

Приложение
к приказу МКДОУ № 9
от 01.09.2023 № 97

Политика информационной безопасности МКДОУ № 9

2023
г. Мирный

Определения

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информация ограниченного доступа - информация, доступ к которой ограничен федеральными законами;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Обозначения и сокращения

КИ - Конфиденциальная информация;

МЭ - Межсетевой экран;

НСД - Несанкционированный доступ;

СЗИ - Система защиты информации;

СКЗИ - Средство криптографической защиты информации;

СрЗИ - Средство защиты информации;

ФСБ России - Федеральная служба безопасности Российской Федерации;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю.

1 Общие положения

1.1 Настоящая Политика является документом, доступным всем сотрудникам МКДОУ № 9 и всем пользователям его ресурсов. Представляет собой официально принятую руководством МКДОУ № 9 систему взглядов на обеспечение информационной безопасности в МКДОУ № 9.

1.2 Основной задачей в области информационной безопасности МКДОУ № 9 признается совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов МКДОУ № 9 в контексте развития законодательства и норм регулирования информационной деятельности.

1.3 В рамках своей деятельности МКДОУ № 9 обязуется предпринимать все возможные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности или других противоправных действий, связанных с нарушением информационной безопасности МКДОУ № 9.

1.4 Требования информационной безопасности, которые предъявляются МКДОУ № 9, соответствуют целям деятельности МКДОУ № 9 и предназначены для снижения рисков, связанных с информационной безопасностью до приемлемого уровня.

1.5 Реализация и контроль исполнения требований, установленных настоящей Политикой, осуществляется работниками, ответственными за информационную безопасность, в соответствии со своими должностными инструкциями и другими внутренними документами МКДОУ № 9 по информационной безопасности.

2 Цели и задачи обеспечения информационной безопасности

2.1 Целями обеспечения информационной безопасности МКДОУ № 9 являются:

- защита интересов МКДОУ № 9, работников и иных субъектов информационных отношений, взаимодействующих с МКДОУ № 9, от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем МКДОУ № 9, нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;
- обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов МКДОУ № 9 и предоставляемых сервисов;
- соблюдение правового режима использования массивов и программ обработки информации;
- предотвращение реализации угроз безопасности для деятельности МКДОУ № 9.

2.2 Объектами информационных правоотношений являются:

- информационные ресурсы, в том числе с ограниченным доступом;
- процессы обработки информации в информационных системах МКДОУ № 9, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;
- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации;

- системы и средства защиты информации, объекты и помещения, в которых размещены хранилища информации.

2.3 Субъектами информационных отношений при использовании информационных систем МКДОУ № 9, заинтересованными в обеспечении информационной безопасности, являются:

- МКДОУ № 9, как собственник информационных ресурсов и оператор персональных данных;

- работники МКДОУ № 9, как пользователи и поставщики информации в информационные системы;

- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах МКДОУ № 9.

2.4 Субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности определенной части информации;

- целостности информации;

- своевременного доступа к необходимой им информации;

- защиты от навязывания им ложной (недостоверной, искаженной) информации;

- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

- защиты соответствующей части информации от незаконного ее тиражирования и распространения.

2.5 Для достижения целей защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности МКДОУ № 9 должна обеспечивать решение следующих задач:

2.5.1 Защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи).

2.5.2 Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей).

2.5.3 Регистрацию и периодический контроль действий пользователей при использовании защищаемых ресурсов и периодический контроль корректности их действий.

2.5.4 Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.

2.5.5 Защиту от несанкционированной модификации и контроль целостности используемых в МКДОУ № 9 программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ.

2.5.6 Защиту информации ограниченного доступа, хранимой, обрабатываемой в МКДОУ № 9, от несанкционированного разглашения или искажения.

2.5.7 Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации.

2.5.8 Обеспечение исправности применяемых в информационных системах МКДОУ № 9 средств защиты информации.

2.5.9 Своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации.

2.5.10 Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в МКДОУ № 9.

2.6 Решение вышеперечисленных задач в МКДОУ № 9 осуществляется:

2.6.1 Учетом всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств).

2.6.2 Регламентацией процессов обработки подлежащей защите информации, действий работников МКДОУ № 9 и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационнораспорядительных документов по вопросам обеспечения информационной безопасности.

2.6.3 Назначением и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в МКДОУ № 9.

