Приложение № 1 к приказу
от 04.07.2023 № 04-01/208-П

Санкт-Петербургское государственное унитарное предприятие
«Санкт-Петербургский информационно-аналитический центр»
(СПб ГУП «СПб ИАЦ»)

УТВЕРЖДАЮ
Директор
СПб ГУП «СПб ИАЦ»
_____А.В.Максименко
«04» 07 2023 г.

Политика
информационной безопасности
Санкт-Петербургского государственного унитарного предприятия
«Санкт-Петербургский информационно-аналитический центр»

На 24 листах

Санкт-Петербург
2023

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Аутентификация	–	Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации
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 информации	–	Состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно
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	–	Действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению 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	–	Информация, данные, представленные в форме, предназначенной для хранения и обработки в системах и сетях
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, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или 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	–	Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, 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 нарушения безопасности информации
Уязвимость	–	Недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации
Целостность	–	Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ГОСТ РФ	– Государственный стандарт Российской Федерации
Политика	– Политика информационной безопасности Санкт-Петербургского государственного унитарного предприятия «Санкт-Петербургский информационно-аналитический центр»
СПб ГУП «СПб ИАЦ»	– Санкт-Петербургское государственное унитарное предприятие «Санкт-Петербургский информационно-аналитический центр»
ФСБ России	– Федеральная служба безопасности Российской Федерации
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика является документом, определяющим основные принципы обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач информационной безопасности, как одно или несколько правил, процедур, практических приемов, которыми руководствуется СПб ГУП «СПб ИАЦ», 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 СПб ГУП «СПб ИАЦ» признает совершенствование мер и средств обеспечения защиты информации, информационных ресурсов СПб ГУП «СПб ИАЦ» в контексте развития законодательства Российской Федерации и норм регулирования в сфере информационных технологий 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 СПб ГУП «СПб ИАЦ» обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

Требования информационной безопасности соответствуют целям деятельности СПб ГУП «СПб ИАЦ» и предназначены для снижения возможности реализации угроз безопасности информации.

Политика доступна всем работникам СПб ГУП «СПб ИАЦ» и всем пользователям его ресурсов.

2 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Субъекты информационных отношений

Субъектами при обеспечении информационной безопасности в СПб ГУП «СПб ИАЦ» являются:

работники структурных подразделений (в том числе уволенные);

граждане, работающие по договорам гражданско-правового характера;

физические лица, представители контрагентов в рамках исполнения договорных обязательств;

физические лица, направившие обращение в адрес СПб ГУП «СПб ИАЦ»;

юридические лица, в рамках исполнения договорных обязательств или во исполнение требований законодательства Российской Федерации;

органы государственной власти.

Объекты информационных отношений

Объектами информационных отношений являются:

информационные ресурсы СПб ГУП «СПб ИАЦ»;

государственные информационные системы, оператором которых является СПб ГУП «СПб ИАЦ»;

информационная инфраструктура, включающая системы обработки и анализа информации, программные и программно-аппаратные средства, в том числе каналы связи и телекоммуникации;

объекты и помещения, в которых размещены средства обработки информации.

Цели обеспечения информационной безопасности

Основной целью обеспечения информационной безопасности СПб ГУП «СПб ИАЦ» являются действия, направленные 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:

обеспечение отказоустойчивого функционирования программных и аппаратно-программных средств СПб ГУП «СПб ИАЦ» и предоставляемых сервисов;

соблюдение правового режима использования массивов и средств обработки информации;

снижение возможности реализации угроз безопасности информации.

Задачи обеспечения информационной безопасности

Достижение целей обеспечения информационной безопасности и свойств информации в СПб ГУП «СПб ИАЦ» решается следующими задачами:

защита от несанкционированного доступа к информационным ресурсам;

управление доступом субъектов доступа к объектам доступа;

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

контроль целостности среды исполнения программ и ее восстановление в случае нарушения;

обеспечение аутентификации и идентификации пользователей при эксплуатации информационных систем;

обеспечение работоспособности применяемых в информационных системах СПб ГУП «СПб ИАЦ» средств защиты информации;

своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

функционирование службы мониторинга и реагирования на угрозы безопасности информации и негативные последствия;

создание условий для минимизации наносимого ущерба неправомерными действиями, и устранение последствий нарушения информационной безопасности

в СПб ГУП «СПб ИАЦ».

