УТВЕРЖДЕНО
приказом ФГБУ «Камчаттехмордирекция»
от « 01 » февраля 2023 г. № 4

Политика информационной безопасности ФГБУ «Камчаттехмордирекция»

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с положениями:

– Конституции Российской Федерации;

– Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

– Национального стандарта РФ ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 683-ст);

– общепризнанных принципов и норм международного права при осуществлении деятельности по обеспечению информационной безопасности.

1.2. Политика представляет собой совокупность положений, правил, требований и принятых решений, определяющих порядок доступа к информационным ресурсам ФГБУ «Камчаттехмордирекция» (далее – Учреждение), основные направления и способы защиты информации Учреждения.

1.3. Настоящая Политика является документом, доступным всем работникам Учреждения и всем пользователям его ресурсов.

1.4. Требования информационной безопасности, которые предъявляются Учреждением, соответствуют целям деятельности Учреждения и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня.

2. Цели и задачи обеспечения информационной безопасности, Субъекты правоотношений, связанных с использованием информации и обеспечением ее безопасности

2.1. Целями обеспечения информационной безопасности Учреждения являются:

– защита интересов Учреждения, работников и иных субъектов информационных отношений, взаимодействующих с Учреждением, от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем Учреждения, нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;

– обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов Учреждения и предоставляемых сервисов;

– соблюдение правового режима использования массивов и программ обработки информации;

– предотвращение реализации угроз безопасности для деятельности Учреждения.

2.2. Объектами информационных правоотношений являются:

– информационные ресурсы, в том числе с ограниченным доступом;

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

– информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации;

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

2.3. Субъектами информационных отношений при использовании информационных систем Учреждения, заинтересованными в обеспечении информационной безопасности, являются:

– Учреждение, как собственник информационных ресурсов и оператор персональных данных;

– работники подразделений Учреждения, как пользователи и поставщики информации в информационные системы;

– юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационных системах Учреждения.

2.4. Субъекты информационных отношений заинтересованы в обеспечении:

– конфиденциальности определенной части информации;

– целостности информации;

– своевременного доступа к необходимой им информации;

– защиты от навязывания им ложной (недостоверной, искаженной) информации;

– разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

– возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;

– защиты соответствующей части информации от незаконного ее тиражирования и распространения.

2.5. Для достижения целей защиты и обеспечения указанных свойств информации, система обеспечения информационной безопасности Учреждения должна обеспечивать решение следующих задач:

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

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

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

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

2.5.5. Защиту от несанкционированной модификации и контроль целостности используемых в Учреждении программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ.

2.5.6. Защиту информации ограниченного доступа, хранимой, обрабатываемой в Учреждении, от несанкционированного разглашения или искажения.

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

2.5.8. Обеспечение исправности применяемых в информационных системах Учреждения средств защиты информации.

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

2.5.10. Создание условий для минимизации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации в Учреждении.

2.6. Решение вышеперечисленных задач в Учреждении осуществляется:

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

2.6.2. Регламентацией процессов обработки подлежащей защите информации, действий работников Учреждения и персонала, осуществляющего обслуживание и модификацию программных и технических средств, на основе утвержденных организационно распорядительных документов по вопросам обеспечения информационной безопасности.

2.6.3. Назначением и подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в Учреждении.

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

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

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

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

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

2.6.9. Использованием физических и технических (программно-аппаратных)

средств защиты ресурсов Учреждения и административной поддержкой их использования.

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

2.6.11.Юридической защитой интересов Учреждения при взаимодействии с юридическими и физическими лицами от противоправных и несанкционированных действий со стороны этих лиц.

2.6.12.Проведением анализа эффективности принятых мер и применяемых средств защиты информации в Учреждении. Разработкой и реализацией предложений по совершенствованию системы защиты информации (далее – СЗИ) в Учреждении.

3. Угрозы безопасности информации и их источники

3.1. Угрозы безопасности информации, с которыми сталкивается Учреждение, могут быть связаны с проблемами:

– несанкционированного доступа к информации,

– несанкционированной передачи информации,

– внесения вредоносной программы, отказа от факта приема или источника информации,

– отказа в обслуживании и недоступности информации или услуг.

