ПОСТАНОВЛЕНИЕ

АДМИНИСТРАЦИИ ИЗОБИЛЬНЕНСКОГО МУНИЦИПАЛЬНОГО ОКРУГА СТАВРОПОЛЬСКОГО КРАЯ

20 марта 2026 г. **г. Изобильный** № 499

Об утверждении Политики защиты информации в администрации Изобильненского муниципального округа Ставропольского края

В соответствии со статьями 6, 16 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», подподпункта. «а» пункта 14 приказа Федеральной службы по техническому и экспертному контролю России от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», администрация Изобильненского муниципального округа Ставропольского края

ПОСТАНОВЛЯЕТ:

1. Утвердить прилагаемую Политику защиты информации в администрации Изобильненского муниципального округа Ставропольского края.

2. Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Изобильненского муниципального округа Ставропольского края Пастухова Н.В.

3. Настоящее постановление вступает в силу после его официального опубликования.

Глава Изобильненского муниципального
округа Ставропольского края Р.А.Коврыга

УТВЕРЖДЕНА

постановлением администрации
Изобильненского муниципального
округа Ставропольского края
от 20 марта 2026 г. № 499

ПОЛИТИКА ЗАЩИТЫ ИНФОРМАЦИИ
в администрации Изобильненского муниципального округа Ставропольского края

I. Общие положения

Политика защиты информации (далее – Политика ЗИ) определяет принятие правовых, организационных и технических мер, которыми руководствуется администрация Изобильненского муниципального округа Ставропольского края (далее – администрация ИМО СК), в своей деятельности, направленной на:

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

соблюдение конфиденциальности информации ограниченного доступа;

реализацию права на доступ к информации.

Основными составными элементами Политики ЗИ являются:

защита информации при организации работ с персональными данными;

защита информации, не составляющей государственную тайну, в автоматизированных и информационных системах;

защита информации с ограниченным доступом, не составляющей государственную тайну, с использованием средств криптографической защиты информации;

защита информации, размещаемой на официальном сайте администрации ИМО СК в информационно-телекоммуникационной сети Интернет.

Общее руководство обеспечением защиты информации в администрации ИМО СК осуществляет Глава Изобильненского муниципального округа Ставропольского края, непосредственное руководство обеспечением защиты информации в аппарате администрации ИМО СК возложено на отдел по информатизации, защите информации и информационной политике. Выполнение обязанностей по обеспечению информационной безопасности и защите информации, а также осуществление контроля за соблюдением требований по защите информации в аппарате администрации ИМО СК возлагается на консультанта отдела по информатизации, защите информации и информационной политике администрации ИМО СК распоряжением администрации Изобильненского муниципального округа Ставропольского края.

II. Область применения

Настоящая Политика ЗИ распространяется на аппарат администрации ИМО СК и обязательна к исполнению всеми работниками аппарата администрации ИМО СК.

Работники аппарата администрации ИМО СК обязаны соблюдать порядок обращения с конфиденциальными документами, ключевыми носителями и другой защищаемой информацией, соблюдать требования настоящей Политики ЗИ и иных документов, регламентирующих деятельность в области защиты информации и информационной безопасности.

Действие Политики ЗИ 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.

III. Термины и определения

В настоящей Политике ЗИ используются следующие термины:

автоматизированная система - система, состоящая из персонала (работников) и комплекса средств автоматизации их деятельности, реализующая информационную технологию выполнения установленных функций;

аудит информационной безопасности администрации ИМО СК - процесс проверки выполнения установленных требований по обеспечению защиты информации. Может проводиться как самой администрацией ИМО СК (внутренний аудит), так и с привлечением независимых внешних организаций (внешний аудит);

вредоносная программа - компьютерная программа либо иная компьютерная информация, предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых актов или требованиями, устанавливаемыми собственником информации;

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 ИМО СК;

информационный технологический процесс - часть производственного технологического процесса, содержащая операции над информацией, необходимой для функционирования администрации ИМО СК;

информационная безопасность администрации ИМО СК - состояние защищенности информационных активов администрации ИМО СК в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационной безопасности конфиденциально-

стью, целостностью, доступностью информационных активов и инфраструктуры администрации ИМО СК;

