СОГЛАСОВАНО:
Председатель профсоюзного комитета МДОУ «Центр развития ребенка – Детский сад № 2»
Протокол № 1 от «24» августа 2022 г.

УТВЕРЖДЕНО:
Заведующий МДОУ «Центр развития ребенка – Детский сад № 2»
_____ /И.Г. Холодова/
подпись расшифровка подписи

Приказ № 49 - О от 26.08.2022 г.

Политика информационной безопасности
Муниципального дошкольного образовательного учреждения «Центр развития ребенка – Детский сад № 2» (МДОУ № 2)

Юридический адрес:
155900, Ивановская обл.,
г. Шуя, ул. Кооперативная, д. 31-а
Телефон: 8(49351) 4-57-60
E-mail: mdou_crr_2@mail.ru

Холодова Ирина Геннадьевна

Подписано цифровой подписью: Холодова Ирина Геннадьевна
DN: cn=Холодова Ирина Геннадьевна, o=должность: Заведующий, ou=Муниципальное дошкольное образовательное учреждение "Центр развития ребенка-Детский сад № 2", email=mdou_crr_2@mail.ru, c=RU

1. Общие положения

1. 1 Политика информационной безопасности МДОУ «Центр развития ребенка _Детский сад № 2» (далее - МДОУ) определяет цели и задачи системы обеспечения информационной безопасности (далее - ИБ) и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области ИБ, которыми руководствуются работники МДОУ при осуществлении своей деятельности.

1. 2 Основной целью политики информационной безопасности МДОУ является защита информации МДОУ при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в МДОУ.

1. 3 Политика информационной безопасности разработана в соответствии с Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Федеральным законом от 27 июля 2006г. №152-ФЗ «О персональных данных», Федеральным законом от 10 января 2002г. №1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6 марта 1997г. №188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №781 от 17.11.2007г. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства РФ №687 от 15.09.2008г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также в соответствии с рядом иных нормативных правовых актов в сфере защиты информации.

1. 4 Выполнение требований Политики ИБ является обязательным для работников МДОУ, осуществляющих обработку данных с использованием средств автоматизации.

1. 5 Ответственность за соблюдение ИБ несет каждый сотрудник МДОУ, осуществляющий обработку данных с использованием средств автоматизации.

2. Цель и задачи политики информационной безопасности

2. 1 Основными целями политики ИБ являются:

- Сохранение конфиденциальности критичных информационных ресурсов;
- Обеспечение непрерывности доступа к информационным ресурсам МДОУ;
- Защита целостности информации с целью поддержания возможности оказания услуг более высокого качества и принятия эффективных управленческих решений;
- Определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности МДОУ;
- Повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
- Предотвращение и(или) снижение ущерба от инцидентов ИБ.

2. 2 Основными задачами политики ИБ являются:

- Разработка требований по обеспечению ИБ;
- Контроль выполнения установленных требований по обеспечению ИБ;
- Повышение уровня эффективности, непрерывности, контролируемости мер по обеспечению и поддержанию ИБ;
- Разработка нормативных документов по обеспечению ИБ МДОУ;
- Выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ МДОУ;
- Организация антивирусной защиты информационных ресурсов МДОУ; . Защита информации от несанкционированного доступа и утечки по техническим каналам связи;
- Организация периодической проверки соблюдения ИБ.

3. Концептуальная схема обеспечения информационной безопасности

3. 1 Политика ИБ МДОУ направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников Учреждения, технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора, хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3. 2 Наибольшими возможностями для нанесения ущерба обладает собственный персонал МДОУ. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников

и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3. 3 Стратегия обеспечения ИБ МДОУ заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников МДОУ.

4. Основные принципы обеспечения информационной безопасности

4. 1 Основными принципами обеспечения ИБ являются:

- Постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов МДОУ;
- Своевременное обнаружение проблем, потенциально способных повлиять на ИБ МДОУ, корректировка моделей угроз и нарушителя;
- Разработка и внедрение защитных мер;
- Контроль эффективности принимаемых защитных мер;
- Персонификация и разделение ролей и ответственности между сотрудниками МДОУ за обеспечение ИБ МДОУ исходя из принципа персональной и единоличной ответственности за совершаемые операции.

5. Объекты защиты

5. 1 Объектами защиты с точки зрения ИБ МДОУ являются:

- информационный процесс профессиональной деятельности;
- информационные активы МДОУ.

5. 2 Защищаемая информация делится на следующие виды:

- информация по финансово - экономической деятельности МДОУ;
- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности

6. 1 В отношении всех собственных информационных активов МДОУ, активов, находящихся под контролем МДОУ, а также активов, используемых для получения доступа к инфраструктуре МДОУ, должна быть определена ответственность соответствующего сотрудника МДОУ. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами МДОУ должна доводиться до сведения руководителя МДОУ.

6. 2 Все работы в пределах МДОУ должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в МДОУ.

6. 3 Внос в здание и помещения МДОУ личных портативных компьютеров и внешних носителей информации (дисков, дискет, флэш-карт), а также вынос их за пределы учреждения производится только с согласия руководителя МДОУ.

6. 4 Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну МДОУ и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6. 5 В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

6. 6 Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи близким.

