Государственное бюджетное дошкольное
образовательное учреждение ГБДОУ
детский сад № 99 компенсирующего вида
Выборгского района
Санкт-Петербурга

ПРИНЯТО
решением Общего собрания
протокол № 1
от 09.01.2023 г

УТВЕРЖДАЮ
Приказ № 4/1 от 09.01.2023 г.
И.о. заведующего
_____Г.Б. Николенко

# ПОЛИТИКА

## информационной безопасности

Санкт-Петербург
2023

# Политика информационной безопасности

## 1. Общие положения

1.1. Политика информационной безопасности (далее – Политика) 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 государственного бюджетного дошкольного образовательного учреждения детского сада № 99 компенсирующего вида Выборгского района Санкт-Петербурга (далее – ГБДОУ), при осуществлении своей деятельности.

1.2. Основной целью Политики является защита информации ГБДОУ 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 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. № 176 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №781 от 17.11.07г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ № 687 от 15.09.08г. «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 ГБДОУ. На лиц, работающих по договорам гражданско- правового характера, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

1.5. В Политике используются следующие понятия:

- **Информационная безопасность организаци (ИБ)** организации: состояние защищенности интересов организации в условиях угроз в информационной сфере.
- **Объект защиты информации**: информация или носитель информации, или информационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации.
- **Защищаемый процесс (информационной технологии)**: процесс, используемый в информационной технологии для обработки защищаемой информации с требуемым уровнем ее защищенности.
- **Нарушение информационной безопасности организации**: случайное или преднамеренное неправомерное действие физического лица (субъекта, объекта) в отношении активов организации, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах, вызывающее негативные последствия (ущерб/вред) для организации.
- **Чрезвычайная ситуация (ЧС)**: обстановка на определенной территории или акватории, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей природной среде,

значительные материальные потери и нарушение условий жизнедеятельности людей.

- **Инцидент информационной безопасности:** любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (утрата услуг, оборудования или устройств; системные сбои или перегрузки; ошибки пользователей; несоблюдение политики или рекомендаций по ИБ; нарушение физических мер защиты; неконтролируемые изменения систем; сбои программного обеспечения и отказы технических средств; нарушение правил доступа).

1.6. В Политике используются следующие обозначения и сокращения

| | |
|---|---|
| АРМ | Автоматизированное рабочее место |
| АС | Автоматизированная система |
| ГБДОУ | Государственное бюджетное дошкольное образовательное учреждение |
| ИБ | Информационная безопасность |
| ИР | Информационный ресурс |
| ИС | Информационная система |
| ИТ | Информационные технологии |
| НСД | Несанкционированный доступ |
| ОКЗ | Орган криптографической защиты |
| ПО | Программное обеспечение |
| СКЗИ | Средство криптографической защиты информации |
| СУИБ | Система управления информационной безопасностью |

## 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 ГБДОУ;
- защита целостности информации с целью поддержания возможности ГБДОУ по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами ГБДОУ;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности.
- 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 эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
- разработка нормативных документов для обеспечения ИБ ГБДОУ; выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ ГБДОУ;
- организация антивирусной защиты информационных ресурсов ГБДОУ; защита информации ГБДОУ от несанкционированного доступа (далее- НСД) и утечки по техническим каналам связи;

## 3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ ГБДОУ 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 ГБДОУ, 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 ГБДОУ. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников их способностью к адекватным и незамедлительным действиям в нештатной ситуации

3.3. Стратегия обеспечения ИБ ГБДОУ 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 ГБДОУ.

## 4. Основные принципы обеспечения информационной безопасности

4.1. Основными принципами обеспечения ИБ:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов ГБДОУ;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ ГБДОУ, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками ГБДОУ за обеспечение ИБ школы исходит из принципа персональной и единоличной ответственности за совершаемые операции.

## 5.Объекты защиты

5.1. Объектами защиты с точки зрения ИБ в управлении являются:

- информационный процесс профессиональной деятельности;
- информационные активы ГБДОУ.

5.2. 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».

## 6. Требования по информационной безопасности

6.1. 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.

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

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

6.4. Заведующий должен периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

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 и 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. 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 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 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 школы, включая членов семьи сотрудников.

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

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

6.11. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и

программного обеспечения. Все изменения производит администратор ЛВС.

6.12. 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 школой, является ее собственностью и предназначено для использования исключительно в производственных целях.

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

6.14. 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.

6.15. 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.

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

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

6.18. 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.

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

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

6.20. Сотрудники ГБДОУ НЕ ДОЛЖНЫ:

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

6.21. 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.

6.22. Использование сотрудниками ГБДОУ публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.

6.23. Сотрудники ГБДОУ для обмена документами должны использовать только свой официальный адрес электронной почты.

6.24. 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.

6.25. 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.

6.26. 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.

6.27. В случае кражи переносного компьютера следует незамедлительно сообщить заведующему ГБДОУ.

6.28. 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 школы до тех пор, пока на нем не будет произведено удаление обнаруженного вирусаи 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.

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

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

## 7. Управление информационной безопасностью

7.1. 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.

## 8. Реализация политики информационной безопасности

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

## 9. Порядок внесения 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 приведения 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 ГБДОУ возлагается на сотрудника, назначенного приказом заведующего ГБДОУ.

10.2. Заведующий ГБДОУ на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.