Приложение к приказу
Департамента ЗАГС
Забайкальского края
от 02.09.2019 № 90

ПОЛИТИКА
информационной безопасности
в Департаменте ЗАГС Забайкальского края

г. Чита
2019

Содержание

I. Назначение

1.1. В соответствии с:

- п п.2.12, п.4.1- п.4.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;
- п.3.1.48, п. А.6.3 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
- разд.5.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.9.2.3 ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности;
- п.5.1, разд. 11.5 ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности
- п.3.2.4 и разд. 3.6 ГОСТ Р ИСО/МЭК 27000-2012. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология и др.

в организациях должен быть разработан документ под названием Политика информационной безопасности (Правила информационной безопасности), который определяет общую совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

При этом в соответствии с нормативными актами разработка политики информационной безопасности в организации является отправным мероприятием по управлению информационной безопасностью[1].

1.2. Целью Политики информационной безопасности в Департаменте ЗАГС Забайкальского края (далее- Политики) является определение основных правил обеспечения безопасности объектов защиты Департамента ЗАГС Забайкальского края от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизации ущерба от возможной реализации угроз безопасности защищаемой информации.

1.3. Структура Политики разработана в соответствии с Примерным перечнем вопросов, входящих в состав политики безопасности информационных технологий организации[2].

1.4. Национальные стандарты в области защиты информации[3] отводят политикам

---

[1] См.: п.0.6 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[2] См.: Приложение А «Примерный перечень вопросов, входящих в состав политики безопасности информационных технологий организации» ГОСТ Р ИСО/МЭК ТО 13335-3—2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

[3] См.:

- ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

информационной безопасности в организациях роль основного документа, в котором описаны основополагающие принципы, конкретизируемые затем в отдельных организационно- распорядительных актах по вопросам информационной безопасности. При этом издаваемые организационно-распорядительные акты не должны противоречить Политике.

1.5. В соответствии с п. 5.1.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий, Департамент ЗАГС Забайкальского края обязан опубликовать настоящую Политику.

II. Область применения

2.1. Настоящая Политика информационной безопасности в Департаменте ЗАГС Забайкальского края (далее – Политика) определяет общие правила, процедуры, практические приемы и руководящие принципы в области безопасности информации, которыми руководствуется Департамент ЗАГС Забайкальского края в своей деятельности и которые применяются для регламентирования единых подходов в Департаменте ЗАГС Забайкальского края к построению системы защиты информации информационных систем (далее- СЗИИС).

2.2. В Политике определены объекты защиты, общий замысел защиты информации Департамента ЗАГС Забайкальского края, принципы построения системы защиты информационных систем, требования к пользователям информационных систем, степень ответственности персонала, структура и необходимый уровень защищенности[4], статус и должностные обязанности лиц, ответственных за обеспечение безопасности информации, обрабатываемой в информационных системах Департамента ЗАГС Забайкальского края.

2.3. Требования Политики обязательны для всех гражданских служащих и работников Департамента ЗАГС Забайкальского края[5], представителей контрольно- надзорных органов, допущенных к защищаемой информации на законных основаниях, а также индивидуальных лиц и работников иных организаций допущенных к защищаемой информации для проведения работ по гражданско- правовым договорам[6].

– ГОСТ Р ИСО/МЭК ТО 13335-3—2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий и др.

[4] См.:

– п.2, п.9 ч.2, п.1 ч.3, ч.4, ч.11 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
– ст.8- ст.16 Требований к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
– п.8 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 №28608).

[5] Далее по тексту вместе- сотрудники.

[6] Заключенным на основании и условиях:

– ч.3 ст.6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
– ст.3 Требований к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
– п.3 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разделом 8.4.2 Политики в отношении обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 92;

III. Нормативные ссылки

3.1. Настоящая Политика разработана в соответствии с требованиями следующих нормативных правовых актов:

- Конституции Российской Федерации;
- Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- Федерального закона от 27.07.2004 №79-ФЗ «О государственной гражданской службе Российской Федерации»;
- Федерального закона от 15.11.1997 №143-ФЗ "Об актах гражданского состояния";
- Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ;
- Указа Президента Российской Федерации от 06.03.97 № 188 «Об утверждении Перечня сведений конфиденциального характера»;
- Указа Президента РФ от 17.03.2008 №351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";
- Постановления Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановления 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";
- Постановления Правительства Российской Федерации от 15.09.2008 №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановления Правительства Российской Федерации от 26.06.1995 №608"О сертификации средств защиты информации";
- Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- приказа ФСТЭК России от 11.02.2013 №17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- приказа 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" (зарегистрировано в Минюсте России 18.08.2014 №33620);

- п.6.2.7 Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

- приказа Роскомнадзора от 05.09.2013 №996 «Об утверждении Требований и методов по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ» (зарегистрировано в Минюсте России 10.09.2013 №29935);
- Методического документа «Меры защиты информации в государственных информационных системах» (утверждено ФСТЭК России 11.02.2014);
- Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-662;
- Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008;
- ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
- ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения;
- ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство;
- раздела 7.2 ГОСТ Р ИСО/МЭК ТО 13335-3-2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий;
- ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер;
- ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
- ГОСТ Р ИСО/МЭК 12207-99. Информационная технология. Процессы жизненного цикла программных средств;
- ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности;
- ГОСТ Р ИСО/МЭК 18044. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности;
- ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования;
  ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования и др.

IV. Термины, обозначения и сокращения

4.1. В настоящей Политике используются следующие термины и обозначения:

4.1.1. **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники[7].

4.1.2. **Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[8].

4.1.3. **Администратор безопасности информации** - лицо, отвечающее за защиту информационных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации[9].

4.1.4. **Анализ уязвимостей** - мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба[10].

4.1.5. **Аттестация объектов информатизации** – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации[11].

4.1.6. **Аутентификация** - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности

---

[7] См.: ч.4. ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

[8] См.:

- п.1.3 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п.1.1 ГОСТ 34. 003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

[9] См.:

- ст. 14 и ст. 15 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- ст.18 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного Постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;
- п.1.5, п.3.16 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.п.16-17 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620);
- п.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- п.2 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 (зарегистрировано в Минюсте России 14.05.2013 №28375);
- п.5.1.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства
- обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

[10] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[11] См.: п. 3.6 ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования.

субъекта доступа в информационной системе)[12].

4.1.7. **Безопасность информации [данных]** - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность[13]; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами[14].

4.1.8. **Виртуализация** - технология преобразование формата или параметров программных или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы[15].

4.1.9. **Вредоносная программа** - программа, используемая для несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы[16].

4.1.10. **Государственные информационные системы** - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов[17].

4.1.11. **Документооборот** - движение документов в организации с момента их создания или получения до завершения исполнения или отправления[18].

4.1.12. **Должностное лицо**-сотрудник Департамента ЗАГС Забайкальского края, правомочный от имени Департамента ЗАГС Забайкальского края исполнять определенные, предусмотренные должностными регламентами (должностными обязанностями) действия.

4.1.13. **Доступность (санкционированная доступность) информации** - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к

---

[12] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[13] См.:
- п. 2.4.5 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ;
- п.3.1.4 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[14] См. п. 1.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 №282.

[15] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[16] См.:
- п.3.9 ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
- п.3.2.17«Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[17] См.: п.1) ч.1 ст.13 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации". В соответствии с п.1 приказа Департамента ЗАГС Забайкальского края от 09.12.2013 №91 «О государственной информационной системе Департамента ЗАГС Забайкальского края» многоуровневая автоматизированная информационная система Департамента ЗАГС Забайкальского края «МАИС ЗАГС» является региональной государственной информационной системой.

[18] См.: п.73 ГОСТ Р 7.0.8-2013 СИБИД. Делопроизводство и архивное дело. Термины и определения.

информации субъектов, имеющих на это полномочия[19].

4.1.14. **Жизненный цикл СКЗИ** - разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация.[20]

4.1.15. **Замысел защиты информации** - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации[21].

4.1.16. **Идентификатор** - представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе[22].

4.1.17. **Идентификация** - присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов[23].

4.1.18. **Информационная система (ИС)** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.[24]

4.1.19. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [25].

4.1.20. **Информационные системы Департамента ЗАГС Забайкальского края** – государственные информационные системы[26] и иные информационные системы, включая информационные системы персональных данных[27], представляющие собой совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий и

---

[19] См.:
- п.1.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.3.1.9 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[20] См.: подпункт «б» п. 10 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620).

[21] См.: п. 2.4.1 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

[22] См.:
- п.2.3. Части 1. «Введение и общая модель» Руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», введенного в действие приказом Гостехкомиссии России от 19.06.02 № 187;
- Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[23] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[24] См.: ч.3 ст.2 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации".

[25] См.:
- ч.10 ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» ;
- абзац первый л.4 Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008.

[26] См.: п. 4.1.10 настоящей Политики.

[27] См.: п.4.1.19 настоящей Политики.

технических средств.

4.1.21. **Инцидент** - непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности)[28].

4.1.22. **Компьютерный вирус** - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам[29].

4.1.23. **Контролируемая зона** – это пространство, в котором исключено неконтролируемое пребывание работников и посетителей оператора и посторонних транспортных, технических и иных материальных средств[30].

4.1.24. **Конфиденциальный документ** - информация, зафиксированная на материальном носителе, содержащая коммерческую, служебную или иную охраняемую законом тайну, с реквизитами, позволяющими ее идентифицировать и обеспечивать защиту, доступ к которой ограничивается федеральными законами, а также ее обладателем[31].

4.1.25. **Криптографические средства защиты информации** – а) средства шифрования – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении; б) средства имитозащиты – аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации; в) средства электронной цифровой подписи – аппаратные, программные и аппаратно–программные средства, обеспечивающие на основе криптографических преобразований

---

[28] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[29] См.: п.3 ГОСТ Р 51188-98. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

[30] См.:

- п. ЗНИ.3, п. ЗТС.2 , п. ЗИС.3 Приложения 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 №28608);
- подпункт «в» п. 10 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620);
- п.1.16, п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- раздел 1 Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Федеральной службой по техническому и экспортному контролю 15.02.2008.

[31] См.: п.11) ст.2 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации".

реализацию хотя бы одной из следующих функций: создание электронной цифровой подписи с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи, создание закрытых и открытых ключей электронной цифровой подписи; г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций; д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации); е) ключевые документы (независимо от вида носителя ключевой информации)[32].

4.1.26. **Машинные носители информации** - физическое устройство (дискета, e-Token, смарт-карта и т.д.), предназначенное для хранения информации в электронной форме.

4.1.27. **Межсетевой экран (средство межсетевого экранирования)** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС[33].

4.1.28. **Модель угроз** - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации[34].

4.1.29. **Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых

---

[32] См.:

- п.2 Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденного постановлением Правительства РФ от 16.04.2012 №313;
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;
- Положение о разработке, производстве, реализации и шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», зарегистрировано Минюстом России (регистрационный № 6382 от 03.03.2005);
- раздел 1 Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденных руководством 8 Центра ФСБ России 21.02.2008 №149/54-144..

[33] См.:

- п.1.19. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- раздел 3 Руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», утвержденные решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25.07.1997.

[34] См.: п.2.6.8 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

средствами вычислительной техники или информационными системами[35].

4.1.30. **Обработка информации** - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией[36].

4.1.31. **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных[37].

4.1.32. **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа[38].

4.1.33. **Объект защиты информации** - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации[39].

4.1.34. **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[40].

4.1.35. **Организационные меры защиты информации** - под организационными мерами (оргмерами) понимаются организационные мероприятия по обеспечению физической защиты информации, предусматривающие установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты[41]. Организационные меры по защите персональных данных включают в себя:

- разработку организационно – распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных;
- перечень мероприятий по защите персональных данных: определение круга лиц, допущенного к обработке персональных данных; организация доступа в помещения, где осуществляется обработка ПДн и (или) размещены СКЗИ[42]; разработка должностных инструкций по работе с

[35] См.: п.1.20. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.

[36] См.: п.3.1 ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования.

[37] См.: ч.3. ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

[38] См.: п.1.4 «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. (Утверждено решением председателя Гостехкомиссии России от 30.03.1992).

[39] См.: п. 2.5.1 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

[40] См. п.3.2 ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования.

[41] См.: примечание 1 к п.2.2.4 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

[42] В соответствии с подпунктом а) п.6 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ин-формационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных

персональными данными; установление персональной ответственности за нарушения правил обработки ПДн; определение продолжительности хранения ПДн и т.д.[43]

4.1.36. **Оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных[44].

4.1.37. **Оператор персональных данных (оператор ПДн)** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными[45].

4.1.38. **Ответственный за организацию обработки персональных данных** - должностное лицо оператора ПДн, осуществляющее:

- внутренний контроль за соблюдением сотрудниками Департамента ЗАГС Забайкальского края законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения сотрудников Департамента ЗАГС Забайкальского края положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организацию прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющее контроль за приемом и обработкой таких обращений и запросов[46];
- контроль организации допуска сотрудников Департамента ЗАГС Забайкальского края к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности[47].

4.1.39. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[48].

4.1.40. **Политика безопасности (информации в организации)** - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности[49].

данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620).

[43] См.: Организационные меры защиты персональных данных. http://stavkombez.ru/conf/category/section1/.

[44] См.: п.12) ст.2 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации".

[45] См.: ч.2. ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

[46] См.: ст.22.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

[47] См.: п. 7.1.2, п.7.2.2. Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91.

[48] См.: ч.1.ст. Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

[49] См.:

- п.2.3. Части 1. «Введение и общая модель» Руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», введенного в действие приказом Гостехкомиссии России от 19.06.02 № 187;
- п. 2.4.4 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.
- п.3.3.2 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

4.1.41. **Пользователь (потребитель) информации** – 1) субъект или внешний объект ИТ, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею[50]; 2) сотрудник Департамента ЗАГС Забайкальского края или сотрудник иного органа (организации), допущенный в установленном порядке к работе с защищаемой информацией[51], полномочия которого регламентированы внутренними организационно - распорядительными актами[52] Департамента ЗАГС Забайкальского края.