2.6.4 Наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам.

2.6.5 Знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства, требований организационнораспорядительных документов по вопросам обеспечения информационной безопасности.

2.6.6 Персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем.

2.6.7 Реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных.

2.6.8 Принятием мер по обеспечению физической целостности технических средств информационных систем и поддержанием необходимого уровня защищенности их компонентов.

2.6.9 Использованием физических и технических (программно-аппаратных) средств защиты ресурсов МКДОУ № 9 и административной поддержкой их использования.

2.6.10 Контролем соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.

2.6.11 Юридической защитой интересов МКДОУ № 9 при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.

2.6.12 Проведением анализа эффективности принятых мер и применяемых средств защиты информации в МКДОУ № 9. Разработкой и реализацией предложений по совершенствованию СЗИ в МКДОУ № 9.

3 Принципы обеспечения информационной безопасности

3.1 Принцип законности

3.1.1 При выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство.

3.1.2 Принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством.

3.1.3 Программно-технические средства, применяемые в МКДОУ № 9, должны иметь соответствующие лицензии, официально приобретаться МКДОУ № 9 у представителей разработчиков этих средств.

3.2 Принцип системности

При построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов МКДОУ № 9, согласованное применение методов и средств защиты информационных ресурсов МКДОУ № 9.

3.3 Принцип координации

3.3.1 При организации действий по обеспечению информационной безопасности руководство МКДОУ № 9 обеспечивает четкую взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.

3.3.2 При построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство МКДОУ № 9 обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

3.4 Принцип дружелюбности и простоты

3.4.1 Система обеспечения информационной безопасности в МКДОУ № 9 формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем МКДОУ № 9 процессы ее функционирования.

3.4.2 Система обеспечения информационной безопасности в МКДОУ № 9 выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников МКДОУ № 9 в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами информационных систем МКДОУ № 9.

3.5 Принцип превентивности

Меры, применяемые МКДОУ № 9 с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

3.6 Принцип оптимальности и многоуровневости

3.6.1 Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.

3.6.2 Применение разнородных программно-технических средств защиты, с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей.

3.6.3 Использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.

3.7 Принцип экономической целесообразности

3.7.1 Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для МКДОУ № 9 в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.

3.7.2 Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.

3.8 Принцип непрерывности и недопустимости открытого состояния

3.8.1 Система обеспечения информационной безопасности в МКДОУ № 9 строится таким образом, чтобы процесс защиты информационных систем МКДОУ № 9 осуществлялся непрерывно и целенаправленно на протяжении всего жизненного цикла информационных систем.

3.8.2 Система обеспечения информационной безопасности в МКДОУ № 9 при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.

3.9 Принцип профессионализма

3.9.1 Привлечение для разработки и внедрения системы обеспечения информационной безопасности, при необходимости, специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнения работ и практический опыт в данной области.

3.9.2 Организация профессиональной подготовки своих работников для эксплуатации компонентов системы обеспечения информационной безопасности.

3.10 Принцип выбора решений защиты

3.10.1 Ориентация на применение современных высокотехнологичных решений и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятных и не сложных в эксплуатации.

3.10.2 Использование оценки степени корректности функционирования и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.

3.11 Принцип развития

3.11.1 Развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности.

3.11.2 Ориентация на преемственность принятых ранее решений по защите, на анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.

3.12 Принцип персональной ответственности и разделения обязанностей

3.12.1 Руководство МКДОУ № 9 определяет права и ответственность каждого конкретного работника (в пределах его должностных обязанностей) за обеспечение безопасности информационных ресурсов МКДОУ № 9.

3.12.2 Система обеспечения информационной безопасности МКДОУ № 9 обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между работниками, исключая возможность нарушения критически важных для МКДОУ № 9 процессов или создания уязвимостей в защите информационных ресурсов.

3.13 Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих функций в МКДОУ № 9, в соответствии со своими должностными обязанностями.

4 Зоны ответственности участников процесса обеспечения информационной безопасности

4.1 Руководство МКДОУ № 9

4.1.1 Создает условия, при которых каждый работник МКДОУ № 9 знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.

4.1.2 Назначает работников, ответственных за создание и использование СЗИ, информации обрабатываемой в МКДОУ № 9, реализацию процессов обеспечения информационной безопасности, а также их контроля.

4.1.3 Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление СЗИ, а также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности МКДОУ № 9.

