ПРАВИТЕЛЬСТВО
СВЕРДЛОВСКОЙ ОБЛАСТИ

**МИНИСТЕРСТВО
ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО
ОБРАЗОВАНИЯ
СВЕРДЛОВСКОЙ ОБЛАСТИ**

Малышева, ул., д. 33, г.Екатеринбург, 620075
тел. (343) 371-20-08, факс (343) 371-34-08; 359-83-24
E-mail: info@minobraz.ru http://www.minobraz.ru

14.05.2018 № 02-01-82/3890

На № _____ от _____

Руководителям подведомственных образовательных организаций

О направлении информации
для обеспечения информационной
безопасности

Уважаемые коллеги!

Министерство общего и профессионального образования Свердловской области (далее – Министерство) направляет для использования в работе Основные положения по формированию Политики обеспечения информационной безопасности в органах исполнительной власти субъектов Российской Федерации и органах местного самоуправления.

Действие данного документа распространяется на подведомственные Министерству организации, выступающие в качестве пользователей информационных ресурсов, в частности – федеральной информационной системы (далее – ФИС) обеспечения проведения государственной итоговой аттестации обучающихся, ФИС «Федеральный реестр сведений о документах об образовании и (или) о квалификации, документах об обучении» и других.

Министерство рекомендует руководствоваться данным документом при планировании и осуществлении мероприятий по обеспечению информационной безопасности.

Приложение: на 17 л. в 1 экз.

Заместитель Министра И.А. Серкова

Лариса Александровна Амбаева
(343) 371-47-85

Приложение к письму
от 14.05.18 № 3890

Основные положения по формированию Политики обеспечения информационной безопасности в органах исполнительной власти субъектов Российской Федерации и органах местного самоуправления (выдержки)

Основные понятия

В настоящем документе используются следующие основные понятия:

Доступность информации – состояние информации, при котором субъекты, имеющие права доступа, могут реализовать ее беспрепятственно.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информация – сведения (сообщения, данные) независимо от формы их представления.

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 в информационных системах: библиотеках, архивах, фондах, банках данных, других видах информационных систем.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Компьютерный инцидент – факт нарушения или прекращения функционирования объекта информационной инфраструктуры Российской Федерации и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе вызванный компьютерной атакой.

Несанкционированный доступ к информации – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

Объект защиты информации – информация, носитель информации или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

Обеспечение информационной безопасности – осуществление взаимоувязанных правовых, организационных, научно- технических, информационно-аналитических, кадровых и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Политика безопасности (информации в организации) – совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные для обеспечения защиты информации.

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушение безопасности информации.

Уязвимость (информационной системы) – свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации.

Целостность информации – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

1. Общие положения

1.1. Основные положения по формированию Политики обеспечения информационной безопасности в органах исполнительной власти субъектов Российской Федерации и органах местного самоуправления (далее – Основные положения) разработаны в соответствии с «...» рекомендациями Координационного совета по защите информации при полномочном представителе Президента Российской Федерации в Уральском федеральном округе (далее – УрФО).

1.2. Руководителям органов исполнительной власти субъектов Российской Федерации и органов местного самоуправления, расположенных в пределах УрФО (далее – органы власти и местного самоуправления) и должностным лицам, ответственным за организацию и обеспечение информационной безопасности, рекомендуется руководствоваться Основными положениями при планировании и осуществлении мероприятий по обеспечению информационной безопасности, а также при формировании в органе власти и местного самоуправления Политики обеспечения информационной безопасности (далее – Политика).

1.3. Органы власти и местного самоуправления входят в организационную основу обеспечения информационной безопасности и осуществляют правомочия обладателя информации. Обладатель информации при осуществлении своих прав обязан соблюдать права и законные интересы иных лиц, принимать меры по защите информации и ограничивать доступ к информации, в установленных федеральными законами Российской Федерации случаях. При этом деятельность органов власти и местного самоуправления основывается на планировании, реализации и оценки эффективности комплекса мер по обеспечению информационной безопасности.

2. Назначение и правовая основа Политики обеспечения информационной безопасности

2.1. Политика обеспечения информационной безопасности в органе власти и местного самоуправления определяет единую систему взглядов на проблему обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач обеспечения информационной безопасности, как одно или несколько правил, практических приемов и руководящих принципов в области информационной безопасности, которыми следует руководствоваться в своей деятельности при формировании и развитии системы обеспечения информационной безопасности.