Решение вышеперечисленных задач в СПб ГУП «СПб ИАЦ» осуществляется посредством:

учета всех подлежащих защите информационных ресурсов;

журналирования действий персонала, осуществляющего обслуживание и модификацию программных и программно-аппаратных средств информационных систем;

регламентации процессов обработки информации, действий работников, осуществляющих эксплуатацию программных и программно-аппаратных средств, на основе утвержденных организационно-распорядительных документов по защите информации;

назначения и подготовки работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности;

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 защите информации, в том числе персональных данных;

персональной ответственности каждого работника за свои действия, участвующего в рамках своих должностных обязанностей в процессах обработки информации и имеющего доступ к информационным ресурсам СПб ГУП «СПб ИАЦ»;

реализации технологических процессов при обработке информации с использованием программных и программно-аппаратных средств защиты информации;

принятия мер по обеспечению физической целостности программно-аппаратных средств информационных систем и поддержанием необходимого уровня защищенности;

контроля соблюдения пользователями организационно-распорядительных документов по защите информации, в том числе персональных данных;

проведения оценки эффективности принятых мер защиты информации и применяемых средств защиты информации в СПб ГУП «СПб ИАЦ»;

разработки и реализации предложений по совершенствованию систем защиты информации в СПб ГУП «СПб ИАЦ».

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. Программные и программно-аппаратные средства, применяемые в СПб ГУП «СПб ИАЦ», должны иметь соответствующие лицензии, официально приобретаться у представителей разработчиков этих средств или являться интеллектуальной собственностью СПб ГУП «СПб ИАЦ».

Принцип системности

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

Принцип комплексности

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

При построении, внедрении и эксплуатации системы защиты информации руководство СПб ГУП «СПб ИАЦ» обеспечивает условия для эффективной координации действий всех лиц, обеспечивающих информационную безопасность.

Принцип своевременности

Разработка системы защиты информации должна вестись параллельно с разработкой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные информационные системы, обладающие достаточным уровнем защищенности.

Принцип преемственности

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

Принцип достаточности

Соответствие уровня затрат на обеспечение информационной безопасности и ценности информационных ресурсов на величину возможного ущерба от нарушения конфиденциальности, целостности и доступности. Используемые меры и средства защиты информации не должны ухудшать эргономические показатели компонентов информационных систем.

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 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 квалифицированными специалистами.

Привлечение специализированных организаций к разработке средств и реализации мер защиты информации, имеющих лицензию на деятельность по технической защите конфиденциальной информации.

Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями, минимально достаточными для выполнения своих должностных обязанностей в СПб ГУП «СПб ИАЦ».

4 ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Система защиты информации должна предусматривать комплекс организационных и технических мер по защите информации в процессе ее обработки.

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

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей персональных данных;

регистрация событий безопасности;

антивирусная защита;

обнаружение вторжений;

контроль (анализ) защищенности персональных данных;

обеспечение целостности информационной системы и персональных данных;

обеспечение доступности персональных данных;

защита среды виртуализации;

защита технических средств;

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

выявление инцидентов и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

СПб ГУП «СПб ИАЦ», 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.

СПб ГУП «СПб ИАЦ» вправе, в том числе, 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.

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);

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

Организация защиты информации

При организации защиты информации в СПб ГУП «СПб ИАЦ» 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, обязательному исполнению подлежат требования к составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные 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» и 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, в отношении которых СПб ГУП «СПб ИАЦ» является Оператором.

В СПб ГУП «СПб ИАЦ» помимо реализации основных мер защиты информации осуществляется:

регулярная оценка актуальных угроз безопасности информации;

информирование, обучение и повышение квалификации работников СПб ГУП «СПб ИАЦ» в сфере информационной безопасности;

методическая помощь работникам в вопросах обеспечения информационной безопасности;

анализ и поиск возможностей по повышению уровня защищенности информации.

