ПРИНЯТО
Общим собранием работников
МАДОУ «Конструктор успеха»
г. Перми
Протокол №6 от 08.12.2023

УТВЕРЖДЕНО
приказом заведующего МАДОУ
«Конструктор успеха» г. Перми
от 11.12.2023 г. №01-08/325
Заведующий М.В. Пынзарь

Политика
информационной безопасности в МАДОУ «Конструктор успеха» г.Перми

1. Общие положения.

1.1. Политика информационной безопасности (далее - Политика) является документом, определяющим направления деятельности в области обеспечения информационной безопасности муниципального автономного дошкольного образовательного учреждения «Конструктор успеха» г. Перми (далее - ДОУ) и определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности, которыми- руководствуются работники ДОУ при осуществлении своей деятельности.

1.2. Основной целью Политики информационной безопасности ДОУ является защита информации ДОУ 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 управлении.

1.3 Политика разработана в соответствии с: Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным закон 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» (в редакции от 13.07.2015 №357), Постановлением Правительства РФ №781 от 17.11.2007г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ № 687 от 15.09.2008г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник ДОУ. На лиц, работающих по договорам гражданско-правового характера, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

2. Цель и задачи Политики

2.1. Политика информационной безопасности направлена на защиту информационных ресурсов
(активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий

работников ДОУ, 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.

2.2. Основной целью обеспечения информационной безопасности ДОУ являются действия направленные на защиту информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, в том числе:

- обеспечения отказоустойчивого функционирования программных и аппаратно-программных средств ДОУ и предоставляемых сервисов;
- соблюдения правового режима использования массивов и средств обработки информации;
- предотвращения реализации угроз безопасности информации при осуществлении деятельности ДОУ.

2.3. Задачи обеспечения информационной безопасности:

- защита от несанкционированного доступа к информационным ресурсам ДОУ;
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам;
- контроль целостности среды исполнения программ и ее восстановление в случае нарушения;
- обеспечение аутентификации и идентификации пользователей, участвующих в информационном обмене;
- обеспечение исправности применяемых в информационных системах ДОУ средств защиты информации;
- своевременное выявление источников угроз безопасности информации;
- создание условий для минимизации наносимого ущерба неправомерными действиями, и устранение последствий нарушения информационной безопасности ДОУ.

2.4. Решение вышеперечисленных задач в ДОУ осуществляется посредством:

- учета всех подлежащих защите информационных ресурсов;
- назначения и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ДОУ;
- наделения каждого работника минимально необходимыми правами при работе;
- в информационной инфраструктуре согласно их должностным обязанностям;
- соблюдения всеми работниками, эксплуатирующими и обслуживающими программные и программно-аппаратные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;
- персональной ответственностью каждого работника за свои действия, участвующего
- в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем;
- реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, программно-аппаратных средств;
- принятия мер по обеспечению физической целостности программно-аппаратных средств информационных систем и поддержанием необходимого уровня защищенности компонентов;
- использования программных и программно-аппаратных средств защиты информации обрабатываемом в ДОУ и административной поддержкой их использования;
- проведения анализа эффективности принятых мер защиты информации и применяемых средств защиты информации в ДОУ.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ДОУ 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 ДОУ, 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 ДОУ. 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 ДОУ 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 ДОУ.

4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения информационной безопасности:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов ДОУ;
- своевременное обнаружение проблем, потенциально способных повлиять на ДОУ;
- корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками ДОУ за

Обеспечение ДОУ исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5. Объекты защиты

5.1. Объектами защиты с точки зрения информационной безопасности в управлении являются:

- информационный процесс профессиональной деятельности;
- информационные активы ДОУ.

5.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности ДОУ;
- 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 месторождения, 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 ДОУ, активов, находящихся под контролем ДОУ, а также активов, используемых для получения доступа к инфраструктуре ДОУ, должна быть определена ответственность соответствующего сотрудника ДОУ. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами ДОУ должна доводиться до сведения заведующего ДОУ.

6.2. Все работы в пределах ДОУ должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

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

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

6.5. 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 и близким.

6.6. 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.

6.7. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

- сотрудникам ДОУ 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/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- работа сотрудников ДОУ с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации ДОУ в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем ДОУ;
- сотрудники ДОУ перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть ДОУ для всех лиц, не являющихся сотрудниками ДОУ, включая членов семьи сотрудников.

6.8. Администратор имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.9. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация ДОУ.

6.10. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор локальной вычислительной сети (ЛВС).

6.11. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы

типа «мышь», шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное ДОУ, является его собственностью и предназначено для использования исключительно в производственных целях.

6.12. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.13. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки». Для установки 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.

6.14. 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 дает гарантии полного удаления записанной на нем информации.

6.15. Порты передачи данных, в том числе CD дисководы в стационарных компьютерах сотрудников ДОУ блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.

6.16. Все программное обеспечение, установленное на предоставленном ДОУ компьютерном оборудовании, является собственностью ДОУ и должно использоваться исключительно в производственных целях.

6.17. 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 непосредственно заведующему ДОУ.

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

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

6.19. Сотрудники ДОУ не должны:

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

6.20. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается.

Сотрудникам запрещается направлять конфиденциальную информацию ДОУ по электронной почте без использования систем шифрования. Строго конфиденциальная информация ДОУ, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.21. Использование сотрудниками ДОУ публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.
6.22. Сотрудники ДОУ для обмена документами должны использовать только свой официальный адрес электронной почты.
6.23. 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 непосредственному получателю.
6.24. Не допускается при использования 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.
6.25. 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.
6.26. В случае кражи переносного компьютера следует незамедлительно сообщить администратору и/или заведующему ДОУ.
6.27. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
- проинформировать администратора;
- не использовать и не включать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети ДОУ до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.
6.28. Сотрудникам ДОУ запрещается:
- нарушать информационную безопасность и работу сети ДОУ;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;