Политика информационной безопасности
Санкт-Петербургского государственного казенного учреждения
«Санкт-Петербургский информационно-аналитический центр»

1. Общие положения

1.1. Настоящая Политика информационной безопасности Санкт-Петербургского государственного казенного учреждения «Санкт-Петербургский информационно-аналитический центр» (далее – Политика и СПб ГКУ «СПб ИАЦ» или Учреждение, соответственно) является локальным нормативным актом Учреждения, 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 Учреждение в своей деятельности, а также организационных, технологических и процедурных аспектов обеспечения информационной безопасности.

1.2. Положения настоящей Политики не распространяются на обеспечение информационной безопасности сведений, составляющих государственную тайну.

1.3. Основной задачей в области информационной безопасности Учреждение признает совершенствование мер и средств обеспечения защиты информации объектов информатизации Учреждения, а также объектов информатизации исполнительных органов государственной власти Санкт-Петербурга в рамках реализации Учреждением полномочий Комитета по информатизации и связи, возложенных постановлением Правительства Санкт-Петербурга от 19.09.2024 № 816 «О внесении изменений в постановление Правительства Санкт-Петербурга от 30.12.2013 № 1095 и реорганизации Санкт-Петербургского государственного унитарного предприятия «Санкт-Петербургский информационно-аналитический центр», в контексте развития законодательства Российской Федерации и норм регулирования в сфере информационных технологий в текущих условиях функционирования информационного поля.

1.4. 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.

1.5. В рамках своей деятельности СПб ГКУ «СПб ИАЦ» обязуется предпринимать все возможные меры для защиты информации от угроз безопасности информации.

1.6. Требования информационной безопасности соответствуют целям деятельности СПб ГКУ «СПб ИАЦ» и предназначены для снижения вероятности реализации угроз безопасности информации.

1.7. Политика подлежит опубликованию на сайте Учреждения.

2. Цели и задачи обеспечения информационной безопасности

2.1. Субъектами информационных отношений являются:

работники структурных подразделений (в том числе уволенные);

физические лица, представители контрагентов в рамках исполнения договорных обязательств;

граждане, работающие по договорам гражданско-правового характера;

физические лица, направившие обращение в адрес Учреждения;

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

исполнительные органы государственной власти Санкт-Петербурга (далее – ИОГВ).

2.2. Объектами информационных отношений являются:

государственные информационные системы Санкт-Петербурга, оператором которых является Учреждение;

государственные информационные системы Санкт-Петербурга, создание и развитие которых осуществляется Учреждением;

государственные информационные системы Санкт-Петербурга, эксплуатация которых

осуществляется Учреждением;

информационно-телекоммуникационная инфраструктура центра обработки данных, на базе которой функционируют объекты информатизации ИОГВ, включая каналы связи и телекоммуникации;

объекты информатизации Учреждения.

2.3. Основной целью обеспечения информационной безопасности Учреждения 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 Учреждения и предоставляемых сервисов;

соблюдение правового режима использования массивов и средств обработки информации;

снижение вероятности реализации угроз безопасности информации.

2.4. Достижение целей обеспечения информационной безопасности и свойств информации в Учреждении решается следующими задачами:

защита от несанкционированного доступа к информации объектов информационных отношений;

управление доступом субъектов доступа к объектам доступа;

регистрация и контроль действий пользователей при работе с основными техническими средствами и системами объектов информатизации Учреждения;

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 средств защиты информации;

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

функционирование Ведомственного центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

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

3. Принципы обеспечения информационной безопасности

3.1. Принцип законности

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

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

3.1.3. Программные и программно-аппаратные средства, включая средства защиты информации, применяемые в Учреждении, должны иметь соответствующие лицензии и сертификаты соответствия (для средств защиты информации), официально приобретаться у представителей разработчиков таких средств.

3.2. Принцип системности

3.2.1. При создании системы защиты информации 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.

