УТВЕРЖДАЮ

Заместитель Губернатора Курганской области — директор Департамента строительства, госэкспертизы и жилищно-коммунального хозяйства Курганской области

_____Р.А. Ванюков

"____" _____ 2018 года

Политика обеспечения информационной безопасности в Департаменте строительства, госэкспертизы и жилищно-коммунального хозяйства Курганской области

Содержание

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

Информационная безопасность (далее - ИБ) является одним из критических факторов успешной и стабильной работы Департамента строительства, госэкспертизы и жилищно-коммунального хозяйства Курганской области (далее – Департамент). Обеспечение ИБ Департамента, его работников, а также представителей третьих сторон является одной из первостепенных задач.

Политика информационной безопасности Департамента (далее – Политика) является основополагающим документом, отражающим видение руководства Департамента обеспечения ИБ.

2. Назначение и правовая основа Политики обеспечения информационной безопасности.

Политика обеспечения ИБ в Департаменте определяет единую систему взглядов на проблему обеспечения информационной безопасности и представляет собой систематизированное изложение целей и задач обеспечения информационной безопасности.

Реализация Политики осуществляется руководителями Департамента путем выработки четкой позиции в решении вопросов информационной безопасности. Политика должна быть доведена до всех сотрудников Департамента и быть доступной в установленном порядке для заинтересованных сторон (Политика размещается на официальном веб-сайте Департамента в информационно-телекоммуникационной сети «Интернет»).

Политика является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности информации в Департаменте, и в подведомственных учреждениях (организациях);
- 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 Департамента 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 Департаменте.

По решению руководителя Департамента действие Политики может распространяться на другие организации и учреждения, взаимодействующие с Департаментом в качестве пользователей информационных ресурсов.

Действие 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.

Политика обеспечения ИБ должна отражать подходы к защите информации и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Политика в Департаменте должна формироваться из нескольких уровней. К верхнему уровню относятся решения руководства, затрагивающие деятельность Департамента в целом, то есть настоящая Политика.

Политика определяет сферу влияния и ограничения при определении целей безопасности информации, какими ресурсами (материальными, структурными, организационными) они будут достигнуты, и установить 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:

предусматривает разработку регламентов информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;

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

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

К документам нижнего уровня относятся инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Департамента по реализации документов высшего и нижнего уровней, а также отчётные документы о выполнении требований документов всех уровней.

Документы по обеспечению ИБ всех уровней обязательны для исполнения всеми сотрудниками Департамента.

Политика должна пересматриваться не реже одного раза в два года, 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.

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, действующих в области обеспечения информационной безопасности используемые при разработке Политики обеспечения информационной безопасности в Департаменте

Политика разрабатывалась 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

Политика определяет цели, задачи и объекты обеспечения ИБ в Департаменте.

Кроме того, рассматриваются методы и средства предотвращения и нейтрализации угроз безопасности информации, а также особенности обеспечения ИБ в Департаменте.

Содержание Политики может меняться и дорабатываться с учетом изменений законодательства Российской Федерации в области обеспечения ИБ и особенностей информационной инфраструктуры Департамента.

5.1. Цели и задачи обеспечения информационной безопасности

Политика направлена на достижение следующих основных целей:

- защита информации от реальных и потенциальных угроз;
- минимизация и локализация последствий при воздействии угроз;
- защита информации, содержащейся в информационных системах Департамента 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 информации система обеспечения ИБ должна решить следующие задачи:

- выявление, предупреждение и нейтрализация реальных и потенциальных угроз ИБ, а также установление причин и условий их возникновения;
- совершенствование механизмов оперативного реагирования на угрозы ИБ;
- эффективное управление рисками ИБ;
- информирование, обучение, контроль знаний работников Департамента по вопросам ИБ.
- оценка состояния ИБ, прогнозирование и обнаружение угроз безопасности информации, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
- укрепление вертикали управления и централизация сил обеспечения ИБ в Департаменте;
- совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения ИБ;
- обеспечение соблюдения требований законодательства Российской Федерации в области ИБ;
- организация и координация руководством Департамента работ по обеспечению ИБ;
- возложение ответственности за обеспечение безопасности информации в информационных системах на каждого сотрудника Департамента в пределах его полномочий;
- обеспечение непрерывного функционирования информационных систем и системы обеспечения ИБ;

