

**Санкт-Петербургское государственное учреждение
«Территориальная централизованная библиотечная система Пушкинского района»**

Приложение № 1
к приказу от 14.09.2022 № 133

**Политика информационной безопасности
Санкт-Петербургского государственного бюджетного
учреждения «Территориальная централизованная
библиотечная система Пушкинского района»**

2022
Санкт-Петербург, г. Пушкин

Содержание

Определения	2
Обозначения и сокращения	3
1 Общие положения	4
2 Цели и задачи обеспечения информационной безопасности	4
3 Принципы обеспечения информационной безопасности	6
4 Зоны ответственности участников процесса обеспечения информационной безопасности	9
5 Основные требования по защите информации ограниченного доступа	11
6 Основные требования к процессам обеспечения информационной безопасности	14
7 Основные требования к процессам управления информационной безопасностью	17
8 Заключение	19

Определения

Защита информации	— деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
Информация	— сведения (сообщения, данные) независимо от формы их представления
Информация ограниченного доступа	— информация, доступ к которой ограничен федеральными законами
Информационная система	— совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Конфиденциальность информации	— обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
Обладатель информации	— лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам
Персональные данные	— любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных)

Обозначения и сокращения

КИ	–	Конфиденциальная информация
МЭ	–	Межсетевой экран
НСД	–	Несанкционированный доступ
СЗИ	–	Система защиты информации
СКЗИ	–	Средство криптографической защиты информации
СрЗИ	–	Средство защиты информации
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю

1 Общие положения

1.1 Настоящая Политика является документом, доступным всем сотрудникам СПб ГБУ «ТЦБС Пушкинского района» и всем пользователям его ресурсов. Представляет собой официально принятую руководством СПб ГБУ «ТЦБС Пушкинского района» систему взглядов на обеспечение информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района».

1.2 Основной задачей в области информационной безопасности СПб ГБУ «ТЦБС Пушкинского района» признает совершенствование мер и средств обеспечения информационной безопасности информационных ресурсов СПб ГБУ «ТЦБС Пушкинского района» в контексте развития законодательства и норм регулирования информационной деятельности.

1.3 В рамках своей деятельности СПб ГБУ «ТЦБС Пушкинского района» обязуется предпринимать все возможные меры для защиты информации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности или других противоправных действий, связанных с нарушением информационной безопасности СПб ГБУ «ТЦБС Пушкинского района».

1.4 Требования информационной безопасности, которые предъявляются СПб ГБУ «ТЦБС Пушкинского района», соответствуют целям деятельности СПб ГБУ «ТЦБС Пушкинского района» и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

1.5 Реализация и контроль исполнения требований, установленных настоящей Политикой, осуществляется работниками структурных подразделений СПб ГБУ «ТЦБС Пушкинского района», ответственных за информационную безопасность, в соответствии со своими должностными инструкциями и другими внутренними документами СПб ГБУ «ТЦБС Пушкинского района» по информационной безопасности.

2 Цели и задачи обеспечения информационной безопасности

2.1 Целями обеспечения информационной безопасности СПб ГБУ «ТЦБС Пушкинского района» являются:

- защита интересов СПб ГБУ «ТЦБС Пушкинского района», работников и иных субъектов информационных отношений, взаимодействующих с СПб ГБУ «ТЦБС Пушкинского района», от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем СПб ГБУ «ТЦБС Пушкинского района», нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;
- обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов СПб ГБУ «ТЦБС Пушкинского района» и предоставляемых сервисов;
- соблюдение правового режима использования массивов и программ обработки информации;
- предотвращение реализации угроз безопасности для деятельности СПб ГБУ «ТЦБС Пушкинского района».

2.2 Объектами информационных правоотношений являются:

- информационные ресурсы, в том числе с ограниченным доступом;
- процессы обработки информации в информационных системах СПб ГБУ «ТЦБС Пушкинского района», информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации;

- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации;
- системы и средства защиты информации, объекты и помещения, в которых размещены хранилища информации.

2.3 Субъектами информационных отношений при использовании информационных систем СПб ГБУ «ТЦБС Пушкинского района», заинтересованными в обеспечении информационной безопасности, являются:

- СПб ГБУ «ТЦБС Пушкинского района», как собственник информационных ресурсов и оператор персональных данных;
- работники структурных подразделений СПб ГБУ «ТЦБС Пушкинского района», как пользователи и поставщики информации в информационные системы;
- юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах СПб ГБУ «ТЦБС Пушкинского района».

