УТВЕРЖДАЮ
исполняющий обязанности министра
цифрового и технологического
развития Сахалинской области

_____ Р.В. Чужинов
«16» июля 2024 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО РЕАЛИЗАЦИИ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

г. Южно-Сахалинск
2024

1. Термины и определения

Аттестация объекта информатизации – комплекс организационно-технических мероприятий, результатом которых является подтверждение соответствия системы защиты информации объекта информатизации требованиям безопасности информации, установленным регулятором;

Безопасность информации – состояние защищённости информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

Вредоносная компьютерная программа – программа (программное обеспечение), предназначенная для осуществления несанкционированного доступа к информации и или деструктивного воздействия на информацию или ресурсы информационной системы нарушение их целостности и/или доступности;

Государственная информационная система – федеральная информационная система или региональная информационная система, созданная на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов, в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях (ГИС);

Муниципальная информационная система – информационная система, созданная на основании решения органа местного самоуправления (МИС);

Доступ к информации – возможность получения информации и ее использования;

Доступность информации – состояние информации (ресурсов информационной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно;

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информация ограниченного доступа – информация, доступ к которой ограничен федеральными законами;

Инцидент информационной безопасности – одно или несколько нежелательных, или не ожидаемых событий информационной безопасности, которые со значительной вероятностью приводят к компрометации бизнес-операций и создают угрозы для информационной безопасности (инцидент безопасности);

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

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

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров;

Система защиты информации – совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

2. Общие положения

Настоящие Методические рекомендации по реализации организационных и технических мер защиты информации (далее – Методические рекомендации) разработаны в соответствии с пунктом 2.4.1. Решения совета по защите информации при Правительстве Сахалинской области от 27.06.2024 № 52 утвержденного Губернатором Сахалинской области В.И. Лимаренко 05.07.2024 в целях оказания методической помощи по реализации организационных и технических мер защиты информации на объектах информатизации.

Методические рекомендации могут применяться при формировании подхода к обоснованию выбора организационных и технических мер по защите информации и противодействию угрозам безопасности информации, а также выработке мер защиты от угроз безопасности информации и повышению уровня информационной безопасности организаций.

3. Состав нормативно-правовых и методических документов, устанавливающих требования по защите информации

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 21.03.2012 № 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 01.11.2012 № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных»;

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

- Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

- Приказ ФСТЭК России от 29.04.2021 № 77 «Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

- Приказ Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных»;

- Методический документ «Методика оценки угроз безопасности информации», утвержден ФСТЭК России 05.02.2021;

- Методический документ «Методика тестирования обновлений безопасности программных, программно-аппаратных средств», утвержден ФСТЭК России 28.10.2022;

- Методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств», утвержден ФСТЭК России 28.10.2022;

- Методический документ «Руководство по организации процесса управления уязвимостями в органе (организации)», утвержден ФСТЭК России 17.05.2023.

4. Принятие решения о необходимости защиты информации, содержащейся в объекте информатизации, этапы создания системы защиты информации

4.1. Проведение предварительного обследования состояния организации защиты информации организации. Определение факторов, анализ условий и осуществление выбора и обоснования требований по защите информации. На стадии обследования организации:

- изучается состав защищаемой информации и объекты защиты;
- устанавливается наличие конфиденциальной информации в разрабатываемой системе защиты информации, оценивается уровень конфиденциальности и объемы;
- определяются режимы обработки информации, состав комплекса технических средств, общесистемные программные средства и т.д.;
- анализируется возможность использования имеющихся на рынке сертифицированных средств защиты информации;
- определяется степень участия персонала, функциональных служб, специалистов и вспомогательных работников объекта информатизации в обработке информации, характер их взаимодействия между собой и со службой безопасности.

4.2. Определение типа объекта информатизации.

4.3. Определение функций защиты, обеспечивающих требуемый уровень в потенциально возможных условиях функционирования объекта информатизации.

4.4. Выявление потенциально возможных угроз информации и вероятностей их появления. Формирование на их основе модели угроз и определение уровня возможного ущерба и соответствующего уровня требований к защищенности.

4.5. Составление модели потенциально возможных нарушителей.

4.6. Выявление каналов утечки защищаемой информации и определение возможностей и основных каналов несанкционированного доступа к защищаемой информации.