4.1.42. **Правовые меры защиты информации**[53]- под правовыми мерами понимается защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением[54]. Правовые методы защиты информации для Департамента ЗАГС Забайкальского края заключаются в применении существующих законов и иных нормативных правовых актов, а также в контроле их исполнения.

4.1.43. **Программная среда** - совокупность программного обеспечения, используемого в информационной системе для решения одной или нескольких задач[55].

4.1.44. **Регуляторы** - Федеральная служба по техническому и экспортному контролю (ФСТЭК России)[56], Федеральная служба безопасности (ФСБ России)[57], Федеральная служба по надзору в сфере связи, информационных

---

[50] См.: п.2.3. Части 1. «Введение и общая модель» Руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», введенного в действие приказом Гостехкомиссии России от 19.06.02 № 187.

[51] В соответствии с:

- разделом VII Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91;
- разделом VI Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

[52] См.:

- п.7.1.2 Политики информационной безопасности в Департаменте ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 90;
- раздела 7.1.2 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100.

[53] См.:

- ч.1 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- ч.1 ст.16 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации".

[54] См.: п.2.2.1 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

[55] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[56] Полномочия установлены в соответствии с:

- ч.9 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- ст.1 Положения о Федеральной службе по техническому и экспертному контролю, утвержденному Указом Президента Российской Федерации от 16.08.2004 №1085.

[57] Полномочия установлены в соответствии с:

- ч.9 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.11.2, п. «и.1» ст.12 Федерального закона от 03.04.1995 №40-ФЗ "О Федеральной службе безопасности";
- ст.5 Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных

технологий и массовых коммуникаций (Роскомнадзор)[58].

4.1.45. **Роль** - предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой[59].

4.1.46. **Система защиты информации информационных систем (СЗИИС)** – 1) система по обеспечению безопасности защищаемой информации, создаваемая в соответствии с нормативными правовыми актами[60] с целью нейтрализации актуальных угроз безопасности защищаемой информации; 2) система защиты информации информационных систем включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации и информационных технологий, используемых в информационных системах[61].

4.1.47. **Событие безопасности (информационной)** - идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации[62].

4.1.48. **Субъект доступа** - пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа[63].

4.1.49. **Технические меры защиты информации** - под техническими мерами защиты информации в узком смысле слова понимается защита информации,

---

систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденного Постановлением Правительства РФ от 16.04.2012 №313.

[58] Полномочия установлены в соответствии с:
- ст.23 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- ст.1. и ст.5 Положения о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, утвержденного Постановлением Правительства РФ от 16.03.2009 №228.

[59] См.:
- п.2.3. Части 1. «Введение и общая модель» Руководящего документа «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий», введенного в действие приказом Гостехкомиссии России от 19.06.02 № 187;
- Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[60] См.:
- ч.5 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- ст.2 Требований к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.12 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[61] См.: часть вторую ст..2 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119.

[62] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[63] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств[64]. В широком смысле слова под техническими средствами защиты информации понимается защита информации как некриптографическими методами, так и методами преобразования при помощи шифрования[65].

4.1.50. **Требования безопасности информации** - требования, выполнение которых позволяет защитить информацию от утечки по техническим каналам, от несанкционированного доступа и от специальных воздействий на нее и ее носители. Требования безопасности информации устанавливаются федеральными законами, нормативными правовыми актами Президента Российской Федерации, уполномоченных федеральных органов исполнительной власти, национальными стандартами, владельцем информации или объекта информатизации[66].

4.1.51. **Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных[67].

4.1.52. **Управление доступом** - ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа[68].

4.1.53. **Уязвимость информационной системы** - недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации[69].

4.1.54. **Целостность информации** – 1) Устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации[70]. Состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их)

---

[64] См.: п.2.2.2 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

[65] Именно в широком смысле термин техническая защита употреблен законодателем в:

- Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- ст.2 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119, и др.

[66] См. п.3.4 ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования.

[67] См.:

- разд.1 «Общие положения» Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена Заместителем директора ФСТЭК России 14.02.2008);
- п.2.6.1. ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

[68] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[69] См.: Приложение 1 к методическому документу «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[70] См.: п.1.27. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.

изменение осуществляется только преднамеренно субъектами, имеющими на него право[71].

4.1.55. **Цель защиты информации** - заранее намеченный результат защиты информации[72].

4.2. В настоящем Положении используются следующие сокращения:

4.2.1. **АС**- автоматизированная система;

4.2.2. **Департамент** - Департамент ЗАГС Забайкальского края;

4.2.3. **ИС**- информационная система;

4.2.4. **ИСПДн**- информационная система персональных данных;

4.2.5. **КЗ**- контролируемая зона;

4.2.6. **КСЗИ**- криптографическое средство защиты информации;

4.2.7. **МНИ**- машинные носители информации;

4.2.8. **МЭ**- межсетевой экран;

4.2.9. **НСД**- несанкционированный доступ;

4.2.10. **оператор**- оператор ИС (в тексте настоящей Инструкции под оператором ИС понимается Департамент ЗАГС Забайкальского края);

4.2.11. **оргмеры**- организационные меры защиты персональных данных;

4.2.12. **ПДн**- персональные данные;

4.2.13. **СЗИ**- средства защиты информации;

4.2.14. **СЗИИС**- система защиты информации информационных систем;

4.2.15. **сотрудники Департамента**- гражданские служащие и (или) работники Департамента ЗАГС Забайкальского края.

V. Объекты и общий замысел защиты информации Департамента ЗАГС Забайкальского края

5.1. Объектами защиты Департамента ЗАГС Забайкальского края являются[73]:

5.1.1. информационные ресурсы, содержащие конфиденциальную информацию, а также открытая (общедоступная) информация[74], необходимая для работы Департамента ЗАГС Забайкальского края, независимо от формы и вида ее представления;

5.1.2. процессы обработки информации в информационных системах Департамента ЗАГС Забайкальского края, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий

---

[71] См.: п.3.1.8 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[72] См.: п.2.4.2 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

[73] См.:

- п.8, п. 15.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- абзац шестой раздела 1. Общие положения Методического документа «Меры защиты информации в государственных информационных системах» (утверждено ФСТЭК России 11.02.2014).

[74] См.:

- п.1 и п.3 ст.16 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- п.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- абзацы пятый и шестой раздела 1. Общие положения Методического документа «Меры защиты информации в государственных информационных системах» (утверждено ФСТЭК России 11.02.2014).

персонал;

5.1.3. информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы информационной среды.

5.2. Состав объектов защиты представлен в техническом задании и техническом проекте на создание системы защиты информации информационных систем[75].

5.3. Общий замысел защиты информации исходит из того, что:

- безопасность защищаемой информации достигается путем исключения несанкционированного, в том числе случайного, доступа к защищаемой конфиденциальной информации (включая и персональные данные), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий[76];
- выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и осуществления конкретных мероприятий по обеспечению безопасности конфиденциальной информации (включая и персональные данные) в Департаменте ЗАГС Забайкальского края[77];
- информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей[78];

---

[75] См.:
- Техническое задание «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». СЗ-ЗАГС.

[76] Исполняется в соответствии с:
- п.6 ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» ;
- ст.6 Требований к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.20.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п.ОЦЛ.1 и п.ОЦЛ.2 Приложения №2 к указанным Требованиям;
- п.2.8. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.ОЦЛ.1 и п.ОЦЛ.2 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п.ОЦЛ.1 и п.ОЦЛ.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[77] См.: п. 3.1. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

[78] Исполняется в соответствии с:
- п.12, п.20, п.20.10 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п.ОДТ.1 п.ОДТ.5, п.ОДТ.7 Приложения №2 к указанным Требованиям;
- п. 1.9, п.6.3.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;

- должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных[79];
- должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных[80].

5.4. Состав каждой информационной системы, подлежащей защите, представлен в паспорте конкретной информационной системы[81].

- п.ОДТ.1 п.ОДТ.5, п.ОДТ.7 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п.ОДТ.1 п.ОДТ.5, п.ОДТ.7. Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[79] Исполняется в соответствии с:
- п.6) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п16.2, п.18, п.18.2, п.20.5- п.20.7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п. РСБ.4, п. РСБ.5 , п. ОЦЛ.4 , п. ЗИС.7 - п. ЗИС.9 Приложения №2 к указанным Требованиям;
- п. 3.24. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.6.3. ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью»;
- п. РСБ.4, п. РСБ.5 , п. ОЦЛ.4 , п. ЗИС.7 - п. ЗИС.9 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. РСБ.4, п. РСБ.5 , п. ОЦЛ.4 , п. ЗИС.7 - п. ЗИС.9 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[80] Исполняется в соответствии с:
- п.7) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- ст.6 Требований к защите персональных данных при их обработке в информационных системах персональных данных утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п. 20.6- п.20.7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п. ЗИС.3Приложения №2 к указанным Требованиям;
- п.6.1.2., п.6.3.7., п.6.3.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п. ЗИС.3 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ЗИС.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[81] См.:
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 2. Паспорт ГИС «МАИС ЗАГС». СЗ-ЗАГС.ПС. 01-ОР;

5.5. Основополагающими принципами построения системы защиты информации информационных систем Департамента ЗАГС Забайкальского края являются следующие положения:

5.5.1. информационные системы Департамента ЗАГС Забайкальского края представляют собой совокупность государственной информационной системы[82] и иных информационных систем;

5.5.2. для упрощения системы защиты информации информационных систем персональных данных, не являющихся государственными информационными системами в соответствии с положениями нормативных правовых актов Регуляторов[83] в Департаменте ЗАГС Забайкальского края применяются требования для защиты информации, содержащейся в государственных информационных системах.

VI. Цели, задачи и принципы обеспечения информационной безопасности в Департаменте ЗАГС Забайкальского края

6.1. Цели обеспечения информационной безопасности в Департаменте ЗАГС Забайкальского края

6.1.1. В соответствии с:

- ст.9, ч.1 и ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- п.12 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608;
- абзацем пятым раздела I методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014),

установлены следующие цели обеспечения защиты информации ограниченного доступа в Департаменте ЗАГС Забайкальского края:

- 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;
- реализация права на доступ к информации.

6.1.2. В соответствии с:

- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 3. Паспорт ИСПДн «1С Бухгалтерия». СЗ - ЗАГС. ПС.02-ОР;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 4. Паспорт ИСПДн «1С Зарплата и кадры». СЗ - ЗАГС. ПС .03-ОР.

[82] См.: п.1 приказа Департамента ЗАГС Забайкальского края от 09.12.2013 №91 «О государственной информационной системе Департамента ЗАГС Забайкальского края».

[83] См.:

- п.6 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- абзац седьмой раздела 1. Общие положения Методического документа «Меры защиты информации в государственных информационных системах» (утверждено ФСТЭК России 11.02.2014).

- п.1 и п. 3 ч.1 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- п.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608),

установлены следующие цели обеспечения защиты общедоступной информации в Департаменте ЗАГС Забайкальского края:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- реализация права на доступ к информации.

6.2. Задачи обеспечения информационной безопасности в Департаменте ЗАГС Забайкальского края

6.2.1. Для достижения целей защиты информации, указанных в разделе 6.1 настоящей Политики в Департаменте ЗАГС Забайкальского края создается система информационной безопасности, включающая в себя систему защиты информации информационных систем[84] и внутренние организационно-распорядительные акты, регламентирующие обращение защищаемой информации как на электронных, так и на бумажных носителях.

6.2.2. Система защиты информации информационных систем Департамента ЗАГС Забайкальского края призвана решать задачи[85]:

- идентификации и аутентификации субъектов доступа и объектов доступа[86];
- управления доступом субъектов доступа к объектам доступа[87];

---

[84] См.:
- Техническое задание «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». СЗ-ЗАГС.

[85] См.:
- п.20 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.2.3, п.3.1- п.3.13 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[86] См.:
- п.20.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом I Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.1 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п.9.3 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[87] См.:
- п.20.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом II Приложения №2 к указанным Требованиям;

- ограничения программной среды[88];
- защиты машинных носителей информации[89];
- регистрации событий безопасности[90];
- антивирусной защиты[91];

- п.2.3, разд.3.2 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.4 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[88] См:

- п. ОПС.1Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- п. ОПС.1 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ОПС.1Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной за-писки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- разд.9.5. Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[89] См.:

- п.20.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом IV Приложения №2 к указанным Требованиям;
- разд.9.6 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[90] См.:

- п.20.5 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом V Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.4 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.6.1.5 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- разд.9.7 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[91] См.:

- п.20.6 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом VI Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.3, разд.3.6 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п.5.5 Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107;
- разд.9.8 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

- обнаружения (предотвращения) вторжений[92];
- контроля (анализа) защищенности информации[93];
- целостности информационной системы и информации[94];
- доступности информации[95];
- защиты среды виртуализации[96];

---

[92] См.:
- п.20.7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом VII Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.7 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.9. Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94

[93] См.:
- п.20.8 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом VIII Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.8 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.10 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[94] См.:
- п.20.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом IX Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.8 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.11 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п.6.4.1.3, п.6.1.5.5.1.8 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[95] См.:
- п.20.10 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом X Приложения №2 к указанным Требованиям;
- разд.3.2 методического документа «Меры защиты информации в государственных ин-формационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.12 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[96] См.:
- п.20.11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом XI Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.11 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.13 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

- защиты технических средств[97];
- защиты информационной системы, ее средств, систем связи и передачи данных[98].