2.4 Субъекты информационных отношений заинтересованы в обеспечении:

- конфиденциальности определенной части информации;
- целостности информации;
- своевременного доступа к необходимой им информации;
- защиты от навязывания им ложной (недостовой, искаженной) информации;
- разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты соответствующей части информации от незаконного ее тиражирования и распространения.

2.5 Для достижения целей защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности СПб ГБУ «ТЦБС Пушкинского района» должна обеспечивать решение следующих задач:

2.5.1 Защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи).

2.5.2 Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей).

2.5.3 Регистрацию и периодический контроль действий пользователей при использовании защищаемых ресурсов и периодический контроль корректности их действий.

2.5.4 Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения.

2.5.5 Защиту от несанкционированной модификации и контроль целостности используемых в СПб ГБУ «ТЦБС Пушкинского района» программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ.

2.5.6 Защиту информации ограниченного доступа, хранимой, обрабатываемой в СПб ГБУ «ТЦБС Пушкинского района», от несанкционированного разглашения или искажения.

2.5.7 Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации.

2.5.8 Обеспечение исправности применяемых в информационных системах СПб ГБУ «ТЦБС Пушкинского района» средств защиты информации.

2.5.9 Своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации.

2.5.10 Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в СПб ГБУ «ТЦБС Пушкинского района».

2.6 Решение вышеперечисленных задач в СПб ГБУ «ТЦБС Пушкинского района» осуществляется:

2.6.1 Учетом всех подлежащих защите информационных ресурсов (каналов связи, аппаратных и программных средств).

2.6.2 Регламентацией процессов обработки подлежащей защите информации, действий работников СПб ГБУ «ТЦБС Пушкинского района» и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

2.6.3 Назначением и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района».

2.6.4 Наделением каждого работника минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам.

2.6.5 Знанием и строгим соблюдением всеми работниками, использующими и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности.

2.6.6 Персональной ответственностью за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющего доступ к ресурсам информационных систем.

2.6.7 Реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, технических средств и данных.

2.6.8 Принятием мер по обеспечению физической целостности технических средств информационных систем и поддержанием необходимого уровня защищенности их компонентов.

2.6.9 Использованием физических и технических (программно-аппаратных) средств защиты ресурсов СПб ГБУ «ТЦБС Пушкинского района» и административной поддержкой их использования.

2.6.10 Контролем соблюдения пользователями информационных систем требований по обеспечению информационной безопасности.

2.6.11 Юридической защитой интересов СПб ГБУ «ТЦБС Пушкинского района» при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.

2.6.12 Проведением анализа эффективности принятых мер и применяемых средств защиты информации в СПб ГБУ «ТЦБС Пушкинского района». Разработкой и реализацией предложений по совершенствованию СЗИ в СПб ГБУ «ТЦБС Пушкинского района».

3 Принципы обеспечения информационной безопасности

3.1 Принцип законности

3.1.1 При выборе защитных мероприятий, реализуемых системой обеспечения информационной безопасности, должно соблюдаться действующее законодательство.

3.1.2 Принятые меры защиты не должны препятствовать доступу к защищаемой информации со стороны государственных или правоохранительных органов, если такой доступ необходим в случаях, предусмотренных законодательством.

3.1.3 Программно-технические средства, применяемые в СПб ГБУ «ТЦБС Пушкинского района», должны иметь соответствующие лицензии, официально приобретаться СПб ГБУ «ТЦБС Пушкинского района» у представителей разработчиков этих средств.

3.2 Принцип системности

При построении системы обеспечения информационной безопасности необходимо применять системный подход, который предполагает взаимосвязь процессов организации защиты информационных ресурсов СПб ГБУ «ТЦБС Пушкинского района», согласованное применение методов и средств защиты информационных ресурсов СПб ГБУ «ТЦБС Пушкинского района».

3.3 Принцип координации

3.3.1 При организации действий по обеспечению информационной безопасности руководство СПб ГБУ «ТЦБС Пушкинского района» обеспечивает четкую взаимосвязь соответствующих структурных подразделений между собой, с представителями сторонних организаций, оказывающих услуги в рамках договорных обязательств.

