Государственное бюджетное дошкольное образовательное учреждение
детский сад № 18 комбинированного вида Кировского района Санкт-Петербурга

ПРИНЯТО

Советом образовательного учреждения
ГБДОУ детского сада № 18
Кировского района Санкт-Петербурга
протокол от 11 января 2023 г. № 1

УТВЕРЖДАЮ

Заведующий ГБДОУ детского сада № 18
Кировского района Санкт-Петербурга

_____ Ю.В. Иванова
приказ от 11.01.2023 г. № 33-ОД

СОГЛАСОВАНО
Решением Совета родителей
ГБДОУ детского сада №18
Кировского района Санкт-Петербурга
Протокол №1 от 11.01.2023 г.

Иванова Юлия Викторовна
Подписано цифровой подписью: Иванова Юлия Викторовна
Дата: 2023.01.12 15:20:20 +03'00'

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Государственного бюджетного дошкольного образовательного учреждения
детского сада № 18 комбинированного вида Кировского района Санкт-Петербурга

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности Государственного бюджетного дошкольного образовательного учреждения детского сада № 18 комбинированного вида Кировского района Санкт-Петербурга (далее – ГБДОУ №18) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее - ИБ), которыми руководствуются работники ГБДОУ №18 при осуществлении своей деятельности.

1.2. Основной целью Политики информационной безопасности ГБДОУ №18 является защита информации ГБДОУ №18 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 информационной безопасности разработана в соответствии с: Федеральным законом от 27 июля 2006г. (с изменениями на 29 декабря 2022 года) (редакция, действующая с 9 января 2023 года) № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. (с изменениями на 14 июля 2022 года) № 152-ФЗ «О персональных данных», , Указом Президента Российской Федерации от 6 марта 1997г. (с изменениями на 13 июля 2015 года) № 188 «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 № 18. 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 ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Основными целями политики ИБ являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам ГБДОУ №18;
- защита целостности информации с целью поддержания возможности ГБДОУ №18 по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами ГБДОУ №18;
- 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 №18;
- выявление, оценка, прогнозирование и предотвращение реализацииугроз ИБ ГБДОУ №18;
- организация антивирусной защиты информационных ресурсов ГБДОУ №18;
- защита информации ГБДОУ№18 от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи;

3. КОНЦЕПТУАЛЬНАЯ СХЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Политика ИБ ГБДОУ № 18 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 №18, 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 №18. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации

3.3. Стратегия обеспечения ИБ ГБДОУ №18 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 № 18.

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 №18;
- своевременное обнаружение проблем, потенциально способных повлиять на ИБ ГБДОУ №18, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;

– персонификация и разделение ролей и ответственности между сотрудниками ГБДОУ №18 за обеспечение ИБ ГБДОУ №18 исходит из принципа персональной и единоличной ответственности за совершаемыеоперации.

5. ОБЪЕКТЫ ЗАЩИТЫ

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

– информационный процесс профессиональной деятельности;

– информационные активы ГБДОУ №18

5.2. Защищаемая информация делится на следующие виды:

– информация по финансово-экономической деятельности ГБДОУ №18;

– 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 вышевидов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В отношении всех собственных информационных активов ГБДОУ №18, активов, находящихся под контролем ГБДОУ №18, а также активов, используемых для получения доступа к инфраструктуре ГБДОУ №18, должна быть определена ответственность соответствующего сотрудника ГБДОУ №18. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами ГБДОУ №18 должна доводиться до сведения Заведующего ГБДОУ №18

6.2. Все работы в пределах ГБДОУ №18 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 №18 и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.4. Ответственные лица должны периодически пересматривать права доступа 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 записьдругим, 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 №18 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 №18 с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации ГБДОУ №18 в сеть Интернет;

– сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем ГБДОУ №18;

– сотрудники ГБДОУ №18 перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

– запрещен доступ в Интернет через сеть ГБДОУ №18 для всех лиц, не являющихся сотрудниками ГБДОУ №18, включая членов семьи сотрудников.

6.9. Ответственный за обеспечение ИБ 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 №18.

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, дисководыдля CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное ГБДОУ №18, является его 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 кадминистратору. 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. 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. Простоепереформатирование носителя не дает гарантии полного удаления записанной на нем информации.

6.15. Порты передачи данных, в том числе CD дисководы в стационарных компьютерах сотрудников ГБДОУ №18 блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора.

6.16. Все программное обеспечение, установленное на предоставленном компьютерном оборудовании, является собственностью ГБДОУ № 18 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 имеющееотношения 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 Заведующий ГБДОУ №18.

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 ГБДОУ № 18 не должны:
– блокировать антивирусное программное обеспечение;
– устанавливать другое антивирусное программное обеспечение;
– изменять настройки и конфигурацию антивирусного программногообеспечения.

6.20. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целяхне допускается. Сотрудникам запрещается направлять конфиденциальнуюинформацию ГБДОУ № 18 по электронной почте без использования системшифрования. Строго конфиденциальная информация ГБДОУ № 18, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.21. Использование сотрудниками ГБДОУ № 18 публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условииприменения механизмов шифрования.

6.22. Сотрудники ГБДОУ №18 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, чтои 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 (независимоот 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 ответственному за обеспечение ИБ и/или Заведующему ГБДОУ №18.

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 ГБДОУ №18 до тех пор, пока на нем не будет произведено удаление обнаруженного вирусаи полное антивирусное сканирование

администратором.

6.28. Сотрудникам ГБДОУ № 18 запрещается:

- нарушать информационную безопасность и работу сети ГБДОУ №18;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обходсистемы идентификации пользователя или безопасности;
- передавать информацию о сотрудниках или списки сотрудников ГБДОУ №18посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы ипрочие 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 служебныхданных и программного обеспечения.

6.31. Все заявки на проведение технического обслуживания компьютеров должны направляться администратору.

7. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

7.1. Управление ИБ ГБДОУ №18 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 № 18 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 № 18 возлагается на сотрудника, назначенного приказом Заведующего ГБДОУ № 18.

10.2. Заведующий ГБДОУ №18 на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.