6.3. Принципы обеспечения информационной безопасности в Департаменте ЗАГС Забайкальского края

6.3.1. Политика информационной безопасности в Департаменте ЗАГС Забайкальского края основана на принципах[99]:

- законности[100];
- системности[101];
- комплексности[102];
- непрерывности[103];
- своевременности[104];

---

[97] См.:
- п.20.12 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом XII Приложения №2 к указанным Требованиям;
- подпунктом а) п.5 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ин-формационных 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620).
- разд.3.2 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.14 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[98] См.:
- п.20.13 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом XIII Приложения №2 к указанным Требованиям;
- разд.3.8 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- Техническое задание «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». СЗ-ЗАГС;
- разд.9.15 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[99] См.:
- раздел 3.1 «Принципы безопасности» ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;
- п. А.10.4 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.6.1.5, п.9.1.5, п.10.1.3, п.11.1.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[100] См.: п. 6.3.2 настоящей Политики.
[101] См.: п. 6.3.3 настоящей Политики.
[102] См.: п. 6.3.4 настоящей Политики.
[103] См.: п. 6.3.5 настоящей Политики.
[104] См.: п. 6.3.6 настоящей Политики.

- преемственности и непрерывности совершенствования[105];
- разумной достаточности (экономической целесообразности)[106];
- персональной ответственности[107];
- минимизации полномочий[108];
- исключения конфликта интересов[109];
- взаимодействия и сотрудничества[110];
- гибкости системы защиты[111];
- открытости алгоритмов и механизмов защиты[112];
- простоты применения средств защиты[113];
- обоснованности и технической реализуемости[114];
- специализации и профессионализма[115];
- обязательности контроля[116].

6.4.1. Принцип законности информационной безопасности в Департаменте ЗАГС Забайкальского края предполагает осуществление защитных мероприятий и разработку системы безопасности информации в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных правовых актов Регуляторов. Принятые меры безопасности информации не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством случаях к информации конкретных подсистем.

6.4.2. Принцип системности построения системы защиты информации в Департаменте ЗАГС Забайкальского края предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности информации в Департаменте ЗАГС Забайкальского края. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем Департамента ЗАГС Забайкальского края, а также характер, возможные объекты и направления атак на них со стороны нарушителей, пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

6.4.3. Принцип комплексности методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами,

[105] См.: п. 6.3.7 настоящей Политики.
[106] См.: п. 6.3.8 настоящей Политики.
[107] См.: п. 6.3.9 настоящей Политики.
[108] См.: п. 6.3.10 настоящей Политики.
[109] См.: п. 6.3.11 настоящей Политики.
[110] См.: п. 6.3.12 настоящей Политики.
[111] См.: п. 6.3.13 настоящей Политики.
[112] См.: п. 6.3.14 настоящей Политики.
[113] См.: п.6.3.15 настоящей Политики.
[114] См.: п. 6.3.16 настоящей Политики.
[115] См.: п. 6.3.17 настоящей Политики.
[116] См.: п. 6.3.18 настоящей Политики.

организационными и правовыми мерами.

6.4.4. Принцип непрерывности защиты означает, что защита информации является составной частью работ по созданию и эксплуатации информационных систем и обеспечивается на всех стадиях (этапах) их создания и в ходе эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационных системах, в рамках системы (подсистемы) защиты информации информационных систем (далее - система защиты информации информационных систем)[117].

6.4.5. Принцип своевременности предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их системы защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

6.4.6. Принцип преемственности и совершенствования предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Департамента ЗАГС Забайкальского края и системы их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

6.4.7. Принцип разумной достаточности (экономической целесообразности) предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов информационных систем Департамента ЗАГС Забайкальского края.

6.4.8. Принцип персональной ответственности предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого гражданского служащего или работника Департамента ЗАГС Забайкальского края в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей гражданских служащих и работников Департамента ЗАГС Забайкальского края строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

6.4.9. Принцип минимизации полномочий означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо пользователю для выполнения его

[117] См.: п.12 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

должностных регламентов (обязанностей).[118]

6.4.10. Принцип исключения конфликта интересов (разделения функций) предполагает четкое разделение обязанностей гражданских служащих и работников Департамента ЗАГС Забайкальского края и исключение ситуаций, когда сфера ответственности гражданских служащих и работников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что ни один гражданский служащий или работник Департамента ЗАГС Забайкальского края не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение гражданских служащих и работников полномочиями, порождающими конфликт интересов, дает им возможность манипулировать информацией в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными гражданскими служащими (работниками) или подразделениями Департамента ЗАГС Забайкальского края. Необходимо проводить периодические проверки обязанностей, функций и деятельности гражданских служащих или работников, выполняющих ключевые функции, с тем чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между гражданскими служащими и (или) работниками.

6.4.11. Принцип взаимодействия и сотрудничества предполагает создание благоприятной атмосферы в коллективах структурных подразделений Департамента ЗАГС Забайкальского края. В такой обстановке гражданские служащие и работники должны осознанно соблюдать установленные правила и оказывать содействие деятельности лицам, ответственным за безопасность информации[119].

6.4.12. Принцип гибкости системы защиты заключается в том, что система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Департаментом ЗАГС Забайкальского края своей деятельности. В число таких

---

[118] См.:

- п. УПД.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- п. УПД.5 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. УПД.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.9.4.5 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94
- п.6.2.4 и п.6.2.5. Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

[119] См.: п.4 приказа Департамента ЗАГС Забайкальского края от 02.09.2019 № 94 «Об утверждении Положения об администраторе безопасности информации информационных систем Департамента ЗАГС Забайкальского края».

изменений входят:

- изменения организационной и штатной структуры Департамента ЗАГС Забайкальского края;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства;
- новые виды деятельности.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

6.4.13. Принцип открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет конфиденциальности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна[120].

6.4.14. Принцип простоты применения средств защиты заключается в том, что механизмы и методы защиты должны быть понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

6.4.15. Принцип обоснованности и технической реализуемости заключается в том, что информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы в соответствии с требованием законодательства, обоснованы с точки зрения достижения заданного уровня безопасности информации (например, уровня защищенности персональных данных[121]) и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

6.4.16. Принцип специализации и профессионализма предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы, лицензии на право оказания услуг в этой области. Реализация организационно - распорядительных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Департамента ЗАГС Забайкальского края[122]

---

[120] См.: Приложение №1 к Положению о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденному приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91.

[121] См.:

- ст.8- ст.16 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.27 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[122] Во исполнение:

или уполномоченными лицами[123]).

6.4.17. Принцип обязательности контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности информации, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль, за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

VII. Организация и инфраструктура информационной безопасности в Департаменте ЗАГС Забайкальского края

7.1. Организация информационной безопасности в Департаменте ЗАГС Забайкальского края

Организация информационной безопасности в Департаменте ЗАГС Забайкальского края заключается в:

- определении лиц, ответственных за организацию и поддержание информационной безопасности в Департаменте ЗАГС Забайкальского края;
- регламентации оборота конфиденциальной информации на бумажных и электронных носителях;
- построении, вводе в эксплуатацию и аттестации системы защиты информационных систем;
- обучении пользователей по вопросам информационной безопасности[124].

- ст.14 и п. «б» ст.16 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- ст.18 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного Постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;
- п.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.3.16 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.5.1.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

[123] Осуществляющему деятельность по гражданско- правовому договору в соответствии с:

- ст. 3 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[124] См.:

- п.6) ч.1 ст.18.1, п.2) ч.4. ст.22.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п.18.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

7.1.1. Лица, ответственные за организацию и поддержание информационной безопасности в Департаменте ЗАГС Забайкальского края

7.1.1.1. Руководитель Департамента ЗАГС Забайкальского края как первый руководитель Департамента несет персональную ответственность за регламентацию порядка безопасной обработки конфиденциальной информации и обеспечение требований по технической защите конфиденциальной информации[125].

7.1.1.2. Руководитель подразделения безопасности информации[126], администратор безопасности информации[127] или уполномоченное

- п.3.16. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.21 «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденную приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06. 2001 № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
- п.2.3. «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;
- п.5.2 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100;
- п.6.2.6, п.7.3. Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96;
- п.7.6., п.7.12, п.7.16 Регламента безопасного функционирования подсистемы криптографической защиты информации системы защиты информации информационных систем Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 103.
- п. 3.1.2.4.5, п.3.1.2.4.6 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[125] В соответствии с:

- п.2.18 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.5.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[126] См.: п.1 приказа Департамента ЗАГС Забайкальского края от 02.09.2019 № 94 «Об утверждении Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края».

[127] Назначается во исполнение:

- ст. 3 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- ст.18 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного Постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;
- п.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.2.15. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.13 Требований о защите информации, содержащейся в информационных системах общего пользования, утвержденных приказом ФСБ России, ФСТЭК России от 31.08.2010 №489;
- п.5.1.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства

лицо[128] несут ответственность за защиту информационных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации информационных систем[129].

7.1.1.3. Лицо, ответственное за организацию обработки персональных данных,[130] несет ответственность за:

– осуществление внутреннего контроля за соблюдением гражданскими служащими и работниками законодательства Российской Федерации о защите персональных данных, в том числе требований к защите персональных данных[131];

– обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;
– п.6.1.5.7.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[128] Осуществляющее деятельность по гражданско- правовому договору в соответствии с:
– ст. 3 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
– п.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[129] См.:
– ст. 14 и ст. 15 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
– ст.18 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного Постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;
– п.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– п. 1.5, п.3.16 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
– п.10.4 ГОСТ Р ИСО/МЭК ТО 13335-3- 2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий;
– раздел IX Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[130] Назначается в соответствии с:
– ч.4 ст.22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
– абзаца 3 п. б) ст.1 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, утвержденного Постановлением Правительства Российской Федерации от 21.03.2012 №211.

[131] Осуществляется в соответствии с:
– п.4) ч.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
– п. д) ст.1 Постановления 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";
– ст.10 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного Постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;

- доведение до сведения гражданских служащих и работников Департамента ЗАГС Забайкальского края положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных[132];
- организации приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществлении контроля за приемом и обработкой таких обращений и запросов[133];
- осуществление контроля организации допуска сотрудников Департамента ЗАГС Забайкальского края к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности[134].

7.1.2. Регламентация оборота конфиденциальной информации на бумажных и электронных носителях в Департаменте ЗАГС Забайкальского края

7.1.2.1. В Департаменте ЗАГС Забайкальского края оборот конфиденциальной информации на бумажных носителях регламентирован следующими внутренними организационно-распорядительными актами:

- Положением о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденным приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91;
- разделом 6.6 Политики в отношении обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 92;
- Положением об архиве Департамента ЗАГС Забайкальского края, утвержденным приказом Департамента ЗАГС Забайкальского края

- разделом IX Политики в отношении обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 92;
- п.7.1.1 Положения об ответственном за организацию обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 93;
- Планом проведения периодических проверок условий обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденным приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 118.

[132] В соответствии с:

- п.6) ч.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п.7.1.2. Положения об ответственном за организацию обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 93.

[133] См.:

- ст.22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- п.7.1.3. Положения об ответственном за организацию обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 93.

[134] См.:

- п.7.1.3. Положения об ответственном за организацию обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 93;
- п.7.1.2 и п. 7.2.2 Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91.

от 02.09.2019 № 113;

- Положением об экспертной комиссии Департамента ЗАГС Забайкальского края, утвержденным приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 114;
- приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 116 «Об утверждении сроков и мест хранения материальных носителей персональных данных в Департаменте ЗАГС Забайкальского края».

7.1.2.2. В Департаменте ЗАГС Забайкальского края оборот конфиденциальной информации на электронных носителях регламентирован требованиями следующих внутренними организационно- распорядительных актов:

- Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96;
- Положения о порядке организации и проведении работ по защите конфиденциальной информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 97;
- приказа Департамента ЗАГС Забайкальского края от 02.09.2019 № 98 «О контролируемой зоне Департамента ЗАГС Забайкальского края»;
- Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100;
- Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 101;
- Инструкции по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 102;
- Регламента безопасного функционирования подсистемы криптографической защиты информации системы защиты информации информационных систем Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 103;
- Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107;
- Инструкции по организации парольной защиты информационных

систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 108;

- Инструкции по внесению изменений в конфигурацию информационных систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 110;
- Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111;
- Инструкции по резервному копированию информационных ресурсов информационных систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 112;
- Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91;
- Политики в отношении обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 92;
- приказа Департамента ЗАГС Забайкальского края от 02.09.2019 № 116 «Об утверждении сроков и мест хранения материальных носителей персональных данных в Департаменте ЗАГС Забайкальского края»

7.1.3. Система защиты информации информационных систем в Департаменте ЗАГС Забайкальского края

7.1.3.1. Система защиты информации информационных систем[135] в Департаменте ЗАГС Забайкальского края должна строиться на основании применения правовых[136], организационных[137] и технических[138] мер по обеспечению безопасности защищаемой информации.

7.1.3.2. В организационно - распорядительных документах, указанных в разделе 7.1.2. настоящей Политики, определяется необходимый уровень защищенности информации информационных систем Департамента ЗАГС Забайкальского края. На основании анализа актуальных угроз безопасности информации, описанного в Модели угроз[139], сделано заключение о необходимости использования

---

[135] См.:

- п.3) ч.1. ст.18.1, ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- ст.2 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119;
- п.12, п.14.4, п.15, п.15.1- п.15.2, п.16, п.16.1- п.16.7, п.17, п.17.1- п.17.5 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[136] См.: п.4.1.42 настоящей Политики.

[137] См.: п.4.1.35 настоящей Политики.

[138] См.: п.4.1.49 настоящей Политики.

[139] См.: Техническое задание «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края».

технических средств и организационных мероприятий для обеспечения безопасности защищаемой информации. Выбранные необходимые технические мероприятия отражены в Техническом проекте[140] и в Плане мероприятий защите информации информационных систем[141].

7.1.3.3. Для каждой информационной системы в соответствующем разработанном Паспорте информационной системы[142] составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке информации в информационной системе.

7.1.3.4. В зависимости от уровня защищенности информационных систем, актуальных угроз и предъявляемых требований к защите информации[143] система защиты включает следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- система защиты информации от НСД;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи[144].

---

[140] См.: Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». СЗ-ЗАГС.

[141] См.: План проведения периодических проверок условий обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденный приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 118.

