 1.2 | Проведение серии ОД с детьми старшего дошкольного возраста «Учимся пользоваться интернетом правильно» | 1 раз в квартал | Воспитатели групп старшего дошкольного возраста | Ознакомление детей с информацией о правилах безопасного поведения в интернет- пространстве |
| 1.3 | Консультирование родителей по вопросам защиты детей от распространения вредной для них информации:  «О защите детей от информации, причиняющей вред их здоровью и развитию**»**  «Безопасный интернет детям»  «Что такое информационная безопасность ребенка» | Сентябрь      Январь    Апрель | Старший воспитатель, воспитатели | Информирование родителей о механизмах предупреждения доступа несовершеннолетних к информации, причиняющей вред их здоровью и (или) развитию |
| 1.4. | Информирование педагогов по вопросам защиты детей от  распространения вредной для них информации: |  | Старший воспитатель | Информирование педагогов о механизмах предупреждения доступа |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Консультация  «Обеспечение  информационной безопасности дошкольника» | Октябрь |  | несовершеннолетних к информации, причиняющей вред их здоровью и (или) развитию |
| ***II. Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно - программных и технико - технологических устройств*** | | | | |
| 2.1 | Организация  функционирования контент-фильтрации DNS-сервера |  | Заведующий, заведующий хозяйством | Проведение доступа к сети Интернет с обеспечением программного продукта, обеспечивающего контент-фильтрацию |
| 2.2 | Мониторинг качества предоставления провайдером услуги доступа к сети  Интернет | Ежемесячно | Ответственный за инф. безопасность (старший воспитатель) | Проведение оценки доступа к сети  Интернет |
| 2.3 | Мероприятия по антивирусной защите компьютерной техники в детском саду | В течении года | Администрация  Ответственный за информационную безопасность (старший воспитатель) | Систематическое обновление программно-  технических средств по антивирусной защите компьютерной техники в ДОУ |
| ***III. Профилактика интернет-зависимости, игровой зависимости и правонарушений с использованием информационно - телекоммуникационных технологий, формирование навыков ответственного и безопасного поведения в современной информационно -***  ***телекоммуникационной среде через обучение их способам защиты от вредной информации*** | | | | |
| 3.1 | Проведение серии ОД с детьми старшего дошкольного возраста «Учимся пользоваться интернетом правильно» | 1 раз в квартал | Воспитатели групп старшего дошкольного возраста | Ознакомление детей с информацией о правилах безопасного поведения в интернет- пространстве |
| 3.2 | Проведение конкурсов рисунков в группах старшего дошкольного возраста по теме | Январь | воспитатели | Ознакомление детей с информацией о  правилах безопасного поведения в интернет- |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | «Информационная безопасность» |  |  | пространстве и  закрепление знаний детей о правилах  безопасного поведения в интернет- пространстве |
| ***IV. Информационное просвещение граждан о возможности защиты детей от информации, причиняющей вред их здоровью и развитию*** | | | | |
| 4.1 | Проведение родительского собрания «Управление безопасностью детей в Интернете» | Февраль | воспитатели | Повышение информационной грамотности родителей |
| 4.2 | Размещение на официальном сайте детского сада ссылок на электронные адреса по проблемам информационной безопасности для всех участников образовательного процесса | В течении года | Ответственный за информационную безопасность | Повышение информационной грамотности родителей |
| 4.3 | Размещение на сайте детского сада сведений о лучших ресурсах для детей и  родителей | В течении года | Ответственный за информационную безопасность | Повышение информационной грамотности родителей |
| 4.4 | Размещение на сайте детского сада материалов касающихся вопросов защиты детей от распространения вредной для них информации:  «О защите детей от информации, причиняющей вред их здоровью и развитию**»**  «Безопасный интернет детям»  «Что такое информационная безопасность ребенка» | В течении года | Ответственный за информационную безопасность (старший воспитатель) | Повышение информационной грамотности родителей |
| 4.5 | Размещение на сайте детского сада ссылок на сайты по вопросам информационной безопасности детей и взрослых | В течении года | Ответственный за информационную безопасность (старший воспитатель) | Повышение информационной грамотности родителей |

Приложение № 4

к приказу № 79 от 03.03.2025г.

Примерная форма журнала

Регистрации отключения работы системы контентной фильтрации по запросу педагогических работников

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата отключения СКФ | ФИО  педагога | №  компьютера педагога | IP адрес компьютера педагога | Документ- основание  отключения СКФ | Дата восстановления работы СКФ | ФИО  ответственного сотрудника | Подпись  ответственного сотрудника |
|  |  |  |  |  |  |  |  |  |