Для организации защиты информации СПб ГУП «СПб ИАЦ» вправе применять средства и методы технической защиты, не противоречащие законодательству Российской Федерации.

В рамках трудовых отношений необходимо ознакомить работников, доступ которых к информации ограниченного доступа необходим для выполнения ими своих должностных обязанностей, с перечнем информации ограниченного доступа и принятыми в СПб ГУП «СПб ИАЦ» мерами защиты информации.

Особенности защиты персональных данных

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

Перечень мер, выполнение которых обеспечивает СПб ГУП «СПб ИАЦ» в качестве оператора персональных данных, должен включать:

назначение в СПб ГУП «СПб ИАЦ» ответственного за организацию обработки персональных данных;

разработка документов, определяющих правила в отношении обработки персональных данных в СПб ГУП «СПб ИАЦ», 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»;

оценка вреда, который может быть причинен субъектам персональных данных, в случае нарушения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

ознакомление работников СПб ГУП «СПб ИАЦ», непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими требования СПб ГУП «СПб ИАЦ» в отношении обработки персональных данных и соответствующее обучение, при необходимости, указанных работников.

Обеспечение безопасности персональных данных достигается, в частности:

определением угроз и нарушителей безопасности персональных данных при их обработке в информационных системах персональных данных;

определением уровня защищенности персональных данных в соответствии с требованиями Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

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

оценкой эффективности принимаемых мер по защите персональных данных до ввода в эксплуатацию информационной системы персональных данных;

восстановлением персональных данных вследствие несанкционированного уничтожения;

установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационных системах персональных данных;

контролем за принимаемыми мерами по защите персональных данных и определенного уровня защищенности персональных данных при их обработке в информационных системах персональных данных в процессе их эксплуатации.

5 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методическое руководство, разработку решений по защите информации, согласование выбора средств вычислительной техники, программных и программно-аппаратных средств защиты информации, организацию работ по выявлению возможностей и предупреждению утечки и свойств защищаемой информации, аттестацию объектов информатизации осуществляют компетентные структурные подразделения СПб ГУП «СПб ИАЦ».

Физическая безопасность

Принятые организационные и технические меры по защите помещений СПб ГУП «СПб ИАЦ», серверного и коммутационного оборудования, автоматизированных рабочих мест пользователей информационных систем обеспечивают реализацию следующих мер по:

разграничению доступа работников в помещения СПб ГУП «СПб ИАЦ» 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 помещениях СПб ГУП «СПб ИАЦ», в которых ведется обработка информации ограниченного доступа и размещены аппаратные средства информационной системы;

организации режима контролируемого вноса/выноса средств обработки информации.

Помещения СПб ГУП «СПб ИАЦ» должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации.

Основное серверное и коммутационное и сетевое оборудование СПб ГУП «СПб ИАЦ» должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания и резервного дизель-генератора. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам СПб ГУП «СПб ИАЦ» в соответствии с рекомендациями производителя.

Мобильные технические средства не должны оставаться за пределами контролируемой зоны СПб ГУП «СПб ИАЦ» без контроля со стороны работников СПб ГУП «СПб ИАЦ».

Безопасность на рабочем месте

Запрещается вести запись паролей в открытом виде на материальных носителях, за исключением 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 завершена, рабочий стол заблокирован. Вход пользователя в систему не должен выполняться автоматически.

Документы, содержащие информацию ограниченного доступа, должны сразу изыматься из печатающих устройств. Для утилизации конфиденциальных документов должны использоваться уничтожители документов не ниже 4 уровня по стандарту безопасности, применяемому к уничтожителям документов.

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

Нахождение представителей юридических лиц в рамках исполнения договорных обязательств в помещениях, в которых ведется обработка информации ограниченного доступа, возможно только в сопровождении работника СПб ГУП «СПб ИАЦ», допущенного до обработки такой информации.

Размещение технических средств вывода информации в помещениях СПб ГУП «СПб ИАЦ» производится с учетом исключения возможности визуального

просмотра информации посторонними лицами и работниками, не допущенными 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

Технические средства СПб ГУП «СПб ИАЦ» должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированными специалистами.