3.2. Указанные угрозы могут быть связаны с утратой:

– конфиденциальности информации и программы (в сетях и системах, соединенных с сетями);

– целостности информации и программы (в сетях и системах, соединенных с сетями);

– доступности информации и сетевых услуг (и систем, соединенных с сетями);

– неотказуемости сетевых транзакций (обязательств);

– подотчетности сетевых транзакций;

– подлинности информации (а также аутентичности сетевых пользователей и администраторов);

– достоверности информации и программы (в сетях и системах, соединенных с сетями);

– способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов;

– способности контролировать злоупотребление санкционированным доступом.

4. Зоны ответственности участников процесса обеспечения информационной безопасности

4.1. Руководство Учреждения

4.1.1. Создает условия, при которых каждый работник Учреждения знает свои обязанности и задачи в отношении информационных ресурсов и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.

4.1.2. Назначает работников, ответственных за создание и использование СЗИ, информации обрабатываемой в Учреждении, реализацию процессов обеспечения информационной безопасности, а также их контроля.

4.1.3. Обеспечивает достаточную численность и квалификацию персонала,

ответственного за построение и поддержание процессов обеспечения информационной безопасности, контроль и мониторинг текущего состояния системы обеспечения информационной безопасности Учреждения.

4.1.4. Инициирует, осуществляет поддержку и контролирует выполнение всех процессов обеспечения информационной безопасности в Учреждении.

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

4.2. Компетентные лица ответственные за информационную безопасность Учреждения

4.2.1. Подготавливают предложения по доработке Политики информационной безопасности в части технического обеспечения информационных систем Учреждения.

4.2.2. Разрабатывают процедуры эффективного управления техническими и программными средствами информационных систем и применяют их в практической деятельности в отношении всех систем, действующих в Учреждении.

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

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

4.2.5. Осуществляют мероприятия по поддержке сопровождения и использования информационных систем.

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

4.2.7. Регулярно обновляют программные и программно-аппаратные комплексы СЗИ в Учреждении.

4.2.8. Осуществляют поддержку функционирования информационных систем и принимают необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности в Учреждении.

4.2.9. Контролируют работоспособность устройств бесперебойного питания критичных для Учреждения информационных систем.

4.2.10. Обеспечивают защиту информационных ресурсов Учреждения от случайного или намеренного уничтожения, искажения, разглашения.

4.3. Руководители структурных подразделений Учреждения

4.3.1. Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов Учреждения в части обеспечения информационной безопасности.

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

4.3.3. Организуют проведение необходимого инструктажа по вопросам выполнения правил информационной безопасности для всех работников своего

структурного подразделения.

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

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

4.4. Работники Учреждения

4.4.1. Соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов, документов Учреждения по вопросам информационной безопасности.

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

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

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

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

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

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

4.5. Сторонние физические и юридические лица соблюдают и выполняют требования Политики информационной безопасности, соответствующих локальных актов и документов Учреждения и других распоряжений руководства по вопросам информационной безопасности при исполнении договорных обязательств.

5. Основные требования по защите информации ограниченного доступа

5.1. Общие требования

5.1.1. В Учреждении необходимо соблюдать режим безопасности, предусматривающий реализацию организационно-технических мероприятий, направленных на обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации.

5.1.2. В Учреждении осуществляется обработка и хранение информации ограниченного доступа (доступ к которой ограничен федеральными законами и служебной необходимостью).

5.1.3. В Учреждении должен быть разработан перечень информации ограниченного доступа.

5.1.4. Учреждение, как обладатель информации ограниченного доступа, при осуществлении своих прав обязано:

– соблюдать права и законные интересы иных лиц;

– принимать меры по защите информации;

– ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

5.1.5. Учреждение, как обладатель информации ограниченного доступа, если иное не предусмотрено федеральными законами, вправе:

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

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

– передавать информацию другим лицам на установленном законом основании;

– защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

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

5.1.6. Учреждение, являясь обладателем информации ограниченного доступа, в случаях, установленных законодательством РФ, обязано обеспечить:

– предотвращение несанкционированного доступа (далее – НСД) к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременное обнаружение фактов НСД к информации;

– недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– возможность регламентированного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянный контроль за обеспечением уровня защищенности информации.