3.3.2 При построении, внедрении и эксплуатации системы обеспечения информационной безопасности руководство СПб ГБУ «ТЦБС Пушкинского района» обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

3.4 Принцип дружелюбности и простоты

3.4.1 Система обеспечения информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района» формируется таким образом, чтобы сделать максимально прозрачными для пользователей информационных систем СПб ГБУ «ТЦБС Пушкинского района» процессы ее функционирования.

3.4.2 Система обеспечения информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района» выстраивается таким образом, чтобы ограничения организационного и технического характера, налагаемые на сотрудников СПб ГБУ «ТЦБС Пушкинского района» в связи с реализацией защитных мер, существенно не затрудняли работу с ресурсами информационных систем СПб ГБУ «ТЦБС Пушкинского района».

3.5 Принцип превентивности

Меры, применяемые АПР с целью обеспечения информационной безопасности, должны носить упреждающий характер и не допускать реализацию соответствующих угроз и атак.

3.6 Принцип оптимальности и многоуровневости

3.6.1 Выбор единых программно-технических средств с целью сокращения расходов на создание и поддержку функционирования компонентов системы обеспечения информационной безопасности.

3.6.2 Применение разнородных программно-технических средств защиты, с целью построения целостной системы обеспечения информационной безопасности и устранения возможных уязвимостей.

3.6.3 Использование для создания разных рубежей обеспечения информационной безопасности средств, которые имеют схожие друг с другом функции, но разработанные различными производителями и имеющие различную логику построения защитных механизмов.

3.7 Принцип экономической целесообразности

3.7.1 Осуществление оценки уровня затрат на обеспечение безопасности, ценности информационных ресурсов и величины возможного ущерба для СПб ГБУ «ТЦБС Пушкинского района» в случае нарушения конфиденциальности, целостности и доступности информационных ресурсов.

3.7.2 Выбор необходимого и достаточного уровня защиты информационных ресурсов, при котором затраты, риск и размер возможного ущерба являются приемлемыми.

3.8 Принцип непрерывности и недопустимости открытого состояния

3.8.1 Система обеспечения информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района» строится таким образом, чтобы процесс защиты информационных систем СПб ГБУ «ТЦБС Пушкинского района» осуществлялся непрерывно и целенаправленно на протяжении всего жизненного цикла информационных систем.

3.8.2 Система обеспечения информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района» при любых возникающих обстоятельствах либо полностью выполняет свои функции, либо полностью блокирует доступ.

3.9 Принцип профессионализма

3.9.1 Привлечение для разработки и внедрения системы обеспечения информационной безопасности, при необходимости, специализированных организаций, наиболее подготовленных к конкретному виду деятельности и имеющих соответствующие лицензии на выполнения работ и практический опыт в данной области.

3.9.2 Организация профессиональной подготовки своих работников для эксплуатации компонентов системы обеспечения информационной безопасности.

3.10 Принцип выбора решений защиты

3.10.1 Ориентация на применение современных высокотехнологичных решений и программно-технических средств защиты, хорошо зарекомендовавших себя, интуитивно понятных и не сложных в эксплуатации.

3.10.2 Использование оценки степени корректности функционирования и исполнения защитных функций, отказоустойчивости, проверки согласованности конфигурации различных компонентов и возможности осуществления централизованного администрирования при выборе решений по защите информационных систем.

3.11 Принцип развития

3.11.1 Развитие и обновление на регулярной основе существующей системы обеспечения информационной безопасности.

3.11.2 Ориентация на преемственность принятых ранее решений по защите, на анализ функционирования информационных систем и самой системы обеспечения информационной безопасности.

3.12 Принцип персональной ответственности и разделения обязанностей

3.12.1 Руководство СПб ГБУ «ТЦБС Пушкинского района» определяет права и ответственность каждого конкретного работника (в пределах его должностных обязанностей) за обеспечение безопасности информационных ресурсов СПб ГБУ «ТЦБС Пушкинского района».

3.12.2 Система обеспечения информационной безопасности СПб ГБУ «ТЦБС Пушкинского района» обеспечивает разделение полномочий в информационных системах, обязанностей и ответственности между работниками, исключая возможность нарушения критически важных для СПб ГБУ «ТЦБС Пушкинского района» процессов или создания уязвимостей в защите информационных ресурсов.

3.13 Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих функций в СПб ГБУ «ТЦБС Пушкинского района», в соответствии со своими должностными обязанностями.

