Государственное бюджетное дошкольное образовательное учреждение детский сад №70 комбинированного вида Приморского района Санкт-Петербурга

УТВЕРЖДЕНА
Приказом ГБДОУ детского сада №70
Приморского района
Санкт-Петербурга
от 19.06.2023 № 31

Щедрина О.В.
cn=Щедрина О.В., o=ГБДОУ детский сад № 70 Приморского района Санкт-Петербурга, ou=заведующий, email=gdou70@mail.ru, c=RU

Политика
информационной безопасности

Государственного бюджетного дошкольного образовательного учреждения детского сада №70 комбинированного вида Приморского района Санкт-Петербурга

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Политика информационной безопасности (далее – Политика) является документом, определяющим направления деятельности в области обеспечения информационной безопасности Государственного бюджетного дошкольного образовательного учреждения детского сада №70 комбинированного вида Приморского района Санкт-Петербурга (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 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

2.1 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.

2.2 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.

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 ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности осуществляется в соответствии со следующими основными принципами:

Принцип законности

Соблюдение действующего законодательство Российской Федерации в сфере защиты информации.

Все работники должны иметь представление об ответственности за правонарушения в сфере защиты информации. Программно-аппаратные средства, применяемые в ДОУ, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств или являться интеллектуальной собственностью ДОУ.

Принцип системности

При создании системы защиты должны учитываться актуальные угрозы безопасности информации, возможные объекты и направления атак на нее со стороны нарушителей. Система защиты должна строиться с учетом не только известных каналов утечки информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

Принцип комплексности

Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей все существенные угрозы безопасности информации.

Принцип своевременности

Разработка системы защиты информации должна вестись параллельно с разработкой и информационной системы.

Принцип преемственности

Постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите информации.

Принцип достаточности

Соответствие уровня затрат на обеспечение информационной безопасности и ценности информационных ресурсов на величину возможного ущерба от их разглашения, уничтожения и искажения.

Принцип ответственности

Возложение ответственности за обеспечение безопасности информации и ее обработки на каждого работника в пределах его полномочий.

Принцип обоснованности и технической реализуемости

Информационные технологии, программные и программно-аппаратные средства, меры защиты информации должны быть реализованы по современным решениям, обоснованы с точки зрения достижения заданного уровня защищенности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по безопасности информации.

Принцип профессионализма

Реализация мер защиты информации и эксплуатация средств защиты информации должна осуществляться профессиональными специалистами.

Возможно привлечение специализированных организаций к разработке средств и реализации мер защиты информации.

4. ОБЪЕКТЫ ЗАЩИТЫ

4.1 Объектами защиты с точки зрения информационной безопасности являются:
- информационный процесс профессиональной деятельности;
- Информационные активы ДОУ.

4.2. 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 место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

5 ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организация защиты информации

При организации в ДОУ защиты информации выполняются требования Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации. В том числе требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденные приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» для государственных информационных систем по которым ДОУ является Оператором.

В ДОУ помимо реализации основных мер защиты информации осуществляется:

- регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;
- информирование, обучение и повышение квалификации работников ДОУ в сфере информационной безопасности;
- анализ и поиск возможностей по повышению уровня защищенности информации.

Работники, имеющие доступ к информации ограниченного доступа, под роспись знакомятся с перечнем информации ограниченного доступа и принятыми в ДОУ мерами защиты информации.

Особенности защиты персональных данных

При организации обработки персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Перечень мер, выполнение которых обеспечивает ДОУ в качестве оператора персональных данных, включает:

- назначение ответственного за организацию обработки персональных данных;
- разработку локальных актов, определяющих правила в отношении обработки персональных данных в ДОУ;
- применение 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»;
- выполнение требований по составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных утверждённых Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда
  и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;
- ознакомление работников ДОУ, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных.

Физическая безопасность

Принятые организационные и технические меры по защите помещений, серверного и коммутационного оборудования, автоматизированных рабочих мест пользователей ДОУ обеспечивают реализацию следующих мер по:

Помещения ДОУ должны быть оборудованы детекторами огня и дыма, огнетушителями, средствами охранно-пожарной сигнализации.

Основное серверное и коммутационное оборудование ДОЦУ должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Портативные технические средства не должны оставаться за пределами контролируемой зоны ДОУ без контроля со стороны работников ДОУ.

Безопасность на рабочем месте

Запрещается вести запись паролей в открытом виде на материальных носителя, за исключением случаев, регламентированных методов хранения.

Документы и носители с информацией ограниченного доступа должны убираться в опечатываемые места (сейфы, шкафы и т.п.), при уходе с рабочего места. На автоматизированном рабочем месте Пользователя рабочая сессия должна быть прервана, рабочий стол заблокирован. Вход пользователя в систему не должен выполняться автоматически.

Документы, содержащие информацию ограниченного доступа, должны сразу изыматься из печатающих устройств.

При использовании мобильных технических средств необходимо соблюдать дополнительные меры по регламентации и контролю использования в информационной системе мобильных технических средств.

Размещение технических средств вывода информации производится с учетом исключения возможности визуального просмотра информации посторонними лицами и работниками, не допущенным к работе с данной информацией.

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

Техническое обслуживание оборудования

Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированными специалистами.

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

Управление жизненным циклом информационных систем

Мероприятия в процессе жизненного цикла информационных систем ДОУ должны быть направлены на обеспечение защиты информации при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации.

Любое планируемое к внедрению изменение информационной системы предварительно должно быть проанализировано на совместимость и отсутствие нарушений работоспособности системных компонентов в том числе средств защиты информации.