При техническом обслуживании оборудования сторонними организациями должна быть исключена вероятность нарушения конфиденциальности защищаемой информации.

Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности СПб ГУП «СПб ИАЦ» при взаимодействии с третьими лицами должно выполнять следующие мероприятия по:

заключению соглашения о неразглашении информации ограниченного доступа, полученной в ходе исполнения договорных обязательств;

осуществлению контроля за действиями представителей контрагентов в пределах контролируемой зоны СПб ГУП «СПб ИАЦ».

Управление жизненным циклом информационных систем

Мероприятия в процессе жизненного цикла информационных систем СПб ГУП «СПб ИАЦ» должны быть направлены на обеспечение защиты информации при вводе в действие, эксплуатации, сопровождении и модернизации или выводе из эксплуатации.

Основанием при разработке информационных систем должны являться решения, принятые на стадии формирования требований, содержащие требования в том числе по системе защиты информации.

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

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

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

Все процедуры обеспечения защиты информации, установленные в СПб ГУП «СПб ИАЦ» в отношении информационных систем, должны выполняться и контролироваться ответственными лицами за организацию работ по защите информации.

Контроль доступа к информационным системам

Уровень полномочий пользователя в информационной системе СПб ГУП «СПб ИАЦ» должен определяться в соответствии с его должностными обязанностями.

Доступ пользователей к информационным системам СПб ГУП «СПб ИАЦ» должен контролироваться администратором информационной системы.

Должен осуществляться регулярный контроль выполнения организационно-распорядительных документов, касающихся регламентации допуска работников СПб ГУП «СПб ИАЦ» к информации, обрабатываемой в информационной системе.

Идентификация и аутентификация

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

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

Управление доступом

В СПб ГУП «СПб ИАЦ» должно осуществляться управление доступом к информационной системе посредством реализации необходимых методов, типов и правил разграничения доступа пользователям информационной системы. В том числе должен быть обеспечен защищенный удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

Безопасность при работе с носителями информации

Работники СПб ГУП «СПб ИАЦ» должны использовать только учтенные съемные машинные носители информации для выполнения своих должностных обязанностей. Использование съемных машинных носителей информации в СПб ГУП «СПб ИАЦ» в иных целях строго запрещено.

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

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

При выводе из эксплуатации съемного машинного носителя информации, все данные, хранящиеся на нем, должны быть удалены определенной комиссией из числа работников СПб ГУП «СПб ИАЦ». Факт уничтожения информации на съемном машинном носителе информации фиксируется в акте об уничтожении информации.

Регистрация событий

В СПб ГУП «СПб ИАЦ» должна осуществляться регистрации событий безопасности на всех компонентах информационных систем СПб ГУП «СПб ИАЦ», в которых обрабатывается защищаемая информация.

Антивирусная защита

В целях обнаружения и устранения вредоносных программ в СПб ГУП «СПб ИАЦ» 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 обновлении на северном оборудовании должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

Обновление баз сигнатур для средства антивирусной защиты информации должно осуществляться ежедневно.

Пользователи без прав администратора информационной системы СПб ГУП «СПб ИАЦ» не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

Контроль защищенности информации

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

Использование программного обеспечения

Выбор программного обеспечения для производственных нужд СПб ГУП «СПб ИАЦ» должен производиться в приоритете к отечественному, внесенному в единый реестр

российских программ для электронных вычислительных машин и баз данных или единый реестр программ для электронных вычислительных машин и баз данных государств – членов Евразийского экономического союза. В случае отсутствия аналога в едином реестре российских программ для электронных вычислительных машин и баз данных, в том числе в едином реестре программ для электронных вычислительных машин и баз данных государств – членов Евразийского экономического союза, допускается использование программного обеспечения импортного производства и пакетов обновления к нему только из доверенного репозитория.

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 СПб ГУП «СПб ИАЦ» 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 СПб ГУП «СПб ИАЦ» должен быть создан орган криптографической защиты.

