УТВЕРЖДАЮ
Директор ГБОУ школы № 6
_____ Путилова В.А.
«___» _____ 2023г.

Политика
информационной безопасности ГБОУ школы № 6

На 21 листе

Санкт-Петербург
2023

СОДЕРЖАНИЕ

Термины и определения 3
Обозначения и сокращения 5
1 Общие положения 6
2 Цели и задачи обеспечения информационной безопасности 7
3 Принципы обеспечения информационной безопасности 8
4 Основные требования по защите информации ограниченного доступа 10
5 Основные требования к процессам обеспечения информационной безопасности 12
6 Основные требования к процессам управления информационной безопасностью 17
7 Заключение 19
8 Список использованных источников 20

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ГОСТ Р	− Государственный стандарт Российской Федерации
Политика	− Политика информационной безопасности Санкт-Петербургского государственного унитарного предприятия «Санкт Петербургский информационно аналитический центр»
Комитет	− Комитет_____
ФСБ России	− Федеральная служба безопасности Российской Федерации
ФСТЭК России	− Федеральная служба по техническому и экспортному контролю

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Политика является документом, определяющим направления деятельности в области обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач информационной безопасности, как одно или несколько правил, процедур, практических приемов и руководящих принципов, которыми руководствуется Комитет, 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 Комитет признает совершенствование мер и средств обеспечения защиты информации информационных ресурсов Комитет в контексте развития законодательства Российской Федерации и норм регулирования информационной деятельности в текущих условиях функционирования информационного поля.

При разработке Политики учитывались основные принципы создания систем защиты информации, характеристики и возможности организационно-технических мер и современных программных и аппаратно-программных средств защиты информации.

В рамках своей деятельности Комитет обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

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

Политика доступна всем работникам Комитет и всем пользователям его ресурсов.

2 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Субъекты информационный отношений

Субъектами при обеспечении информационной безопасности в Комитет 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, подавшие обращение в адрес Комитет;

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

органы государственной власти.

Объекты информационных отношений

Объектами информационных отношений являются:

информационные ресурсы Комитет;

государственные информационные системы Оператором которых является Комитет;

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

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

системы и средства защиты информации, объекты и помещения, в которых размещены средства обработки информации.

Цели обеспечения информационной безопасности

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

обеспечения отказоустойчивого функционирования программных и аппаратно-программных средств Комитет и предоставляемых сервисов;

соблюдения правового режима использования массивов и средств обработки информации;

предотвращения реализации угроз безопасности информации при осуществлении деятельности Комитет.

Задачи обеспечения информационной безопасности

Достижение целей обеспечения информационной безопасности и свойств информации, Комитет решается следующими задачами:

защиты от несанкционированного доступа к информационным ресурсам;

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

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

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

обеспечения аутентификации и идентификации пользователей, участвующих в информационном обмене;

обеспечения исправности применяемых в информационных системах Комитет средств защиты информации;

своевременного выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам

информационных отношений;

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

созданием условий для минимизации наносимого ущерба неправомерными действиями, и устранение последствий нарушения информационной безопасности в Комитет.

Решение вышеперечисленных задач в Комитет 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 Комитет, осуществляющих эксплуатацию программных и программно-аппаратных средств, на основе утвержденных организационно-распорядительных документов по защите информации;

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

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

соблюдения всеми работниками, эксплуатирующими и обслуживающими программные и программно-аппаратные средства, требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

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

реализацией технологических процессов обработки информации с использованием комплексов организационно-технических мер защиты программного обеспечения, программно-аппаратных средств;

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

использования программных и программно-аппаратных средств защиты информации обрабатываемом в Комитет и административной поддержкой их использования;

контроля соблюдения пользователями информационных систем требований по обеспечению информационной безопасности;

проведения анализа эффективности принятых мер защиты информации и применяемых средств защиты информации в Комитет;

разработки и реализации предложений по совершенствованию систем защиты информации в Комитет.

3 ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

Принцип законности

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

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

Принцип системности

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

информации, но и с учетом возможности появления новых уязвимостей в программном обеспечении.

Принцип комплексности

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

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

Принцип своевременности

Разработка системы защиты информации должна вестись параллельно с разработкой и 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 перехвата информации, нормативных требований по защите информации.

Принцип достаточности

Соответствие уровня затрат на обеспечение информационной безопасности и ценности информационных ресурсов на величину возможного ущерба от их разглашения, уничтожения и искажения. 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 реализованы по современным решениям, обоснованы с точки зрения достижения заданного уровня защищенности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по безопасности информации.

Принцип профессионализма

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

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

Принцип минимизации привилегий пользователей

Обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих должностных обязанностей в Комитет.

4 ОСНОВНЫЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

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

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

идентификации и аутентификации субъектов доступа и объектов доступа;

управлению доступом субъектов доступа к объектам доступа;

ограничению программной среды;

защите машинных носителей персональных данных;

регистрации событий безопасности;

антивирусной защите;

обнаружению вторжений;

контролю (анализу) защищенности персональных данных;

обеспечению целостности информационной системы и персональных данных;

обеспечению доступности персональных данных;

защиты среды виртуализации;

защиты технических средств;

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

выявлению инцидентов и реагирование на них;

управлению конфигурацией информационной системы и системы защиты персональных данных.

Комитет, как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

соблюдать права и законные интересы иных лиц;

принимать необходимые меры по защите информации;

ограничивать доступ к информации, если такая обязанность установлена законодательством Российской Федерации.

В том числе Комитет, вправе если иное не предусмотрено законодательством Российской Федерации:

разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

использовать информацию, в том числе распространять ее, по своему усмотрению;

передавать информацию другим лицам на установленном законодательством Российской Федерации основании;

защищать установленными законодательством Российской Федерации способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

осуществлять иные действия с информацией или разрешать осуществление таких действий, если эти действия не противоречат федеральным законам и другим нормативно-правовым актам Российской Федерации.