2.2. Политика оформляется как документированная информация и утверждается руководителем органа власти и местного самоуправления. Разработка и реализация Политики осуществляется высшим руководством органа власти и местного самоуправления путем выработки четкой позиции в решении вопросов информационной безопасности. Политика должна быть доведена до всех сотрудников органа власти и местного самоуправления и быть доступной в установленном порядке для заинтересованных сторон.

2.3. Политика является методологической основой для:

формирования и проведения единой политики в области обеспечения безопасности информации в органе власти и местного самоуправления, в подведомственных учреждениях (организациях), включая территориально удаленные;

принятия управленческих решений и разработке практических мер по воплощению политики обеспечения информационной безопасности и выработки комплекса мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;

координации деятельности структурных подразделений органа власти и местного самоуправления при проведении работ по созданию, эксплуатации информационных систем и вывода их из эксплуатации с соблюдением требований по обеспечению безопасности информации;

разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в органе власти и местного самоуправления.

По решению руководителя органа власти и местного самоуправления действие Политики может распространяться на другие организации и учреждения, взаимодействующие с органом власти и местного самоуправления в качестве пользователей информационных ресурсов.

Использование Политики в качестве основы для построения комплексной системы обеспечения информационной безопасности позволит оптимизировать затраты на ее построение. При разработке Политики необходимо учитывать основные принципы создания комплексных систем обеспечения информационной безопасности, характеристики и возможности организационно-технических методов и аппаратно-программных средств защиты информации и противодействия угрозам безопасности информации.

Основные положения Политики должны базироваться на качественном осмыслении вопросов обеспечения информационной безопасности и не затрагивать вопросы экономического анализа рисков и обоснования необходимых затрат на обеспечение защиты информации.

2.4. Действие разрабатываемой Политики не распространяется на отношения, возникающие при обработке информации ограниченного доступа, содержащей сведения, составляющие государственную тайну. Защита информации, содержащей сведения, составляющие государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

3. Формирование Политики обеспечения информационной безопасности

3.1. Главная цель административных мер, предпринимаемых на высшем управленческом уровне – это сформировать Политику, отражающую подходы к защите информации и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. С практической точки зрения Политику

в органе власти и местного самоуправления целесообразно разделить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность органа власти и местного самоуправления в целом.

Политика верхнего уровня должна четко определить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности информации и детализирует (регламентирует) эти правила.

Политика нижнего уровня должна:

предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

определять принципы и методы разделения и разграничения доступа к информации ограниченного распространения, не содержащей сведения, составляющие государственную тайну;

выбирать программно-технические (аппаратные) средства криптозащиты, противодействия несанкционированному доступу, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих нейтрализацию угроз безопасности информации.

3.2. Руководителем органа власти и местного самоуправления целесообразно определить порядок и периодичность пересмотра Политики в соответствии с изменениями требований законодательства Российской Федерации в области защиты информации, возникновением новых угроз и уязвимостей информационной безопасности, выявлением инцидентов нарушения информационной безопасности, структурно-функциональных характеристик информационных систем.

Периодические пересмотры Политики включают в себя:

проверку эффективности Политики, исходя из характера, числа и последствий зарегистрированных инцидентов нарушения информационной безопасности;

определение мероприятий по совершенствованию системы обеспечения информационной безопасности;

обследование органа власти и местного самоуправления с целью выявления изменений порядка обработки информации и проектных (технологических) решений.

4. Перечень нормативных правовых актов Российской Федерации, нормативных и методических документов, а также национальных стандартов, действующих в области обеспечения информационной безопасности, которыми следует руководствоваться при разработке Политики обеспечения информационной безопасности

Политика разрабатывается с учетом требований нормативных правовых актов Российской Федерации, нормативных и методических документов, а также национальных стандартов, действующих в области обеспечения информационной безопасности:

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

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

Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 05.12.2016 № 646;

Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 06.03.1997 № 188;

Указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Указ Президента Российской Федерации от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации»;

Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные Постановлением Правительства Российской Федерации от 01.11.2012 № 1119;

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства Российской Федерации от 15.09.2008 № 687;

Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденный Постановлением Правительства Российской Федерации от 21.03.2012 № 211;

Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденные Постановление Правительства Российской Федерации от 06.07.2015 № 676;

Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11.02.2013 № 17;