4 Зоны ответственности участников процесса обеспечения информационной безопасности

4.1 Руководство (директор) СПб ГБУ «ТЦБС Пушкинского района»

4.1.1 Создает условия, при которых каждый работник СПб ГБУ «ТЦБС Пушкинского района» знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.

4.1.2 Назначает работников, ответственных за создание и использование СЗИ, информации обрабатываемой в СПб ГБУ «ТЦБС Пушкинского района», реализацию процессов обеспечения информационной безопасности, а также их контроля.

4.1.3 Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности, внедрение и управление СЗИ, а также контроль и мониторинг текущего состояния системы обеспечения информационной безопасности СПб ГБУ «ТЦБС Пушкинского района».

4.1.4 Иницирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района».

4.1.5 Анализирует результаты работ по обеспечению информационной безопасности и на их основе принимает решения о необходимости развития системы обеспечения информационной безопасности, ее развития, о возможности принятия остаточных рисков информационной безопасности, о выделении ресурсов, необходимых для реализации Политики информационной безопасности.

4.2 Компетентные подразделения СПб ГБУ «ТЦБС Пушкинского района»

4.2.1 Подготавливают предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем СПб ГБУ «ТЦБС Пушкинского района».

4.2.2 Разрабатывают процедуры эффективного управления техническими и программными средствами информационных систем и применяют их в практической деятельности в отношении всех систем, действующих в СПб ГБУ «ТЦБС Пушкинского района».

4.2.3 Организуют проведение необходимого инструктажа работников структурных подразделений в части вопросов безопасной эксплуатации информационных систем.

4.2.4 Обеспечивают защиту доступа ко всему серверному и коммутационному оборудованию, носителям информации, которые используются в соответствующих структурных подразделениях.

4.2.5 Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.

4.2.6 Обеспечивают отказоустойчивость всего программно-аппаратного комплекса и процедуру регламентированного восстановления работоспособности после отказов компонентов.

4.2.8 Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в СПб ГБУ «ТЦБС Пушкинского района».

4.2.9 Осуществляют поддержку функционирования информационных систем и принимают необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности СПб ГБУ «ТЦБС Пушкинского района».

4.2.10 Контролируют работоспособность устройств бесперебойного питания критичных для СПб ГБУ «ТЦБС Пушкинского района» информационных систем.

4.2.11 Обеспечивают физическую защиту помещений, в которых располагаются критичные для СПб ГБУ «ТЦБС Пушкинского района» информационные системы.

4.2.12 Обеспечивают сопровождение устройств контроля доступа в помещения СПб ГБУ «ТЦБС Пушкинского района».

4.2.13 Обеспечивают защиту информационных ресурсов СПб ГБУ «ТЦБС Пушкинского района» от случайного или намеренного уничтожения, искажения, разглашения.

4.2.14 Контролируют выполнение установленных правил и процедур обеспечения информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района».

4.3 Руководители структурных подразделений СПб ГБУ «ТЦБС Пушкинского района»

4.3.1 Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов СПб ГБУ «ТЦБС Пушкинского района» в части обеспечения информационной безопасности.

4.3.2 Обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют компетентное подразделение о любых подозрительных событиях или нарушениях действующих правил обеспечения информационной безопасности.

4.3.3 Обеспечивают соответствие действий работников подразделения Политике информационной безопасности, внутренним документам по информационной безопасности и любым другим распоряжениям руководства СПб ГБУ «ТЦБС Пушкинского района» по вопросам информационной безопасности.

4.3.4 Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников своего структурного подразделения.

4.3.5 Контролируют выполнение работниками в своем структурном подразделении установленных правил в целях обеспечения физической безопасности компьютерного оборудования и носителей информации.

4.3.6 Своевременно информируют руководство о всех выявленных сбоях в работе информационных систем.

4.3.7 Контролируют доступ к необходимым информационными ресурсам работников своего структурного подразделения в соответствии с потребностью в пределах служебных обязанностей.

4.4 Работники СПб ГБУ «ТЦБС Пушкинского района»

4.4.1 Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов СПб ГБУ «ТЦБС Пушкинского района» по вопросам информационной безопасности.

4.4.2 Соблюдают конфиденциальность данных, доступ к которым был ими получен.

4.4.3 Обеспечивают физическую безопасность всего технического оборудования и носителей информации, используемых в работе.