[142] См.:

- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 2. Паспорт ГИС «МАИС ЗАГС». СЗ-ЗАГС.ПС. 01-ОР;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 3. Паспорт ИСПДн «1С Бухгалтерия». СЗ - ЗАГС. ПС.02-ОР;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 4. Паспорт ИСПДн «1С Зарплата и кадры». СЗ - ЗАГС. ПС .03-ОР.

[143] См.:

- ч.3 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.2.2. методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[144] См.:

- приказ ФАПСИ от 13.06.2001 №152 "Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну" (Зарегистрировано в Минюсте РФ 06.08.2001 № 2848);
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденные приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620).

7.1.3.5. Разработанная в Техническом проекте система защиты информации ИС включает следующие функции защиты (меры по обеспечению безопасности персональных данных), обеспечиваемые штатными средствами обработки информации, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты[145]:

- идентификации и аутентификации субъектов доступа и объектов доступа[146];
- управления доступом субъектов доступа к объектам доступа[147];
- ограничения программной среды[148];

---

[145] Перечень мер защиты устанавливается в соответствии с:

- п.20 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- подпунктом "б" п.5, п.7 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620).
- п.2.3, п.3.1, п.3.2 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[146] См.:

- п.20.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом I Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.1 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.3 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[147] См.:

- п.20.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом II Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.2 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.4 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[148]См:

- п. ОПС.1Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- п. ОПС.1 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ОПС.1Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной за-писки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- разд.9.5. Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

- защиты машинных носителей информации[149];
- регистрации событий безопасности[150];
- антивирусной защиты[151];
- обнаружения (предотвращения) вторжений[152];
- контроля (анализа) защищенности информации[153];

---

[149] См.:
- п.20.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом IV Приложения №2 к указанным Требованиям;
- разд.9.6 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[150] См.:
- п.20.5 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом V Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.4 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.6.1.5 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- разд.9.7 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[151] См.:
- п.20.6 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом VI Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.3, разд.3.6 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п.5.5 Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107;
- разд.9.8 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[152] См.:
- п.20.7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом VII Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.7 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- разд.9.9. Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[153] См.:
- п.20.8 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом VIII Приложения №2 к указанным Требованиям;
- п.2.3, разд.3.8 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);

– целостности информационной системы и информации[154];
– доступности информации[155];
– защиты среды виртуализации[156];
– защиты технических средств[157];
– защиты информационной системы, ее средств, систем связи и

– разд.9.10 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[154] См.:
– п.20.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом IX Приложения №2 к указанным Требованиям;
– п.2.3, разд.3.8 методического документа «Меры защиты информации в государственных ин-формационных системах» (утвержден ФСТЭК России 11.02.2014);
– разд.9.11 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
– п.6.1.2.3.4.1, п.6.1.5.5.1.8, п.6.4.1.3 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[155] См.:
– п.20.10 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом X Приложения №2 к указанным Требованиям;
– разд.3.2 методического документа «Меры защиты информации в государственных ин-формационных системах» (утвержден ФСТЭК России 11.02.2014);
– разд.9.12 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[156] См.:
– п.20.11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом XI Приложения №2 к указанным Требованиям;
– п.2.3, разд.3.11 методического документа «Меры защиты информации в государственных ин-формационных системах» (утвержден ФСТЭК России 11.02.2014);
– разд.9.13 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[157] См.:
– п.20.12 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом XII Приложения №2 к указанным Требованиям;
– подпунктом а) п.5 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ин-формационных 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620).
– разд.3.2 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
– разд.9.14 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

передачи данных[158].

7.1.3.6. Список используемых технических средств отражается в Техническом проекте на создание системы защиты информации информационных систем[159]. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИС, соответствующие изменения должны быть внесены в Технический проект по согласованию с разработчиком[160].

7.1.3.7. Подсистемы СЗИИС имеют различный функционал в зависимости от типов актуальных угроз и необходимого уровня защищенности персональных данных, определяемого в соответствии с:

- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных утвержденными Постановлением Правительства РФ от 01.11.2012 №1119;
- Приложением № 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных Приказом ФСТЭК России № 17 от 11.02.2013;
- Составом и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации,

---

[158] См.:

- п.20.13 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом XIII Приложения №2 к указанным Требованиям;
- разд.3.8 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- Техническое задание «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». СЗ-ЗАГС;
- разд.9.15 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[159] См.:

- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 2. Паспорт ГИС «МАИС ЗАГС». СЗ-ЗАГС.ПС. 01-ОР;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 3. Паспорт ИСПДн «1С Бухгалтерия». СЗ - ЗАГС. ПС.02-ОР;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 4. Паспорт ИСПДн «1С Зарплата и кадры». СЗ - ЗАГС. ПС .03-ОР.

[160] Исполняется в соответствии с:

- п.5.4.2., п.6.3.19 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282, а также п.5. Приложения 2 к указанным Специальным требованиям;
- п.6.1.5.7.2, п.6.3.2.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- п.6.4.2 Инструкции по внесению изменений в конфигурацию информационных систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 110.

необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденными приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620).

7.1.4. Обучение пользователей по вопросам информационной безопасности

7.1.4.1. Перед допуском к самостоятельной работе с информацией ограниченного доступа пользователи должны быть соответствующим образом проинструктированы администратором безопасности информации (или уполномоченным лицом, на который возложены обязанности по защите информации) или иным образом обучены правилам обращения с конфиденциальной информацией и средствами защиты информации[161].

7.2. Инфраструктура информационной безопасности в Департаменте ЗАГС Забайкальского края

Инфраструктура информационной безопасности заключается в[162]:

[161] Проводится в соответствии с:

- п.6) ч.1 ст.18.1, п.2) ч.4. ст.22.1 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п.18.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.3.16. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.21 «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденную приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06. 2001 № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
- п.2.3. «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;
- п.5.2 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100;
- п.6.2.6, п.7.3. Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96;
- п.7.6, п.7.12, п.7.16-п.7.17. Регламента безопасного функционирования подсистемы криптографической защиты информации системы защиты информации информационных систем Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 103;
- разд.9.2 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п.3.1.2.4.5 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[162] Состав инфраструктуры информационной безопасности установлен в соответствии с аб.5 п.10.3 ГОСТ Р ИСО/МЭК ТО 13335-3- 2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

- определении ролей и обязанностей пользователей по обеспечению информационной безопасности[163];
- регулярной проверке согласованности мер защиты информации[164];
- обработке инцидентов, связанных с нарушением безопасности[165].

7.2.1. Определение ролей и обязанностей должностных лиц по обеспечению информационной безопасности

7.2.1.1. В Техническом проекте определены следующие категории лиц, допущенных к работе в информационных системах Департамента ЗАГС Забайкальского края [166]:

- администратор информационной системы;
- администратор безопасности информации;
- пользователь.

7.2.1.2. В Паспортах информационных систем указанного Технического проекта разработаны матрицы доступа[167] для каждого вида лиц, допущенных к ресурсам информационной системы.

7.2.1.3. Данные о группах пользователей и администраторов, уровне их доступа и информированности отражены также в организационно распорядительных актах Департамента ЗАГС Забайкальского края[168].

7.2.1.4. Администратор информационной системы:

7.2.1.4.1. Администратор информационной системы – должностное лицо Департамента ЗАГС Забайкальского края или уполномоченное лицо (работник уполномоченного лица)[169],

---

[163] См.: п. 7.2.1 настоящей Политики.

[164] См.: п. 7.2.2 настоящей Политики.

[165] См.: п. 7.2.3 настоящей Политики.

[166] См.:

- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 2. Паспорт ГИС «МАИС ЗАГС». СЗ-ЗАГС.ПС. 01-ОР;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 3. Паспорт ИСПДн «1С Бухгалтерия». СЗ - ЗАГС. ПС.02-ОР;
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». Том 4. Паспорт ИСПДн «1С Зарплата и кадры». СЗ - ЗАГС. ПС .03-ОР.

В данном случае речь идет не о конкретных должностях, а о ролях при осуществлении прав доступа к защищаемым ресурсам. Поэтому руководитель подразделения безопасности информации при замещении администратора безопасности информации получает права доступа администратора безопасности информации, при замещении администратора ИС получает права доступа системного администратора.

[167] Разработаны во исполнение:

- п.1.24, п.5.1.3., п.5.9.1., п.5.9.2., п.6.3.2., п.6.3.11.4. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п. 15.1, п.16.3, п.18.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[168] См.:

- разд.6.1.1. Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- раздел VII Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

[169] Осуществляющее свои функциональные обязанности по гражданско-правовому договору, заключенному

ответственное за настройку, внедрение и сопровождение информационных систем[170]. Администратор информационной системы обеспечивает функционирование подсистемы управления доступом ИС и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя к элементам, хранящим защищаемую информацию.

7.2.1.4.2. Администратор информационной системы обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИС;
- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;
- обладает правами конфигурирования и административной настройки технических средств ИС.

7.2.1.5. Администратор безопасности информации:

7.2.1.5.1. Администратор безопасности информации - должностное лицо Департамента ЗАГС Забайкальского края или уполномоченное лицо (работник уполномоченного лица)[171], ответственное за функционирование СЗИИС, включая обслуживание и настройку административной, серверной и клиентской компонент.

7.2.1.5.2. Администратор безопасности информации обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИС;
- обладает полной информацией об ИС;
- имеет доступ к средствам защиты информации и протоколирования, а также к части ключевых элементов ИС;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

7.2.1.5.3. Администратор безопасности информации уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИС;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других органов власти и организаций.

7.2.1.6. Пользователь:

в соответствии с ч.3 ст.6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

[170] См.: п.6.1.5.7.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[171] Осуществляющее свои функциональные обязанности по гражданско- правовому договору, заключенному в соответствии с:

- ст.3Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119;
- п.10 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

7.2.1.6.1. Пользователь[172] - должностное лицо Департамента ЗАГС Забайкальского края или иного государственного (муниципального) органа (организации), допущенный в установленном порядке к работе с защищаемой информацией[173], полномочия которого регламентированы внутренними организационно - распорядительными актами[174] Департамента ЗАГС Забайкальского края. Обработка защищаемой информации включает: возможность просмотра информации, ручной ввод информации в информационную систему, формирование справок и отчетов по информации, полученной из ИС. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗИИС.

7.2.1.6.2. Пользователь обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;
- располагает конфиденциальными данными, к которым имеет доступ.

7.2.1.7. Конкретизация ролей производится в должностных регламентах (должностных обязанностях) лиц, допущенных к работе в ИС.

7.2.2. Регулярная проверка согласованности мер защиты информации

7.2.2.1. В Департаменте ЗАГС Забайкальского края должны проводиться следующие мероприятия по проверке согласованности мер защиты информации:

- поддержании в актуальном состоянии организационных мер защиты информации[175];
- контроле за неизменностью защищаемой инфраструктуры[176];
- контроле за работоспособностью средств защиты информации[177];
- выявлении и анализе уязвимостей ИС[178].

---

[172] См.: определение в п.4.1.41 настоящей Политики.

[173] В соответствии с:

- разделом VII Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91;
- разделами VI и VII Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

[174] См.:

- п.7.1.2 Политики информационной безопасности в Департаменте ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 90;
- раздела VI Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100.

[175] См.: п.8.5 и п.8.6. Положения о порядке организации и проведении работ по защите конфиденциальной информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 97.

[176] См.: разд.6.2.4 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[177] См.: разд.6.4.2 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[178] Исполняется в соответствии с:

- п.16.6 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013

7.2.3. Обработка инцидентов, связанных с нарушением безопасности информации[179]

7.2.3.1. В Департаменте ЗАГС Забайкальского края должны проводиться следующие мероприятия по обработке инцидентов, связанных с нарушением безопасности информации:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение и идентификация инцидентов, 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;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами[180];
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий[181];

№17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608):

- п.6.1.1. Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п. 3.1.5 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119;
- п.6.2.4.2.2 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[179] Осуществляется в соответствии с:

- п. 18.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разделом 6.2 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[180] См.:

- п.18.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.5.3. Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100;
- п.6.2.3.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[181] См.:

- п.6.1.1. Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п. 3.1.5 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев[182], устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов[183].

VIII. Политика в отношении безопасности аппаратно-программного обеспечения в Департаменте ЗАГС Забайкальского края

Политика в отношении безопасности аппаратно- программного обеспечения в Департаменте ЗАГС Забайкальского края строится на осуществлении политик более низкого уровня[184]:

- политики идентификации и аутентификации субъектов доступа[185];
- политики управления доступом субъектов доступа к объектам доступа[186];
- политики ограничения программной среды [187];

---

[182] Применяется только для ГИС «МАИС ЗАГС». См.:
- п. ОДТ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. 3.9 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п. ОДТ.5 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ОДТ.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п. 5.5 Инструкции по резервному копированию информационных ресурсов информационных систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 112;
- разд.6.1.2, разд.6.2.5 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- п.9.12.5 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п.3.3.2.3 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[183] См.: п.6.2.6.3 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[184] См.: аналогичный методический подход применительно к п. ИАФ.0, п. УПД.0, п. ОПС.0, п. ЗНИ.0, п. АУД.0, п. АВЗ.0, п. СОВ.0, п. ОЦЛ.0, п. ОДТ.0, п. ЗТС.0, п. ЗИС.0, п. ИНЦ.0, п. УКФ.0, п. ОПО.0, п. ПЛН.0, п. ДНС.0, п. ИПО.0 Приложения к Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСТЭК России от 25.12.2017 №239 (Зарегистрировано в Минюсте России 26.03.2018 №50524).

[185] См.: п.8.1 настоящей Политики.

[186] См.: п.8.2 настоящей Политики.

[187] См.: п.8.3 настоящей Политики.

- политики защиты машинных носителей информации[188];
- политики регистрации событий безопасности [189];
- политики антивирусной защиты [190];
- политики обнаружения вторжений;[191]
- политики контроля (анализа) защищенности информации [192]
- политики обеспечения целостности информационной системы и информации [193];
- политики обеспечения доступности информации[194];
- политики защиты среды виртуализации;[195]
- политика защиты технических средств[196].