- обеспечение эффективной работы механизмов оперативного реагирования на компьютерные инциденты ИБ;

- 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), то есть защиту информации от несанкционированного доступа;

- защита 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 ИБ;

- создание системы непрерывного обучения, тренировки и проверки осведомленности сотрудников по вопросам обеспечения ИБ;

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

Цели и задачи обеспечения ИБ достигаются:

- 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 ИБ.

5.2. Объекты обеспечения информационной безопасности

К объектам обеспечения ИБ в Департаменте относятся:

- 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 ИБ 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.

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена.

5.3. Основные направления деятельности Департамента по обеспечению информационной безопасности

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

К основным направлениям обеспечения ИБ Департамента относятся:

- правовое обеспечение ИБ – создание и поддержание в актуальном состоянии системы локальных нормативных актов, регламентирующих деятельность по обеспечению ИБ;

- организация деятельности по обеспечению ИБ – создание документированных процессов обеспечения ИБ между всеми подразделениями Департамента;

- обеспечение ИБ при управлении информационными ресурсами – идентификация, классификация информационных систем и ресурсов, а также их владельцев, формирование и поддержание необходимого уровня ИБ информационных ресурсов;

- обеспечение ИБ, связанное с сотрудниками –минимизация рисков, вызванных действиями сотрудников в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки осведомленности всех сотрудников по вопросам обеспечения ИБ;

- физическая безопасность информационных ресурсов – минимизация и предотвращение ущерба, вызванного физическим воздействием на информационные системы и ресурсы;

- обеспечение ИБ на этапах жизненного цикла информации в информационной инфраструктуре – минимизация рисков, возникающих в процессе создания, обработки, обмена и уничтожения информации в информационных системах;

- управление доступом к информационным ресурсам – создание порядка доступа к информационным ресурсам, контроль и мониторинг доступа;

- управление инцидентами ИБ – проведение мероприятий по своевременному выявлению и реагированию на инциденты ИБ;

- соответствие обязательным требованиям – соответствие требованиям законодательства Российской Федерации, нормативным актам Департамента по обеспечению ИБ.

5.4. Принципы формирования системы обеспечения информационной безопасности в Департаменте

Основными принципами формирования системы обеспечения ИБ являются:

законность – разработка системы обеспечения ИБ в соответствии с действующим законодательством Российской Федерации в данной области с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией;

системность – учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, имеющих существенное значение для понимания и решения проблемы обеспечения ИБ;

централизация управления – деятельность по обеспечению ИБ должна быть встроена в управленческие процессы, подчиняться понятным руководителям закономерностям и оцениваться с позиций эффективности, для этого процессы обеспечения ИБ должны быть организованы и управляемы;

персональная ответственность – ответственность каждого сотрудника в пределах его должностных полномочий за несоблюдение регламентирующих документов в области обеспечения ИБ;

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

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

комплексный подход – всестороннее обеспечение ИБ путем использования взаимоувязанных программно-технических, организационных, правовых мер обеспечения ИБ на единой концептуальной основе;

непрерывность – непрерывный, целенаправленный процесс по выявлению угроз ИБ и принятию адекватных мер защиты руководством, подразделением безопасности и сотрудниками;

совершенствование – 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 – создание благоприятной атмосферы в коллективах структурных подразделений;

гибкость системы защиты – система обеспечения ИБ должна быть способна реагировать на изменения внешней среды и условий осуществления своих полномочий;

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

обязательность контроля – обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения ИБ.

5.5. Требования к организации обеспечения безопасности информационных систем.

Для обеспечения безопасности информации, содержащейся в информационной системе, необходимо проводить 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 Департамента 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 Департаменте

Руководство Департамента принимает на себя ответственность за реализацию настоящей Политики.