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

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

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

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

5.2. Организация защиты конфиденциальной информации

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

5.2.2. В Учреждении необходимо соблюдать режим защиты конфиденциальной информации (далее – КИ):

– ограничение доступа к КИ, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

– учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;

– использование материальных носителей, содержащих КИ в соответствии с утвержденным порядком, исключающим несанкционированный доступ к ним.

5.2.3. Для обеспечения защиты КИ, Учреждение вправе применять средства и методы технической защиты, предпринимать другие, не противоречащие

законодательству РФ, меры.

5.2.4. Работники Учреждения, обязаны выполнять установленный в Учреждении режим защиты КИ, не разглашать информацию, составляющую КИ, и не использовать эту информацию в личных целях.

5.3. Особенности защиты персональных данных

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

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

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

– назначение ответственного за организацию обработки персональных данных;

– издание документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений;

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

– ознакомление работников Учреждения, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ 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 обучение, при необходимости, указанных работников.

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

5.3.5. Обеспечение безопасности персональных данных достигается, в частности:

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

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

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для

выполнения требований к защите персональных данных, исполнение которых обеспечивает выбранные уровни защищенности персональных данных;

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

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

– учетом машинных носителей персональных данных;

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

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

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

5.3.6. Работники Учреждения должны быть ознакомлены под роспись с документами Учреждения, устанавливающими порядок обработки персональных данных, а также об их правах, обязанностях и ответственности.

6. Основные требования к процессам обеспечения информационной безопасности

6.1. Общие положения

Методическое руководство, разработку конкретных требований по защите информации, согласование выбора средств вычислительной техники и связи, технических и программных средств защиты, организацию работ по выявлению возможностей и предупреждению утечки и нарушения целостности защищаемой информации осуществляют компетентные ответственные лица за информационную безопасность Учреждения.

6.2. Физическая безопасность и безопасность на рабочем месте

6.2.1. Система защиты зданий и помещений Учреждения, объектов и технических средств информационных систем Учреждения обеспечивает выполнение следующих функций:

– разграничение доступа работников в помещения Учреждения в соответствии с их полномочиями и функциональными обязанностями;

– регистрацию фактов входа посторонних лиц в здания Учреждения;

– предотвращение доступа посторонних лиц в помещения, где размещены аппаратные и сетевые ресурсы информационных систем;

– разрешительный режим вноса/выноса (ввоза/вывоза) компьютерного оборудования, средств записи и хранения информации.

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

– основные информационные серверы и средства вычислительной техники, на которых осуществляется обработка и хранение информации ограниченного распространения;

– сетевое оборудование и серверы, обеспечивающие работу критических систем;

– файловые серверы, на которых хранятся данные, в том числе резервные;

6.2.3. Контролируемые зоны защищаются соответствующими системами контроля и управления доступом, обеспечивая доступ только авторизованному персоналу.

6.2.4. Доступ в контролируемые зоны сторонних лиц или представителей

других организаций возможен только в сопровождении уполномоченного работника Учреждения.

6.2.5. Размещение и эксплуатация рабочих станций, серверов и сетевого оборудования Учреждения осуществляется в помещениях, оборудованных замками, средствами сигнализации.

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

6.2.7. Работники Учреждения на момент своего отсутствия на рабочем месте обязаны исключить возможность наличия на рабочем столе документов или носителей с защищаемой информацией.

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

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

6.2.10. Основное техническое оборудование Учреждения должно быть защищено от перебоев в подаче электроэнергии путем подключения к электросети с применением источников бесперебойного питания. Источники бесперебойного питания необходимо регулярно тестировать и проверять уполномоченным работникам Учреждения в соответствии с рекомендациями производителя.

6.2.11. Пользователи портативных технических средств не должны оставлять техническое оборудование и носители информации без присмотра.