информационные активы администрации ИМО СК – активы администрации ИМО СК, имеющие отношение к информационной сфере и представляющие ценность для неё с точки зрения достижения установленных целей;

инцидент информационной безопасности - действительное, предпринимаемое или вероятное нарушение информационной безопасности, приводящее к нарушению доступности, конфиденциальности и целостности информационных активов администрации ИМО СК;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечение их обработки с использованием 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 правообладателя;

мониторинг информационной безопасности администрации ИМО СК - постоянное наблюдение за объектами, влияющими на обеспечение защиты информации администрации ИМО СК, 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, предназначенных для защиты информации;

политика защиты информации администрации ИМО СК – это комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых администрацией ИМО СК 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 ИМО СК. К субъектам относятся работники администрации ИМО СК, посетители, а также инициируемые от их имени действия над объектами. Объектами являются аппаратные и программные средства, информационные ресурсы, услуги и процессы, составляющие автоматизированную систему в целом;

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 ИМО СК практику (стажировку);

угроза - опасность, предполагающая возможность потери (блокирования) информации;

управление информационной безопасностью администрации ИМО СК - совокупность целенаправленных действий по защите информации, осуществляемых в рамках настоящей Политики ЗИ в условиях угроз в информационной сфере, включающих 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 ИМО СК в целом 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.

IV. Основные принципы обеспечения защиты информации

Основными принципами обеспечения защиты информации являются:

постоянный и всесторонний анализ автоматизированных систем и информационных технологий с целью выявления уязвимостей информационных активов администрации ИМО СК;

своевременное обнаружение возникающих проблем, потенциально способных повлиять на информационную безопасность администрации ИМО СК, корректировка моделей угроз и нарушителя;

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 защиты информации, не должны усложнять деятельность

администрации ИМО СК, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности;

контроль эффективности принимаемых защитных мер;

персонификация и адекватное разделение ролей и ответственности между работниками аппарата администрации ИМО СК, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

V. Цели и задачи защиты информации

Основной целью является защита информации, содержащейся в информационных системах администрации ИМО СК от наиболее распространенных угроз информационной безопасности, вызванных неэффективностью процедур контроля, технологических сбоев, несанкционированных действий работников 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 защиты информации в администрации ИМО СК должна обеспечивать эффективное решение следующих задач, таких как:

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

укрепление вертикали управления и централизация сил обеспечения защиты информации в администрации ИМО СК;

совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения защиты информации;

обеспечение соблюдения требований законодательства Российской Федерации в области защиты информации;

организация и координация руководством администрации ИМО СК работ по обеспечению защиты информации;

возложение ответственности за обеспечение безопасности информации в информационных системах аппарата администрации ИМО СК на каждого сотрудника аппарата администрации ИМО СК в пределах его полномочий;

обеспечение непрерывного функционирования информационных систем и системы обеспечения защиты информации;

обеспечение эффективной работы механизмов оперативного реагирования на компьютерные инциденты при обеспечении защиты информации;

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 кон-

кретным пользователям для выполнения своих служебных (трудовых) обязанностей), то есть защита 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 защиты информации;

создание системы непрерывного обучения, тренировки и проверки осведомленности сотрудников аппарата администрации ИМО СК по вопросам обеспечения защиты информации;

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 защиты информации 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 защиты информации;

подготовкой работников, ответственных за организацию и осуществление мероприятий по обеспечению защиты информации;

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

персональной ответственностью за свои действия каждого работника аппарата администрации ИМО СК, имеющего доступ к информационным ресурсам, в рамках выполнения своих трудовых обязанностей;

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

VI. Объекты обеспечения защиты информации

К объектам для обеспечения защиты информации 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 для защиты информации 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.

Специализированная защита всех вышеуказанных объектов создаст условия для надежного функционирования администрации ИМО СК.

VII. Основные направления деятельности администрации ИМО СК по обеспечению защиты информации

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

К основным направлениям обеспечения защиты информации относятся:

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

организация деятельности по обеспечению защиты информации – деятельность направлена на создание документированных процессов обеспечения информационной безопасности аппарата администрации ИМО СК;

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

обеспечение защиты информации, связанной с сотрудниками аппарата администрации ИМО СК – деятельность направлена на минимизацию рисков, вызванных действиями сотрудников в отношении информационных ресурсов, путем создания системы непрерывного обучения, тренировки и проверки осведомленности всех сотрудников аппарата администрации ИМО СК 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 защиты информации на всех 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 правовых актов по обеспечению информационной безопасности и защиты информации.