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18.02.2013 № 21;

Состав и содержание 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, утвержденные приказом ФСБ России от 10.07.2014 № 378;

Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденное приказом ФСБ России от 09.02.2005 № 66;

Инструкция 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, утвержденная приказом ФАПСИ от 13.06.2001 № 152;

методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11.02.2014;

ГОСТ Р 50922-2006 Основные термины и определения;

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы;

ГОСТ 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении;

ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования;

ГОСТ Р ИСО МЭК 17799 - 2005 «Информационная технология. Практические правила управления информационной безопасностью»;

ГОСТ Р ISO/МЭК 27001 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

5. Структура и основные тезисы Политики обеспечения информационной безопасности

В Политике определяются цели, задачи и объекты обеспечения информационной безопасности в органах власти и местного самоуправления. Кроме того, рассматриваются методы и средства предотвращения и нейтрализации угроз безопасности информации, а также особенности обеспечения информационной безопасности в органах власти и местного самоуправления.

Ниже приведена примерная структура Политики, а также основные тезисы, которые она может в себя включать. Содержание Политики может меняться и дорабатываться с учетом изменений законодательства Российской Федерации в области обеспечения информационной безопасности и особенностей информационной инфраструктуры органов власти и местного самоуправления.

5.1. Цели и задачи обеспечения информационной безопасности

Основной целью, на достижение которой должны быть направлены положения разрабатываемой Политики, является защита информации, содержащейся в информационных системах органа власти и местного самоуправления от наиболее распространенных угроз информационной безопасности, вызванных неэффективностью процедур контроля, технологических сбоев, несанкционированных действий сотрудников или иных форм незаконного вмешательства в информационные ресурсы и информационные системы.

Указанная цель достигается посредством обеспечения и постоянного поддержания конфиденциальности, целостности и доступности информации.

Для достижения цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности должна обеспечивать эффективное решение следующих задач, таких как:

оценка состояния информационной безопасности, прогнозирование и обнаружение угроз безопасности информации, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

укрепление вертикали управления и централизация сил обеспечения информационной безопасности в органе власти и местного самоуправления;

совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

обеспечение соблюдения требований законодательства Российской Федерации в области информационной безопасности;

организация и координация руководством органа власти и местного самоуправления работ по обеспечению информационной безопасности;

возложение ответственности за обеспечение безопасности информации в информационных системах на каждого сотрудника органа власти и местного самоуправления в пределах его полномочий;

обеспечение непрерывного функционирования информационных систем и системы обеспечения информационной безопасности;

обеспечение эффективной работы механизмов оперативного реагирования на компьютерные инциденты информационной безопасности;

ведение мониторинга состояния защищенности информации при ее обработке в информационных системах;

защита от вмешательства в процесс функционирования информационной системы посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных (трудовых) обязанностей), о есть защиту информации от несанкционированного доступа;

защиту конфиденциальной информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

обеспечение работоспособности криптографических средств защиты информации;

постоянный контроль выполнения требований законодательства Российской Федерации в области обеспечения информационной безопасности;

создание системы непрерывного обучения, тренировки и проверки осведомленности сотрудников по вопросам обеспечения информационной безопасности;

обеспечение защиты информации от несанкционированного доступа, предотвращение утраты, искажения или уничтожения информации на этапах сбора, обработки, хранения и предоставления конечному потребителю информации.

Достижение намеченной цели обеспечения информационной безопасности зависит от качественного решения основных задач в вопросе обеспечения информационной безопасности. В данном разделе целесообразно указать основные пути решения задач по обеспечению информационной безопасности в органе власти и местного самоуправления.

Поставленные основные цели и задачи обеспечения информационной безопасности достигаются, например:

учетом всех подлежащих защите ресурсов информационной системы (информации, задач, документов, каналов связи, серверов, автоматизированных систем);

полнотой и непротиворечивостью требований организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности;

наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих служебных (трудовых) обязанностей полномочиями по доступу к информационным ресурсам;

четким знанием и строгим соблюдением всеми пользователями информационной системы требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

персональной ответственностью за свои действия каждого сотрудника, имеющего доступ к информационным ресурсам, в рамках выполнения своих служебных (трудовых) обязанностей;

эффективным контролем за соблюдением пользователями информационных ресурсов обязательных требований по обеспечению информационной безопасности.

