Архангельская область
Приморский район
Муниципальное образование «Приморское»
Администрация

Распоряжение

от 27 февраля 2017 г. № 8

дер. Рикасиха

Об утверждении
политики информационной безопасности администрации
муниципального образования «Приморское»

В связи с проведением организационно-технических мероприятий в администрации муниципального образования «Приморское» по приведению в соответствие с требованиями законодательства по защите информации и в целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» процедур защиты, сбора, обработки и хранения информации и персональных данных:

1. Утвердить прилагаемую политику информационной безопасности администрации муниципального образования «Приморское» (далее – Политика).
2. Разместить настоящее распоряжение на официальном информационном сайте администрации муниципального образования «Приморское».

Глава муниципального образования А.В. Семенова

УТВЕРЖДЕНО
распоряжением администрации
муниципального образования
«Приморское»

от « 27 » февраля 2017 г. № 8

ПОЛИТИКА

информационной безопасности

администрации
муниципального образования
«Приморское»

дер. Рикасиха
2017 год

Содержание

1. Введение

Политика информационной безопасности (далее – Политика) администрации муниципального образования «Приморское» (далее – местная администрация) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется местная администрация в своей деятельности.

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

Общее руководство обеспечением информационной безопасности местной администрации осуществляет Глава муниципального образования.

Контроль за соблюдением требований по информационной безопасности несет комиссия по организации работ по защите персональных данных администрации муниципального образования «Приморское» (далее – комиссия).

Работники местной 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 обязательна к исполнению всеми работниками и ответственными лицами администрации муниципального образования «Приморское». Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах местной администрации, а также в договорах.

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 местной администрации - процесс проверки выполнения установленных требований по обеспечению информационной безопасности. Может проводиться как самой местной 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 местной администрации.

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

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

Информационные активы местной администрации - активы местной 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 местной администрации.

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

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

Мониторинг информационной безопасности местной администрации - постоянное наблюдение за объектами, влияющими на обеспечение информационной безопасности местной 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 местной администрации - комплекс взаимоувязанных руководящих принципов и разработанных на их основе правил, процедур и практических приемов, принятых местной 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 местной администрации. К субъектам относятся персонал местной 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), позволяющие местной администрации при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов и реализующие меры по охране конфиденциальной 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 местной администрации практику (стажировку).

Средство криптографической защиты информации - средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Угроза **- о**пасность, предполагающая возможность потерь (ущерба).

Управление информационной безопасностью местной 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 местной администрации при реализации угроз в информационной сфере.

Электронная подпись (Электронная цифровая 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. Обозначения и сокращения

АС - автоматизированная система;
АСП - аналог собственноручной подписи
ИБ - информационная безопасность;
ИС - информационная система;
ИСПДн – информационная система персональных данных
ЛВС - локальная вычислительная сеть;
НСД - несанкционированный доступ;
ОС - операционная система;
РФ - Российская Федерация;
СКЗИ - средство криптографической защиты информации;
СУБД - система управления базами данных;
ЭВМ - электронная вычислительная машина;
ЭЦП - электронная цифровая подпись.

5. Нормативные ссылки

Настоящая Политика разработана с учетом следующих документов:

- Федеральный закон от 27 июля 2006 № 149-ФЗ "Об информации, информационных технологиях и защите информации";
- Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 17 марта 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;
- Постановление Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня 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»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспертному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержание

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденные приказом Гостехкомиссии от 30 августа 2002 года № 282.

6. Исходная концептуальная схема обеспечения ИБ

6.1. Концептуальная схема ИБ местной администрации направлена на защиту ее информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

6.2. Наибольшими возможностями для нанесения ущерба местной администрации обладает ее собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне местной администрации), либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

6.3. Для противодействия угрозам ИБ местной администрации на основе имеющегося опыта составляется модель предполагаемых угроз. Чем точнее сделан прогноз (составлена модель угроз), тем ниже риски нарушения ИБ местной администрации при минимальных ресурсных затратах.

6.4. Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз.

6.5. Стратегия обеспечения ИБ местной администрации заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала местной администрации и других пользователей АС.