3.3. Принцип комплексности

3.3.1. Комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты информации, перекрывающей все актуальные угрозы безопасности информации.

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

3.4. Принцип своевременности

3.4.1. 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.

3.5. Принцип преемственности

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

3.6. Принцип достаточности

3.6.1. 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.

3.7. Принцип ответственности

3.7.1. Возложение персональной 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.

3.8. Принцип обоснованности и технической реализуемости

3.8.1. 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.

3.9. Принцип профессионализма

3.9.1. Реализация мер защиты информации и эксплуатация средств защиты информации должна осуществляться квалифицированными специалистами.

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

3.10. Принцип минимизации привилегий пользователей

3.10.1. Обеспечение пользователей привилегиями, минимально достаточными для выполнения своих должностных обязанностей в Учреждении.

4. Основные требования по защите информации ограниченного доступа

4.1. Организация защиты информации

4.1.1. Учреждение при осуществлении своей деятельности обязано:

соблюдать права и законные интересы субъектов персональных данных;

принимать необходимые меры по защите информации;

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

4.1.2. Учреждение 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 нормативным правовым актам Российской Федерации.

4.1.3. 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).

4.1.4. При организации защиты информации в Учреждении должны выполняться требования федеральных законов:

от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ-152);

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

4.1.5. Системы защиты информации объектов информатизации, являющихся государственными информационными системами Санкт-Петербурга, должны предусматривать реализацию комплекса организационных и технических мер по защите информации, определенных Требованиями о защите информации, не составляющей государственную тайну, содержащихся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации;

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности информации;

целостность информационной системы и информации;

доступность информации;

защита среды виртуализации;

защита технических средств;

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

защита информационной системы от атак, направленных на отказ в обслуживании.

4.1.6. Системы защиты информации объектов информатизации, являющихся информационными системами персональных данных, должны предусматривать реализацию комплекса организационных и технических мер по защите информации, определенных Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом ФСТЭК России от 18.02.2013 № 21:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные;

регистрация событий безопасности;

антивирусная защита;

обнаружение (предотвращение) 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 (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных, и реагирование на них;

управление конфигурацией информационной системы и системы защиты персональных данных.

4.1.7. Системы защиты информации объектов информатизации, являющихся значимыми объектами критической информационной инфраструктуры Российской Федерации, должны предусматривать реализацию комплекса организационных и технических мер по защите информации, определенных Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом ФСТЭК России от 25.12.2017 № 239:

идентификация и аутентификация субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защита машинных носителей информации;

аудит безопасности;

антивирусная защита;

предотвращение вторжений (компьютерных атак);

обеспечение целостности;

обеспечение доступности;

защита технических средств и систем;

защита информационной (автоматизированной) системы и ее компонентов;

планирование мероприятий по обеспечению безопасности;

управление конфигурацией;

управление обновлениями программного обеспечения;

реагирование на инциденты информационной безопасности;

обеспечение действий в нештатных ситуациях;

информирование и обучение персонала;

защита значимых объектов от атак, направленных на отказ в обслуживании.

4.1.8. Учреждением помимо реализации основных мер защиты информации осуществляется:

методическая помощь работникам в вопросах обеспечения информационной безопасности;

анализ и поиск возможностей по повышению уровня защищенности информации.

4.1.9. Для организации защиты информации Учреждение вправе применять средства и методы технической защиты информации, не противоречащие законодательству Российской Федерации.

4.1.10. 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 Учреждении мерами защиты информации.