5.2. Объекты обеспечения информационной безопасности

К объектам обеспечения информационной безопасности в органе власти и местного самоуправления могут относиться:

информационные ресурсы, в которых обрабатывается информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну (служебная тайна, персональные данные и другая информация ограниченного распространения), а также общедоступная (открытая) информация;

системы формирования, распространения и использования информационных ресурсов, включающие в себя информационные системы различного класса и назначения, правила и процедуры сбора, обработки, хранения и передачи информации;

информационная инфраструктура, включающая центры обработки и анализа информации, средства, системы связи и передачи данных.

При этом, в информационной системе объектами информационной безопасности являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео-, и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

Информационная безопасность всех вышеуказанных объектов создаст условия надежного функционирования органа власти и местного самоуправления.

5.3. Основные направления деятельности органов власти и местного самоуправления по обеспечению информационной безопасности

Деятельность по обеспечению информационной безопасности призвана способствовать снижению рисков от угроз в информационной сфере, повышению эффективности и устойчивости в управлении информационными ресурсами и системами.

Каждый орган власти и местного самоуправления определяет для себя основные направления деятельности по обеспечению информационной безопасности в зависимости от выполняемых функций и полномочий.

К основным направлениям обеспечения информационной безопасности относятся:

правовое обеспечение информационной безопасности – деятельность направлена на создание и поддержание в актуальном состоянии системы локальных нормативных актов, регламентирующих деятельность по обеспечению информационной безопасности;

организация деятельности по обеспечению информационной безопасности – деятельность направлена на создание документированных процессов обеспечения

информационной безопасности между всеми подразделениями органа власти и местного самоуправления;

обеспечение информационной безопасности при управлении информационными ресурсами – деятельность направлена на идентификацию, классификацию информационных систем и ресурсов, а также их владельцев, формирование и поддержание необходимого уровня информационной безопасности информационных ресурсов;

обеспечение информационной безопасности, связанное с сотрудниками – деятельность направлена на минимизацию рисков, вызванных действиями сотрудников в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки осведомленности всех сотрудников по вопросам обеспечения информационной безопасности;

физическая безопасность информационных ресурсов – деятельность направлена на минимизацию и предотвращение ущерба, вызванного физическим воздействием на информационные системы и ресурсы;

обеспечение информационной безопасности на этапах жизненного цикла информации в информационной инфраструктуре – деятельность направлена на минимизацию рисков, возникающих в процессе создания, обработки, обмена и уничтожения информации в информационных системах;

управление доступом к информационным ресурсам – деятельность направлена на создание порядка доступа к информационным ресурсам, контроль и мониторинг доступа;

управление инцидентами информационной безопасности – деятельность направлена на проведение мероприятий по своевременному выявлению и реагированию на инциденты информационной безопасности;

соответствие обязательным требованиям – деятельность направлена на соответствие требованиям законодательства Российской Федерации, локальных нормативных актов по обеспечению информационной безопасности.

5.4. Принципы формирования системы обеспечения информационной безопасности в органах власти и местного самоуправления

Построение системы обеспечения информационной безопасности в органах власти и местного самоуправления и ее функционирование осуществляется в соответствии с основными принципами формирования системы обеспечения информационной безопасности (данные принципы указываются в Политике).

К основным принципам формирования системы обеспечения информационной безопасности в органе власти и местного самоуправления относятся:

законность – предполагает разработку системы обеспечения информационной безопасности в соответствии с действующим законодательством Российской Федерации в данной области с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией. Все пользователи информационных систем должны иметь представление об ответственности за правонарушения в области обеспечения информационной безопасности;

системность – предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблемы обеспечения информационной безопасности. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем, а также характер, возможные

объекты и направления атак на них со стороны нарушителей, пути проникновения в информационные системы и несанкционированного доступа к информации;

централизация управления – предполагает, что деятельность по обеспечению информационной безопасности должна быть встроена в управленческие процессы органа власти и местного самоуправления, подчиняться понятным руководителям закономерностям и оцениваться с позиций эффективности, для этого процессы обеспечения информационной безопасности должны быть организованы и управляемы;

персональная ответственность – предполагает возложение персональной ответственности на каждого сотрудника в пределах его должностных полномочий за несоблюдение регламентирующих документов в области обеспечения информационной безопасности;

минимизация полномочий – предполагает предоставление прав доступа сотрудникам к информационным ресурсам в том случае и объеме, необходимом для качественного выполнения своих служебных (трудовых) обязанностей;