Руководители управлений, структурных подразделений, работники Департамента несут ответственность за безусловное полное выполнение своих обязанностей по поддержанию деятельности по обеспечению и выполнению требований ИБ в соответствии с документами Департамента, а представители третьих сторон, имеющие доступ к информационным ресурсам Департамента - в соответствии с договорными обязательствами.

Ответственное структурное подразделение Департамента несет ответственность за поставленные руководством Департамента цели и задачи, а также контроль выполнения требований, отраженных в документах Департамента. Все исключения из этих требований в обязательном порядке согласовываются с ответственным структурным подразделением.

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

Меры защиты информации.

Правовые (законодательные) меры обеспечения безопасности информационных систем:

- разработка и поддержание в актуальном состоянии всех необходимых документов по защите информации;

- нарушители обязательных требований по обеспечению ИБ несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Организационные меры обеспечения безопасности информационных систем:

- разработка и утверждение инструкций и требований к пользователю информационных систем и персональных компьютеров;

- разработка руководства пользователей информационных систем, разграничение ролей доступа в информационные системы;

- контроль доступа в помещения, где ведется обработка данных в информационных системах Департамента.

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 (перечень размещен на официальном сайте ФСТЭК России www.fstec.ru).

Применение организационных и технических мер 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.

Криптографические методы и средства защиты.

Методы необходимо применять для решения задач:

организации обеспечения защищенного документооборота, как внутри, так и при взаимоотношениях с другими организациями в различных информационных системах;

универсализации методов обеспечения доступа пользователей к информационным системам Департамента.

Должны использоваться средства криптографической защиты информации, прошедшие в установленном порядке процедуру оценки соответствия (перечень средств криптографической защиты информации, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России www.clsz.fsb.ru).

Физические меры защиты.

Применяются для обеспечена физической защиты здания, помещений, объектов и средств информатизации, с помощью технических средств охраны или иными способами, для предотвращения или затруднения проникновения посторонних лиц, в частности путем установки охранной сигнализации, механических устройств.

5.8. Порядок реагирования на компьютерные инциденты.

Реагирование на компьютерные инциденты включает в себя следующие мероприятия:

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;

ликвидация последствий инцидента;

контроль ликвидации последствий;

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

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

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

Все пользователи информационных систем Департамента должны самостоятельно изучать нормативные правовые документы в сфере защиты информации, обработки персональных данных, знакомиться с организационно-распорядительными документами по обеспечению ИБ, в части, их касающейся, должны знать и неукоснительно выполнять инструкции и знать общие обязанности по обеспечению ИБ.

В случае направления специалистов на курсы повышения квалификации, её форма и продолжительность, а также тематика программ повышения квалификации, подлежащих освоению специалистами, определяются в соответствии с утвержденными ФСТЭК России примерными программами повышения квалификации.

5.10. Контроль состояния информационной безопасности.

Контроль состояния ИБ должен осуществляться 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 ИБ, оценке эффективности применяемых мер и технических решений для обеспечения ИБ, организации работы по обеспечению ИБ.

Общий контроль состояния ИБ осуществляется руководителем Департамента.

Текущий контроль соблюдения настоящей Политики осуществляет структурное подразделение, уполномоченное на проведение мероприятий по обеспечению ИБ. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ Департамента, по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Нарушение требований нормативных актов Департамента по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

Контроль может проводиться 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.

Структурное подразделение, уполномоченное на организацию и проведение мероприятий по обеспечению ИБ каждые два года пересматривает положения настоящей Политики. Изменения и дополнения вносятся по его инициативе или инициативе руководителя Департамента и утверждаются руководителем Департамента.

Порядок пересмотра документов второго и третьего уровней определяется в данных документах.

Все изменения, внесённые в настоящую Политику ИБ должны учитываться в листе «История изменений».

Главный специалист-эксперт отдела
информатизации жилищно-коммунального
хозяйства управления жилищно-коммунального хозяйства Т.Г. Гребенщикова

История изменений

Версия	Дата утверждения	Изменения	Кто внёс изменения