8.1. Политика идентификации и аутентификации субъектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа в информационные системы Департамента ЗАГС Забайкальского края должны обеспечиваться присвоением субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверкой принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности)[197].

Применяемая в Департаменте ЗАГС Забайкальского края политика идентификации и аутентификации устанавливает требования к:

---

[188] См.: п.8.4 настоящей Политики.
[189] См.: п.8.5 настоящей Политики.
[190] См.: п.8.6 настоящей Политики.
[191] См.: п.8.7 настоящей Политики.
[192] См.: п.8.8 настоящей Политики.
[193] См.: п.8.9 настоящей Политики.
[194] См.: п.8.10 настоящей Политики.
[195] См.: п.8.11 настоящей Политики.
[196] См.: п.8.12 настоящей Политики.
[197] Исполняется в соответствии с:

- п.20.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п.ИАФ.1 - п. ИАФ.6 Приложения №2 к указанным Требованиям;
- абзаца второго п.2.3., п.3.1 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п.1.15 РД «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. (Утверждено решением председателя Гостехкомиссии России от 30.03.1992);
- п.ИАФ.1 - п. ИАФ.6 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п.ИАФ.1 - п. ИАФ.6 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.9.3.1, п.9.3.2 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п.6.1.1. Инструкции по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 102.

- идентификации и аутентификации пользователей, являющихся работниками оператора[198];
- идентификации и аутентификации устройств, в том числе стационарных, мобильных и портативных[199];
- управлению идентификаторами, в том числе созданию, присвоению, уничтожению идентификаторов[200];
- управлению средствами аутентификации, в том числе хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации[201];
- защите обратной связи при вводе аутентификационной информации[202];
- идентификации и аутентификации пользователей, не являющихся работниками оператора (внешних пользователей)[203].

8.1.1. Идентификация и аутентификация пользователей, являющихся работниками оператора

8.1.1.1. Должны выполняться следующие требования Регуляторов к реализации идентификации и аутентификации пользователей, являющихся работниками оператора:[204]

8.1.1.1.1. В информационной системе должна обеспечиваться идентификация и аутентификация пользователей, являющихся работниками оператора.

8.1.1.1.2. При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками оператора (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

8.1.1.1.3. К внутренним пользователям в целях настоящего документа, относятся должностные лица оператора (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств информационной системы в соответствии с должностными регламентами (инструкциями) утвержденными оператором и которым в информационной системе присвоены учетные записи.

8.1.1.1.4. В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования информационной системы (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами оператора и которым в информационной системе также присвоены учетные записи.

---

[198] См.: разд.8.1.1. настоящей Политики.
[199] См.: разд.8.1.2. настоящей Политики.
[200] См.: разд.8.1.3. настоящей Политики.
[201] См.: разд.8.1.4. настоящей Политики.
[202] См.: разд.8.1.5. настоящей Политики.
[203] См.: разд.8.1.6. настоящей Политики.
[204] См.: разд. «Требования к реализации ИАФ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.16-л.17.

8.1.1.1.5. Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации требованиями Регуляторов[205].

8.1.1.1.6. Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, биометрических характеристик, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств. В информационной системе должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

8.1.1.2. Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах по защите информации.

8.1.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по идентификации и аутентификации пользователей, являющихся работниками оператора[206]:

8.1.1.3.1. В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами привилегированных учетных записей (администраторов):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

б) без использования сети связи общего пользования.

8.1.1.3.2. В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для удаленного доступа в систему с правами непривилегированных учетных записей (пользователей):

а) с использованием сети связи общего пользования, в том числе сети Интернет;

б) без использования сети связи общего пользования.

8.1.1.3.3. В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами привилегированных учетных записей (администраторов).

8.1.1.3.4. В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация для локального доступа в систему с правами непривилегированных учетных записей (пользователей).

---

[205] См.:

- УПД.11 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.11» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.37.

[206] См.: разд. «Требования к реализации ИАФ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.17.

8.1.1.3.5. В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами привилегированных учетных записей (администраторов), где один из факторов обеспечивается аппаратным устройством аутентификации, отделенным от информационной системы, к которой осуществляется доступ.

8.1.1.3.6. В информационной системе должна обеспечиваться многофакторная (двухфакторная) аутентификация при доступе в систему с правами непривилегированных учетных записей (пользователей), где один из факторов обеспечивается устройством, отделенным от информационной системы, к которой осуществляется доступ.

8.1.1.3.7. В информационной системе должен использоваться механизм одноразовых паролей при аутентификации пользователей, осуществляющих удаленный или локальный доступ.

8.1.1.3.8. В информационной системе для аутентификации пользователей должно обеспечиваться применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

8.1.2. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных[207]

8.1.2.1. Должны выполняться следующие требования Регуляторов к реализации идентификация и аутентификации устройств, в том числе стационарных, мобильных и портативных:[208]

8.1.2.1.1. В информационной системе до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация и аутентификация устройств (технических средств).

8.1.2.1.2. Оператором должен быть определен перечень типов устройств, используемых в информационной системе и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

8.1.2.1.3. Идентификация устройств в информационной системе обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC адресам) устройства или по комбинации имени, логического и (или) физического адресов

---

[207] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- п. ИАФ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.02.2013 №17 (Зарегистрировано в Минюсте России 31.05.2013 № 28608);
- п. ИАФ. 2 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ИАФ.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[208] См.: разд. «Требования к реализации ИАФ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.18.

устройства.

8.1.2.1.4. Аутентификация устройств в информационной системе обеспечивается с использованием соответствующих протоколов аутентификации или с применением в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

8.1.2.2. Правила и процедуры идентификации и аутентификации устройств регламентируются в организационно-распорядительных документах оператора по защите информации.

8.1.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по идентификации и аутентификации устройств, в том числе стационарных, мобильных и портативных[209]:

8.1.2.3.1. В информационной системе должна обеспечиваться аутентификация устройств до начала информационного взаимодействия с ними:

а) взаимная аутентификация устройства и средства вычислительной техники (или другого взаимодействующего устройства);

б) аутентификация по уникальным встроенным средствам аутентификации.

8.1.3. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

8.1.3.1. Должны выполняться следующие требования Регуляторов к реализации управления идентификаторами, в том числе созданием, присвоением, уничтожением идентификаторов:[210]

8.1.3.1.1. Оператором должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в информационной системе:

- определение должностного лица (администратора) оператора, ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств;
- формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство; присвоение идентификатора пользователю и (или) устройству;
- предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного оператором периода времени;
- блокирование идентификатора пользователя после установленного оператором времени неиспользования.

8.1.3.2. Правила и процедуры управления идентификаторами регламентируются в организационно-распорядительных документах оператора по защите информации.

8.1.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению идентификаторами, в том

---

[209] См.: разд. «Требования к реализации ИАФ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.18.

[210] См.: разд. «Требования к реализации ИАФ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.19- л.20.

числе созданием, присвоением, уничтожением идентификаторов:[211]

8.1.3.3.1. Оператором должно быть исключено повторное использование идентификатора пользователя в течение:

а) не менее одного года;

б) не менее трех лет; в) в течение всего периода эксплуатации информационной системы.

8.1.3.3.2. Оператором должно быть обеспечено блокирование идентификатора пользователя через период времени неиспользования:

а) не более 90 дней;

б) не более 45 дней.

8.1.3.3.3. Оператором должно быть обеспечено использование различной аутентификационной информации (различных средств аутентификации) пользователя для входа в информационную систему и доступа к прикладному (специальному) программному обеспечению.

8.1.3.3.4. Оператором должно быть исключено использование идентификатора пользователя информационной системы при создании учетной записи пользователя публичной электронной почты или иных публичных сервисов.

8.1.3.3.5. Оператором должно быть обеспечено управление идентификаторами внешних пользователей, учетные записи которых используются для доступа к общедоступным ресурсам информационной системы.

8.1.4. Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

8.1.4.1. Должны выполняться следующие требования Регуляторов к реализации управления средствами аутентификации, в том числе хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации:[212]

8.1.4.1.1. Оператором должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в информационной системе:

- определение должностного лица (администратора) оператора, ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации

[211] См.: разд. «Требования к реализации ИАФ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675л.20.

[212] См.: разд. «Требования к реализации ИАФ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.20- л.22.

информационной системы; выдача средств аутентификации пользователям;

- генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);
- установление характеристик пароля (при использовании в информационной системе механизмов аутентификации на основе пароля):
  а) задание минимальной сложности пароля с определяемыми оператором требованиями к регистру, количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
  б) задание минимального количества измененных символов при создании новых паролей;
  в) задание максимального времени действия пароля;
  г) задание минимального времени действия пароля;
  д) запрет на использование пользователями определенного оператором числа последних использованных паролей при создании новых паролей;
- блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;
- назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);
- обновление аутентификационной информации (замена средств аутентификации) с периодичностью, установленной оператором;
- защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

8.1.4.2. Правила и процедуры управления средствами аутентификации (аутентификационной информацией) регламентируются в организационно-распорядительных документах оператора по защите информации.

8.1.4.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению средствами аутентификации, в том числе хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации[213]:

8.1.4.3.1. В случае использования в информационной системе механизмов аутентификации на основе пароля (иной последовательности символов, используемой для аутентификации) или применения пароля в качестве одного из факторов многофакторной аутентификации, его характеристики должны быть следующими:

а) длина пароля не менее шести символов, алфавит пароля не менее 30 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в

[213] См.: разд. «Требования к реализации ИАФ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.21- л.22.

случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут, смена паролей не более чем через 180 дней;

б) длина пароля не менее шести символов, алфавит пароля не менее 60 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 5 до 30 минут, смена паролей не более чем через 120 дней;

в) длина пароля не менее шести символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 8 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 10 до 30 минут, смена паролей не более чем через 90 дней;

г) длина пароля не менее восьми символов, алфавит пароля не менее 70 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 4 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 до 60 минут, смена паролей не более чем через 60 дней.

8.1.4.3.2. В информационной системе должно быть обеспечено использование автоматизированных средств для формирования аутентификационной информации (генераторов паролей) с требуемыми характеристиками стойкости (силы) механизма аутентификации и для оценки характеристик этих механизмов.

8.1.4.3.3. В информационной системе должно быть обеспечено использование серверов и (или) программного обеспечения аутентификации для единой аутентификации в компонентах информационной системы и компонентах программного обеспечения, предусматривающего собственную аутентификацию.

8.1.4.3.4. Оператор должен обеспечить получение (запросить) у поставщика технических средств и программного обеспечения информационной системы аутентификационную информацию, заданную производителем этих технических средств и программного обеспечения и не указанную в эксплуатационной документации.

8.1.4.3.5. Оператором должны быть определены меры по исключению возможности использования пользователями их идентификаторов и паролей в других информационных системах.

8.1.5. Защита обратной связи при вводе аутентификационной информации

8.1.5.1. Должны выполняться следующие требования Регуляторов к реализации защиты обратной связи при вводе аутентификационной

информации:[214]

8.1.5.1.1. В информационной системе должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

8.1.5.1.2. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации.

8.1.5.1.3. Вводимые символы пароля могут отображаться условными знаками «*», « » или иными знаками.

8.1.5.2. Требования к мероприятиям по усилению защиты обратной связи при вводе аутентификационной информации Регуляторами не установлены[215].

8.1.6. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

8.1.6.1. Должны выполняться следующие требования Регуляторов к реализации идентификации и аутентификации пользователей, не являющихся работниками оператора (внешних пользователей):[216]

8.1.6.1.1. В информационной системе должна осуществляться однозначная идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей), или процессов, запускаемых от имени этих пользователей.

8.1.6.1.2. К пользователям, не являющимся работникам оператора (внешним пользователям), относятся все пользователи информационной системы, не указанные в ИАФ.1 в качестве внутренних пользователей.

8.1.6.1.3. Примером внешних пользователей являются граждане, на законных основаниях через сеть Интернет получающие доступ к информационным ресурсам портала Государственных услуг Российской Федерации «Электронного правительства» или официальным сайтам в сети Интернет органов государственной власти.

8.1.6.1.4. Пользователи информационной системы должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с требованиями Регуляторов[217]. Идентификация и

---

[214] См.: разд. «Требования к реализации ИАФ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.22.

[215] См.: разд. «Требования к реализации ИАФ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.22.

[216] См.: разд. «Требования к реализации ИАФ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.23.

[217] См.:

– УПД.11 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом

аутентификация внешних пользователей в целях предоставления государственных услуг осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28 ноября 2011 г. № 977.

8.1.6.2. Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

8.1.6.3. Требования к усилению мероприятий по идентификации и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) Регуляторами не установлены[218].

8.2. Политика управления доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа в информационные системы Департамента ЗАГС Забайкальского края должны обеспечиваться управлением правами и привилегиями субъектов доступа, разграничением доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечении контроля соблюдения этих правил[219].

Применяемая в Департаменте ЗАГС Забайкальского края политика управления доступом субъектов доступа к объектам доступа устанавливает требования к:

- управлению (заведению, активации, блокированию и уничтожению)

ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

- разд. «Требования к реализации УПД.11» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.37.

[218] См.: разд. «Требования к реализации ИАФ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.23.

[219] Исполняется в соответствии с:

- п. 20.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п.УПД.1- п.УПД.6, п.УПД.9- п.УПД.17 Приложения №2 к указанным Требованиям;;
- п.2.3, п.3.2, п. методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п.УПД.1- п.УПД.6, п.УПД.9- п.УПД.17 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п.УПД.1- п.УПД.6, п.УПД.9- п.УПД.17 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.9.4.2 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- разд.6.1.1. Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

учетными записями пользователей, в том числе внешних пользователей[220];

- реализации необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа[221];
- разделению полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы[222];
- назначению минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы[223];
- ограничению неуспешных попыток входа в информационную систему (доступа к информационной системе)[224];
- ограничению числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы[225];
- блокированию сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу[226];
- разрешению (запрету) действий пользователей, разрешенных до идентификации и аутентификации[227];
- обеспечению доверенной загрузки средств вычислительной техники[228].