6.2.12. Портативные технические средства не должны оставаться за пределами контролируемой зоны Учреждения дольше, чем того требует служебная необходимость, если иное не определено руководством Учреждения.

6.3. Безопасность при работе с носителями информации

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

6.3.2. Работники Учреждения должны использовать электронные носители информации только для выполнения своих служебных обязанностей. Использование электронных носителей информации в Учреждении в иных целях строго запрещено.

6.3.3. Электронные носители информации в Учреждении должны быть учтены путем присвоения каждому носителю инвентаризационного номера и назначения владельца.

6.3.4. Электронные носители информации должны храниться в помещениях, исключающих получение к ним НСД, при этом должен быть обеспечен контроль доступа к носителям.

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

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

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

6.3.8. Факт уничтожения информации и утилизации носителя информации фиксируется в соответствии с порядком, установленным в Учреждении.

6.4. Техническое обслуживание оборудования

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

6.4.2. Ремонт и сервисное обслуживание оборудования должны выполняться только квалифицированным персоналом.

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

6.5. Взаимодействие с третьими лицами

В целях обеспечения информационной безопасности Учреждение при взаимодействии с третьими лицами должны выполняться следующие мероприятия:

– контроль за действиями третьих лиц;

– в договорах с третьими лицами предусматривать право Учреждения на проведение аудита обеспечения безопасности той информации, которая передается третьим лицам.

6.6. Управление жизненным циклом информационных систем

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

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

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

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

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

6.6.6. Все процедуры обеспечения информационной безопасности, установленные в Учреждении в отношении информационных систем, должны выполняться и контролироваться ответственными за информационную безопасность лицами.

6.7. Контроль доступа к информационным системам

6.7.1. Все работники Учреждения, допущенные к работе с информационными системами несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи,

находящихся в их распоряжении защищаемых ресурсов системы.

6.7.2. Уровень полномочий пользователя в информационной системе Учреждения должен определяться в соответствии с его должностными обязанностями и производственной необходимостью.

6.7.3. Доступ пользователей к информационным системам Учреждения должен контролироваться администратором системы.

6.8. Идентификация и аутентификация

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

6.8.2. Получение пользователем имени в системе и парольной информации, которые обеспечивают доступ пользователя к ресурсам системы, должно осуществляться по представлению руководителей структурных подразделений.

6.9. Безопасность пароля

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

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

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

6.9.4. При вводе пароля пользователем для доступа к информационной системе Учреждения должно исключаться отображение парольной информации на экране монитора в открытом виде.

6.9.5. Процедура смены парольной информации в информационных системах Учреждения должна проводиться на регулярной основе.

6.10. Регистрация событий

Осуществление регистрации событий безопасности на всех компонентах информационных систем Учреждения, в которых обрабатывается, хранится или по средствам которых передается защищаемая информация.

6.11. Использование средств криптографической защиты информации (далее – СКЗИ)

Решение об использовании СКЗИ в интересах защиты собственных информационных ресурсов принимается руководством Учреждения в соответствии с законодательством Российской Федерации.

6.12. Безопасность информационной сети

6.12.1. Установление надлежащего контроля в отношении локальной вычислительной сети и всех внешних информационных коммуникаций Учреждения для обеспечения защиты данных и защиты информационных систем Учреждения от НСД.

6.12.2. Должны быть определены цели использования сети Интернет и требования к процедуре использования ресурсов сети Интернет. Использование сети Интернет работников в личных целях должно быть строго запрещено.

6.12.3. Контроль использования работниками ресурсов сети Интернет должен осуществляться уполномоченными работниками на постоянной основе.

6.13. Использование корпоративной электронной почты

6.13.1. Система корпоративной электронной почты должна использоваться в Учреждении с целью организации обмена электронными сообщениями между работниками, а также между работниками Учреждения и внешними абонентами.

6.13.2. В Учреждении должны быть четко определены требования к использованию системы корпоративной электронной почты.

6.13.3. Предоставление и прекращение доступа к ресурсам корпоративной электронной почты должно осуществляться только на основе оформленной заявки.