4.4.4 Не допускают самовольного подключения и использования в автоматизированной информационной системе личного компьютерного и цифрового оборудования, а также носителей информации.

4.4.5 Не допускают самовольную установку программного обеспечения на компьютеры, входящие в состав информационной системы.

4.4.6 Своевременно информируют руководителя своего структурного подразделения о всех случаях нарушения информационной безопасности и о всех выявленных сбоях в работе программных и программно-аппаратных средств.

4.4.7 Проявляют осмотрительность в отношении любых действий, которые могут повлечь за собой снижение уровня информационной безопасности.

4.5 Сторонние физические и юридические лица

Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов СПб ГБУ «ТЦБС Пушкинского района» и других распоряжений по вопросам информационной безопасности

5 Основные требования по защите информации ограниченного доступа

5.1 Общие требования

5.1.1 В СПб ГБУ «ТЦБС Пушкинского района» необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, направленных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации.

5.1.2 В СПб ГБУ «ТЦБС Пушкинского района» осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью).

5.1.3 В СПб ГБУ «ТЦБС Пушкинского района» разработан перечень информации ограниченного доступа.

5.1.4 СПб ГБУ «ТЦБС Пушкинского района», как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

5.1.5 СПб ГБУ «ТЦБС Пушкинского района», как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

- 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 законом основании;
- защищать установленными законом 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 регуляторов.

5.1.6 СПб ГБУ «ТЦБС Пушкинского района», являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством РФ, обязано обеспечить:

- предотвращение НСД к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов НСД к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации.

5.1.7 Защита информации ограниченного доступа представляет собой принятие правовых, 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).

5.2 Организация защиты конфиденциальной информации

5.2.1 При организации в СПб ГБУ «ТЦБС Пушкинского района» защиты информации ограниченного доступа, необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», которые регулируют отношения, связанные с установлением, изменением и прекращением режима обработки защищаемой информации.

5.2.2 В СПб ГБУ «ТЦБС Пушкинского района» необходимо соблюдать режим защиты конфиденциальной информации (далее – КИ):

- ограничение доступа к КИ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию КИ, с работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- использование материальных носителей, содержащих КИ в соответствии с утвержденным порядком, исключающим несанкционированный доступ к ним.

5.2.3 Для обеспечения защиты КИ, СПб ГБУ «ТЦБС Пушкинского района» вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству РФ, меры.

5.2.4 В целях охраны КИ, в рамках трудовых отношений необходимо:

- ознакомить под расписку работников, доступ которых к КИ, необходим для выполнения ими своих служебных обязанностей, с перечнем КИ, и установленным в СПб ГБУ «ТЦБС Пушкинского района» режимом защиты КИ, а также мерами ответственности за его нарушение;
- создать работникам необходимые условия для соблюдения установленного режима защиты КИ.

5.2.5 Работники СПб ГБУ «ТЦБС Пушкинского района», обязаны выполнять установленный в СПб ГБУ «ТЦБС Пушкинского района» режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

5.3 Особенности защиты персональных данных

5.3.1 При организации в СПб ГБУ «ТЦБС Пушкинского района» защиты персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», который регулирует отношения, связанные с обработкой и хранением персональных данных граждан и определяет требования по защите их конфиденциальности.

5.3.2 СПб ГБУ «ТЦБС Пушкинского района» самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом №152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено Федеральным законом №152-ФЗ или другими федеральными законами.

5.3.3 Перечень мер, выполнение которых обеспечивает СПб ГБУ «ТЦБС Пушкинского района» в качестве оператора персональных данных, должен включать:

- назначение в АПР ответственного за организацию обработки персональных данных;
- издание СПб ГБУ «ТЦБС Пушкинского района» документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона №152-ФЗ;

- 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 СПб ГБУ «ТЦБС Пушкинского района», непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику СПб ГБУ «ТЦБС Пушкинского района» в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и обучение, при необходимости, указанных работников.

5.3.4 СПб ГБУ «ТЦБС Пушкинского района» при обработке персональных данных обязано принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

5.3.5 Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн);

- проведением классификации ИСПДн в соответствии с требованиями Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», и определение класса защищенности для ИСПДн;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает выбранные уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

- учетом машинных носителей персональных данных;

- обнаружением фактов НСД к персональным данным и принятием мер;

- восстановлением персональных данных, модифицированных или уничтоженных вследствие НСД к ним;

- установлением правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн.