8.2.1. Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

8.2.1.1. Должны выполняться следующие требования Регуляторов к реализации управления (заведения, активации, блокирования и уничтожения) учетными записями пользователей, в том числе внешних пользователей:[229]

8.2.1.1.1. Оператором должны быть установлены и реализованы следующие функции управления учетными записями пользователей, в том числе внешних пользователей:

- определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);
- объединение учетных записей в группы (при необходимости);
- верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя; заведение, активация, блокирование и уничтожение учетных записей пользователей;
- пересмотр и, при необходимости, корректировка учетных записей пользователей с периодичностью, определяемой

[220] См.: разд. 8.2.1 настоящей Политики.
[221] См.: разд. 8.2.2 настоящей Политики.
[222] См.: разд. 8.2.3 настоящей Политики.
[223] См.: разд. 8.2.4 настоящей Политики.
[224] См.: разд. 8.2.5 настоящей Политики.
[225] См.: разд. 8.2.6 настоящей Политики.
[226] См.: разд. 8.2.7 настоящей Политики.
[227] См.: разд. 8.2.8 настоящей Политики.
[228] См.: разд. 8.2.9 настоящей Политики.
[229] См.: разд. «Требования к реализации УПД.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.25-л.26.

оператором;

- порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов;
- оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;
- уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;
- предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами.

8.2.1.1.2. Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

8.2.1.2. Правила и процедуры управления учетными записями пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

8.2.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению учетными записями пользователей, в том числе внешних пользователей[230]:

8.2.1.3.1. Оператором должны использоваться автоматизированные средства поддержки управления учетными записями пользователей.

8.2.1.3.2. В информационной системе должно осуществляться автоматическое блокирование временных учетных записей пользователей по окончании установленного периода времени для их использования.

8.2.1.3.3. В информационной системе должно осуществляться автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей после периода времени неиспользования:

а) более 90 дней;

б) более 45 дней.

8.2.1.3.4. В информационной системе должно осуществляться автоматическое блокирование учетных записей пользователей:

а) при превышении установленного оператором числа неуспешных попыток аутентификации пользователя;

б) при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к

[230] См.: разд. «Требования к реализации УПД.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.26.

событиям нарушения безопасности информации.

8.2.1.3.5. В информационной системе должен осуществляться автоматический контроль заведения, активации, блокирования и уничтожения учетных записей пользователей и оповещение администраторов о результатах автоматического контроля.

8.2.2. Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа

8.2.2.1. Должны выполняться следующие требования Регуляторов к реализации необходимых методов, типов и правил разграничения доступа:[231]

8.2.2.1.1. В информационной системе для управления доступом субъектов доступа к объектам доступа должны быть реализованы установленные оператором методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа.

8.2.2.1.2. Методы управления доступом реализуются в зависимости от особенностей функционирования информационной системы, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов:

- дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;
- ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);
- мандатный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий.

8.2.2.1.3. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа.

8.2.2.1.4. Правила разграничения доступа реализуются на основе установленных оператором списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей

[231] См.: разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.26- л.28.

(групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

8.2.2.2. Правила разграничения доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

8.2.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по реализации необходимых методов, типов и правил разграничения доступа[232]:

8.2.2.3.1. В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов при входе в информационную систему.

8.2.2.3.2. В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к техническим средствам, устройствам, внешним устройствам.

8.2.2.3.3. В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым общесистемным (общим) программным обеспечением.

8.2.2.3.4. В информационной системе правила разграничения доступа должны обеспечивать управление доступом субъектов к объектам, создаваемым прикладным и специальным программным обеспечением.

8.2.3. Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы

8.2.3.1. Должны выполняться следующие требования Регуляторов к реализации разделению полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы:[233]

8.2.3.1.1. Оператором должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей).

---

[232] См.: разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.27- л.28.

[233] См.: разд. «Требования к реализации УПД.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.30- л.31.

8.2.3.1.2. Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с требованиями Регуляторов[234].

8.2.3.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по разделению полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы[235]:

8.2.3.2.1. Оператором должно быть обеспечено выполнение каждой роли по обработке информации, администрированию информационной системы, ее системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы отдельным должностным лицом.

8.2.3.2.2. Оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по обработке информации и полномочиями (ролью) по администрированию информационной системы и (или) ее системы защиты информации, контролю (мониторингу) за обеспечением уровня защищенности информации, обеспечению функционирования информационной системы.

8.2.3.2.3. Оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по контролю (мониторингу) за обеспечением уровня защищенности информации и полномочиями (ролью) по администрированию информационной системы и (или) ее системы защиты информации и обеспечению функционирования информационной системы.

8.2.3.2.4. Оператором должно быть обеспечено исключение наделения одного должностного лица полномочиями (ролью) по администрированию системы защиты информации информационной системы и полномочиями (ролью) по обеспечению функционирования информационной системы.

8.2.3.2.5. Оператором должен быть определен администратор, имеющий права по передаче полномочий по администрированию информационной системы и системы защиты информации другим лицам и осуществляющий контроль за использованием переданных полномочий (супервизор).

8.2.4. Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы

8.2.4.1. Должны выполняться следующие требования Регуляторов к

---

[234] См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.27- л.28.

[235] См.: разд. «Требования к реализации УПД.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.30- л.31.

реализации назначения минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы:[236]

8.2.4.1.1. Оператором должно быть обеспечено назначение прав и привилегий пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование информационной системы, минимально необходимых для выполнения ими своих должностных обязанностей (функций), и санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями.

8.2.4.1.2. Оператором должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий.

8.2.4.1.3. Доступ к объектам доступа с учетом минимально необходимых прав и привилегий обеспечивается в соответствии с требованиями Регуляторов[237].

8.2.4.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по назначению минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы:[238]

8.2.4.2.1. Оператором должно быть обеспечено предоставление прав и привилегий по доступу к функциям безопасности (параметрам настройки) средств защиты информации исключительно администратору, наделенному полномочиями по администрированию системы защиты информации (администратору безопасности).

8.2.4.2.2. Запрет предоставления расширенных прав и привилегий внешним пользователям (пользователям, не являющимся внутренними пользователями).

8.2.5. Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)

8.2.5.1. Должны выполняться следующие требования Регуляторов к реализации ограничения неуспешных попыток входа в

---

[236] См.: разд. «Требования к реализации УПД.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.31- л.32.

[237] См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.27- л.28.

[238] См.: разд. «Требования к реализации УПД.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.31- л.32.

информационную систему (доступа к информационной системе):[239]

8.2.5.1.1. В информационной системе должно быть установлено и зафиксировано в организационно-распорядительных документах оператора по защите информации (задокументировано) ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе).

8.2.5.1.2. Ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) должно обеспечиваться в соответствии с требованиями Регуляторов.[240]

8.2.5.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по ограничению неуспешных попыток входа в информационную систему (доступа к информационной системе)[241]:

8.2.5.2.1. В информационной системе обеспечивается автоматическое блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени с возможностью разблокирования только администратором или иным лицом, имеющим соответствующие полномочия (роль).

8.2.5.2.2. В информационной системе обеспечивается автоматическое удаление информации с мобильного технического средства, входящего в состав информационной системы, при превышении допустимого числа неуспешных попыток входа в информационную систему (доступа к информационной системе) за установленный период времени, осуществляемых с мобильного устройства.

8.2.5.2.3. В информационной системе обеспечивается противодействие автоматизированному подбору паролей с использованием однократных кодов, требующих визуального распознавания (в том числе с использованием технологии CAPTCHA).

---

[239] См.: разд. «Требования к реализации УПД.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.32- л.33.

[240] См.:

- ИАФ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.20- л.22.

[241] См.: разд. «Требования к реализации УПД.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.32- л.33.

8.2.6. Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы[242]

8.2.6.1. Должны выполняться следующие требования Регуляторов к реализации ограничения числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы[243]:

8.2.6.1.1. В информационной системе должно быть обеспечено предупреждение пользователя в виде сообщения («окна») при его входе в информационную систему (до процесса аутентификации) о том, что в информационной системе реализованы меры защиты информации, а также о том, что при работе в информационной системе пользователем должны быть соблюдены установленные оператором правила и ограничения на работу с информацией.

8.2.6.1.2. Вход в информационную систему и предоставление пользователю возможности работы в информационной системе осуществляются только после подтверждения пользователем ознакомления с предупреждением.

8.2.6.2. Требования к усилению мероприятий по ограничению числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы Регуляторами не установлены[244].

8.2.7. Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу

8.2.7.1. Должны выполняться следующие требования Регуляторов к реализации блокирования сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу:[245]

8.2.7.1.1. В информационной системе должно обеспечиваться блокирование сеанса доступа пользователя после установленного оператором времени его бездействия (неактивности) в информационной системе или по запросу пользователя.

---

[242] Исполняется только для 1 класса защищенности информационной системы. См.:

- УПД.9 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- УПД.9 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- УПД.9 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[243] См.: разд. «Требования к реализации УПД.9» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.35- л.36.

[244] См.: разд. «Требования к реализации УПД.9» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.35- л.36.

[245] См.: разд. «Требования к реализации УПД.10» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.36- л.37.

8.2.7.1.2. Блокирование сеанса доступа пользователя в информационную систему обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к информационной системе (без выхода из информационной системы).

8.2.7.1.3. Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

8.2.7.1.4. Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации в соответствии с требованиями Регуляторов[246].

8.2.7.2. Правила и процедуры блокирования сеансов доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

8.2.7.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по блокированию сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу[247]:

8.2.7.3.1. В информационной системе обеспечивается блокирование сеанса доступа пользователя после времени бездействия (неактивности) пользователя:

а) до 15 минут;

б) до 5 минут.

8.2.7.3.2. В информационной системе на устройстве отображения (мониторе) после блокировки сеанса не должна отображаться информация сеанса пользователя (в том числе использование «хранителя экрана», гашение экрана или иные способы).

8.2.7.3.3. В информационной системе обеспечивается завершение сеанса пользователя (выхода из системы) после превышения установленного оператором времени бездействия (неактивности) пользователя.

8.2.8. Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации

8.2.8.1. Должны выполняться следующие требования Регуляторов к реализации разрешения (запрет) действий пользователей, разрешенных до идентификации и аутентификации:[248]

---

[246] См.:

- ИАФ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.16-л.17.

[247] См.: разд. «Требования к реализации УПД.10» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.36- л.37.

[248] См.: разд. «Требования к реализации УПД.11» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014),

8.2.8.1.1. Оператором должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации.

8.2.8.1.2. Разрешение действий пользователей до прохождения ими процедур идентификации и аутентификации осуществляется, в том числе, при предоставлении пользователям доступа к общедоступной информации (вебсайтам, порталам, иным общедоступным ресурсам).

8.2.8.1.3. Также администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

8.2.8.2. Правила и процедуры определения действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, регламентируются в организационно-распорядительных документах оператора по защите информации.

8.2.8.3. Требования к усилению мероприятий по разрешению (запрету) действий пользователей, разрешенных до идентификации и аутентификации Регуляторами не установлены[249].

8.2.9. Обеспечение доверенной загрузки средств вычислительной техники[250]

8.2.9.1. Должны выполняться следующие требования Регуляторов к реализации обеспечения доверенной загрузки средств вычислительной техники:[251]

8.2.9.1.1. В информационной системе должно обеспечиваться исключение несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники информационной системы на этапе его загрузки.

8.2.9.1.2. Доверенная загрузка должна обеспечивать: блокирование попыток несанкционированной загрузки нештатной

---

https://fstec.ru/component/attachments/download/675, л.37.

[249] См.: разд. «Требования к реализации УПД.11» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.37.

[250] Исполняется только для информационных систем 1 и 2 классов защищенности. См.:

- УПД.17 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- УПД.17 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- УПД.17 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[251] См.: разд. «Требования к реализации УПД.17» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.45-л.46.

операционной системы (среды) или недоступность информационных ресурсов для чтения или модификации в случае загрузки нештатной операционной системы; контроль доступа пользователей к процессу загрузки операционной системы; контроль целостности программного обеспечения и аппаратных компонентов средств вычислительной техники.

8.2.9.1.3. В информационной системе применяется доверенная загрузка на разных уровнях (уровня базовой системы ввода-вывода, уровня платы расширения и уровня загрузочной записи).

8.2.9.2. Правила и процедуры обеспечения доверенной загрузки средств вычислительной техники регламентируются в организационно-распорядительных документах оператора по защите информации.

8.2.9.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обеспечению доверенной загрузки средств вычислительной техники:

8.2.9.3.1. В информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения.

8.2.9.3.2. В информационной системе должна осуществляться доверенная загрузка уровня базовой системы ввода-вывода или уровня платы расширения, реализованные на основе программно-аппаратного модуля.

8.2.9.3.3. В информационной системе должна осуществляться доверенная загрузка программного обеспечения телекоммуникационного оборудования.

8.3. Политика ограничения программной среды

Применяемая в Департаменте ЗАГС Забайкальского края политика ограничения программной среды устанавливает требования к:

- управлению запуском (обращениями) компонентов программного обеспечения, в том числе определению запускаемых компонентов, настройке параметров запуска компонентов, контролю за запуском компонентов программного обеспечения[252];
- управлению установкой (инсталляцией) компонентов программного обеспечения, в том числе определению компонентов, подлежащих установке, настройке параметров установки компонентов, контролю за установкой компонентов программного обеспечения[253];
- установке (инсталляции) только разрешенного к использованию программного обеспечения и (или) его компонентов[254].

8.3.1. Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения[255]

[252] См.: разд.8.3.1 настоящей Политики.

[253] См.: разд.8.3.2 настоящей Политики.

[254] См.: разд.8.3.3 настоящей Политики.