7. Основные принципы обеспечения ИБ

Основными принципами обеспечения ИБ являются:

7.1. Постоянный и всесторонний анализ АС и информационных технологий с целью выявления уязвимостей информационных активов местной администрации.

7.2. Своевременное обнаружение проблем, потенциально способных повлиять на ИБ местной администрации, корректировка моделей угроз.

7.3. 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 достижение уставных целей местной администрации, а также повышать трудоемкость технологических процессов обработки информации и создавать дополнительные сложности.

7.4. Контроль эффективности принимаемых защитных мер.

7.5. Персонификация и адекватное разделение ролей и ответственности между работниками местной администрации, исходя из принципа персональной и единоличной ответственности за совершаемые операции.

8. Цели и задачи ИБ

8.1. Основными целями ИБ местной администрации являются:

- повышение стабильности функционирования местной администрации в целом;
- достижение адекватности мер по защите от реальных угроз ИБ;
- предотвращение или снижение ущерба от инцидентов ИБ.

8.2. Основными задачами деятельности по обеспечению ИБ местной администрации являются:

- выполнение требований действующего законодательства РФ по обеспечению ИБ;
- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ с учетом требований системы менеджмента качества;
- разработка и совершенствование организационно-распорядительных документов местной администрации в области обеспечения ИБ;
- выявление, оценка и прогнозирование угроз ИБ;
- выработка рекомендаций по устранению уязвимостей;
- организация антивирусной защиты информационных активов;
- защита информации от НСД и утечки по техническим каналам связи.

9. Объекты защиты

9.1. Объектами защиты информации местной администрации являются:

- управленческий процесс;
- межведомственное взаимодействие;
- финансово-экономическая информация;
- информационный технологический процесс;

- персональные данные;
- различного рода носители защищаемой информации, в том числе информационные ресурсы, документы на бумажных и машинных носителях, определенные как защищаемые.

9.2. Защищаемая информация делится на следующие виды:

- информация, составляющая коммерческую тайну (научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны);
- персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
- иная информация, не относящаяся ни к одному из указанных выше видов, которая определена как защищаемая в соответствии с нормативно-правовыми актами РФ.

Защищаемая информация определяется «Перечнем информации, содержащей сведения конфиденциального характера» местной администрации.

10. Модели угроз

10.1. Модели угроз являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения ИБ местной администрации.

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

11. Требования по обеспечению ИБ

11.1. Общие требования по обеспечению ИБ формулируются для следующих областей:

- назначение и распределение ролей и доверия к персоналу;
- стадии жизненного цикла АС;
- эксплуатации АС;
- защита информационных технологических процессов;
- защита от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи.

11.2. Требования по обеспечению ИБ при назначении и распределении ролей и обеспечении доверия к персоналу местной администрации:

11.2.1. Для эффективного выполнения целей местной администрации и задач по управлению активами определяются соответствующие роли персонала местной администрации. Роли определяются исходя из задач, функциональных и процедурных требований, и обеспечиваются соответствующими ресурсами. Роли персонифицируются с установлением ответственности за их исполнение. Ответственность фиксируется в должностных инструкциях.

11.2.2. С целью снижения рисков нарушения ИБ не рекомендуется, в рамках одной роли совмещать следующие функции:

- разработки и сопровождения системы или программного обеспечения;
- разработки и эксплуатации системы или программного обеспечения;
- сопровождения и эксплуатации системы или программного обеспечения;
- администратора системы и администратора ИБ системы;
- выполнения операций в системе и контроля их выполнения.

11.2.3. Контроль за исполнением требований ИБ осуществляется комиссией.

11.2.4. Персонал местной администрации, а также лица, принимаемые на работу по срочным трудовым договорам и для прохождения практики (стажировки), подписывают обязательство о неразглашении конфиденциальной информации.

11.2.5. Компетентность персонала местной администрации в области обеспечения ИБ достигается с помощью обучения правилам безопасной (с точки зрения ИБ) работы, изучения соответствующих регламентирующих документов, осведомленности персонала об источниках потенциальных угроз и уязвимостях, а также периодических проверок его знаний и навыков.

11.2.6. Обязанности персонала по выполнению требований ИБ включаются в трудовые контракты (соглашения, договоры, должностные инструкции).