VIII. Принципы формирования системы обеспечения защиты информации

Построение системы обеспечения защиты информации и её функционирование осуществляется в соответствии с основными принципами формирования системы обеспечения информационной безопасности.

К основным принципам формирования системы обеспечения защиты информации относятся:

законность – предполагает разработку системы обеспечения защиты информации 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 защиты информации. 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 защиты информации должна быть встроена в управленческие процессы аппарата администрации ИМО СК, 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 аппарата администрации

ИМО СК в пределах его должностных полномочий за несоблюдение регламентирующих документов в области обеспечения защиты информации;

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

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

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

непрерывность – предполагает непрерывный, целенаправленный процесс по выявлению угроз информационной безопасности и принятию адекватных мер защиты информации руководством, специалистом по обеспечению безопасности и работниками аппарата администрации ИМО СК;

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 аппарата администрации ИМО СК. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственных работников за обеспечение информационной безопасности. Все сотрудники должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе;

гибкость системы защиты информации – система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления аппаратом администрации ИМО СК 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 и проблемы системы обеспечения защиты информации должны немедленно доводиться до сведения Главы Изобильненского муниципального округа Ставропольского края, а также оперативно устраняться.

IX. Модель угроз

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности и доступности).

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в её отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности её функционирования.

Модель угроз безопасности должна содержать описание информационной системы и её структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Модели угроз являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения защиты информации в аппарате администрации ИМО СК.

Источники угроз, уязвимости и объекты нападений, пригодные для реализации уязвимости, типы возможных потерь, масштабы потенциального ущерба определяются документом «Модель угроз и нарушителя», утверждаемым постановлением администрации ИМО СК.

X. Требования по обеспечению защиты информации

Обеспечение безопасности защиты 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.

В качестве методов защиты информации применяются:

1) регламентация доступа в служебные помещения аппарата администрации ИМО СК.

Регламентация доступа в служебные помещения осуществляется в целях обеспечения физической сохранности носителей информации, оборудования и исключения возможности несанкционированного доступа в служебные помещения, в том числе в которых ведется обработка конфиденциальной информации;

2) разграничение доступа к техническим средствам и информационным ресурсам аппарата администрации ИМО СК.

Разграничение доступа к техническим средствам и информационным ресурсам направлено на предотвращение получения информации, обрабатываемой в электронном виде, в том числе в информационных системах, с нарушением регламентируемых нормативными правовыми актами или владельцами информации правил, следствием которых может быть нарушение конфиденциальности, целостности и (или) доступности информации.

Для работы с информационными ресурсами работнику предоставляется автоматизированное рабочее место (далее – АРМ). Программное обеспечение устанавливается и обновляется системным администратором (специалистом) со специальных ресурсов или съемных носителей в соответствии с лицензионным соглашением. При передаче АРМ другому сотруднику производится удаление профиля (учетной записи) пользователя АРМ.

Для обеспечения безопасности информации и её защиты, 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.

К работе с информационными ресурсами допускаются работники, ознакомленные с настоящей Политикой ЗИ. Для осуществления доступа к информационным ресурсам, работнику аппарата администрации ИМО СК создается учетная запись - присваивается уникальный идентификатор (имя, логин) и пароль доступа. При увольнении учетная запись работника блокируется;

3) применение антивирусной защиты.

Антивирусная защита применяется с целью защиты информационных ресурсов и программного обеспечения (далее – ПО) от несанкционированных действий (утраты, модификации, изменения) путем внедрения в информаци-

онную среду вирусов, вредоносных программ (далее - вирус) посредством использования, специализированного ПО (далее - антивирусное ПО).

Антивирусное ПО должно быть развернуто на всех технических средствах, подверженных воздействию вирусов (АРМ, серверах). Антивирусные механизмы должны быть актуальными, постоянно включенными. Должны вестись журналы протоколирования событий. Отключение антивирусного ПО или отказ от автоматического обновления антивирусных баз не допускается;

4) применение криптографической защиты информации.