6. 7 В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

6. 8 Каждый сотрудник обязан немедленно уведомлять ответственного по информационной безопасности (далее - ответственного по ИБ) обо всех случаях предоставления доступа третьего лица к информационным ресурсам Учреждения. Доступ третьих лиц к информационным системам учреждения должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам МДОУ должен быть четко определен, контролируем защищен.

6. 9 Сотрудникам, использующим в работе портативные компьютеры МДОУ, может быть предоставлен удаленный доступ к сетевым ресурсам МДОУ, при наличии в МДОУ локальной вычислительной сети.

6. 10 Сотрудникам, работающим за пределами МДОУ с использованием компьютера, не принадлежащего МДОУ, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6. 11 Сотрудники, имеющие право удаленного доступа к информационным ресурсам МДОУ, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети МДОУ и к каким- либо другим сетям, не принадлежащим МДОУ.

6. 12 Все компьютеры, подключаемые посредством удаленного доступа к информационной сети МДОУ, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

6. 13 Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности. Рекомендованные правила:

- сотрудникам МДОУ разрешается использовать сеть Интернет только в служебных целях;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия или сходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- сотрудники МДОУ не должны использовать сеть Интернет для хранения данных МДОУ;
- работа сотрудников МДОУ с Интернет-ресурсами допускается только в режиме просмотра информации, исключая возможность передачи информации МДОУ в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем МДОУ;
- сотрудники МДОУ перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в сеть Интернет через сеть МДОУ для всех лиц, не являющихся сотрудниками МДОУ, включая членов семей сотрудников.

6. 14 Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация МДОУ.

6. 15 Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит ответственный по ИБ.

6. 16 Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа «мышь», шаровые манипуляторы,

дисководы для CD- дисков), коммуникационное оборудование (факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются «компьютерное оборудование». Компьютерное оборудование является собственностью МДОУ и предназначено исключительно для использования в производственных целях.

6. 17 Каждый сотрудник, получивший в использование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6. 18 Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавише и после выхода из режима «Экранной заставки». Для установления режимов защиты пользователь должен обратиться к администратору. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

6. 19 При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не даст гарантии полного удаления содержащейся на нем информации.

6. 20 Порты передачи данных, в том числе FDD и CD-дисководы в стационарных компьютерах сотрудников МДОУ блокируются, за исключением тех случаев, когда сотрудником получено разрешение администратора по ИБ на запись.

6. 21 Все программное обеспечение, установленное на предоставленном Организацией компьютерном оборудовании, является собственностью МДОУ и должно использоваться исключительно в производственных целях.

6. 22 Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю МДОУ.

6. 23 На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений.

6. 24 Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной администратором по ИБ.

6. 25 Сотрудники МДОУ не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6. 26 Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию МДОУ по электронной почте без использования системы шифрования. Строго конфиденциальная информация МДОУ, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6. 27 Использование сотрудниками МДОУ публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным администратором по ИБ при условии применения механизмов шифрования.

6. 28 Сотрудники МДОУ для обмена документами должны использовать только свой официальный адрес электронной почты.

6. 29 Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственно получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать администратора по ИБ. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6. 30 Не допускается при использовании электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться. как уголовное преступление или административный проступок, либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6. 31 Объем пересылаемого сообщения по электронной почте не должен превышать 2 МБ.

6. 32 Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6. 33 В случае кражи переносного компьютера следует незамедлительно сообщить администратору по ИБ.

6. 34 Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать администратора по ИБ;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети МДОУ до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором по ИБ.

6. 35 Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

6. 36 Перечень помещений с техническими средствами информационной безопасности утверждается руководителем МДОУ.

6. 37 Участникам заседаний запрещается входить в помещение с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с администратором по ИБ.

6. 38 Аудио/видео запись, фотографирование во время конференциальных заседаний может вести только сотрудник МДОУ, который отвечает за подготовку заседания, после получения письменного разрешения руководителя.

6. 39 Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

6. 40 Сотрудникам МДОУ запрещается:

- нарушать информационную безопасность и работу сети;

- сканировать порты и систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации или безопасности;
- использовать любые программы, скриншоты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников МДОУ посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.

6. 41 Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6. 42 Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6. 43 Только администратор по ИБ на основании заявок руководителя может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

6. 44 Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

6. 45 Все заявки на проведение технического обслуживания компьютеров должны направляться администратору по ИБ.

6. 46 Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы и согласованы с администратором по ИБ.

7. Управление информационной безопасностью

7. 1 Управление ИБ МДОУ включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно - методических документов по обеспечению ИБ;
- обеспечение бесперебойного функционирования комплекса средств ИБ;
- осуществление контроля (мониторинга) функционирования системы ИБ; оценку рисков, связанных с нарушением ИБ.

8. Реализация информационной безопасности

8. 1 Реализация Политики ИБ МДОУ осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в МДОУ.

9. Порядок изменений и дополнений в политику информационной безопасности

9. 1 Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью проведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10.Контроль за соблюдением Политики информационной безопасности

10. 1 Текущий контроль за соблюдением выполнения требований Политики информационной безопасности МДОУ возлагается на сотрудника - администратора по информационной безопасности, назначенного приказом руководителя МДОУ.

10. 2 Руководитель на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.