4.2. Особенности защиты персональных данных, в отношении которых Учреждение является оператором

4.2.1. Перечень мер, выполнение которых обеспечивает Учреждение в качестве оператора персональных данных, должен включать:

назначение ответственного за организацию обработки персональных данных в Учреждении;

издание документов, определяющих политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, определяющих для каждой цели обработки персональных данных категории и перечень обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, способы, сроки их обработки и хранения, порядок уничтожения персональных данных при достижении целей их обработки или при наступлении иных законных оснований, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

оценка вреда в соответствии с требованиями, установленными уполномоченным органом по защите прав субъектов персональных данных, который может быть причинен субъектам персональных данных в случае нарушения ФЗ-152, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных ФЗ-152;

ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику Учреждения в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

опубликование или обеспечение неограниченного доступа к документу, определяющему политику Учреждения в отношении обработки персональных данных, к сведениям о реализуемых Учреждением требованиях к защите персональных данных.

4.2.2. 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 на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, осуществляют структурные подразделения Учреждения.

5.1. Физическая безопасность

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

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

организации режима контролируемого вноса/выноса средств обработки информации.

5.1.2. Помещения Учреждения должны быть оборудованы средствами охранно-пожарной сигнализации.

5.1.3. Основное серверное и сетевое оборудование Учреждения должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания и резервного дизель-генератора. Источники бесперебойного питания должны регулярно тестироваться и проверяться уполномоченными работникам Учреждения в соответствии с рекомендациями производителя.

5.1.4. Мобильные технические средства не должны оставаться за пределами контролируемой зоны Учреждения без контроля со стороны работников Учреждения.

5.2. Безопасность на рабочем месте

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

5.2.2. 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.

5.2.3. 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.

5.2.4. При использовании мобильных технических средств должны соблюдаться дополнительные меры по регламентации и контролю использования в информационной системе мобильных технических средств.

5.2.5. Нахождение представителей юридических лиц в рамках исполнения договорных обязательств в помещениях, в которых ведется обработка информации ограниченного доступа, возможно только в сопровождении работника Учреждения, допущенного до обработки такой информации.

5.2.6. Размещение технических средств вывода информации в помещениях Учреждения должно производиться с учетом исключения возможности визуального просмотра информации посторонними лицами и работниками, не допущенными к работе с данной информацией.

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

5.3. Техническое обслуживание оборудования

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

5.3.2. Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированными специалистами.

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

5.4. Взаимодействие с третьими лицами

5.4.1. При взаимодействии с третьими лицами должны выполняться следующие мероприятия по:

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

осуществлению контроля за действиями представителей контрагентов в пределах контролируемой зоны Учреждения.

5.5. Управление жизненным циклом информационных систем

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

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

5.5.3. 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.

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

5.5.5. 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.

5.5.6. Все процедуры обеспечения защиты информации информационных систем, должны выполняться и контролироваться ответственными лицами за организацию работ по защите информации.

5.6. Контроль доступа к информационным системам

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

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

5.6.3. Должен осуществляться регулярный контроль выполнения локальных нормативных актов по защите информации, касающихся регламентации допуска работников Учреждения к информации, обрабатываемой в информационной системе.

5.7. Идентификация и аутентификация

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

5.8. Управление доступом

5.8.1. В Учреждении 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.

5.9. Безопасность при работе с носителями

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

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

5.9.3. 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.

5.10. Регистрация событий безопасности

5.10.1. В Учреждении должна осуществляться регистрация событий безопасности на всех компонентах объектов информатизации.

5.10.2. При предоставлении доступа к компонентам информационно-телекоммуникационной инфраструктуры центра обработки данных, на базе которой функционируют объекты информатизации ИОГВ, должен осуществляться контроль и учет действий привилегированных пользователей.

5.11. Антивирусная защита информации

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

5.11.2. 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.

5.11.3. При установке программного обеспечения или его обновлении на северном оборудовании должна автоматически выполняться предварительная проверка данного программного обеспечения на отсутствие вредоносного программного обеспечения.

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

5.11.5. Непривилегированные пользователи не должны иметь возможность получения доступа к конфигурации антивирусного средства защиты или его отключения.

5.12. Контроль защищенности информации

5.12.1. 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.