своевременность – предполагает своевременность выявления проблем, связанных с обеспечением информационной безопасности, и обнаружение угроз безопасности информации, потенциально способных нанести ущерб;

комплексный подход – предполагает всестороннее обеспечение информационной безопасности и предусматривает использование взаимоувязанных программно-технических, организационных, правовых мер обеспечения информационной безопасности на единой концептуальной основе;

непрерывность – предполагает непрерывный, целенаправленный процесс по выявлению угроз информационной безопасности и принятию адекватных мер защиты руководством, подразделением безопасности и сотрудниками органов власти и местного самоуправления;

совершенствование – предполагает постоянное совершенствование мер и средств защиты информации на основе модернизации организационных и технических решений, кадрового состава, анализа функционирования информационной системы и системы ее защиты с учетом изменений в методах и средствах перехвата информации, обязательных требований по защите информации;

взаимодействие и сотрудничество – предполагает создание благоприятной атмосферы в коллективах структурных подразделений. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственных за обеспечение информационной безопасности. Все сотрудники должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе;

гибкость системы защиты – система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления органом власти и местного самоуправления своих полномочий. В число таких изменений входят изменения организационной и штатной структуры; изменение существующих или внедрение принципиально новых информационных систем; технических средств;

обоснованность и техническая реализуемость – информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по информационной безопасности;

обязательность контроля – предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения информационной безопасности. Выявленные недостатки системы обеспечения информационной безопасности должны немедленно доводиться до сведения руководителя органа власти и местного самоуправления, а также оперативно устраняться.

5.5. Требования к организации обеспечения безопасности информационных систем

Обеспечение безопасности информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы.

Для обеспечения безопасности информации, содержащейся в информационной системе, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в информационной системе;

разработка системы защиты информации информационной системы;

внедрение системы защиты информации информационной системы;

аттестация информационной системы по требованиям защиты информации и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

Для проведения работ по обеспечению безопасности информации в ходе создания и эксплуатации информационной системы обладателем информации (заказчиком) в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

5.6. Ответственные за обеспечение информационной безопасности в органах власти и местного самоуправления

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в органе власти и местного самоуправления руководителем назначается структурное подразделение или должностное лицо (сотрудник), ответственное за обеспечение информационной безопасности.

На это подразделение (сотрудника) возлагается решение следующих основных задач:

анализ текущего состояния обеспечения информационной безопасности в органе власти и местного самоуправления;

организация мероприятий и координация работ всех подразделений по обеспечению информационной безопасности;

контроль и оценка эффективности принятых мер и применяемых средств защиты информации.

Основные функции подразделения (сотрудника) обеспечения информационной безопасности заключаются в следующем:

формирование требований к системе обеспечения информационной безопасности в процессе создания и дальнейшего развития существующих компонентов информационной системы;

участие в проектировании системы обеспечения информационной безопасности, ее испытаниях и вводе в эксплуатацию;

обеспечение функционирования системы защиты информации и ее элементов, включая управление криптографическими системами;

обучение пользователей и обслуживающего персонала правилам обработки информации;

оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;

контроль за соблюдением пользователями и обслуживающим персоналом установленных правил обращения с конфиденциальной информацией;

организация по указанию руководства служебного расследования по фактам нарушения правил обращения с конфиденциальной информацией и оборудованием;

принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;

участие в работе по выявлению и устранению компьютерных инцидентов информационной безопасности.

Для решения задач, возложенных на подразделение обеспечения информационной безопасности, его сотрудники должны иметь следующие права:

определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в данной области;

контролировать деятельность пользователей информационной системы органа власти и местного самоуправления по вопросам обеспечения информационной безопасности;

требовать письменных объяснений у лиц по фактам нарушений требований информационной безопасности;

готовить предложения руководству органа власти и местного самоуправления по совершенствованию системы обеспечения информационной безопасности.

5.7. Основные организационные, технические и правовые меры обеспечения безопасности информации

Для организации и внедрения системы защиты информации в информационной инфраструктуре органов власти и местного самоуправления важное значение имеет анализ технических, структурных, эксплуатационных и иных особенностей информационных систем, используемых технологий и архитектурных решений.

В данном разделе целесообразно указать меры защиты информации, включающие в себя правовые (законодательные), организационные, технические и физические, а также применение криптографических методов и средств защиты информации, необходимых для обеспечения информационной безопасности.