Криптографическая защита информации (шифрование) применяется для защиты информации при передаче по открытым каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи;

5) регламентация использования электронной почты.

Система электронной почты используется в информационных целях, в том числе оповещения, организации работы, обеспечения внутренних и внешних коммуникаций. Регламентация использования электронной почты осуществляется с целью снижения риска умышленной или неумышленной несанкционированной рассылки информации, заражения информационных ресурсов вирусами.

Угрозы, связанные с электронной почтой:

возможность создания писем с фальшивыми адресами;

возможность нарушения конфиденциальности электронных писем;

возможность изменения в процессе передачи содержимого электронных писем;

осуществление сетевых атак посредством отправки упакованного в архив сообщения, распаковка которого приводит к выводу системы из строя, заражению вирусами;

получение спама.

Отправка, получение официальных запросов и ответов в целях исполнения своих функций работниками аппарата администрации ИМО СК осуществляется с использованием официальных адресов электронной почты.

Перечень официальных адресов электронной почты аппарата администрации ИМО СК утверждается распоряжением администрации ИМО СК.

Официальный адрес электронной почты размещается на официальном портале органов местного самоуправления ИМО СК в информационно-телекоммуникационной сети Интернет, на бланках администрации ИМО СК.

Отправка, и получение электронных сообщений в целях исполнения должностных обязанностей работником, осуществляется с использованием корпоративного электронного адреса, присвоенного каждому отделу аппарата администрации ИМО СК.

При работе с электронной почтой работники обязаны:

перед отправкой тщательно проверять сообщения на отсутствие информации ограниченного доступа;

периодически удалять из электронного почтового ящика ненужные сообщения и перемещать необходимые сообщения в архивные почтовые папки;

проверять сообщения электронной почты на наличие вирусов;

При работе с электронной почтой работнику запрещено:

осуществлять действия, запрещенные законодательством Российской Федерации;

отправлять конфиденциальную информацию по открытым каналам связи;

отправлять сообщения с иного электронного почтового ящика или от имени другого сотрудника без предоставления полномочий;

использовать электронную почту для создания, отправки, пересылки или хранения любых подрывных, оскорбительных, неэтичных, незаконных материалов, включая оскорбительные комментарии по поводу расы, пола, цвета, инвалидности, возраста, сексуальной ориентации, порнографии, терроризма, религиозных убеждений и верований, политических убеждений, национального происхождения, гиперссылок или других ссылок на веб-сайты, содержащие указанные материалы, массовые рассылки спама;

рассылать компьютерные коды, файлы или ПО, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования, вирусы или другое злонамеренное ПО, программы для осуществления несанкционированного доступа, серийные номера к программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети Интернет, ссылки на указанную информацию;

самостоятельно устанавливать на АРМ дополнительное ПО, полученное в сети Интернет;

перехватывать, изменять, удалять, сохранять или публиковать сообщения иных сотрудников, кроме случаев, санкционированных руководителями, или в целях администрирования систем;

открывать страницы сайтов, если имеются сомнения в надежности сайта и (или) имеются уведомления о возможном заражении вирусами;

передавать информацию, обрабатываемую в администрации ИМО СК, посредством иностранных интернет-сервисов, в том числе систем обмена мгновенными сообщениями, голосовой и видеоинформацией (ICQ, QIP, Jabber, Viber, WhatsApp, Skype и другие), социальных сетей (Twitter, Facebook, LiveJournal и другие), облачных сервисов (iCloud, Google Drive, Dropbox и другие).

использовать веб-сервисы Google, Gmail, Hotmail, Yahoo, Яндекс или подобные почтовые системы третьих сторон («вебмайл») для отправки и (или) получения служебной корреспонденции;

загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным ПО, переходить по активным ссылкам, полученным от отправителей, если имеются сомнения в надежности отправителя и (или) полученного сообщения.

Содержимое электронного почтового ящика работника может быть проверено системным администратором (специалистом по защите информации) без предварительного уведомления сотрудника в случае подозрения на осуществление рассылки писем, содержащих вредоносное ПО, спам, информацию, распространение которой запрещено правовыми актами. Информация о выявленных нарушениях направляется работнику и его руководителю.