[255] Исполняется только для ИС 1 категории защищенности. См.:

- ОПС.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

8.3.1.1. Должны выполняться следующие требования Регуляторов к реализации управления запуском (обращениями) компонентов программного обеспечения, в том числе определения запускаемых компонентов, настройки параметров запуска компонентов, контроля за запуском компонентов программного обеспечения:[256]

8.3.1.1.1. Оператором должны быть реализованы следующие функции по управлению запуском (обращениями) компонентов программного обеспечения:

- определение перечня (списка) компонентов программного обеспечения (файлов, объектов баз данных, хранимых процедур и иных компонентов), запускаемых автоматически при загрузке операционной системы средства вычислительной техники;
- разрешение запуска компонентов программного обеспечения, включенных в перечень (список) программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;
- ограничение запуска компонентов программного обеспечения от имени администраторов безопасности (например, разрешение такого запуска только для программного обеспечения средств защиты информации: сенсоры систем обнаружения вторжений, агенты систем мониторинга событий информационной безопасности, средства антивирусной защиты);
- настройка параметров запуска компонентов программного обеспечения от имени учетной записи администратора безопасности таким образом, чтобы текущий пользователь средства вычислительной техники не мог получить через данные компоненты доступ к объектам доступа, на доступ к которым у него нет прав в соответствии требованиями Регуляторов[257];
- контроль за запуском компонентов программного обеспечения, обеспечивающий выявление компонентов программного обеспечения, не включенных в перечень

- ОПС.1 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОПС.1 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[256] См.: разд. «Требования к реализации ОПС.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.47-л.48.

[257] См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.26- л.28.

(список) компонентов, запускаемых автоматически при загрузке операционной системы средства вычислительной техники.

8.3.1.2. Правила и процедуры управления запуском программного обеспечения (в том числе списки программного обеспечения, ограничения запуска, параметры запуска компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации.

8.3.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению запуском (обращениями) компонентов программного обеспечения[258]:

8.3.1.3.1. В информационной системе обеспечивается разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности.

8.3.1.3.2. В информационной системе обеспечивается использование средств автоматизированного контроля перечня (списка)компонентов программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники.

8.3.1.3.3. В информационной системе обеспечивается использование автоматизированных механизмов управления запуском (обращениями) компонентов программного обеспечения.

8.3.1.3.4. В информационной системе обеспечивается управление удаленным запуском компонентов программного обеспечения (например, запрет запуска компонентов программного обеспечения на одном средстве вычислительной техники командой с другого средства вычислительной техники).

8.3.1.3.5. В информационной системе обеспечивается управление временем запуска и завершения работы компонентов программного обеспечения (например, ограничение запуска только в течение рабочего дня).

8.3.1.3.6. В информационной системе обеспечивается контроль целостности (состояния) запускаемых компонентов программного обеспечения (файлов (в том числе конфигурационных), объектов баз данных, подключаемых библиотек и др.) в соответствии с требованиями Регуляторов[259].

8.3.1.3.7. В информационной системе обеспечивается контроль обновления запускаемых компонентов программного обеспечения.

8.3.1.3.8. В информационной системе обеспечивается регистрация событий, связанных с контролем состояния и обновлением

---

[258] См.: разд. «Требования к реализации ОПС.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.48.

[259] См.:

- ОЦЛ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ОЦЛ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.86-л.87.

запускаемых компонентов программного обеспечения.

8.3.1.3.9. В информационной системе обеспечивается запрет (блокирование) запуска определенных оператором компонентов программного обеспечения, не прошедших аутентификацию в соответствии с требованиями Регуляторов[260].

8.3.2. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения[261]

8.3.2.1. Должны выполняться следующие требования Регуляторов к реализации управления установкой (инсталляцией) компонентов программного обеспечения:[262]

8.3.2.1.1. Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:

- определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;
- настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);
- выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации,

---

[260] См.:

- ИАФ.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.24.

[261] Исполняется только для ИС 1 и 2 класса защищенности информационной системы. См.:

- ОПС.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОПС.2 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОПС.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[262] См.: разд. «Требования к реализации ОПС.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.48-л.50.

предусматривающие включение в домен, или не включение в домен);

- контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);
- определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.

8.3.2.2. Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.

8.3.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению установкой (инсталляцией) компонентов программного обеспечения[263]:

8.3.2.3.1. В информационной системе должно обеспечиваться использование средств автоматизации для применения и контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации.

8.3.2.3.2. В информационной системе должны быть реализованы автоматизированные механизмы реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации, предусматривающие блокирование доступа к средству вычислительной техники и (или) информации, автоматическое восстановление параметров настройки или другие действия, препятствующие несанкционированному доступу к информации, который может быть получен вследствие несанкционированного изменения параметров настройки.

8.3.2.3.3. В информационной системе должно обеспечиваться использование средств автоматизации для инсталляции и централизованного управления процессами инсталляции, в том числе с применением пакетов соответствующих дистрибутивов программного обеспечения.

8.3.3. Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

8.3.3.1. Должны выполняться следующие требования Регуляторов к реализации установки (инсталляции) только разрешенного к

[263] См.: разд. «Требования к реализации ОПС.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.49-л.50.

использованию программного обеспечения и (или) его компонентов:[264]

8.3.3.1.1. Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

8.3.3.1.2. Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке («белый список»), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации (документируются).

8.3.3.1.3. Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с требованиями Регуляторов[265].

8.3.3.1.4. Оператором должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с требованиями Регуляторов[266], а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.

8.3.3.2. Требования к усилению мероприятий по установке (инсталляции) только разрешенного к использованию программного обеспечения и (или) его компонентов Регуляторами не установлены[267].

---

[264] См.: разд. «Требования к реализации ОПС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.50.

[265] См.:

- УПД.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.31-л.32.

[266] См.:

- АНЗ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации АНЗ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.83.

[267] См.: разд. «Требования к реализации ОПС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.50.

8.4. Политика защиты машинных носителей информации

Применяемая в Департаменте ЗАГС Забайкальского края политика защиты машинных носителей информации устанавливает требования к:

- учету машинных носителей информации[268];
- управлению доступом к машинным носителям информации[269];
- контролю использования интерфейсов ввода (вывода) информации на машинные носители информации[270];
- уничтожению (стиранию) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контролю уничтожения (стирания)[271].

8.4.1. Учет машинных носителей информации

8.4.1.1. Должны выполняться следующие требования Регуляторов к реализации учета машинных носителей информации[272]:

8.4.1.1.1. Оператором должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации.

8.4.1.1.2. Учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

8.4.1.1.3. Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров носителям.

8.4.1.1.4. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера.

8.4.1.1.5. Учет съемных машинных носителей информации ведется в журналах учета машинных носителей информации[273].

8.4.1.1.6. Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе

---

[268] См.: разд.8.4.1 настоящей Политики.

[269] См.: разд.8.4.2 настоящей Политики.

[270] См.: разд.8.4.3 настоящей Политики.

[271] См.: разд.8.4.4 настоящей Политики.

[272] См.: разд. «Требования к реализации ЗНИ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.52-л.53.

[273] См. Приложение к Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 101.

соответствующих технических средств.

8.4.1.1.7. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.

8.4.1.1.8. Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации.

8.4.1.1.9. Раздельному учету в журналах учета подлежат съемные (в том числе портативные) перезаписываемые машинные носители информации (флэш-накопители, съемные жесткие диски).

8.4.1.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по учету машинных носителей информации:

8.4.1.2.1. Оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая:

а) информацию о возможности использования машинного носителя информации вне информационной системы;

б) информацию о возможности использования машинного носителя информации за пределами контролируемой зоны (конкретных помещений);

в) атрибуты безопасности, указывающие на возможность использования этих машинных носителей информации для обработки (хранения) соответствующих видов информации.

8.4.1.2.2. Оператором обеспечивается маркировка машинных носителей информации (технических средств), дополнительно включающая неотторгаемую цифровую метку носителя информации для обеспечения возможности распознавания (идентификации) носителя в системах управления доступом.

8.4.1.2.3. Оператором обеспечиваться маркировка машинных носителей информации (технических средств), дополнительно включающая использование механизмов распознавания (идентификации) носителя информации по его уникальным физическим характеристикам.

8.4.2. Управление доступом к машинным носителям информации

8.4.2.1. Должны выполняться следующие требования Регуляторов к реализации управления доступом к машинным носителям информации:[274]

8.4.2.1.1. Оператором должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в информационной системе:

8.4.2.1.1.1. определение должностных лиц, имеющих физический доступ к машинным носителям информации, а именно к следующим:

– съемным машинным носителям информации (флэш-

[274] См.: разд. «Требования к реализации ЗНИ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.53-л.54.

накопители, внешние накопители на жестких дисках и иные устройства);

- портативным вычислительным устройствам, имеющим встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинным носителям информации, стационарно устанавливаемым в корпус средств вычислительной техники (например, накопители на жестких дисках);

8.4.2.1.1.2. предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций).

8.4.2.2. Правила и процедуры доступа к машинным носителям информации регламентируются в организационно-распорядительных документах оператора по защите информации.

8.4.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению доступом к машинным носителям информации[275]:

8.4.2.3.1. Применение автоматизированной системы контроля физического доступа в помещения, в которых осуществляется хранение машинных носителей информации.

8.4.2.3.2. Опечатывание корпуса средства вычислительной техники, в котором стационарно установлен машинный носитель информации.

8.4.2.3.3. В информационной системе должно обеспечиваться применение программных (программно-технических) автоматизированных средств управления физическим доступом к машинным носителям информации.

8.4.2.3.4. Контроль физического доступа лиц к машинным носителям информации в соответствии с атрибутами безопасности, установленными для этих носителей.

8.4.3. Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации[276]

8.4.3.1. Должны выполняться следующие требования Регуляторов к

---

[275] См.: разд. «Требования к реализации ЗНИ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.54.

[276] Исполняется только для ИС 1 и 2 класса защищенности информационной системы. См.:

- ЗНИ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗНИ.5 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗНИ.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

реализации контроля использования интерфейсов ввода (вывода) информации на машинные носители информации:[277]

8.4.3.1.1. В информационной системе должен осуществляться контроль использования интерфейсов ввода (вывода).

8.4.3.1.2. Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать:

- определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе;
- определение оператором категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода);
- принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода);
- контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода).

8.4.3.1.3. В качестве мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода), могут применяться:

- опечатывание интерфейсов ввода (вывода);
- использование механических запирающих устройств;
- удаление драйверов, обеспечивающих работу интерфейсов ввода (вывода);
- применение средств защиты информации, обеспечивающих контроль использования интерфейсов ввода (вывода).

8.4.3.2. Правила и процедуры контроля использования интерфейсов ввода (вывода) регламентируются в организационно-распорядительных документах оператора по защите информации.

8.4.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю использования интерфейсов ввода (вывода) информации на машинные носители информации[278]:

8.4.3.3.1. В информационной системе должна быть обеспечена регистрация использования интерфейсов ввода (вывода) в соответствии с требованиями Регуляторов[279].

8.4.3.3.2. Оператором обеспечивается конструктивное (физическое) исключение из средства вычислительной техники запрещенных к использованию интерфейсов ввода (вывода).

8.4.3.3.3. Оператором информационной системы обеспечивается

---

[277] См.: разд. «Требования к реализации ЗНИ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.56- л.57.

[278] См.: разд. «Требования к реализации ЗНИ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.56- л.57.

[279] См.:

- РСБ.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации РСБ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.66-л.67.

программное отключение запрещенных к использованию интерфейсов ввода (вывода).

8.4.4. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)

8.4.4.1. Должны выполняться следующие требования Регуляторов к реализации уничтожению (стиранию) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контролю уничтожения (стирания):[280]

8.4.4.1.1. Оператором должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации.

8.4.4.1.2. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

8.4.4.1.3. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

8.4.4.2. Процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации должны быть разработаны оператором и включены в организационно-распорядительные документы по защите информации.

8.4.4.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по уничтожению (стиранию) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контролю уничтожения (стирания)[281]:

8.4.4.3.1. Оператором должны быть обеспечены регистрация и контроль действий по удалению защищаемой информации и уничтожению машинных носителей информации.

8.4.4.3.2. Оператором должны проводиться периодическая проверка процедур и тестирование средств стирания информации и контроля удаления информации.

8.4.4.3.3. Оператором перед подключением к информационной системе должно быть обеспечено уничтожение (стирание) информации с носителей информации после их приобретения и при первичном подключении к информационной системе, при использовании в иных информационных системах, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта, а также в иных случаях,

[280] См.: разд. «Требования к реализации ЗНИ.8» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.59- л.60.

[281] См.: разд. «Требования к реализации ЗНИ.8» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.60.

определяемых оператором.

8.4.4.3.4. Оператором должно быть обеспечено уничтожение машинных носителей информации, которые не подлежат очистке (неперезаписываемые машинные носители информации, такие как оптические диски типа CD-R).

8.4.4.3.5. Оператором должны применяться следующие меры по уничтожению (стиранию) информации на машинных носителях, исключающие возможность восстановления защищаемой информации:

а) удаление файлов штатными средствами операционной системы и (или) форматирование машинного носителя информации штатными средствами операционной системы;

б) перезапись уничтожаемых (стираемых) файлов случайной битовой последовательностью, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью с последующим форматированием;

в) очистка всего физического пространства машинного носителя информации, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

г) полная многократная перезапись машинного носителя информации специальными битовыми последовательностями, зависящими от типа накопителя и используемого метода кодирования информации, затем очистка всего физического пространства накопителя, включая сбойные и резервные элементы памяти специализированными программами или утилитами производителя;

д) размагничивание машинного носителя информации;

е) физическое уничтожение машинного носителя информации (в том числе сжигание, измельчение, плавление, расщепление, распыление и другое).

8.5. Политика регистрации событий безопасности

Применяемая в Департаменте ЗАГС Забайкальского края политика регистрации событий безопасности устанавливает требования к:

- определению событий безопасности, подлежащих регистрации, и сроков их хранения[282];
- определению состава и содержания информации о событиях безопасности, подлежащих регистрации[283];
- сбору, записи и хранению информации о событиях безопасности в течение установленного времени хранения[284];
- реагированию на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижения предела или переполнения объема (емкости) памяти[285];
- мониторингу (просмотру, анализу) результатов регистрации событий

[282] См.: разд.8.5.1 настоящей Политики.
[283] См.: разд.8.5.2 настоящей Политики.
[284] См.: разд.8.5.3 настоящей Политики.
[285] См.: разд.8.5.4 настоящей Политики.