Правовые (законодательные) меры обеспечения безопасности информационных систем

К правовым (законодательным) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения принятых в них правил.

Следует учитывать, что лица, виновные в нарушении обязательных требований по обеспечению информационной безопасности несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы.

Организационные меры обеспечения безопасности информационных систем

Организационные меры обеспечения безопасности информационных систем - меры организационного характера, регламентирующие процессы функционирования информационных систем, использование их ресурсов, деятельность обслуживающего персонала, а также порядок обращения пользователей информации с информационными системами таким образом, чтобы в наибольшей степени затруднить либо исключить возможность реализации угроз информационной безопасности, снизить размер потерь в случае реализации угроз.

Технические меры обеспечения безопасности информационных систем

Технические меры обеспечения безопасности информационных систем должны быть основаны на использовании единых программных и технических средств, входящих в состав информационных систем и выполняющих самостоятельно или в комплексе с другими средствами функции защиты.

Технические меры обеспечения безопасности информационных систем реализуются, в том числе посредством применения средств защиты информации, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации. Данный перечень размещен на официальном сайте ФСТЭК России (www.fstec.ru).

Применение организационных и технических мер защиты информации, реализуемых в информационных системах в рамках их систем защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационных систем должны обеспечивать:

идентификацию и аутентификацию субъектов доступа и объектов доступа;
управление доступом субъектов доступа к объектам доступа;
ограничение программной среды;
защиту машинных носителей информации;
регистрацию событий безопасности;
антивирусную защиту;
обнаружение вторжений;
контроль (анализ) защищенности информации;
обеспечение целостности информационной системы и информации;
обеспечение доступности информации;
защиту среды виртуализации;
защиту технических средств;

защиту информационной системы, ее средств, систем связи и передачи данных, в том числе, посредством применения активных и пассивных средств защиты информации, обрабатываемой техническими средствами информационных систем и циркулирующей в помещениях объекта от утечки по техническим каналам.

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на обеспечение конфиденциальности, целостности и доступности информации.

В условиях растущего санкционного давления со стороны политических оппонентов и недружественных стран, осуществляющих контроль компаний-производителей информационно-телекоммуникационного оборудования и программного обеспечения, в том числе с использованием возможностей спецслужб иностранных государств, руководителям органов власти и местного самоуправления необходимо ориентироваться на выбор отечественного программного и информационно-телекоммуникационного оборудования, соответствующего требованиям информационной безопасности, что также соответствуют текущему курсу импортозамещения Правительства Российской Федерации.

Криптографические методы и средства защиты

Криптографические методы и средства защиты (далее – СКЗИ) используются для обеспечения информационной безопасности. Организация в органе власти и местного самоуправления системы информационной безопасности на основе инфраструктуры с использованием СКЗИ позволит решить задачи:

организации обеспечения защищенного документооборота с использованием имеющихся систем, как внутри, так и при взаимоотношениях с другими организациями. Это позволит повысить эффективность и снизить накладные расходы на администрирование системы и использовать единые стандарты защиты данных;

реализации централизованно контролируемой системы информационной безопасности, при этом гибкой и динамически управляемой;

универсализации методов обеспечения доступа пользователей и защиты для системы электронной почты, системы доступа в МКС «Интернет» и других систем с использованием уже имеющихся в этих приложениях механизмов обеспечения информационной безопасности;

использования имеющихся реализаций российских криптографических алгоритмов в операциях с сертификатами и при защите электронного документооборота.

Использование СКЗИ для обеспечения безопасности информации необходимо в случаях, если:

информация подлежит криптографической защите в соответствии с законодательством Российской Федерации;

в информационной системе существуют угрозы, которые могут быть нейтрализованы только с помощью данных средств (передача информации по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче информации, содержащей сведения конфиденциального характера, по информационно-телекоммуникационным сетям общего пользования; хранение информации на носителях, несанкционированный доступ к которым со

стороны нарушителя не может быть исключен с помощью некриптографических методов и способов).

При применении СКЗИ требуется учитывать:

криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;

для обеспечения безопасности информации при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия. Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (www.clsz.fsb.ru).

Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в них посторонних лиц, хищение документов и носителей информации, самих средств информатизации, а также исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств съема информации.