11.3. Требования по обеспечению ИБ АС местной администрации на стадиях жизненного цикла:

11.3.1. ИБ АС должна обеспечиваться на всех стадиях жизненного цикла АС, автоматизирующих технологические и управленческие процессы местной администрации, с учетом всех сторон, вовлеченных в процессы жизненного цикла АС.

11.3.2. Ввод в действие и снятие с эксплуатации СКЗИ, средств защиты от НСД АС осуществляется при участии работников ответственных за ИБ.

11.4. Требования по обеспечению ИБ при эксплуатации АС:

11.4.1. Разграничение прав доступа ролей пользователей;

11.4.2. Соблюдение документов по парольной, антивирусной защите и резервному копированию;

11.4.3. Использование в составе АС только сертифицированных или разрешенных к применению средств защиты информации.

11.4.4. Соблюдение организационно-технической документации АС;

11.4.5. Соблюдение документов по обеспечению информационной безопасности при использовании ресурсов международной сети Интернет.

11.4.6. Соблюдение документов описывающих порядок применения СКЗИ в технологических процессах местной администрации.

11.4.7. Соблюдение документов по обращению с носителями ключевой информации.

Контроль за исполнением п. 11.4.1-11.4.7 выполняется ответственным за ИБ.

11.5. Требования по обеспечению ИБ информационных технологических процессов местной администрации:

11.5.1. Система обеспечения ИБ информационного технологического процесса местной администрации строится в соответствии с требованиями пунктов 11.2 - 11.4 настоящей Политики и иных нормативных документов по вопросам ИБ.

11.5.2. Информационный технологический процесс местной администрации определяется в Положениях, Регламентах и других нормативно-методических документах местной администрации.

11.5.3. Работники местной администрации, в том числе администраторы АС и администраторы ИБ, не должны обладать всей полнотой полномочий для бесконтрольного создания, уничтожения и изменения информации, а также проведения операций по изменению состояния записей в базах данных.

11.5.4. Результаты технологических операций по обработке информации контролируются и удостоверяются ответственными лицами или автоматизированными процессами. Ответственные лица или автоматизированные процессы, осуществляющие обработку информации и контроль (проверку) результатов обработки, не зависят друг от друга.

11.5.5. При работе с информацией должны проводиться контроль целостности данной информации.

11.5.6. Обязанности по администрированию доступа пользователей к информации, передаваемой по электронным каналам связи, возлагаются на администраторов соответствующих ИС с отражением этих функций в их должностных инструкциях.

11.5.7. Комплекс мер по обеспечению ИБ технологического процесса местной администрации должен предусматривать:

- защиту информации от искажения, фальсификации, переадресации, несанкционированного доступа и(или) уничтожения;
- минимально необходимый, гарантированный доступ работника местной администрации только к тем ресурсам информационного технологического процесса, которые необходимы ему для исполнения служебных обязанностей или реализации прав, предусмотренных технологией обработки информации;
- контроль исполнения установленной технологии подготовки, обработки, передачи и хранения информации;

- восстановление информации в случае ее умышленного или случайного разрушения (искажения) или выхода из строя средств вычислительной техники;
- гарантированную доставку сообщений местной администрации информационного обмена.

11.5.8. Требования по обеспечению защиты от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи местной администрации описаны в документах определяющих общий порядок резервного копирования и восстановления. Для каждой АС может быть разработана отдельная организационно-техническая документация, описывающая порядок защиты и восстановления при аварийных ситуациях.

11.5.9. При возникновении аварийной ситуации работники местной администрации должны действовать в соответствии с документами п. 11.5.2.

12. Общие требования по обработке персональных данных

12.1. Местной администрацией должен быть определен и документально зафиксирован перечень ИСПДн.

12.2. Для каждой ИСПДн местной администрации должны быть определены и документально зафиксированы:

- цель обработки персональных данных в ИСПДн;
- объем и содержание персональных данных, обрабатываемых в ИСПДн;
- перечень действий с персональными данными и способы обработки персональных данных в ИСПДн.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных данных должны соответствовать действующему законодательству РФ.