4.1.4 Иницирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в МКДОУ № 9.

4.1.5 Анализирует результаты работ по обеспечению информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, ее развития, о возможности принятия остаточных рисков информационной безопасности, о выделении ресурсов, необходимых для реализации Политики информационной безопасности.

4.2 Компетентные подразделения МКДОУ № 9

4.2.1 Подготавливают предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем МКДОУ № 9.

4.2.2 Разрабатывают процедуры эффективного управления техническими и программными средствами информационных систем и применяют их в практической деятельности в отношении всех систем, действующих в МКДОУ № 9.

4.2.3 Организуют проведение необходимого инструктажа работников структурных подразделений в части вопросов безопасной эксплуатации информационных систем.

4.2.4 Обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.

4.2.5 Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.

4.2.6 Обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.

4.2.7 Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в МКДОУ № 9.

4.2.8 Осуществляют поддержку функционирования информационных системы принимают необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности МКДОУ № 9.

4.2.9 Контролируют работоспособность устройств бесперебойного питания критичных для МКДОУ № 9 информационных систем.

4.2.10 Обеспечивают физическую защиту помещений, в которых располагаются критичные для МКДОУ № 9 информационные системы.

4.2.11 Обеспечивают сопровождение устройств контроля доступа в помещения МКДОУ № 9.

4.2.12 Обеспечивают защиту информационных ресурсов МКДОУ № 9 от случайного или намеренного уничтожения, искажения, разглашения.

4.2.13 Контролируют выполнение установленных правил и процедур обеспечения информационной безопасности в МКДОУ № 9.

4.3 Работники МКДОУ № 9

4.3.1 Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов МКДОУ № 9 в части обеспечения информационной безопасности.

4.3.2 Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников своего структурного подразделения.

4.3.3 Своевременно информируют руководство о всех выявленных сбоях в работе информационных систем.

4.3.4 Контролируют доступ к необходимым информационным ресурсам работников своего структурного подразделения в соответствии с потребностью в пределах служебных обязанностей.

4.3.5 Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов МКДОУ № 9 по вопросам информационной безопасности.

4.3.6 Соблюдают конфиденциальность данных, доступ к которым был ими получен.

4.3.7 Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.

4.3.8 Не допускают самовольного подключения и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.

4.3.9 Не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы.

4.3.10 Проявляют осмóтрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.

4.4 Сторонние физические и юридические лица

Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов МКДОУ № 9 и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств

5.1 Общие требования

5.1.1 В МКДОУ № 9 необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, направленных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации.

5.1.2 В МКДОУ № 9 осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью).

5.1.3. МКДОУ № 9, как обладатель информации ограниченного доступа, при осуществлении своих прав обязана:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

5.1.4 МКДОУ № 9, как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам на установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам регуляторов.

5.1.5 МКДОУ № 9, являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством РФ, обязана обеспечить:

- предотвращение НСД к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов НСД к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

5.1.7 Защита информации ограниченного доступа представляет собой принятие правовых, организационных и технических мер, направленных на:

- соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);
- обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);
- реализацию права на доступ к информации (исключение неправомерного блокирования информации).

5.2 Организация защиты конфиденциальной информации

5.2.1 При организации в МКДОУ № 9 защиты информации ограниченного доступа, необходимо руководствоваться требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации.

5.2.2 В МКДОУ № 9 необходимо соблюдать режим защиты конфиденциальной информации (далее – КИ):

- ограничение доступа к КИ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию КИ, с работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

- использование материальных носителей, содержащих КИ в соответствии с утвержденным порядком, исключающим несанкционированный доступ к ним.

5.2.3 Для обеспечения защиты КИ МКДОУ № 9 вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству РФ, меры.

5.2.4 В целях охраны КИ, в рамках трудовых отношений необходимо:

- ознакомить под расписку работников, доступ которых к КИ, необходим для выполнения ими своих служебных обязанностей, с перечнем КИ, и установленным в МКДОУ № 9 режимом защиты КИ, а также мерами ответственности за его нарушение;
- создать работникам необходимые условия для соблюдения установленного режима защиты КИ.

5.2.5 Работники МКДОУ № 9, обязаны выполнять установленный в МКДОУ № 9 режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

5.3 Особенности защиты персональных данных

5.3.1 При организации в МКДОУ № 9 защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой и хранением персональных данных граждан и определяет требования по защите их конфиденциальности.