5.3.6 Работники СПб ГБУ «ТЦБС Пушкинского района» должны быть ознакомлены под роспись с документами СПб ГБУ «ТЦБС Пушкинского района», устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

6 Основные требования к процессам обеспечения информационной безопасности

6.1 Общие положения

Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные подразделения СПб ГБУ «ТЦБС Пушкинского района».

6.2 Физическая безопасность и безопасность на рабочем месте

6.2.1 Система защиты зданий и помещений СПб ГБУ «ТЦБС Пушкинского района», объектов и технических средств информационных систем СПб ГБУ «ТЦБС Пушкинского района» обеспечивает выполнение следующих функций:

- разграничение доступа работников в помещения СПб ГБУ «ТЦБС Пушкинского района» в соответствии с их полномочиями и функциональными обязанностями;
- предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;
- разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.

6.2.2 Определяется перечень технических средств, находящихся в специальных контролируемых зонах.

6.2.3 К техническим средствам, которые выделяются в специальные контролируемые зоны необходимо отнести следующие группы ресурсов:

- основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;
- сетевое оборудование и серверы, обеспечивающие работу критических систем;
- файловые серверы, на которых хранятся данные, в том числе резервные;
- критичные для деятельности СПб ГБУ «ТЦБС Пушкинского района» системы и коммуникационное оборудование, обеспечивающее внешние коммуникации СПб ГБУ «ТЦБС Пушкинского района».

6.2.4. Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования СПб ГБУ «ТЦБС Пушкинского района» осуществляется в помещениях, оборудованных замками, средствами сигнализации

6.2.5 Работники СПб ГБУ «ТЦБС Пушкинского района» на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.

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

6.2.7 Помещения СПб ГБУ «ТЦБС Пушкинского района» должны быть оборудованы детекторами огня и дыма, огнетушителями, средствами охранно-пожарной сигнализации.

6.2.8 Основное техническое оборудование СПб ГБУ «ТЦБС Пушкинского района» должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам СПб ГБУ «ТЦБС Пушкинского района» в соответствии с рекомендациями производителя.

6.3 Безопасность при работе с носителями информации

6.3.1 В СПб ГБУ «ТЦБС Пушкинского района» должны соблюдаться меры по безопасной работе с электронными носителями информации с целью контроля их использования, для предотвращения несанкционированного копирования и разглашения защищаемой информации, внесения изменений или уничтожения указанной информации, а также внесения изменений в работу информационных систем.

6.3.2 Работники СПб ГБУ «ТЦБС Пушкинского района» должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в СПб ГБУ «ТЦБС Пушкинского района» в иных целях строго запрещено.

6.3.3 В случае кражи или потери электронных носителей информации, а также иных инцидентов, которые могут привести к разглашению защищаемой информации, должны проводиться мероприятия по расследованию указанных инцидентов.

6.3.4 При снятии электронного носителя информации с эксплуатации, все данные, хранящиеся на нем, должны быть гарантированно стерты.

6.3.5 При утилизации электронных носителей информации должна быть обеспечена невозможность восстановления записанной на них информации.

6.4 Техническое обслуживание оборудования СПб ГБУ «ТЦБС Пушкинского района» должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

6.5 Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности СПб ГБУ «ТЦБС Пушкинского района» при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

- заключение соглашения о неразглашении конфиденциальной информации;
- контроль за действиями третьих лиц;
- в договорах с третьими лицами предусматривать право СПб ГБУ «ТЦБС Пушкинского района» на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.

6.6 Управление жизненным циклом информационных систем

6.6.1 Мероприятия по управлению жизненным циклом автоматизированных информационных систем должны быть направлены на обеспечение информационной безопасности при вводе в действие, эксплуатации, сопровождении и модернизации, вывода из эксплуатации информационных систем, автоматизирующих деятельность.

6.6.2 Основой при выборе или разработке информационных систем должны являться технические задания, содержащие требования информационной безопасности для информационных систем.

6.6.3 Любое планируемое к внедрению изменение информационной системы предварительно должно быть протестировано на совместимость и отсутствие нарушений работоспособности системных компонентов.

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

6.6.5 Все процедуры обеспечения информационной безопасности, установленные в СПб ГБУ «ТЦБС Пушкинского района» в отношении информационных систем, должны выполняться и контролироваться ответственными за информационную безопасность лицами.