6) регламентация работы в сети Интернет.

Сеть Интернет используется сотрудниками для получения информации в рамках исполнения должностных обязанностей.

Регламентация работы в сети Интернет осуществляется с целью снижения риска заражения информационных ресурсов вирусами.

Доступ к сети Интернет предоставляется работнику с автоматизированного рабочего места, закрепленного за работником для исполнения должностных обязанностей, с использованием учетной записи работника.

Угрозы, связанные с работой в сети Интернет:

легкость перехвата данных и фальсификации IP-адресов в сети Интернет;

заражение вирусами.

Работники аппарата администрации ИМО СК обязаны при обнаружении попыток несанкционированного доступа и (или) при подозрении на наличие вируса немедленно прекратить работу в сети Интернет и сообщить системному администратору (специалисту по защите информации).

Вся информация об информационных ресурсах, посещаемых работником ИМО СК, автоматически протоколируется и при необходимости предоставляется системным администратором (специалистом по защите информации) начальнику отдела по информатизации, защите информации и информационной политике администрации ИМО СК.

Доступ к сети Интернет может быть блокирован системным администратором (специалистом по защите информации) без предварительного уведомления работника при возникновении угрозы безопасности информации.

7) регламентация создания и эксплуатации информационных систем.

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

Срок начала эксплуатации системы не может быть ранее срока окончания последнего мероприятия, предусмотренного правовым актом о вводе системы в эксплуатацию.

Пользователи (работники) осуществляют эксплуатацию системы в соответствии с рабочей документацией.

XI. Ответственные за обеспечение защиты информации в аппарате администрации ИМО СК

Непосредственное руководство обеспечением защиты информации в аппарате администрации ИМО СК возложено на отдел по информатизации, защите информации и информационной политике. Выполнение обязанностей по обеспечению информационной безопасности и защите информации, а также осуществление контроля за соблюдением требований по защите информации в аппарате администрации ИМО СК возлагается на консультанта отдела по информатизации, защите информации и информационной политике администрации ИМО СК распоряжением администрации Изобильненского муниципального округа СК.

На данного работника возлагается решение следующих основных задач:

анализ текущего состояния обеспечения информационной безопасности и защиты информации;

организация мероприятий и координация работ по обеспечению информационной безопасности и защиты информации;

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

Основные функции работника по обеспечению информационной безопасности и защиты информации заключаются в следующем:

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

участие в проектировании системы обеспечения информационной безопасности и защиты информации, её испытаниях и вводе в эксплуатацию;

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

обучение пользователей и работников аппарата администрации ИМО СК правилам обработки информации;

оказание методической помощи работникам аппарата администрации ИМО СК в вопросах обеспечения информационной безопасности и защиты информации;

контроль за соблюдением пользователями и работниками аппарата администрации ИМО СК установленных правил обращения с конфиденциальной информацией;

организация по указанию руководства администрации ИМО СК 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 и защиты информации.

XII. Основные организационные, технические и правовые меры обеспечения защиты информации

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

12.1. 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 и защиты информации 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 работниками аппарата администрации ИМО СК.

12.2. Организационные меры обеспечения безопасности информационных систем и защиты информации.

К организационным мерам обеспечения безопасности информационных систем и защиты информации относятся 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.

При работе с документами, распечатанными на бумажном носителе необходимо придерживаться следующих правил:

держать в (на) столе только те документы, которые необходимы для работы в настоящий момент;

не оставлять документы на столе, если работник покидает рабочее место. Документы необходимо убирать в ящик стола или в соответствующие папки, сейф;

при работе с документами, содержащими информацию ограниченного доступа необходимо убирать их в сейф, если сотрудник отходит от рабочего места;

запрещается записывать пароли, в том числе на доступ к информационной системе, на бумажном носителе информации, за исключением случаев, когда запись может храниться безопасно, а метод хранения был утвержден нормативно - правовым актом администрации ИМО СК.