5.3.2 МКДОУ № 9 самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» или другими федеральными законами.

5.3.3 Перечень мер, выполнение которых обеспечивает МКДОУ № 9 в качестве оператора персональных данных, должен включать:

- назначение в МКДОУ № 9 ответственного за организацию обработки персональных данных;

- издание МКДОУ № 9 документов, определяющих ее политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных

данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;

- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

- ознакомление работников МКДОУ № 9, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику АВР в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучение, при необходимости, указанных работников.

5.3.4 МКДОУ № 9 при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.3.5 Работники МКДОУ № 9 должны быть ознакомлены под роспись с документами МКДОУ № 9, устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

6 Основные требования к процессам обеспечения информационной безопасности

6.1 Общие положения

Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные должностные лица МКДОУ № 9.

6.2 Физическая безопасность и безопасность на рабочем месте

6.2.1 Система защиты зданий и помещений МКДОУ № 9, объектов и технических средств информационных систем МКДОУ № 9 обеспечивает выполнение следующих функций:

- разграничение доступа работников в помещения МКДОУ № 9 в соответствии с их полномочиями и функциональными обязанностями;
- регистрацию фактов входа посторонних лиц в здания МКДОУ № 9;
- предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;
- разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.

6.2.2 К техническим средствам, которые выделяются в специальные контролируемые зоны необходимо отнести следующие группы ресурсов:

- основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;

- сетевое оборудование и серверы, обеспечивающие работу критических систем;

- файловые серверы, на которых хранятся данные, в том числе резервные;

- критичные для деятельности МКДОУ № 9 системы и коммуникационное оборудование, обеспечивающее внешние коммуникации МКДОУ № 9.

6.2.3 Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.

6.2.4 Доступ в контролируемые зоны сторонних лиц или представителей других организаций возможен только в сопровождении уполномоченного работника МКДОУ № 9.

6.2.5 Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования МКДОУ № 9 осуществляется в помещениях, оборудованных замками, средствами сигнализации и (при необходимости) постоянно находящихся под охраной или наблюдением.

6.2.6 Размещение технических средств вывода и отображения информации в помещениях МКДОУ № 9 производится с учетом исключения возможности визуального просмотра информации посторонними лицами и персоналом, не допущенным к работе с данной информацией.

6.2.7 Работники МКДОУ № 9 на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.

6.2.8 Технические средства и оборудование должны размещаться и храниться таким образом, чтобы сократить возможный риск его повреждения и угрозы несанкционированного доступа.

6.2.9 Помещения МКДОУ № 9 должны быть оборудованы детекторами дыма, огнетушителями.

6.2.10 Основное техническое оборудование МКДОУ № 9 должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам МКДОУ № 9 в соответствии с рекомендациями производителя.

6.2.11 Пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра.

6.2.12 Портативные технические средства не должны оставаться за пределами контролируемой зоны МКДОУ № 9 дольше, чем того требует служебная необходимость, если иное не определено руководством МКДОУ № 9.

6.3 Безопасность при работе с носителями информации

6.3.1 В МКДОУ № 9 должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесения изменений в работу информационных систем.

6.3.2 Работники МКДОУ № 9 должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в МКДОУ № 9 в иных целях строго запрещено.

6.3.3 Электронные носители информации в МКДОУ № 9 должны быть учтены путем присвоения каждому носителю инвентаризационного номера.

6.3.4 Электронные носители информации должны храниться в помещениях, исключающих получение к ним НСД, при этом должен быть обеспечен контроль доступа к носителям.

6.3.5 В случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов.

6.3.6 При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.

6.3.7 При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.

6.4 Техническое обслуживание оборудования

6.4.1 Технические средства всех систем МКДОУ № 9 должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

6.4.2 Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.

6.4.3 Техническое обслуживание оборудования и систем сторонними организациями не должно приводить к риску нарушения конфиденциальности защищаемой информации.

6.5 Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности МКДОУ № 9 при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

- заключение соглашения о неразглашении конфиденциальной информации;
- контроль за действиями третьих лиц;
- в договорах с третьими лицами предусматривать право МКДОУ № 9 на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.

6.6 Антивирусная защита

6.6.1 В целях предупреждения, обнаружения и устранения вредоносных программ в МКДОУ № 9 на постоянной основе должны использоваться средства антивирусной защиты.