6.7 Антивирусная защита

6.7.1 В целях предупреждения, обнаружения и устранения вредоносных программ в СПб ГБУ «ТЦБС Пушкинского района» на постоянной основе должны использоваться средства антивирусной защиты.

6.7.2 Обязательному антивирусному контролю должна подлежать любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация, хранимая на подключаемых съемных носителях, при непосредственном обращении к ней.

6.7.3 При установке программного обеспечения на серверы информационных систем СПб ГБУ «ТЦБС Пушкинского района» или их обновлении должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

6.7.4 Сигнатурные базы вредоносного программного обеспечения и антивирусные средства защиты должны регулярно обновляться.

6.7.5 Пользователи информационных систем СПб ГБУ «ТЦБС Пушкинского района» не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

6.7.6 В СПб ГБУ «ТЦБС Пушкинского района» необходимо определить процедуру для обработки и восстановления инфицированных данных и отслеживание источника заражения.

6.8 Контроль доступа к информационным системам

6.8.1 Все работники СПб ГБУ «ТЦБС Пушкинского района», допущенные к работе с информационными системами несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

6.8.2 Уровень полномочий пользователя в информационной системе СПб ГБУ «ТЦБС Пушкинского района» должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.

6.9 Идентификация и аутентификация

6.9.1 Доступ пользователей к информационным системам должен предоставляться только после успешного завершения процедур идентификации, аутентификации и авторизации.

6.10 Безопасность пароля

6.10.1 С целью обеспечения защиты от несанкционированного доступа к информационным системам устанавливаются требования к выбору парольной информации, обеспечивающие достаточную степень стойкости паролей.

6.10.2 Для обеспечения конфиденциальности парольной информации пользователю запрещается хранить значения своих паролей на бумажном носителе в открытом виде и в свободном доступе.

6.10.3 Для обеспечения конфиденциальности парольной информации пользователям запрещается передавать значения своих паролей третьим лицам.

6.10.4 При вводе пароля пользователем для доступа к информационной системе СПб ГБУ «ТЦБС Пушкинского района» должно исключаться отображение парольной информации на экране монитора в открытом виде.

6.10.5 Процедура смены парольной информации в информационных системах СПб ГБУ «ТЦБС Пушкинского района» должна проводиться на регулярной основе.

6.11 Регистрация событий

Осуществление регистрации событий безопасности на всех компонентах информационных систем СПб ГБУ «ТЦБС Пушкинского района» Р, в которых обрабатывается, хранится или по средствам которых передается защищаемая информация.

6.12 Использование СКЗИ

6.12.1 Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством СПб ГБУ «ТЦБС Пушкинского района» в соответствии с законодательством Российской Федерации.

6.12.2 При эксплуатации СКЗИ и ключевой информации ответственные сотрудники СПб ГБУ «ТЦБС Пушкинского района» должны выполнять требования нормативных

правовых актов, издаваемых федеральным органом исполнительной власти в области обеспечения безопасности, документов СПб ГБУ «ТЦБС Пушкинского района» по обеспечению безопасности использования СКЗИ, а также эксплуатационной документации производителя СКЗИ.

6.13 Безопасность информационной сети

6.13.1 Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций СПб ГБУ «ТЦБС Пушкинского района» для обеспечения защиты данных и защиты информационных систем СПб ГБУ «ТЦБС Пушкинского района» от НСД.

6.13.2 Доступ к информационным сервисам сети Интернет предоставляется работникам СПб ГБУ «ТЦБС Пушкинского района» в случае производственной необходимости.

6.13.3 Подключение к сети Интернет должно осуществляться только при организации защиты соединения путем установки МЭ и специальных программных средств защиты.

6.13.4 Разрешительные политики доступа в Интернет должны технически реализовываться специализированным программным обеспечением.

6.14 Резервное копирование и восстановление данных

6.14.1 Осуществление резервного копирования для:

- файловых серверов и серверов приложений, критичных для деятельности СПб ГБУ «ТЦБС Пушкинского района»;
- операционных систем файловых серверов и прикладных программ;
- приложений, критичных для деятельности СПб ГБУ «ТЦБС Пушкинского района»;
- рабочих данных.

6.14.2 Частота и режим резервного копирования устанавливаются таким образом, чтобы обеспечить минимальную потерю данных и допустимое время восстановления.