5.8. Порядок реагирования на компьютерные инциденты

В органе власти и местного самоуправления следует назначить ответственное лицо за выявление и реагирование на инциденты информационной безопасности из состава подразделения, ответственного за обеспечение информационной безопасности, объединяющего в своем составе квалифицированных специалистов в области информационных технологий и защиты информации.

Реагирование на компьютерные инциденты включает в себя выполнение следующих мероприятий:

фиксацию состояния и анализ объектов информационных ресурсов, вовлеченных в инцидент;

координацию деятельности по прекращению воздействия компьютерных атак, проведение которых вызвало возникновение инцидента;

фиксацию и анализ сетевого трафика, циркулирующего в информационном ресурсе, вовлеченном в инцидент;

определение причин инцидента и возможных его последствий для информационного ресурса:

первичный анализ инцидента;

комплексный анализ инцидента;

локализацию инцидента;

сбор сведений для последующего установления причин инцидента;

планирование мер по ликвидации последствий инцидента;

ликвидацию последствий инцидента;

контроль ликвидации последствий;

формирование рекомендаций для совершенствования нормативных документов и навыков специалистов, обеспечивающих информационную безопасность ресурсов.

Решения должны приниматься рабочей группой отдельно для каждого информационного ресурса, затронутого компьютерным инцидентом.

5.9. Обучение сотрудников и повышение осведомленности в вопросах обеспечения информационной безопасности

Все пользователи информационной системы должны быть ознакомлены с организационно - распорядительными документами по обеспечению информационной безопасности, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению безопасности информации. Доведение требований указанных документов до лиц, допущенных к обработке защищаемой информации, осуществляется под подпись. Пользователи информационной системы, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки конфиденциальной информации.

Целью обучения сотрудников является, снижение потерь (материальных, финансовых, ущерб репутации и т.д.) от угроз, связанных с незнанием или непониманием основных положений законодательства Российской Федерации в области обеспечения информационной безопасности и правил по защите информации.

Задачи повышения осведомленности сотрудников в вопросах информационной безопасности:

информирование сотрудников о существующих угрозах и проблемах информационной безопасности, которые могут возникнуть при автоматизированной обработке информации, обновление их теоретических и практических знаний в области обеспечения информационной безопасности;

доведение до сотрудников основных положений, ограничений и требований существующих нормативно-распорядительных документов принятых в органе власти и местного самоуправления;

выработка у сотрудников умения оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски информационной безопасности);

выработка у сотрудников привычек, способствующих поддержанию высокого уровня информационной безопасности;

выработка у сотрудников органа власти умений (навыков) правильно и оперативно действовать при возникновении инцидентов информационной безопасности;

доведение до сотрудников их обязанностей в области обеспечения информационной безопасности и степени их ответственности в случае утечки конфиденциальной информации;

оценка эффективности, развитие и совершенствование проводимых мероприятий по информационной безопасности в целом.

Формы и методы повышения осведомленности сотрудников в области информационной безопасности:

инструктаж при приеме на работу;

повышение квалификации (курсы, семинары, тренинги);

дистанционное обучение;

инструктажи и зачеты по положениям законодательства Российской Федерации в области обеспечения информационной безопасности и Политики;

распространение кратких памяток, рассылки на электронную почту, разделы на внутреннем сайте органа власти и местного самоуправления.

Повышение квалификации сотрудников осуществляется:

с отрывом или без отрыва от служебной деятельности (работы) в соответствии с программами повышения квалификации;

с периодичностью, позволяющей сотрудникам в условиях нарастания количества угроз безопасности информации, а также с учетом необходимости постоянного совершенствования методов и средств их нейтрализации получать новые знания, умения и навыки, необходимые для профессиональной деятельности.

Форма и продолжительность повышения квалификации специалистов, а также тематика программ повышения квалификации, подлежащих освоению специалистами, определяются работодателем в соответствии с утвержденными ФСТЭК России примерными программами повышения квалификации.

5.10. Контроль состояния информационной безопасности

Контроль состояния информационной безопасности осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Основная задача контроля заключается в получении объективных оценок текущего состояния обеспечения информационной безопасности, оценка эффективности применяемых мер и технических решений для обеспечения информационной безопасности, оказание методической помощи по обеспечению защиты информации, организация работы по обеспечению информационной безопасности.

Контроль может проводиться как подразделениями обеспечения информационной безопасности, так и привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности. Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.