Портальные решения СПб ГУП «СПб ИАЦ», предназначенные для доступа из сетей общего пользования, должны разрабатываться с использованием защищенного соединения по протоколу TLS с поддержкой отечественных криптографических алгоритмов, а также с использованием сертификатов проверки подлинности сервера, выданных Министерством цифрового развития, связи и массовых коммуникаций

Использование электронной почты

Электронная почта должна использоваться в СПб ГУП «СПб ИАЦ» с целью организации обмена электронными сообщениями между работниками, а также между работниками СПб ГУП «СПб ИАЦ» и внешними абонентами.

При использовании электронной почты запрещается:

обмен информацией ограниченного доступа;

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

публикация своего рабочего 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

СПб ГУП «СПб ИАЦ» 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.

Информация о посещаемых работниками СПб ГУП «СПб ИАЦ» информационных ресурсов протоколируется для последующего анализа и, при необходимости, может быть представлена руководителям структурных подразделений.

При использовании сети Интернет запрещено:

использовать предоставленный СПб ГУП «СПб ИАЦ» 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 СПб ГУП «СПб ИАЦ», а также фальсифицировать свой IP-адрес.

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 их оперативное восстановление.

Настройка резервного копирования и восстановления ресурсов информационных систем СПб ГУП «СПб ИАЦ» должны проводить уполномоченные работники СПб ГУП «СПб ИАЦ».

Резервное копирование должно осуществляться в автоматическом режиме с применением средства резервного копирования не ниже 6 уровня доверия.

6 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Мониторинг информационной безопасности

На постоянной основе должен проводиться комплексный анализ функционирования информационных систем СПб ГУП «СПб ИАЦ» и возникающих событий информационной безопасности.

Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических мер по защите информации, анализ параметров конфигурации и настройки средств защиты информации, контроль использования работниками информационных ресурсов СПб ГУП «СПб ИАЦ», а также технических средств обработки, хранения и передачи информации.

При проведении контрольных мероприятий, связанных с оценкой реализации мер по защите информации в СПб ГУП «СПб ИАЦ», уполномоченные работники должны придерживаться следующих принципов:

не нарушать функционирование деятельности СПб ГУП «СПб ИАЦ»;

действовать в соответствии с утвержденными организационно-распорядительными документами СПб ГУП «СПб ИАЦ» по защите информации;

не скрывать факты выявленных событий информационной безопасности;

оформлять отчеты, подтверждающие выполнение мероприятий по защите информации.

Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к реализации мер по защите информации, должна консолидироваться и храниться в местах, исключающих получение к ней несанкционированного доступа.

Мониторинг данных о зарегистрированных событиях информационной безопасности должен проводиться с использованием системы мониторинга инцидентов информационной безопасности или встроенных механизмов настройки и аудита событий в программных и программно-аппаратных средствах, используемых в информационной инфраструктуре СПб ГУП «СПб ИАЦ».

Управление рисками

Определение внутренних требований по защите информации, должны основываться на результатах проведения анализа рисков нарушения основных свойств безопасности для информационных ресурсов СПб ГУП «СПб ИАЦ».

Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения целостности, конфиденциальности и доступности информации, обрабатываемой в СПб ГУП «СПб ИАЦ».

Результатом проведения анализа рисков должен быть разработанный комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность СПб ГУП «СПб ИАЦ» при реализации той или иной угрозы безопасности информации и обеспечивающих в дальнейшем достаточный уровень защищенности информационных систем СПб ГУП «СПб ИАЦ».

Управление инцидентами информационной безопасности

Для обеспечения эффективного разрешения инцидентов информационной безопасности в СПб ГУП «СПб ИАЦ», минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться управление инцидентами информационной безопасности.

Для управления инцидентами информационной безопасности функционирует служба мониторинга и реагирования на инциденты информационной безопасности, которая посредством комплекса средств и мероприятий для сбора и консолидации информации об инцидентах решает данную задачу. В отношении каждого произошедшего инцидента работниками из службы мониторинга и реагирования на инциденты информационной

безопасности должен выполняться его анализ и разработка эффективных мер реагирования на данный инцидент.