6.6.2 Обязательному антивирусному контролю должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранящаяся на подключаемых съемных носителях, при непосредственном обращении к ней.

6.6.3 При установке программного обеспечения на серверы информационных систем МКДОУ № 9 или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

6.6.4 Сигнатурные базы вредоносного программного обеспечения и антивирусные средства защиты должны регулярно обновляться.

6.6.5 Пользователи информационных систем МКДОУ № 9 не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

6.7 Контроль доступа к информационным системам

6.7.1 Все работники МКДОУ № 9, допущенные к работе с информационными системами, несут персональную ответственность за нарушения установленного порядка

обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

6.7.2 Уровень полномочий пользователя в информационной системе МКДОУ № 9 должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.

6.7.3 Осуществление регулярного контроля выполнения политики и иных документов, касающихся регламентации допуска работников МКДОУ № 9 к информационным системам.

6.8 Идентификация и аутентификация

6.8.1 Доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации и авторизации.

6.8.2 Получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться по представлению руководителей структурных подразделений.

6.9 Безопасность пароля

6.9.1 С целью обеспечения защиты от несанкционированного доступа к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей.

6.9.2 Для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде и в свободном доступе.

6.9.3 Для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам.

6.9.4 При вводе пароля пользователем для доступа к информационной системе МКДОУ № 9 должно исключаться отображение парольной информации на экране монитора в открытом виде.

6.9.5 Процедура смены парольной информации в информационных системах МКДОУ № 9 должна проводиться на регулярной основе.

6.10 Регистрация событий

Осуществление регистрации событий безопасности на всех компонентах информационных систем МКДОУ № 9, в которых обрабатывается, хранится или по средствам которых передается защищаемая информация.

6.11 Использование СКЗИ

6.11.1 Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством МКДОУ № 9 в соответствии с законодательством Российской Федерации.

6.11.2 При эксплуатации СКЗИ и ключевой информации все сотрудники МКДОУ № 9 должны выполнять требования нормативных правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов МКДОУ № 9 по обеспечению безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.

6.12 Безопасность информационной сети

6.12.1 Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций МКДОУ № 9 для обеспечения защиты данных и защиты информационных систем МКДОУ № 9 от НСД.

6.12.2 Должны быть определены цели использования сети Интернет и требования к процедуре использования ресурсов сети Интернет. Использование сети Интернет работников в личных целях должно быть строго запрещено.

6.12.3 Доступ к информационным сервисам сети Интернет предоставляется работникам МКДОУ № 9 только в случае производственной необходимости.

6.12.4 Подключение к сети Интернет должно осуществляться только при организации защиты соединения и специальных программных средств защиты.

6.12.5 Разрешительные политики доступа в Интернет должны технически реализовываться специализированным программным обеспечением.

6.12.6 Контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.

6.13 Использование электронной почты

6.13.1 Система электронной почты должна использоваться в МКДОУ № 9 с целью организации обмена электронными сообщениями между работниками, а также между работниками МКДОУ № 9 и внешними абонентами.

6.13.2 В МКДОУ № 9 должны быть четко определены требования к использованию системы электронной почты.

6.13.3 Предоставление и прекращение доступа к ресурсам электронной почты должно осуществляться только на основе оформленной заявки.

6.13.4 В МКДОУ № 9 должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.

6.13.5 В МКДОУ № 9 должны быть предусмотрены механизмы архивирования и резервного копирования электронной почты в автоматическом режиме.

6.14 Резервное копирование и восстановление данных

6.14.1 Осуществление резервного копирования для:

- файловых серверов и серверов приложений, критичных для деятельности МКДОУ № 9;
- операционных систем файловых серверов и прикладных программ;
- приложений, критичных для деятельности МКДОУ № 9; рабочих данных.

6.14.2 Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления.

6.14.3 Резервное копирование и восстановление ресурсов информационных систем МКДОУ № 9 должны проводить уполномоченные работники МКДОУ № 9.

6.14.4 Резервное копирование должно осуществляться в автоматическом режиме с применением специализированного программно-аппаратного комплекса.

7 Заключение

7.1 Настоящая Политика является внутренним документом МКДОУ № 9, общедоступной и подлежит размещению на официальном сайте МКДОУ № 9.

7.2 Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция всегда находится на сайте МКДОУ № 9