ПРИНЯТО	УТВЕРЖДЕНО
Общим собранием работников	Заведующий ГБДОУ детский сад № 8
ГБДОУ детский сад № 8	Рожковская С.В.
Протокол № 4 от 29 марта 2023 г.	Приказ № 29 -д от 31 марта 2023 г.

Подписано цифровой подписью: Рожковская Светлана Владимировна
DN: cn=Рожковская Светлана Владимировна, o=Государственное бюджетное дошкольное образовательное учреждение детский сад №8 Приморского района Санкт - Петербурга, ou=Заведующий, email=info.dou8@obr.gov.spb.ru, c=RU
Местонахождение: СПб, Серебристый бульвар дом 6 корпус 2 литера А

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Государственного бюджетного дошкольного образовательного учреждения

детский сад № 8

Приморского района Санкт-Петербурга

Санкт-Петербург
2023

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация	–	Действия по проверке подлинности субъекта доступа в информационной системе
Безопасность информации	–	Состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность
Государственная информационная система	–	Информационная система, создаваемая в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях
Доступ к информации	–	Возможность получения информации и ее использования
Доступность	–	Состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия
Защита информации от несанкционированного доступа	–	Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации
Защищаемая информация	–	Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации
Идентификация	–	Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационная система	–	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Информационные ресурсы	–	Отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов)
Информационные технологии	–	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
Информация	–	Сведения (сообщения, данные) независимо от формы их представления
Контролируемая зона	–	Пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств
Конфиденциальность	–	Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Обработка персональных данных	–	Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение

		(обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных
Оператор	–	гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных
Персональные данные	–	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
Угроза безопасности информации	–	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее
Уязвимость	–	Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации
Целостность	–	Устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ГОСТ Р	−	Государственный стандарт Российской Федерации
Политика	−	Политика информационной безопасности Государственного бюджетного дошкольного образовательного учреждения детский сад №8 Приморского района Санкт - Петербурга
ГБДОУ детский сад №8	−	Государственное бюджетное дошкольное образовательное учреждение детский сад №8 Приморского района Санкт-Петербурга
ФСБ России	−	Федеральная служба безопасности Российской Федерации
ФСТЭК России	−	Федеральная служба по техническому и экспортному контролю

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 Государственное бюджетное дошкольное образовательное учреждение детский сад № 8 Приморского района Санкт-Петербурга (далее ГБДОУ детский сад № 8), 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 № 8 признает совершенствование мер и средств обеспечения защиты информации информационных ресурсов ГБДОУ детский сад № 8 в контексте развития законодательства Российской Федерации и норм регулирования информационной деятельности в текущих условиях функционирования информационного поля.

В рамках своей деятельности ГБДОУ детский сад № 8 обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

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

Политика доступна всем работникам ГБДОУ детский сад № 8 и всем пользователям его ресурсов.

2 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Субъекты информационный отношений

Субъектами при обеспечении информационной безопасности в ГБДОУ детский сад № 8 являются:

физические лица, в рамках исполнения договорных обязательств;

физические лица, подавшие обращение в адрес ГБДОУ детский сад № 8;

юридические лица, в рамках исполнения договорных обязательств или во исполнении требований со стороны законодательства Российской Федерации;

органы государственной власти.

Объекты информационных отношений

Объектами информационных отношений являются:

информационные ресурсы ГБДОУ детский сад № 8;

государственные информационные системы Оператором которых является ГБДОУ детский сад № 8;

процессы обработки информации в информационных системах ДОУ, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

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

Основной целью обеспечения информационной безопасности ДОУ являются действия направлены на достижение защиты субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию.

Задачи обеспечения информационной безопасности

Достижение целей обеспечения информационной безопасности и свойств информации, ГБДОУ детский сад № 8 решается следующими задачами:

защиты от несанкционированного доступа к информационным ресурсам;

разграничения доступа пользователей к информационным, аппаратным, программным и иным ресурсам;

обеспечения исправности, применяемых в информационных системах ГБДОУ детский сад № 8 средств защиты информации;

созданием условий для минимизации наносимого ущерба неправомерными действиями, и устранение последствий нарушения информационной безопасности в ГБДОУ детский сад № 8.

Решение вышеперечисленных задач в ГБДОУ детский сад № 8 осуществляется посредством:

учета всех подлежащих защите информационных ресурсов;

регламентации процессов обработки информации, действий работников ГБДОУ детский сад № 8, осуществляющих эксплуатацию программных и программно-аппаратных средств, на основе утвержденных организационно-распорядительных документов по защите информации;

назначения работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ГБДОУ детский сад № 8;

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;

использования программных и программно-аппаратных средств защиты информации обрабатываемой в ГБДОУ детский сад № 8;

контроля соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.

3 ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности, осуществляется в соответствии со следующими основными принципами:

Принцип законности

При выборе мероприятий по защите информации, соблюдается действующее законодательство Российской Федерации в сфере защиты информации.

Все работники должны иметь представление об ответственности за правонарушения в сфере защиты информации.

Принцип системности

При создании системы защиты учитываются актуальные угрозы безопасности информации.

Принцип комплексности

Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты.

Принцип своевременности

Разработка системы защиты информации ведется параллельно с разработкой информационной системы.

Принцип ответственности

Возложение ответственности за обеспечение безопасности информации и ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения был известен нарушитель.

Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих должностных обязанностей в ГБДОУ детский сад № 8.