Аудит системы обеспечения информационной безопасности

В целях оценки текущего уровня информационной безопасности СПб ГУП «СПб ИАЦ» на регулярной основе должен проводиться аудит информационной безопасности.

Внутренние аудиты должны выполняться работниками СПб ГУП «СПб ИАЦ». В число задач, решаемых при проведении внутренних аудитов информационной безопасности, входят:

сбор и анализ исходных данных об организационной и функциональной структуре информационных систем, необходимых для оценки состояния системы защиты информации;

анализ утвержденных организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их доработке или разработки новых;

обоснование финансовой эффективности вновь приобретаемых средств защиты информации;

проверка правильности выбора и настройки средств защиты информации, формирование предложений по использованию имеющихся средств защиты информации для повышения уровня отказоустойчивости и безопасности информационных систем СПб ГУП «СПб ИАЦ»;

анализ отчетов по произошедшим инцидентам информационной безопасности и принятым мерам по их разрешению.

Повышение осведомленности работников

В рамках организации комплексного противодействия угрозам безопасности информации, исходящим от работников СПб ГУП «СПб ИАЦ», должна постоянно повышаться их осведомленность в области защиты информации.

Повышение осведомленности работников СПб ГУП «СПб ИАЦ» осуществляется:

по утвержденным в СПб ГУП «СПб ИАЦ» организационно-распорядительным документам;

по применяемым в СПб ГУП «СПб ИАЦ» 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 СПб ГУП «СПб ИАЦ», настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также внутренним документам СПб ГУП «СПб ИАЦ».

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

В СПб ГУП «СПб ИАЦ» в приоритетном направлении должен рассматриваться переход на программное обеспечение отечественного производителя, включенное в единый реестр российских программ для электронных вычислительных машин и баз данных или единый реестр программ для электронных вычислительных машин и баз данных государств – членов евразийского экономического союза, в том числе по части серверного, коммутационного и сетевого оборудования и иных 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 НОРМАТИВНО-ПРАВОВЫХ АКТОВ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ

1 Указ Президента РФ от 16.08.2004 № 1085 (ред. от 22.05.2023) «Вопросы Федеральной службы по техническому и экспортному контролю» (Выписка).

2 Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

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

4 Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5 Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6 Федеральный закон от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации».

7 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)».

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

9 Постановление Правительства РФ от 08.02.2018 N 127 (ред. от 20.12.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» (с изм. и доп., вступ. в силу с 21.03.2023).

10 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».

11 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)».

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

13 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».

14 Приказ ФСТЭК России от 14.05.2020 № 68 «О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю

от 18 февраля 2013 г. N 21»."(Зарегистрировано в Минюсте России 08.07.2020 N 58877).

15 «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка)» (утв. приказом ФСТЭК России от 02.06.2020 № 76).

16 Приказ ФСТЭК России от 25.12.2017 № 239 (ред. от 20.02.2020) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 26.03.2018 N 50524) (с изм. и доп., вступ. в силу с 01.01.2023).

17 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».

18 Приказ Роскомнадзора от 15.12.2022 № 201 «Об обработке персональных данных в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (Зарегистрирован 19.05.2023 № 73374).

19 Приказ Роскомнадзора от 10.01.2023 № 1 «О внесении изменений в форму проверочного листа (списка контрольных вопросов, ответы на которые свидетельствуют о соблюдении или несоблюдении контролируемым лицом обязательных требований), применяемого при осуществлении федерального государственного контроля (надзора) за обработкой персональных данных Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций и ее территориальными органами, утвержденную приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 декабря 2021 г. N 253» (Зарегистрировано в Минюсте России 05.04.2023 N 72886).

20 ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

21 ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».

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

23 ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства безопасности. Системы менеджмента информационной безопасности. Требования».

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

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

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

27 ГОСТ Р ИСО/ТО 13569-2007 «Финансовые услуги. Рекомендации по информационной безопасности».

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

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

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

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

32 Концепция информационной безопасности исполнительных органов

государственной власти Санкт-Петербурга от 20.02.2023.

33 Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014).