6.13.4. В Учреждении должно быть установлено специальное программное обеспечение, осуществляющее контроль всех входящих сообщений на наличие вредоносного программного обеспечения.

6.13.5. В Учреждении должны быть предусмотрены механизмы архивирования и резервного копирования корпоративной электронной почты в автоматическом режиме.

6.14. Резервное копирование и восстановление данных

6.14.1. Осуществление резервного копирования для:

– файловых серверов и серверов приложений, критичных для деятельности Учреждения;

– операционных систем файловых серверов и прикладных программ;

– рабочих данных.

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

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

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

6.15. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы.

6.15.1. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

6.15.2. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

6.15.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

6.15.4. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

6.15.5. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов занимает неприемлемо большое время, то допускается проводить выборочную проверку

загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя.

6.15.6. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

6.15.7. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

– осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;

– проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

6.15.8. На всех рабочих станциях и серверах необходимо организовать регулярное обновление антивирусных баз.

6.15.9. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы.

6.15.10. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

– отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

– немедленно сообщить о факте обнаружения вирусов непосредственному руководителю с указанием предположительного источника зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

7. Основные требования к процессам управления информационной безопасностью

7.1. Управление рисками

7.1.1. Выбор требований по информационной безопасности и защитных механизмов, применяемых в системе информационной безопасности, должен основываться на проведении анализа рисков нарушения основных свойств безопасности для наиболее критичных информационных ресурсов Учреждения.

7.1.2. Основой оценки рисков должна быть оценка условий и факторов, которые могут стать причиной нарушения свойств целостности, конфиденциальности и доступности для ресурсов информационной системы Учреждения.

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

7.2. Управление инцидентами информационной безопасности

7.2.1. Для обеспечения эффективного разрешения инцидентов информационной безопасности в Учреждении, минимизации потерь и уменьшения риска возникновения повторных инцидентов должно осуществляться эффективное

управление инцидентами информационной безопасности.

7.2.2. Для управления инцидентами информационной безопасности должна быть создана система учета произошедших инцидентов, которая представляет собой комплекс средств и мероприятий для сбора и консолидации информации об инцидентах.

7.2.3. В отношении каждого произошедшего инцидента должен выполняться его анализ, и разработка эффективных мер реагирования на данный инцидент.

7.3. Мониторинг текущего уровня информационной безопасности

7.3.1. Для обеспечения высокого уровня контроля в отношении системы обеспечения информационной безопасности в Учреждении на постоянной основе должен проводиться комплексный анализ существующих защитных механизмов и возникающих инцидентов информационной безопасности, а также периодический аудит всей системы обеспечения информационной безопасности.

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

7.3.3. При проведении контрольных мероприятий, связанных с оценкой функционирования защитных мер в Учреждении, уполномоченные работники должны придерживаться следующих принципов:

– не нарушать функционирование текущей деятельности Учреждения;

– действовать в соответствии с внутренними документами Учреждения по информационной безопасности;

– не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;

– оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

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

7.4. Аудит системы обеспечения информационной безопасности

7.4.1. В целях оценки текущего уровня информационной безопасности уполномоченные работники Учреждения на регулярной основе должны проводить аудит информационной безопасности.

7.4.2. Внутренние аудиты или самооценки должны выполняться, по возможности, работниками Учреждения.

7.4.3. Результатом выполнения аудитов по информационной безопасности должны стать отчеты о выполненном аудите информационной безопасности.

7.4.4. По результатам аудита уполномоченные работники Учреждения должны определить действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

7.5. Управление персоналом

7.5.1. Организация такого процесса управления персоналом, который обеспечит доверительное отношение к работникам, а также организует комплексное противодействие угрозам информационной безопасности, исходящим от персонала Учреждения.

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

их профессиональных навыков.

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

7.5.4. Повышение осведомленности работников Учреждения:

– по существующей в Учреждении политики информационной безопасности;

– по правильному использованию защитных мер в соответствии с внутренними документами Учреждения.

8. Заключительные положения

8.1. Настоящая Политика является внутренним документом Учреждения, общедоступной и подлежит размещению на официальном сайте Учреждения.

8.2. Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.