12.3. Информационные технологические процессы, в рамках которых обрабатываются персональные данные в ИСПДн, должны быть документированы.

12.4. Местной администрации должен быть определен и документально зафиксирован перечень (список) работников, осуществляющих обработку персональных данных в ИСПДн, либо имеющих доступ к персональным данным. Доступ работников к персональным данным и обработка персональных данных работниками местной администрации должны осуществляться только для выполнения их должностных обязанностей.

12.5. Работники местной администрации, осуществляющие обработку персональных данных в ИСПДн, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также должны быть ознакомлены под роспись со всей совокупностью требований по обработке и обеспечению безопасности персональных данных в части касающихся их должностных обязанностей.

12.6. Местной администрации должен быть определен и документально зафиксирован порядок доступа работников в помещения, в которых ведется обработка персональных данных.

12.7. Местной администрацией должен быть определен и документально зафиксирован порядок хранения материальных носителей персональных данных, устанавливающий:

- места хранения материальных носителей персональных данных;
- требования по обеспечению безопасности персональных данных;
- работников, ответственных за реализацию требований по обеспечению безопасности персональных данных;
- порядок контроля выполнения требований по обеспечению безопасности персональных данных.

12.8. При использовании местной администрацией типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования установленные «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15 сентября 2008 года № 687.

13. Управление информационной безопасностью, распределение функций по обеспечению ИБ между ответственными лицами

13.1. Управление информационной безопасностью местной администрации включает в себя:

- актуализацию настоящей Политики;
- разработку регламентирующих и методических документов обеспечения ИБ;
- осуществление контроля (мониторинга) функционирования системы ИБ;
- обучение с целью поддержки (повышения) квалификации персонала местной администрации;
- оценку рисков, связанных с нарушениями ИБ.

13.2. Распределение функций по обеспечению ИБ между ответственными работниками:

13.2.1. Основными функциями по обеспечению ИБ являются:

- разработка технических, организационных и административных планов реализации политики ИБ;
- проведение единой технической политики, организация и координация работ по защите информации;
- участие в согласовании проектов всех внутренних документов, затрагивающих вопросы безопасности технологий, используемых местной администрации;

- подготовка рекомендаций по выбору средств защиты информации;
- администрирование средств защиты информации местной администрации в части обеспечения работоспособности прикладного программного обеспечения и их обновления;
- участие в обеспечении бесперебойной работы АС местной администрации и восстановлении её работы после сбоев;
- обучение пользователей безопасной работе с информационными активами;
- контроль соблюдения требований по использованию антивирусных средств;
- участие в расследовании событий, связанных с инцидентами ИБ, и в случае необходимости выход с предложениями по применению санкций в отношении лиц, осуществивших НСД, например, нарушивших требования инструкций, руководств и т. п. по обеспечению ИБ местной администрации;
- организация аттестации объектов по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности и/или конфиденциальности;
- организация и проведение работ по контролю эффективности проводимых мероприятий и принимаемых мер по защите информации;
- организация в установленном порядке расследования причин и условий появления нарушений в области защиты информации и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений;
- разработка предложений по организации и совершенствованию системы защиты информации;
- подготовка отчетов о состоянии работы по защите информации.

14. Аудит и самооценка ИБ

14.1. Порядок и периодичность проведения аудита ИБ местной администрации определяется главой муниципального образования на основании потребности в такой деятельности.

14.2. Внешний аудит ИБ проводится независимыми аудиторами. Цель аудита ИБ местной администрации состоит в проверке и оценке ее соответствия требованиям настоящей Политики и других нормативных актов. Внешний аудит ИБ проводится по отдельному решению главы муниципального образования.

14.3. Мониторинг ИБ проводится с целью обнаружения и регистрации отклонений защитных мер от требований ИБ и оценки полноты реализации положений Политики, инструкций и руководств по обеспечению ИБ местной администрации.

15. Порядок пересмотра Политики

15.1. Пересмотр настоящей Политики производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер к реальным условиям и текущим требованиям по защите информации.

15.2. Пересмотр Политики осуществляется комиссией.

15.3. С момента утверждения Политики главой муниципального образования, утрачивает силу предыдущая Политика.