При работе с документами в электронном виде необходимо придерживаться следующих правил:

всегда блокировать (Win+L) рабочий стол при выходе из-за рабочего места даже на непродолжительное время;

устанавливать монитор таким образом, чтобы его изображение не было видно от входной двери;

установить автоматическую блокировку экрана через 10 минут простоя (установив хранитель экрана (Screen Saver) и поставить галочку «Запрашивать пароль» или «Начинать с экрана вход в систему»);

минимизировать заполнение рабочего стола ярлыками программ и папок, не размещать документы на рабочем столе;

не хранить на рабочем столе информацию, содержащую коммерческую тайну, информацию для служебного пользования, персональные данные коллег по работе, клиентов, пароли для входа в систему;

использовать фоны рабочего стола, содержащие общие требования (рекомендации) по информационной безопасности.

12.3. 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 Федеральной службы по техническому и экспортному контролю России (www.fstec.ru).

Применение организационных и технических мер защиты информации, в зависимости от угроз безопасности информации, 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 ИМО СК необходимо ориентироваться на выбор отечественного программного и информационно-телекоммуникационного оборудования, соответствующего требованиям информационной безопасности, что также текущему курсу импортозамещения Правительства Российской Федерации.

12.4. Криптографические методы и средства защиты.

Криптографические методы и средства защиты (далее – СКЗИ) используются для обеспечения информационной безопасности.

Организация системы информационной безопасности на основе инфраструктуры с использованием СКЗИ позволит решать следующие задачи:

организацию 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;

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

универсализацию методов обеспечения доступа пользователей и защиты для системы электронной почты, системы доступа по информационно-телекоммуникационным сетям общего пользования 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 не криптографических 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.

12.5. 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.

XIII. 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:

1) первичный анализ инцидента;

2) комплексный анализ инцидента;

3) локализацию инцидента;

4) сбор сведений для последующего установления причин инцидента;

5) планирование мер по ликвидации последствий инцидента;

6) ликвидацию последствий инцидента;

7) контроль ликвидации последствий.

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

XIV. Обучение работников аппарата администрации ИМО СК и повышение осведомленности в вопросах обеспечения информационной безопасности и защиты информации

Все работники аппарата администрации ИМО СК при использовании информационной системы должны быть ознакомлены с организационно-распорядительными документами по обеспечению информационной безопасности и защиты информации в части, их касающейся, а также 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 роспись.

Пользователи информационной системы, а также работники аппарата администрации ИМО СК 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 работников аппарата администрации ИМО СК 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, преследуемые при повышении осведомленности работников аппарата администрации ИМО СК в вопросах информационной безопасности и защиты информации:

информирование работников аппарата администрации ИМО СК 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 и защиты информации;

доведение до работников аппарата администрации ИМО СК основных положений, ограничений и требований существующих нормативно-распорядительных документов, принятых в администрации ИМО СК;

выработка у работников аппарата администрации ИМО СК умения оценивать возможные последствия своих действий (адекватно оценивать связанные с ними риски информационной безопасности);

выработка у работников аппарата администрации ИМО СК привычек, способствующих поддержанию высокого уровня информационной безопасности;

выработка у работников аппарата администрации ИМО СК умений (навыков) правильно и оперативно действовать при возникновении инцидентов информационной безопасности;

доведение до работников аппарата администрации ИМО СК 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 и защите информации в целом.

Формы и методы, используемые для повышения осведомленности работников аппарата администрации ИМО СК в области информационной безопасности и защиты информации:

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 настоящей Политики ЗИ.

Правила допуска к работе с информационными ресурсами, конфиденциальной информацией лиц, не являющихся работниками администрации ИМО СК, определяются на договорной основе с этими лицами или с организациями, представителями которых являются эти лица.

XV. Контроль состояния информационной безопасности и защиты информации

Контроль состояния информационной безопасности и защиты информации 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 проводится консультантом отдела по информатизации, защите информации и информационной политике администрации ИМО СК и комиссией, назначаемой в аппарате администрации ИМО СК для этой цели.

Оценка эффективности мер защиты информации проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

Мероприятия по контролю конфигураций информационных систем должны исключать несанкционированное изменение состава программных, программно-аппаратных средств информационных систем, их настроек и конфигураций, установленных во внутренних стандартах по защите информации, а также обеспечивать обнаружение фактов несанкционированных изменений и выявление причин изменений.