4.7. Разработка политики безопасности, организационно-распорядительных документов и мероприятий по обеспечению информационной безопасности. Обоснование перечня задач защиты информации, их классификации и эффективности их реализации с точки зрения предотвращения возможных сбоев объекта информатизации.

4.8. Обоснование структуры и технологии функционирования защиты информации в организации. Определение состава технического, программного, информационного обеспечения, нормативно-методических документов и организационно-технических мероприятий по защите информации.

4.9. Моделирование системы защиты информации.

4.10. Проектирование системы защиты информации.

4.11. Тестирование системы защиты информации.

4.12. Внедрение системы защиты информации. Определение эффективности защиты информации с помощью оценки степени ее защищенности. Сравнение полученных результатов с их требуемыми значениями и анализ стоимостных затрат на обеспечение защиты.

4.13. Корректировка, уточнение, внесение необходимых изменений.

4.14. Подготовка и утверждение технической и эксплуатационной документации. Обучение пользователей правилам работы на объекте информатизации;

4.15. Эксплуатация объекта информатизации и сопровождение. Постоянный мониторинг состояния защищенности информационных ресурсов и выработка предложений по ее совершенствованию. Периодический пересмотр организационно-распорядительных документов и самой системы защиты объекта информатизации.

5. Разработка организационно-распорядительной документации

В организационно-распорядительную документацию входит:

№ п/п	Наименование	Примечание
1	Концепция создания объекта информатизации	- концепция создания объекта информатизации разрабатывается только для ГИС/МИС; - Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»
2	Приказ создания, развития, ввода в эксплуатацию или вывода из эксплуатации объекта информатизации	Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»
3	Приказ о назначении ответственного за организацию обработки персональных данных	- пункт 1 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» - часть 1 статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» - Постановление Правительства Российской Федерации от 21.03.2012 № 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»

4	Приказ о назначении ответственного (администратора) за информационную безопасность	
5	Приказ о назначении ответственного (администратора) за антивирусную защиту	
6	Приказ о создании комиссии по классификации объекта информатизации	
7	Технический паспорт на объект информатизации	Форма технического паспорта приведена в Приложении № 1 к Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, не составляющей государственную тайну, утвержденному приказом ФСТЭК России от 29.04.2021 № 77
8	Акт классификации информационной (автоматизированной) системы	- класс защищенности информационной системы определяется на основании исходных данных информационной системы и в соответствии с Приложением № 1 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11.02.2013 № 17; - форма акта классификации информационной (автоматизированной) системы приведена в Приложении № 3 к Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации, не составляющей государственную тайну, утвержденному приказом ФСТЭК России от 29.04.2021 № 77
9	Акт определения уровня защищенности персональных данных при их обработке в информационной (автоматизированной) системе	- уровень защищенности персональных данных определяется на основании исходных данных информационной (автоматизированной) системы и в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119
10	Модель угроз безопасности информации	- при разработке модели угроз безопасности информации руководствоваться методическим документом «Методика оценки угроз безопасности информации», утвержденного ФСТЭК России 05.02.2021; - модель угроз безопасности информации необходимо согласовать с ФСТЭК России в случае если информационная система признана ГИС/МИС
11	Техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы	- данный документ необходимо согласовать с ФСТЭК России в случае если информационная система признана ГИС/МИС

	защиты информации объекта информатизации	
12	Проектная документация на систему защиты информации объекта информатизации	В случае ее разработки в ходе создания объекта информатизации
13	Перечень лиц, допущенных к обработке информации в информационной (автоматизированной) системе	
14	Перечень лиц, допущенных к техническому обслуживанию элементов информационной (автоматизированной) системы	
15	Перечень лиц, имеющих право самостоятельного доступа в помещение, где расположена информационная (автоматизированная) система	
16	Правила обработки персональных данных, устанавливающие процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
17	Правила рассмотрения запросов субъектов персональных данных или их представителей	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
18	Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
19	Правила работы с обезличенными данными в случае обезличивания персональных данных	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
20	Перечень информационных систем персональных данных	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
21	Перечни персональных данных, обрабатываемых в государственном или муниципальном органе в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
22	Перечень должностей служащих государственного или муниципального органа, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
23	Перечень должностей служащих государственного или муниципального органа, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
24	Должностной регламент (должностные обязанности) или должностная инструкция ответственного за организацию обработки персональных данных в государственном или муниципальном органе	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
25	Типовое обязательство служащего государственного или муниципального органа, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта (контракта) или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
26	Типовая форма согласия на обработку персональных данных служащих государственного или муниципального органа, иных субъектов персональных данных	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
27	Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
28	Порядок доступа служащих государственного или муниципального органа в помещения, в которых ведется обработка персональных данных	Постановление Правительства Российской Федерации от 21.03.2012 № 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»
29	Акт оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»	- пункт 5 части 1 статьи 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» - Требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных», утвержденные Приказом Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178
30	Должностной регламент (должностные обязанности) или должностная инструкция ответственного	

