УТВЕРЖДЕНА

распоряжением администрации
Южноуральского городского округа

от _19.01.2018 г №__21-р__

ПОЛИТИКА

информационной безопасности администрации Южноуральского городского округа

1. Общие положения

Политика информационной безопасности (далее – Политика) администрации Южноуральского городского округа определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и принципов в области информационной безопасности, которыми руководствуется администрация Южноуральского городского округа (далее – Администрации), включая структурные подразделения, в своей деятельности.

Основными целями Политики являются защита информации и обеспечение эффективной работы всей информационно-вычислительной системы администрации при осуществлении деятельности.

Общее руководство обеспечением информационной безопасности Администрации осуществляет Глава Южноуральского городского округа. В структурных подразделениях Администрации с правом юридического лица, руководство обеспечением информационной безопасности осуществляет руководитель данного структурного подразделения.

Контроль за соблюдением требований по информационной безопасности несет должностное лицо, назначенное ответственным за информационную безопасность Администрации.

Сотрудники Администрации обязаны соблюдать порядок обращения с конфиденциальными документами, ключевыми носителями и другой защищаемой информацией, соблюдать требования настоящей Политики и иных документов, регламентирующих деятельность в области информационной безопасности.

2. Область применения

Настоящая Политика распространяется на все структурные подразделения Администрации и обязательна к исполнению всеми ее сотрудниками. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах Администрации.

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. Термины и определения

В настоящей Политике используются следующие термины:

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аудит информационной безопасности Администрации - процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самой Администрацией (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит).

Информационная технология - совокупность правил, приемов и методов применения средств вычислительной техники для выполнения функций хранения, обработки, передачи и использования производственной, финансовой, аналитической или иной информации, связанной с функционированием Администрации.

Информационный технологический процесс - часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования Администрации.

Информационная безопасность Администрации - состояние защищенности информационных активов Администрации в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры Администрации.

Информационные активы Администрации – активы Администрации, имеющие отношение к его информационной сфере и представляющие ценность для нее с точки зрения достижения уставных целей.

Инцидент информационной безопасности - действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов Администрации.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств в соответствии с законодательством.

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

Мониторинг информационной безопасности Администрации - постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности Администрации, сбор, анализ и обобщение результатов наблюдения под заданные цели. Объектом мониторинга в зависимости от целей может быть автоматизированная система или ее часть, информационные технологические процессы, информационные услуги и прочее.

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами. Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения средств вычислительной техники или автоматизированных систем.

Политика информационной безопасности Администрации - комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых Администрацией для обеспечения информационной безопасности.

Риск - мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Роль - заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом Администрации. К субъектам относятся сотрудники Администрации, посетители, а также инициируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие автоматизированную систему.

Режим конфиденциальности информации – организационно-технические мероприятия по обеспечению конфиденциальности информации (защите информации), включающие в себя:

- определение перечня информации, составляющей конфиденциальную информацию;

- ограничение доступа к конфиденциальной информации путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

- учет лиц, получивших доступ к конфиденциальной информации, и(или) лиц, которым такая информация была предоставлена или передана;

- регулирование отношений по использованию конфиденциальной информации работниками на основании трудовых договоров, контрагентами на основании гражданско-правовых договоров и соглашений, работниками со срочными трудовыми договорам и проходящих в Администрации практику (стажировку).

Угроза - опасность, предполагающая возможность потерь (ущерба).

Управление информационной безопасностью Администрации - совокупность целенаправленных действий, осуществляемых в рамках настоящей Политики в условиях угроз в информационной сфере, включающая в себя оценку состояния объекта управления (например, оценку и управление рисками), выбор управляющих воздействий и их реализацию (планирование, внедрение и обслуживание защитных мер - защита информации).

Уязвимость - недостатки или слабые места информационных активов, которые могут привести к нарушению информационной безопасности Администрации при реализации угроз в информационной сфере.

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

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

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. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются:

5.1. Постоянный и всесторонний анализ АС и информационных технологий с целью выявления уязвимостей информационных активов Администрации.

5.2. Своевременное обнаружение проблем, потенциально способных повлиять на ИБ Администрации, корректировка моделей угроз.

5.3. Разработка и внедрение защитных мер, адекватных характеру выявленных угроз, с учетом затрат на их реализацию и совместимости этих мер с действующим технологическим процессом. При этом меры, принимаемые для обеспечения ИБ, не должны усложнять деятельность Администрации, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности.

5.4. Контроль эффективности принимаемых защитных мер.

5.5. Персонификация и адекватное разделение ролей и ответственности между работниками Администрации, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

6. Цели и задачи ИБ

Основной целью 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;

- 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 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.

Поставленные основные цели и задачи обеспечения информационной безопасности 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;

- 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.

7. Объекты обеспечения информационной безопасности

К объектам обеспечения информационной безопасности в Администрации 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 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 Администрации.

8. Основные направления деятельности Администрации 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.

Администрация 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.

9. Принципы формирования системы обеспечения информационной безопасности в Администрации

Построение системы обеспечения информационной безопасности в Администрации и ее функционирование осуществляется в соответствии с основными принципами формирования системы обеспечения информационной безопасности.

К основным принципам формирования системы обеспечения информационной безопасности в Администрации 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 Администрации, 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 Администрации;

- 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 Администрацией 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 Администрации, а также оперативно устраняться.

10. Модели угроз

Модели угроз являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения ИБ Администрации.

Источники угроз, уязвимости и объекты нападений, пригодные для реализации уязвимости, типы возможных потерь, масштабы потенциального ущерба определяются документом «Модели угроз».

11. Требования по обеспечению информационной безопасности

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.

12. Ответственные за обеспечение информационной безопасности в Администрации

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Администрации Главой городского округа 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.

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

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

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, Администрации 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.

14. Порядок реагирования на компьютерные инциденты

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;

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

15. 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 Администрации;

- 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 Администрации 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.

16. 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.