Государственное бюджетное дошкольное образовательное учреждение
Центр развития ребенка - детский сад № 37
Приморского района Санкт- Петербурга

УТВЕРЖДЕНО
Заведующий _____А.С. Лищенко
Приказ от 19.06.2023 № 59

Политика
информационной безопасности
в ГБДОУ детский сад № 37
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 Центр развития ребенка - детский сад № 37 Приморского района Санкт-Петербурга
ГБДОУ	− Государственное бюджетное дошкольное образовательное учреждение Центр развития ребенка - детский сад № 37 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 Центра развития ребенка – детский сад №37 Приморского района Санкт-Петербурга (далее ГБДОУ) , 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 признает совершенствование мер и средств обеспечения защиты информации информационных ресурсов ГБДОУ 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 ГБДОУ и всем пользователям его ресурсов.

2 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Субъекты информационный отношений

Субъектами при обеспечении информационной безопасности в ГБДОУ являются:

граждане, работающие по договорам гражданско-правового характера;

физические лица, подавшие обращение в адрес ГБДОУ;

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

Объекты информационных отношений

Объектами информационных отношений являются:

информационные ресурсы ГБДОУ;

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

информационная инфраструктура, включающая системы обработки, хранения и анализа информации, программные 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 ГБДОУ 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, в том числе:

соблюдения правового режима использования массивов и 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:

защиты от несанкционированного доступа к информационным ресурсам;

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

регистрации и периодического контроля действий пользователей при обработке защищаемой информации и периодический контроль корректности их действий;

обеспечения исправности применяемых в информационных системах ГБДОУ средств защиты информации.

Решение вышеперечисленных задач в ГБДОУ осуществляется посредством:

учета всех подлежащих защите информационных ресурсов;

назначения и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в ГБДОУ;

наделения каждого работника минимально необходимыми правами при работе в информационной инфраструктуре согласно их должностным обязанностям;

контроля соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.

3 ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Обеспечение информационной безопасности, должно осуществляться в соответствии со следующими основными принципами:

Принцип законности

При выборе мероприятий по защите информации, должно соблюдаться действующее 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 ГБДОУ, должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств.

Принцип комплексности

Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей все существенные угрозы безопасности информации. Физическая защита должна обеспечиваться физическими средствами и организационными мерами.

При построении, внедрении и эксплуатации системы защиты информации руководство ГБДОУ обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

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. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения был известен нарушитель.

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.

Привлечение специализированных организаций к разработке средств и реализации мер защиты информации, подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и лицензии на право оказания услуг в этой области.

4 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 на объектах информатизации мер по защите информации:

ограничению программной среды;

защите машинных носителей персональных данных;

антивирусной защите;

обеспечению доступности персональных данных.

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.

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

Организация защиты информации

При организации в ГБДОУ защиты информации, должны выполняться 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 является Оператором.

В ГБДОУ помимо реализации основных мер защиты информации осуществляется:

информирование, обучение и повышение квалификации работников ГБДОУ в сфере информационной безопасности.

Для организации защиты информации, ГБДОУ вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству Российской Федерации, меры.

Особенности защиты персональных данных

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

Перечень мер, выполнение которых обеспечивает ГБДОУ в качестве оператора персональных данных, должен включать:

назначение в ГБДОУ ответственного за организацию обработки персональных данных;

разработку документов, определяющих правила в отношении обработки персональных данных в ГБДОУ, 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»;

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 ГБДОУ, 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 в отношении обработки персональных данных и обучение, при необходимости, указанных работников.

5 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Физическая безопасность

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

разграничению доступа работников в помещения ГБДОУ в соответствии с их полномочиями и должностными обязанностями;

регистрации фактов входа работников в помещения в которых ведется обработка персональных данных;

контролируемому пребыванию посторонних лиц в ГБДОУ в помещения, в которых ведется обработка информации ограниченного доступа и размещены аппаратные средства информационной системы;

Помещения ГБДОУ должны быть оборудованы детекторами дыма, огнетушителями, средствами охранно-пожарной сигнализации.

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.

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 ГБДОУ должны быть направлены на обеспечение защиты информации при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации.

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

Идентификация и аутентификация

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

Безопасность при работе с носителями информации

Работники ГБДОУ должны использовать только учтенные съемные машинные носители информации для выполнения своих должностных обязанностей.

Антивирусная защита

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

Обязательному контролю средством антивирусной защиты информации должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по локальной вычислительной сети в том числе и сетям общего пользования, а также информация, хранимая на съемных машинных носителях информации.

При установке программного обеспечения или его обновления должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

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 ГБДОУ 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 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.

Приобретение средств криптографической защиты информации ГБДОУ осуществляется на основании договоров и контрактов с лицами имеющими действующую лицензию ФСБ России на осуществление 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).

В целях организации и обеспечении передачи информации по каналам связи с использованием средств криптографической защиты информации, а также выполнения лицензионных требований ФСБ России в ГБДОУ должен быть создан орган криптографической защиты.

Портальные решения ГБДОУ с возможностью доступа с сетей общего пользования должны в приоритете разрабатываться с организацией защищенного канала посредством протокола TLS с поддержкой алгоритмов ГОСТ 34.10.

Использование электронной почты

Электронная почта должна использоваться в ГБДОУ 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;

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

ГБДОУ оставляет за собой право блокировать или ограничивать доступ работникам к сетям связи общего пользования, в том числе сети Интернет, содержание которых не имеет отношения к исполнению должностных обязанностей, а также к информационным ресурсам, содержание и направленность которых запрещены законодательством Российской Федерации.

При использовании сети Интернет запрещено:

использовать предоставленный ГБДОУ доступ в сеть Интернет в личных целях;

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

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.

Резервное копирование должно осуществляться в автоматическом режиме с применением отечественного специализированного средства резервного копирования

с действующим сертификатом соответствия по требованиям безопасности информации ФСТЭК России.

6 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Мониторинг информационной безопасности

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

Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием системы мониторинга инцидентов информационной безопасности или встроенных механизмов настройки и аудита событий в программных и программно-аппаратных средствах, используемых в информационной инфраструктуре ГБДОУ.

Управление рисками

Определение внутренних требований по защите информации, должны основываться на результатах проведения анализа рисков нарушения основных свойств безопасности для информационных ресурсов ГБДОУ.

Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения целостности, конфиденциальности и доступности для информационных ресурсов ГБДОУ.

Управление инцидентами информационной безопасности

Для обеспечения эффективного разрешения инцидентов информационной безопасности в ГБДОУ, минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться управление инцидентами информационной безопасности.

Повышение осведомленности работников

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

Повышение осведомленности работников ГБДОУ осуществляется:

по существующим в ГБДОУ организационно-распорядительным документам;

по применяемым в ГБДОУ мерам защиты информации;

по правильному использованию средств защиты информации.

7 ЗАКЛЮЧЕНИЕ

При изменении действующего законодательства Российской Федерации в области защиты информации, а также организационно-распорядительных документов ГБДОУ настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также внутренним документам ГБДОУ.

Все требования, установленные действующим законодательством Российской Федерации, подзаконными актами и договорными отношениями, а также подход ГБДОУ к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

ГБДОУ в приоритетном направлении должен рассматриваться переход на программное обеспечение отечественного производителя, включенного в единый реестр российских программ для электронных вычислительных машин и баз данных. В том числе по части серверного, коммутационного оборудования и программно-аппаратных средств включенных в Единый реестр российской радиоэлектронной продукции.

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

8 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.