Бесконтрольная установка обновлений программных, программно-аппаратных средств не допускается.

Контроль обработки и хранения информации ограниченного доступа в программно-аппаратных средствах и ее передачи осуществляется в соответствии с внутренним регламентом по защите информации. О фактах неправомерного распространения информации ограниченного доступа и (или) доступа к средствам ее обработки и хранения должен быть незамедлительно проинформирован Глава Изобильненского муниципального округа Ставропольского края и начальник отдела по информатизации, защите информации и информационной политике администрации ИМО СК.

Контроль использования мобильных устройств должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

При применении пользователями и работниками аппарата администрации ИМО СК мобильных устройств для доступа к информационным системам и содержащейся в них информации, не связанного с выполнением работником своих обязанностей (функций), в том числе для доступа к общедоступной информации, консультантом отдела по информатизации, защите информации и информационной политике администрации ИМО СК должны приниматься меры по защите информационных систем и содержащейся в них информации и, при необходимости, обеспечиваться защита каналов передачи данных, используемых для осуществления доступа.

Контроль удаленного доступа пользователей к информационным системам должен осуществляться в соответствии с внутренними стандартами и регламентами по защите информации.

Точки беспроводного доступа и построенные на их основе беспроводные сети связи, используемые для доступа работников аппарата администрации ИМО СК к информационным системам и содержащейся в них информации в целях выполнения ими своих обязанностей (функций), должны быть изолированы от беспроводных сетей связи, предназначенных для доступа к сети «Интернет» и (или) общедоступной информации, находящейся в информационной системе администрации ИМО СК.

Порядок создания, учета, изменения и блокирования, контроля и удаления привилегированных учетных записей устанавливается внутренним регламентом по защите информации в аппарате администрации ИМО СК.

Требования к применяемым моделям доступа пользователей устанавливаются внутренним стандартом по защите информации в аппарате администрации ИМО СК.

Физический доступ к программно-аппаратным средствам информационных систем, предназначенным для обработки и хранения информации, должен быть предоставлен только тем пользователям, которым указанный доступ необходим для выполнения возложенных на них обязанностей (функций). Программно - аппаратные средства информационных систем, предназначенные для хранения информации, должны быть установлены в помещениях (зонах помещений, шкафах, футлярах, корпусах), несанкционированный физический доступ в которые должен быть исключен.

Контроль физического доступа к программно-аппаратным средствам обработки и хранения информации ограниченного доступа и (или) в помещения (зоны помещений, шкафы, футляры, корпуса), в которых они установлены, должен осуществляться в соответствии с внутренними регламентами по защите информации.

Съемные машинные носители информации, разрешенные для использования в информационных системах, подлежат учету и контролю использования. В информационных системах должны использоваться съемные машинные носители информации, выдаваемые консультантом отдела по информатизации, защите информации и информационной политике администрации ИМО СК.

В случае обнаружения работником съемного машинного носителя информации, принадлежность которого или владельца которого установить не удалось, такой съемный машинный носитель информации должен быть передан консультанту отдела по информатизации, защите информации и информационной политике администрации ИМО СК для анализа содержащейся на нем информации, программ и при необходимости, дальнейшего уничтожения. Подключение обнаруженного съемного машинного носителя информации к информационным системам в аппарате администрации ИМО СК запрещается.

Разработка (развитие) и (или) тестирование программного обеспечения подрядными организациями непосредственно в эксплуатируемых информационных системах аппарата администрации ИМО СК не допускается.

Для проведения работ по разработке (развитию) и (или) тестированию программного обеспечения работникам подрядных организаций должен быть предоставлен доступ к выделенным для проведения таких работ стендам разработки и (или) тестирования, которые должны быть изолированы от эксплуатируемых информационных систем аппарата администрации ИМО СК.

Контроль доступа подрядных организаций к стендам разработки (развития) и (или) тестирования должен осуществляться в соответствии с внутренним регламентом по защите информации в аппарате администрации ИМО СК.