Работы по модернизации информационной системы, в том числе по установке программного обеспечения и обновлений, должны проводиться в нерабочее время или время наименьшей рабочей нагрузки.

При выводе из эксплуатации информационных систем должно обеспечиваться гарантированное удаление обрабатываемой и хранимой в них информации с использованием средств гарантированного уничтожения информации или путем физического уничтожения носителей информации.

Все процедуры обеспечения защиты информации должны выполняться и контролироваться ответственными лицами за организацию работ по защите информации.

Контроль доступа к информационным системам

Все работники ДОУ, допущенные к работе с информационными системами несут персональную ответственность за нарушения установленного порядка обработки информации.

Уровень полномочий пользователя в информационной системе ДОУ должен определяться в соответствии с его должностными обязанностями.

Идентификация и аутентификация

Доступ пользователей к информационным системам должен предоставляться только после успешного завершения идентификации, аутентификации.

Получение пользователем имени в информационной системе и пароля, которые обеспечивают доступ к информационной системе, должно осуществляться по представлению руководителя ДОУ.

Управление доступом

Управление доступом к информационной системе осуществляется посредством реализации необходимых методов, типов и правил разграничения доступа пользователям информационной системы ДОУ. В том числе обеспечен защищенный удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

Безопасность при работе с носителями информации

Работники ДОУ должны использовать только учтенные съемные машинные носители информации для выполнения своих должностных обязанностей. Использование съемных машинных носителей информации в ДОК в иных целях строго запрещено.

Съемные машинные носители информации должны хранится в опечатываемых шкафах, в помещениях в которых предусмотрена обработка информации ограниченного доступа.

В случае кражи или потери съемного машинного носителя информации, а также иных инцидентов, которые могут привести к нарушению свойств информации ограниченного доступа, должны проводиться мероприятия по расследованию таких инцидентов.

При выводе из эксплуатации съемного машинного носителя информации, все данные, хранящиеся на нем, должны быть удалены определенной комиссией из числа работников, средством гарантированного уничтожения информации.

Факт уничтожения информации на съемном машинном носителе информации фиксируется в акте об уничтожении информации со съемного машинного носителя информации.

Антивирусная защита

В целях обнаружения и устранения вредоносных программ в ДОУ должны использоваться средства антивирусной защиты информации.

Контроль защищенности персональных данных

В целях исключения эксплуатации уязвимостей программного обеспечения должны проводится работы по выявлению, анализу уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей. В том числе организация контроля установки обновления программного обеспечения включая средств защиты информации.

Использование программного обеспечения

Выбор программного обеспечения для производственных нужд ДОУ должен производиться в приоритете к отечественному, внесенного в Единый реестр российских программ для электронных вычислительных машин и баз данных. В случае отсутствия аналога в Едином реестре российских программ для электронных вычислительных машин и баз данных допускается использовать программного обеспечение импортного производства.

Использование электронной почты

Электронная почта должна использоваться в ДОУ с целью организации обмена электронными сообщениями между работниками и субъектами информационной безопасности.

При использовании электронной почты запрещается:

обмен информацией для служебного пользования, а также информацией ограниченного доступа;

предоставление доступа к электронной почте с использованием данных своей учетной записи третьим лицам;

публикация своего служебного адреса электронной почты в электронных каталогах, на поисковых машинах и других ресурсах сети Интернет в целях, не связанных с исполнением своих должностных обязанностей;

подписка по электронной почте на различные рекламные материалы, листы рассылки, электронные журналы и т.д., не связанные с выполнением пользователем должностных обязанностей;

открытие (запуск на выполнение) файлов, полученных по электронной почте или из ресурсов сети Интернет, без предварительной проверки их антивирусным программным обеспечением.

Работа в сетях общего пользования

При использовании сети Интернет запрещено:

использовать предоставленный Комитет доступ в сеть Интернет в личных целях;

использовать несанкционированные программные и программно-аппаратные средства, позволяющие получить несанкционированный доступ к сети Интернет;

публиковать, загружать и распространять материалы содержащие недостоверную информацию о ДОУ.

Резервное копирование и восстановление данных

Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и оперативное восстановление.

Резервное копирование должно осуществляться в автоматическом режиме с применением отечественного специализированного средства резервного копирования с действующим сертификатом соответствия по требованиям безопасности информации ФСТЭК России.

Мониторинг информационной безопасности

На постоянной основе должен проводиться комплексный анализ функционирования информационной системы ДОУ и возникающих событий информационной безопасности.

Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических мер по защите информации, анализ параметров конфигурации и настройки средств защиты информации.

Повышение осведомленности работников

В рамках организации комплексного противодействия угрозам безопасности информации, исходящим от работников ДОУ должна постоянно повышаться их осведомленность в области защиты информации.

Повышение осведомленности работников осуществляется:

по существующим локальным актам;

по применяемым мерам защиты информации;

по правильному использованию средств защиты информации.

6. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В ПОЛИТИКУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. 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.

7. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности ДОУ возлагается на работника, назначенного приказом заведующего ДОУ.

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

8.ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Все работники ДОУ должны быть ознакомлены с настоящей Политикой.
8.2. Настоящей Политике должны следовать все работники ДОУ.
8.3 При изменении законодательства в Политику вносятся изменения в установленном законом порядке. После принятия Политики (или изменений и дополнений отдельных пунктов и разделов) в новой редакции предыдущая редакция автоматически отменяется.