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

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

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

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

Средства защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

Организация защиты информации

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

В Комитете помимо реализации основных мер защиты информации осуществляется:

регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;

информирование, обучение и повышение квалификации работников Комитет 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, Комитет вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие законодательству Российской Федерации, меры.

В рамках обеспечения защиты информации, в рамках трудовых отношений необходимо ознакомить под роспись работников, доступ которых к информации ограниченного доступа, необходим для выполнения ими своих должностных обязанностей, с перечнем информации ограниченного доступа, и принятыми в Комитет мерами защиты информации.

Особенности защиты персональных данных

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

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

назначение в Комитет ответственного за организацию обработки персональных данных;

разработку документов, определяющих правила в отношении обработки персональных данных в Комитет, локальных актов по вопросам обработки персональных данных;

применение организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

выполнение требований по составу и содержанию организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных утверждённых Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

оценку вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

ознакомление работников Комитет, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных,

документами, определяющими требования Комитет в отношении обработки персональных данных и 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 получения несанкционированного доступа к ним;

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 информационных системах персональных данных в процессе ее 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 Комитет.

Физическая безопасность

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

разграничению доступа работников в помещения Комитет 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 Комитет в помещения, в которых ведется обработка информации ограниченного доступа и размещены аппаратные средства информационной системы;

организации режима контролируемого вноса/выноса средств обработки информации.

Помещения Комитет должны быть оборудованы детекторами огня и дыма, огнетушителями, системами кондиционирования воздуха, средствами охранно-пожарной сигнализации.

Основное серверное и коммутационное оборудование Комитет 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 Комитет в соответствии с рекомендациями производителя.

Портативные технические средства не должны оставаться за пределами контролируемой зоны Комитет без контроля со стороны работников Комитет.

Безопасность на рабочем месте

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

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

Документы, содержащие информацию ограниченного доступа, должны сразу изыматься из печатающих устройств. 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 информационной системы, возможно только в сопровождении работника Комитет допущенного до обработки такой информации.

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

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

Техническое обслуживание оборудования

Технические средства Комитет должны проходить на регулярной основе сервисное обслуживание в соответствии с рекомендациями производителей оборудования.

Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированными специалистами.

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

Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности Комитет 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 Комитет.

Управление жизненным циклом информационных систем

Мероприятия в процессе жизненного цикла информационных систем Комитет должны быть направлены на обеспечение защиты информации при вводе в действие, эксплуатации, сопровождении и модернизации, вывода 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 Комитет в отношении информационных систем, должны выполняться и контролироваться ответственными лицами за организацию работ по защите информации.

Контроль доступа к информационным системам

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

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

Доступ пользователей к информационным системам Комитет должен контролироваться администратором информационной системы.

Осуществление регулярного контроля выполнения организационно-распорядительных документов, касающихся регламентации допуска работников Комитет к информационным системам.

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

Безопасность при работе с носителями информации

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

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

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

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

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

Регистрация событий

В Комитет должна осуществляться регистрации событий безопасности на всех компонентах информационных систем Комитет, в которых обрабатывается защищаемая информация.

Антивирусная защита

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

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

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

Обновление баз сигнатур для средства антивирусной защиты информации должны обновляться ежедневно.

Пользователи без прав администратора информационной системы Комитет не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

Контроль защищенности персональных данных

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

Использование программного обеспечения

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

Использование средств криптографической защиты информации

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

Приобретение средств криптографической защиты информации Комитет 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 Комитет должен быть создан орган криптографической защиты.

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

Использование электронной почты

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

При использовании электронной почты запрещается:

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

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

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

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

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

Работа в сетях общего пользования

Комитет 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 Комитет информационных ресурсов протоколируется для последующего анализа и, при необходимости, может быть представлена руководителям структурных подразделений, а также руководителю Комитет для контроля.

При использовании сети Интернет запрещено:

использовать предоставленный Комитет доступ в сеть Интернет в личных целях;

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

публиковать, загружать и распространять материалы содержащие недостоверную информацию о Комитет, 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 оперативное восстановление.

Настройка резервного копирования и восстановления ресурсов информационных систем Комитет должны проводить уполномоченные работники Комитет.

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

6 ОСНОВНЫЕ ТРЕБОВАНИЯ К ПРОЦЕССАМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Мониторинг информационной безопасности

На постоянной основе должен проводиться комплексный анализ функционирования информационной системы Комитет 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.

При проведении контрольных мероприятий, связанных с оценкой реализации мер по защите информации в Комитет, уполномоченные работники должны придерживаться следующих принципов:

не нарушать функционирование деятельности Комитет;

действовать в соответствии с утвержденными организационно-распорядительными документами Комитет 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, по возможности, с использованием системы мониторинга инцидентов информационной безопасности или встроенных механизмов настройки и аудита событий в программных и программно-аппаратных средствах, используемых в информационной инфраструктуре Комитет.

Управление рисками

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

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

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

Управление инцидентами информационной безопасности

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

Для управления инцидентами информационной безопасности должна быть создана 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 Комитет на регулярной основе должен проводиться аудит информационной безопасности.

Внутренние аудиты должны выполняться работниками Комитет. 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 надёжности и безопасности информационных систем Комитет;

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 Комитет должна постоянно повышаться их осведомленность в области защиты информации.

Повышение осведомленности работников Комитет осуществляется:

по существующим в Комитет организационно-распорядительным документам;

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

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

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

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

8 СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

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

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

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

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

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

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

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

8 Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

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

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

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

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

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

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

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

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

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

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

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

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

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

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