6.14.3 Резервное копирование и восстановление ресурсов информационных систем АПР должны проводить уполномоченные работники АПР.

6.14.4 Резервное копирование должно осуществляться в автоматическом режиме с применением специализированного программно-аппаратного комплекса.

7 Основные требования к процессам управления информационной безопасностью

7.1 Управление рисками

7.1.1 Выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов СПб ГБУ «ТЦБС Пушкинского района».

7.1.2 Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности и доступности для ресурсов информационной системы СПб ГБУ «ТЦБС Пушкинского района».

7.1.3 Результатом проведения анализа рисков должен быть комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность СПб ГБУ «ТЦБС Пушкинского района» при реализации той или иной угрозы и обеспечивающих достаточный уровень защищенности информационных систем СПб ГБУ «ТЦБС Пушкинского района».

7.2 Управление инцидентами информационной безопасности

7.2.1 Для обеспечения эффективного разрешения инцидентов информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района», минимизации потерь и

уменьшения риска возникновения повторных инцидентов должно осуществляться эффективное управление инцидентами информационной безопасности.

7.3 Мониторинг текущего уровня информационной безопасности

7.3.1 Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в СПб ГБУ «ТЦБС Пушкинского района» на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.

7.3.2 Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов.

7.3.3 При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в СПб ГБУ «ТЦБС Пушкинского района», уполномоченные работники должны придерживаться следующих принципов:

- не нарушать функционирование текущей деятельности СПб ГБУ «ТЦБС Пушкинского района»;
- действовать в соответствии с внутренними документами СПб ГБУ «ТЦБС Пушкинского района» по информационной безопасности;
- не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;
- оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

7.3.4 Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа.

7.3.5 Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться, по возможности, с использованием встроенных механизмов настройки и аудита событий в программных и программно-технических средствах, используемых в информационных системах СПб ГБУ «ТЦБС Пушкинского района».

7.4 Аудит системы обеспечения информационной безопасности

7.4.1 В целях оценки текущего уровня информационной безопасности уполномоченные работники СПб ГБУ «ТЦБС Пушкинского района» на регулярной основе должны проводить аудит информационной безопасности.

7.4.2 Внутренние аудиты или самооценки должны выполняться, по возможности, работниками СПб ГБУ «ТЦБС Пушкинского района»

7.4.3 Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности, которые разрабатываются специалистами СПб ГБУ «ТЦБС Пушкинского района».

7.4.4 По результатам аудита уполномоченные работники и ответственные подразделения СПб ГБУ «ТЦБС Пушкинского района» должны определить действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

7.5 Управление персоналом

7.5.1 Организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала СПб ГБУ «ТЦБС Пушкинского района».

7.5.2 Выполнение обязательных проверок при приеме новых работников на работу с точки зрения достоверности сообщаемых ими данных и с позиции оценки их профессиональных навыков.

7.5.3 Организация работы в направлении повышения осведомленности и обучения в области информационной безопасности.

7.5.4 Повышение осведомленности работников СПб ГБУ «ТЦБС Пушкинского района»:

- по существующим в СПб ГБУ «ТЦБС Пушкинского района» политикам информационной безопасности;
- по применяемым в СПб ГБУ «ТЦБС Пушкинского района» защитным мерам;
- по правильному использованию защитных мер в соответствии с внутренними документами СПб ГБУ «ТЦБС Пушкинского района».

8 Заключение

8.1 Настоящая Политика является внутренним документом СПб ГБУ «ТЦБС Пушкинского района», общедоступной и подлежит размещению на официальном сайте СПб ГБУ «ТЦБС Пушкинского района».

8.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года. При внесении изменений в актуальной редакции указывается дата последнего обновления. Новая редакция Политики вступает в силу с момента ее размещения, если иное не предусмотрено новой редакцией Политики. Действующая редакция всегда находится на сайте СПб ГБУ «ТЦБС Пушкинского района»

8.3. Контроль исполнения требований настоящей Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных СПб ГБУ «ТЦБС Пушкинского района».

8.4. Ответственность должностных лиц СПб ГБУ «ТЦБС Пушкинского района», имеющих доступ к конфиденциальной информации, за невыполнение требований норм, регулирующих обработку и защиту информации, определяется в соответствии с законодательством Российской Федерации и внутренними документами СПб ГБУ «ТЦБС Пушкинского района».