5.13. Использование программного обеспечения

5.13.1. Выбор программного обеспечения для производственных нужд Учреждения 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.

5.14. Использование средств криптографической защиты информации

5.14.1. 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 сертифицированных средств криптографической защиты информации.

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

5.14.3. Портальные решения Учреждения, 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.

5.15. Использование электронной почты

5.15.1. Электронная почта должна использоваться исключительно в целях исполнения должностных обязанностей работника Учреждения.

5.15.2. 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.

5.16. Работа в сетях общего пользования

5.16.1. Учреждение оставляет за собой право блокировать или ограничивать доступ работников 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.

5.16.2. Информация о посещаемых работниками Учреждения информационных ресурсах протоколируется для последующего анализа.

5.16.3. При использовании сети Интернет запрещено:

использовать предоставленный Учреждением 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 об Учреждении, а также фальсифицировать свой IP-адрес.

5.17. Резервное копирование и восстановление данных

5.17.1. Осуществление резервного копирования должно осуществляться для:

информации, обрабатываемой на файловых серверах и серверах приложений, информационных систем;

рабочих мест администраторов информационных систем.

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

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

5.17.4. 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

6.1. Мониторинг информационной безопасности

6.1.1. В Учреждении на постоянной основе должен проводиться комплексный анализ функционирования информационных систем и возникающих событий информационной безопасности.

6.1.2. Процесс мониторинга системы обеспечения информационной безопасности должен включать в себя контроль организационных и технических мер по защите информации, анализ параметров конфигурации, настройки средств защиты информации и действий пользователей при работе с основными техническими средствами и системами объектов информатизации.

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

не нарушать функционирование деятельности Учреждения;

действовать в соответствии с утвержденными локальными нормативными актами Учреждения по защите информации;

не скрывать факты выявленных событий информационной безопасности;

оформлять отчеты, подтверждающие выполнение мероприятий по защите информации.

6.1.4. 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.

6.1.5. 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 Учреждением.

6.2. Управление рисками

6.2.1. Определение внутренних требований по защите информации должно основываться на результатах проведения анализа рисков нарушения основных свойств безопасности информации объектов информатизации.

6.2.2. Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения целостности, конфиденциальности и доступности информации, обрабатываемой в Учреждении.

6.2.3. Результатом проведения анализа рисков должен быть разработанный комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность

Учреждения и ИОГВ при реализации той или иной угрозы безопасности информации и обеспечивающих в дальнейшем достаточный уровень защищенности информации, обрабатываемой объектами информатизации.

6.3. Управление инцидентами информационной безопасности

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

6.3.2. Для управления инцидентами информационной безопасности функционирует Ведомственный центр государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, который посредством комплекса средств и мероприятий для сбора и консолидации информации об инцидентах решает задачи:

реагирования на компьютерные инциденты;

ликвидации последствий компьютерных инцидентов;

анализа результатов ликвидации последствий компьютерных инцидентов;

установления причин компьютерных инцидентов.

6.3.3. В отношении каждого произошедшего инцидента работниками Ведомственного центра государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации должен выполняться анализ и разработка эффективных мер реагирования на данный инцидент.

6.4. Аудит системы обеспечения информационной безопасности

6.4.1. В целях оценки текущего уровня информационной безопасности Учреждением на регулярной основе должен проводиться аудит информационной безопасности.

6.4.2. Внутренние аудиты должны выполняться работниками Учреждения. 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 разработке 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;

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

6.5. Повышение осведомленности работников

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

6.5.2. Повышение осведомленности работников Учреждения осуществляется:

по утвержденным в Учреждении локальным нормативным актам;

по применяемым в Учреждении мерам защиты информации;

по правильному использованию средств защиты информации.

7. Заключение

7.1. При изменении действующего законодательства Российской Федерации в области защиты информации, а также локальных нормативных актов Учреждения, настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также внутренним документам Учреждения.

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

7.3. В Учреждении 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.

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