	(администратора) за информационную безопасность	
31	Должностной регламент (должностные обязанности) или должностная инструкция администратора объекта информатизации (системный администратор)	
32	Инструкция администратора информационной безопасности объекта информатизации	
33	Инструкция администратора объекта информатизации (системного администратора)	
34	Инструкция пользователя по работе на объекте информатизации	
35	Инструкция по организации антивирусной защиты	
36	Инструкция по организации парольной защиты	
37	Инструкция по порядку учета, хранения машинных носителей и съемных машинных носителей защищаемой информации	
38	Инструкция по резервированию и восстановлению работоспособности объекта информатизации	
39	План организационно-технических мероприятий по защите информации не содержащей сведения, составляющие государственную тайну, в организации	
40	Журнал учёта машинных носителей информации	- пункт 5 части 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»
41	Журнал учёта мобильных технических средств	при необходимости
42	Журнал обращений субъектов персональных данных о выполнении их законных прав	
43	Журнал учёта событий информационной безопасности	

6. Определение требования к системе защиты информации

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении к приказу ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в приложении к приказу ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных

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

7. Реализация системы защиты информации

Поставка/внедрение/настройка средств защиты информации согласно разработанной системе защиты информации.

8. Аттестация объекта информатизации

Согласно приказу ФСТЭК России от 29.04.2021 № 77 обязательной аттестации подлежит ГИС/МИС.

Аттестация объектов информатизации проводится на этапе его создания или развития (модернизации) и предусматривает проведение комплекса организационных и технических мероприятий и работ (аттестационных испытаний), в результате которых подтверждается соответствие объекта информатизации требованиям по защите информации в условиях его эксплуатации. Допускается проведение аттестации объекта информатизации на этапе его эксплуатации в случае, если владельцем объекта принято решение об обработке защищаемой информации после ввода в эксплуатацию объекта информатизации (пункт 4 приказ ФСТЭК России от 29.04.2021 № 77).

Для проведения аттестационных испытаний владелец объекта информатизации привлекает организацию, имеющую лицензию на осуществление деятельности по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации), выданную ФСТЭК России в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012 № 79. (пункт 5 приказ ФСТЭК России от 29.04.2021 № 77)

Документы необходимые для проведения работ по аттестации объекта информатизации (согласно пункту 11 приказа ФСТЭК России от 29.04.2021 № 77):

1. Технический паспорт на объект информатизации;
2. Акт классификации информационной (автоматизированной) системы;
3. Модель угроз безопасности информации;
4. Техническое задание на создание (развитие, модернизацию) объекта информатизации и (или) частное техническое задание на создание (развитие, модернизацию) системы защиты информации объекта информатизации;
5. Проектная документация на систему защиты информации объекта информатизации (в случае ее разработки в ходе создания объекта информатизации);
6. Эксплуатационная документация на систему защиты информации объекта информатизации и применяемые средства защиты информации;

7. Организационно-распорядительные документы по защите информации владельца объекта информатизации, регламентирующие защиту информации в ходе эксплуатации объекта информатизации, в том числе план мероприятий по защите информации на объекте информатизации, документы по порядку оценки угроз безопасности информации, управлению (администрированию) системой защиты информации, управлению конфигурацией объекта информатизации, реагированию на инциденты безопасности, информированию и обучению персонала, контролю за обеспечением уровня защищенности информации;

8. Документы, содержащие результаты анализа уязвимостей объекта информатизации и приемочных испытаний системы защиты информации объекта информатизации (в случае проведения анализа и испытаний в ходе создания объекта информатизации).

