Государственное бюджетное дошкольное образовательное учреждение детский сад № 76 общеразвивающего вида с приоритетным осуществлением деятельности по физическому развитию детей Приморского района Санкт-Петербурга

УТВЕРЖДАЮ

и. о. заведующего ГБДОУ детский сад № 76

Приморского района Санкт-Петербурга

_____Э.В. Дорохова

Приказ от «16» июня 2023 г. № 58-ОД

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ГБДОУ детский сад № 76 Приморского района Санкт-Петербурга

Санкт-Петербург
2023

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика является документом, определяющим направления деятельности в области обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач информационной безопасности, как одно или несколько правил, процедур, практических приемов и руководящих принципов, которыми руководствуется Комитет, а также организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

Положения настоящей Политики не распространяются на обеспечение информационной безопасности сведений, составляющих государственную тайну.

Основной задачей в области информационной безопасности ГБДОУ детский сад № 76 Приморского района Санкт-Петербурга (далее - ГБДОУ) признает совершенствование мер и средств обеспечения защиты информации информационных ресурсов в контексте развития законодательства Российской Федерации и норм регулирования информационной деятельности в текущих условиях функционирования информационного поля.

При разработке Политики учитывались основные принципы создания систем защиты информации, характеристики и возможности организационно-технических мер и современных программных и аппаратно-программных средств защиты информации.

В рамках своей деятельности ГБДОУ обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

Требования информационной безопасности, соответствуют целям деятельности ГБДОУ и предназначены для снижения рисков, связанных с реализацией угроз безопасности информации.

Политика доступна всем работникам Комитет и всем пользователям его ресурсов.

2 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Субъекты информационных отношений

Субъектами при обеспечении информационной безопасности в ГБДОУ являются:

- работники ГБДОУ (в том числе уволенные);
- воспитанники ГБДОУ;
- законные представители воспитанников.

Объекты информационных отношений

Объектами защиты с точки зрения ИБ в управлении являются:

- информационный процесс профессиональной деятельности;
- информационные активы ГБДОУ.

Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности ГБДОУ;
- 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»
- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, программные и программно-аппаратные средства, в том числе каналы связи и телекоммуникации;
- системы и средства защиты информации, объекты и помещения, в которых размещены средства обработки информации.

Цели обеспечения информационной безопасности

Основными целями обеспечения информационной безопасности ГБДОУ являются действия, направленные на достижение защиты субъектов информационных отношений 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 ГБДОУ и предоставляемых сервисов;
- соблюдения правового режима использования средств обработки информации;
- предотвращения реализации угроз безопасности информации при осуществлении деятельности ГБДОУ.

Задачи обеспечения информационной безопасности

Достижение целей обеспечения информационной безопасности и свойств информации ГБДОУ решается следующими задачами:

- защита от несанкционированного доступа к информационным ресурсам;
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам;
- регистрация и периодический контроль действий пользователей при обработке защищаемой информации и периодический контроль корректности их действий;
- контроль целостности среды исполнения программ и ее восстановление в случае нарушения;
- обеспечение исправности применяемых в информационных системах ГБДОУ средств защиты информации;
- своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;
- создание условий для минимизации наносимого ущерба неправомерными действиями, и устранение последствий нарушения информационной безопасности в Комитет.

3 ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Система защиты информации должна предусматривать комплекс организационных, программных и программно-аппаратных средств и мер по защите информации в процессе ее обработки.

Выполнение требований достигается за счет реализации в ГБДОУ мер по защите информации:

- управлению доступом субъектов доступа к объектам доступа;
- защите машинных носителей персональных данных;
- антивирусной защите;
- обнаружению вторжений;
- контролю (анализу) защищенности персональных данных;
- обеспечению целостности информационной системы и персональных данных;
- обеспечению доступности персональных данных;
- защиты информационной системы, ее средств, систем связи и передачи данных;
- выявлению инцидентов и реагирование на них;

ГБДОУ как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

- соблюдать права и законные интересы иных лиц;
- принимать необходимые меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена законодательством Российской Федерации.

В том числе ГБДОУ вправе, если иное не предусмотрено законодательством Российской Федерации:

- 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 законодательством Российской Федерации основании;

- защищать установленными законодательством Российской Федерации 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 Российской Федерации.

4 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

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

4.3. Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

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

4.5. 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.

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

Рекомендованные правила:

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

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

4.8. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация ГБДОУ.
4.9. 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 является собственностью ГБДОУ и предназначено для использования исключительно в производственных целях.
4.10. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.
4.11. 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.
4.12. 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.
4.12. . Все программное обеспечение, установленное на предоставленном ГБДОУ компьютерном оборудовании, является собственностью ГБДОУ и должно использоваться исключительно в производственных целях.
4.13. 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 ГБДОУ.
4.14. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации.
4.15. Сотрудники ГБДОУ НЕ ДОЛЖНЫ:
- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.
4.16. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию ГБДОУ по электронной почте без использования систем шифрования. Строго конфиденциальная информация ГБДОУ, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

4.17. Использование сотрудниками ГБДОУ публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.
4.18. Сотрудники ГБДОУ для обмена документами должны использовать только свой официальный адрес электронной почты.
4.19. 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.
4.20. Не допускается при использования электронной почты:
- рассылка сообщений личного характера, использующих 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, 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.
4.21. 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.
4.22. В случае кражи переносного компьютера следует незамедлительно сообщить заведующему ГБДОУ.
4.23. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан не использовать и не включать зараженный компьютер, не подсоединять этот компьютер к компьютерной сети ГБДОУ до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.
Сотрудникам ГБДОУ ЗАПРЕЩАЕТСЯ:
- нарушать информационную безопасность ГБДОУ;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру или учетной записи в обход системы идентификации пользователя или безопасности;
- передавать информацию о сотрудниках или списки сотрудников ГБДОУ посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.
4.24. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

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

5. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

5.1. Управление ИБ ГБДОУ 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;
- оценку рисков, связанных с нарушениями ИБ.

6. РЕАЛИЗАЦИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Реализация Политики ИБ ГБДОУ осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

7. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В ПОЛИТИКУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

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

8. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности ГБДОУ возлагается на сотрудника, назначенного приказом заведующего ГБДОУ.
8.2. Заведующий ГБДОУ на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.