Обеспечение доступности из сети «Интернет» интерфейсов и сервисов информационных систем, подлежащих защите от компьютерных атак, направленных на отказ в обслуживании, должно осуществляться в соответствии с внутренним регламентом по защите информации в аппарате администрации ИМО СК после принятия мер по контролю и фильтрации исходящего и входящего сетевого трафика в соответствии с перечнем ресурсов сети «Интернет», с которыми может взаимодействовать информационная система, включающим исходящий и входящий сетевые потоки, их характеристики и используемые протоколы.

Посредством проведения мероприятий по обеспечению защиты информации при использовании для функционирования информационных систем искусственного интеллекта, должна быть обеспечена возможность исключения несанкционированного доступа к информации или воздействия на информационные системы, несанкционированного распространения и модификации информации, а также использования информационных систем не по их назначению за счет воздействия на наборы данных, применяемые модели искусственного интеллекта и их параметры, процессы и сервисы по обработке данных и поиску решений.

Не допускается передача лицу, разработавшему модель искусственного интеллекта, информации ограниченного доступа, содержащейся в информационных системах, в том числе для улучшения функционирования модели искусственного интеллекта.

При использовании в информационных системах искусственного интеллекта или сервисов на основе искусственного интеллекта должно быть исключено нерегламентированное влияние искусственного интеллекта на параметры модели искусственного интеллекта и на функционирование информационных систем.

В информационных системах должны быть реализованы следующие базовые меры защиты информационных систем и содержащейся в них информации:

а) идентификация и аутентификация;

б) управление доступом;

в) регистрация событий безопасности;

г) защита виртуализации и облачных вычислений;

д) защита технологий контейнерных сред и их оркестрации;

е) защита сервисов электронной почты;

ж) защита веб-технологий;

з) защита программных интерфейсов взаимодействия приложений;

и) защита конечных устройств;

к) защита мобильных устройств;

л) защита технологий интернета вещей;

м) защита точек беспроводного доступа;

н) антивирусная защита;

о) обнаружение и предотвращение вторжений на сетевом уровне;

п) сегментация и межсетевое экранирование;

р) защита от компьютерных атак, направленных на отказ в обслуживании;

с) защита каналов передачи данных и сетевого взаимодействия.

Контроль уровня защищенности информации в аппарате администрации ИМО СК должен проводиться не реже одного раза в три года или после компьютерного инцидента, произошедшего в аппарате администрации ИМО СК. Методы контроля уровня защищенности информации и периодичность его проведения определяются администрацией ИМО СК во внутреннем регламенте.

По результатам проведения контроля уровня защищенности информации разрабатывается отчет, который подписывается лицами, проводившими контроль.

Отчет должен быть представлен в течение 3 рабочих дней с даты завершения контроля уровня защищенности информации заместителю главы администрации, курирующему данное направление деятельности, для последующего доклада Главе Изобильненского муниципального округа Ставропольского края для принятия при необходимости решения о выделении ресурсов с целью повышения уровня защищенности информации в аппарате администрации ИМО СК.

Отчет направляется администрацией ИМО СК в Федеральную службу по техническому контролю и экспертному контролю России в течение 5 рабочих дней с даты завершения контроля уровня защищенности информации в целях мониторинга текущего состояния технической защиты информации.

XVI. Ответственность за нарушение Политики защиты информации в администрации ИМО СК

Ответственность за невыполнение требований Политики ЗИ в администрации ИМО СК несет каждый работник аппарата администрации ИМО СК в рамках своих служебных обязанностей и полномочий.

На основании статьи 192 Трудового кодекса Российской Федерации к работникам, нарушающим требования Политики ЗИ аппарата администрации ИМО СК, могут быть применены меры дисциплинарного взыскания.

Все работники аппарата администрации ИМО СК несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный администрации ИМО СК в результате нарушения ими правил Политики ЗИ (статьи 238 Трудового кодекса Российской Федерации).

За умышленное причинение ущерба, а также за разглашение сведений, составляющих охраняемую законом тайну (служебную, коммерческую или иную), в случаях, предусмотренных федеральными законами, работники аппарата администрации ИМО СК несут материальную ответственность в полном размере причиненного ущерба (статьи 243 Трудового кодекса Российской Федерации).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ, уничтожение, блокирование или модификация защищаемой информации, работники аппарата администрации ИМО СК несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.