По решению владельца объекта информатизации, указанные в настоящем пункте документы (их копии) представляются в орган по аттестации в виде электронных документов.

9. Эксплуатация объекта информатизации

Обеспечение защиты информации в ходе эксплуатации объекта информатизации должно включать следующие мероприятия:

9.1. Своевременная актуализация организационно-распорядительной документации.

9.2. Планирование мероприятий по защите информации:

9.2.1. Определение лиц, ответственных за планирование и контроль мероприятий по защите информации на объекте информатизации;

9.2.2. Определение лиц, ответственных за выявление инцидентов безопасности и реагирование на них;

9.2.3. Разработку, утверждение и актуализацию плана организационно-технических мероприятий по защите информации не содержащей сведения, составляющие государственную тайну, в организации (далее – План);

9.2.4. Определение порядка контроля выполнения мероприятий по обеспечению защиты информации в организации, предусмотренных утвержденным Планом.

9.3. Анализ угроз:

9.3.1. Выявление, анализ и устранение уязвимостей объекта информатизации,

9.3.2. Анализ изменения угроз безопасности информации в объекте информатизации;

9.3.3. Оценка возможных последствий реализации угроз безопасности информации в объекте информатизации.

9.4. Управление (администрирование) системой защиты информации:

9.4.1. Определение лиц, ответственных за управление (администрирование) системой защиты информации объекта информатизации;

9.4.2. Управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в объекте информатизации;

9.4.3. Управление средствами защиты информации объекта информатизации;

9.4.4. Управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования объекта информатизации;

9.4.5. Централизованное управление системой защиты информации объекта информатизации (при необходимости);

9.4.6. Мониторинг и анализ событий безопасности на объекте информатизации (события безопасности);

9.4.7. Управление обеспечение функционирования системы защиты информации объекта информатизации в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

9.5. Управление конфигурацией объекта информатизации и его системой защиты:

9.5.1. Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и ее системы защиты информации, и их полномочий;

9.5.2. Определение компонентов объекта информатизации и его системы защиты, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

9.5.3. Управление изменениями объекта информатизации и его системы защиты: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в объект информатизации и его систему защиты информации, документирование действий по внесению изменений в объект информатизации и сохранение данных об изменениях конфигурации;

9.5.4. Контроль действий по внесению изменений в объект информатизации и его систему защиты информации.

9.6. Реагирование на инциденты безопасности:

9.6.1. Обнаружение и идентификация инцидентов безопасности, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов безопасности;

9.6.2. Своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов безопасности и реагирование на них, о возникновении инцидентов безопасности в информационной системе;

9.6.3. Анализ инцидентов безопасности, в том числе определение источников и причин возникновения инцидентов безопасности, а также оценка их последствий;

9.6.4. Планирование и принятие мер по устранению инцидентов безопасности, в том числе по восстановлению объекта информатизации и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов безопасности;

9.6.5. Планирование и принятие мер по предотвращению повторного возникновения инцидентов безопасности.

9.7. Информирование и обучение персонала.

9.8. Проведение контроля за обеспечение уровня защищенности информации:

9.8.1. Контроль (анализ) защищенности информации с учетом особенностей функционирования объекта информатизации;

9.8.2. Анализ и оценка функционирования объекта информатизации и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации;

9.8.3. Документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в объекте информатизации;

9.8.4. Принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в объекте информатизации, о необходимости доработки (модернизации) ее системы защиты информации;

9.8.5. Проведения периодического контроля уровня защиты информации на аттестованном объекте информатизации:

9.8.5.1. Для ГИС/МИС 1 класса защищенности не реже одного раза в год (пункт 18.7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России от 11.02.2013 № 17);

9.8.5.2. Для ГИС/МИС 2, 3 класса защищенности не реже одного раза в два года (пункт 18.7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России от 11.02.2013 № 17);

9.8.5.3. Для информационных систем персональных данных не реже одного раза в три года (подпункт 6 пункта 1 Состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных, утвержденных Приказом ФСТЭК России от 18.02.2013 № 21).