4 ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

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

Выполнение требований достигается за счет реализации на объектах информатизации мер по защите информации:

идентификации субъектов доступа и объектов доступа;

управлению доступом субъектов доступа к объектам доступа;

ограничению программной среды;

защите машинных носителей персональных данных;

антивирусной защите;

обнаружению вторжений;

контролю (анализу) защищенности персональных данных;

обеспечению целостности информационной системы и персональных данных;

защиты среды виртуализации;

защиты технических средств;

защиты информационной системы, ее средств, систем связи и передачи данных;

ГБДОУ детский сад № 8, 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.

Защита информации ограниченного доступа представляет собой принятие организационных и технических мер, направленных на:

соблюдение конфиденциальности информации (исключение неправомерного доступа, копирования, предоставления или распространения информации);

обеспечение целостности информации (исключение неправомерного уничтожения или модифицирования информации);

реализацию права на доступ к информации (исключение неправомерного блокирования информации).

Организация защиты информации

При организации в ГБДОУ детский сад № 8 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 ГБДОУ детский сад № 8 является Оператором.

В ГБДОУ детский сад № 8 помимо реализации основных мер защиты информации осуществляется:

методическая помощь работникам в вопросах обеспечения информационной безопасности.

В рамках обеспечения защиты информации, в рамках трудовых отношений ГБДОУ детский сад № 8 знакомит под роспись работников, доступ которых к информации

ограниченного доступа, необходим для выполнения ими своих должностных обязанностей, с перечнем информации ограниченного доступа, и принятыми в ДОУ мерами защиты информации.

Особенности защиты персональных данных

ГБДОУ детский сад № 8, при организации обработки персональных данных, руководствуется 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 в ГБДОУ детский сад № 8 ответственного за организацию обработки персональных данных;

разработку документов, определяющих правила в отношении обработки персональных данных в ГБДОУ детский сад № 8, локальных актов по вопросам обработки персональных данных;

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»;

ознакомление работников ГБДОУ детский сад № 8, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими требования ГБДОУ детский сад № 8 в отношении обработки персональных данных.

Обеспечение безопасности персональных данных достигается, в частности:

установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных.

5 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Физическая безопасность

Принятие организационных и технических мер по защите помещений ГБДОУ детский сад № 8, автоматизированных рабочих мест, обеспечивающих реализацию следующих мер по:

разграничению доступа работников в помещения ГБДОУ детский сад № 8 в соответствии с их полномочиями и должностными обязанностями.

Помещения ГБДОУ детский сад № 8 должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации.

Безопасность на рабочем месте

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

Документы и носители с информацией ограниченного доступа должны убираться в защищенные места хранения - 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.

Нахождение представителей юридических лиц в рамках исполнения договорных обязательств в помещениях в которых ведется обработка информации ограниченного доступа информационной системы, возможно только в сопровождении работника ГБДОУ детский сад № 8 допущенного до обработки такой информации.

Размещение технических средств вывода информации в помещениях ГБДОУ детский сад № 8 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

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

Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности ГБДОУ детский сад № 8 при взаимодействии с третьими лицами должно выполнять следующие мероприятия:

заключение соглашения о неразглашении информации ограниченного доступа полученной в ходе исполнения договорных обязательств.

Контроль доступа к информационным системам

Все работники ГБДОУ детский сад № 8, допущенные к работе с информационными системами несут персональную ответственность за нарушения установленного порядка обработки информации.

Идентификация

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

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

Безопасность при работе с носителями информации

Работники ГБДОУ детский сад № 8 должны использовать только учтенные съемные носители информации для выполнения своих должностных обязанностей. Использование съемных носителей информации в ГБДОУ детский сад № 8 в иных целях строго запрещено.

Съемные носители информации должны хранится в помещениях ограниченного доступа.

При выводе из эксплуатации съемного машинного носителя информации, все данные, хранящиеся на нем, должны быть удалены определенной комиссией из числа работников ГБДОУ детский сад № 8.

Антивирусная защита

В целях обнаружения и устранения вредоносных программ в ГБДОУ детский сад № 8 должны использоваться средства антивирусной защиты информации.

Использование средств криптографической защиты информации

Обеспечение защиты информации ограниченного доступа от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны обеспечивается применением средств криптографической защиты информации.

Использование электронной почты

Электронная почта используется в ГБДОУ детский сад № 8 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 ГБДОУ детский сад № 8 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 ГБДОУ детский сад № 8.

Резервное копирование и восстановление данных

Осуществление резервного копирования должно осуществляться для:

информации обрабатываемой на файловом сервере и сервере приложений, информационной системы;

рабочих мест администраторов информационной системы.

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

Настройка резервного копирования и восстановления ресурсов информационных систем ГБДОУ детский сад № 8 должны проводить уполномоченные работники ГБДОУ детский сад № 8.

6 ЗАКЛЮЧЕНИЕ

При изменении действующего законодательства Российской Федерации в области защиты информации, а также организационно-распорядительных документов ГБДОУ детский сад № 8 настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также внутренним документам ГБДОУ детский сад № 8.

Пересмотр и внесение изменений в настоящую Политику осуществляются на периодической и внеплановой основе.

7 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2 Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».

3 Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

4 Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

5 Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

6 Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

7 Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

8 Приказ 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».

9 Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

10 ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

11 ГОСТ Р 51898-2002 «Аспекты безопасности. Правила включения в стандарты».

12 ГОСТ Р 50.1.056-2005 «Техническая защита информации. Основные термины и определения».

13 ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства безопасности. Системы менеджмента информационной безопасности. Требования».

14 ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».

15 ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

16 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети».

17 ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации

по информационной безопасности».

18 ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

19 ГОСТ Р ИСО/МЭК 27004-2021 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание».

20 ГОСТ Р 51897-2021 «Менеджмент риска. Термины и определения».

21 ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения».

22 Концепция информационной безопасности исполнительных органов государственной власти Санкт-Петербурга от 20.02.2023.