безопасности и реагированию на них[286];

- генерированию временных меток и (или) синхронизации системного времени в информационной системе[287];
- защите информации о событиях безопасности[288].

8.5.1. Определение событий безопасности, подлежащих регистрации, и сроков их хранения

8.5.1.1. Должны выполняться следующие требования Регуляторов к реализации определения событий безопасности, подлежащих регистрации, и сроков их хранения:[289]

8.5.1.1.1. Оператором должны быть определены события безопасности в информационной системе, подлежащие регистрации, и сроки их хранения.

8.5.1.1.2. События безопасности, подлежащие регистрации в информационной системе, должны определяться с учетом способов реализации угроз безопасности для информационной системы.

8.5.1.1.3. К событиям безопасности, подлежащим регистрации в информационной системе, должны быть отнесены любые проявления состояния информационной системы и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите информации оператора, а также на нарушение штатного функционирования средств защиты информации.

8.5.1.1.4. События безопасности, подлежащие регистрации в информационной системе, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе.

8.5.1.1.5. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в информационной системе.

8.5.1.1.6. Перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, определяется оператором исходя из возможностей реализации угроз безопасности информации и фиксируется в организационно-распорядительных документах по защите информации (документируется).

8.5.1.1.7. В информационной системе как минимум подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;

---

[286] См.: разд.8.5.5 настоящей Политики.

[287] См.: разд.8.5.6 настоящей Политики.

[288] См.: разд.8.5.7 настоящей Политики.

[289] См.: разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.62-л.63.

- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым оператором защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа; попытки удаленного доступа.

8.5.1.1.8. Состав и содержание информации о событиях безопасности, подлежащих регистрации, определяются в соответствии с требованиями Регуляторов[290].

8.5.1.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по определению событий безопасности, подлежащих регистрации, и сроков их хранения[291]:

8.5.1.2.1. Оператором должен обеспечиваться пересмотр перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

8.5.1.2.2. Оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с действиями от имени привилегированных учетных записей (администраторов).

8.5.1.2.3. Оператором в перечень событий безопасности, подлежащих регистрации, должны быть включены события, связанные с изменением привилегий учетных записей.

8.5.1.2.4. Оператором должен быть обеспечен срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом:

а) осуществляется хранение только записей о выявленных событиях безопасности;

б) осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности;

в) осуществляется хранение журналов приложений, которые послужили основанием для регистрации события безопасности;

---

[290] См.:

- РСБ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации РСБ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63-л.65.

[291] См.: разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63.

г) осуществляется хранение всех записей системных журналов и событий безопасности;

д) осуществляется хранение всех записей журналов приложений.

8.5.2. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

8.5.2.1. Должны выполняться следующие требования Регуляторов к реализации определения состава и содержания информации о событиях безопасности, подлежащих регистрации:[292]

8.5.2.1.1. В информационной системе должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации.

8.5.2.1.2. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

8.5.2.1.3. При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как минимум, включать:

- дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы;
- результат попытки входа (успешная или неуспешная);
- результат попытки загрузки (останова) операционной системы (успешная или неуспешная);
- идентификатор, предъявленный при попытке доступа.

8.5.2.1.4. При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать:

- дату и время подключения машинных носителей информации и вывода информации на носители информации;
- логическое имя (номер) подключаемого машинного носителя информации;
- идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

8.5.2.1.5. При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать:

- дату и время запуска, имя (идентификатор) программы (процесса, задания);
- идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание);

---

[292] См.: разд. «Требования к реализации РСБ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63-л.65.

– результат запуска (успешный, неуспешный).

8.5.2.1.6. При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать:

– дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная);
– идентификатор субъекта доступа (устройства);
– спецификацию защищаемого файла (логическое имя, тип).

8.5.2.1.7. При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать:

– дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная);
– идентификатор субъекта доступа (устройства);
– спецификацию защищаемого объекта доступа (логическое имя (номер).

8.5.2.1.8. При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать:

– дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная);
– идентификатор субъекта доступа (устройства);
– используемый протокол доступа;
– используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

8.5.2.2. Состав и содержание информации о событиях безопасности, подлежащих регистрации, отражаются в организационно-распорядительных документах оператора по защите информации.

8.5.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по определению состава и содержания информации о событиях безопасности, подлежащих регистрации[293]:

8.5.2.3.1. В информационной системе обеспечивается запись дополнительной информации о событиях безопасности, включающую:

а) полнотекстовую запись привилегированных команд (команд, управляющих системными функциями);
б) запись сетевых потоков (дампов), связанных с событием безопасности.

8.5.2.3.2. В информационной системе обеспечивается централизованное управление записями регистрации событий безопасности в рамках сегментов информационной системы, определяемых оператором, и (или) информационной системы в целом.

8.5.2.3.3. В информационной системе обеспечивается индивидуальная регистрация пользователей групповых учетных записей[294].

---

[293] См.: разд. «Требования к реализации РСБ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.64-л.65.

[294] Локальные и доменные группы пользователей.

8.5.2.3.4. В информационной системе обеспечивается регистрация информации о месте (в частности сетевой адрес, географическая привязка и (или) другая информация), с которого осуществляется вход субъектов доступа в информационную систему.

8.5.2.3.5. В информационной системе состав и содержание регистрационных записей при регистрации запуска процессов (приложений) должны включать следующие сведения:

а) параметров запуска процесса (приложения);

б) продолжительность работы;

в) объекты доступа, к которым осуществлялось обращение процесса (приложения);

г) использованные процессом (приложением) устройства.

8.5.2.3.6. В информационной системе обеспечивается запись следующей информации, связанной с доступом к объектам доступа (в частности, к файлам):

а) тип доступа (в том числе чтение, исполнение, запись и (или) иные типы);

б) изменение атрибутов объектов доступа (права доступа, контрольные суммы, размер, содержание, путь, тип и (или) иные атрибуты);

в) продолжительность доступа.

8.5.3. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

8.5.3.1. Должны выполняться следующие требования Регуляторов к реализации сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения:[295]

8.5.3.1.1. В информационной системе должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного оператором времени хранения информации о событиях безопасности.

8.5.3.1.2. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должен предусматривать:

- возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности определенных в соответствии с требованиями Регуляторов[296];
- генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с требованиями Регуляторов[297] с составом и

---

[295] См.: разд. «Требования к реализации РСБ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.66-л.67.

[296] См.:

- РСБ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63.

[297] См.:

содержанием информации, определенными в соответствии с требованиями Регуляторов[298];

– хранение информации о событиях безопасности в течение времени, установленного в соответствии с требованиями Регуляторов[299].

8.5.3.1.3. Объем памяти для хранения информации о событиях безопасности должен быть рассчитан и выделен с учетом типов событий безопасности, подлежащих регистрации в соответствии с требованиями Регуляторов[300], составом и содержанием информации о событиях безопасности, подлежащих регистрации, в соответствии с требованиями Регуляторов[301], прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности в соответствии с требованиями Регуляторов[302].

– РСБ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63.

[298] См.:
– РСБ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации РСБ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63-л.65.

[299] См.:
– РСБ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63.

[300] См.:
– РСБ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63.

[301] См.:
– РСБ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации РСБ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63-л.65.

[302] См.:
– РСБ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом

8.5.3.2. Правила и процедуры сбора, записи и хранения информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

8.5.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по сбору, записи и хранению информации о событиях безопасности в течение установленного времени хранения[303]:

8.5.3.3.1. В информационной системе должно быть обеспечено централизованное автоматизированное управление сбором, записью и хранением информации о событиях безопасности.

8.5.3.3.2. В информационной системе обеспечивается объединение информации из записей регистрации событий безопасности, полученной от разных технических средств (устройств), программного обеспечения информационной системы, в единый логический или физический журнал аудита с корреляцией информации по времени для своевременного выявления инцидентов и реагирования на них.

8.5.3.3.3. В информационной системе обеспечивается объединение информации из записей регистрации событий безопасности, полученной от разных технических средств (устройств), программного обеспечения информационной системы, в единый логический или физический журнал аудита с корреляцией информации по событиям безопасности для своевременного выявления инцидентов и реагирования на них в масштабах оператора.

8.5.3.3.4. В информационной системе обеспечивается хранение записей системных журналов и записей о событиях безопасности в обособленном хранилище, физически отделенном от технических средств, входящих в состав информационной системы.

8.5.4. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти

8.5.4.1. Должны выполняться следующие требования Регуляторов к реализации реагирования на сбои при регистрации событий безопасности:[304]

8.5.4.1.1. В информационной системе должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти.

ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63.

[303] См.: разд. «Требования к реализации РСБ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.66-л.67.

[304] См.: разд. «Требования к реализации РСБ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.67-л.68.

8.5.4.1.2. Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

8.5.4.2. Правила и процедуры реагирования на сбои при регистрации событий безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

8.5.4.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по реагированию на сбои при регистрации событий безопасности[305]:

8.5.4.3.1. В информационной системе обеспечивается выдача предупреждения администратору при заполнении установленной оператором части (процент или фактическое значение) объема памяти для хранения информации о событиях безопасности.

8.5.4.3.2. В информационной системе обеспечивается выдача предупреждения администратору в масштабе времени, близком к реальному, при наступлении критичных сбоев в механизмах сбора информации, определенных оператором.

8.5.4.3.3. В информационной системе обеспечивается запрет обработки информации в случае аппаратных или программных ошибок, сбоев в механизмах сбора информации или достижения предела или переполнения объема (емкости) памяти.

8.5.5. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

8.5.5.1. Должны выполняться следующие требования Регуляторов к реализации мониторинга (просмотра, анализа) результатов регистрации событий безопасности и реагирования на них:[306]

8.5.5.1.1. Оператором должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них.

8.5.5.1.2. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с требованиями Регуляторов[307], и с

---

[305] См.: разд. «Требования к реализации РСБ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.67-л.68.

[306] См.: разд. «Требования к реализации РСБ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.68-л.69.

[307] См.:

- РСБ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом

периодичностью, установленной оператором, и обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе.

8.5.5.1.3. В случае выявление признаков инцидентов безопасности в информационной системе осуществляется планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

8.5.5.2. Правила и процедуры мониторинга результатов регистрации событий безопасности и реагирования на них регламентируются в организационно-распорядительных документах оператора по защите информации. В частности, установлено, что:

8.5.5.2.1. Мониторинг результатов регистрации событий безопасности должен проводиться в форме анализа системных журналов[308] и журналов СЗИ, проводимого администратором безопасности информации с целью своевременного выявления факта попыток несанкционированного доступа к информационным ресурсам в информационные системы Департамента ЗАГС Забайкальского края[309].

8.5.5.2.2. Анализ журналов должен производиться ежедневно[310].

ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

- разд. «Требования к реализации РСБ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.63.

[308] См.: п.А.10.10 ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования.

[309] Выполняется в соответствии с:

- ст.15 и ст. 16 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.16.2, п.18, п.18.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.6 ст.8.1.5 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер;
- разд. 6.1.5.3, разд.6.1.5.5. Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- разд. 9.7 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[310] В соответствии с пунктом 15 Требований к защите персональных данных для обеспечения 2 и выше уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований по защите информации необходимо выполнение требования о том, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.- См.: п.19 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620). См. также: п.6.1.5.4.2 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной

8.5.5.2.3. При анализе журналов СЗИ НСД проверяются[311]:

- журналы контроля целостности программных частей СЗИ[312];
- журналы контроля целостности программного обеспечения ИС[313];
- журналы доступа пользователей и процессов к защищаемым объектам[314];
- журналы создания новых пользователей в СЗИ и изменения полномочий пользователей[315].

8.5.5.3. Должны выполняться следующие требования Регуляторов к

приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[311] См.: п.6.1.5.5.1.6- 6.1.5.5.1.8 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[312] Исполняется в соответствии с:

- п.2.8., п.3.24, п.6.39 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п. 6.1.5.5.1.8 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[313] Исполняется в соответствии с:

- п.2.8., п.3.24, п.6.39 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п. 6.1.5.5.1.8 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[314] Проводится в соответствии с:

- ст.15 и п. «а» ст.16 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п. 6.1.5.5.1.8 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[315] Проводится в соответствии с:

- п. «а» ст.16 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п. ЗИС.21 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п. ЗИС.21 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ЗИС.21 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.5.13, п.5.27, п.5.9.1, п 5.92 и п.6.3.11.4. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п. 6.1.5.5.1.8 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

усилению мероприятий по мониторингу (просмотру, анализу) результатов регистрации событий безопасности и реагирование на них[316]:

8.5.5.3.1. В информационной системе должны обеспечиваться интеграция результатов мониторинга (просмотра и анализа) записей регистрации (аудита) из разных источников (журналов, хранилищ информации о событиях безопасности) и их корреляция с целью выявления инцидентов безопасности и реагирования на них.

8.5.5.3.2. В информационной системе обеспечивается интеграция процессов мониторинга (просмотра, анализа) результатов регистрации событий безопасности с результатами анализа уязвимостей, проводимого в соответствии с требованиями Регуляторов[317], и результатами обнаружения вторжений, проводимого в соответствии с требованиями Регуляторов[318] с целью усиления возможностей по выявлению признаков инцидентов безопасности.

8.5.5.3.3. В информационной системе обеспечивается полнотекстовый анализ привилегированных команд.

8.5.5.3.4. Оператором обеспечивается анализ записанных сетевых потоков (дампов).

8.5.6. Генерирование временных меток и (или) синхронизация системного времени в информационной системе

8.5.6.1. Должны выполняться следующие требования Регуляторов к реализации генерирования временных меток и (или) синхронизации системного времени в информационной системе:[319]

8.5.6.1.1. В информационной системе должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени.

8.5.6.1.2. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита)

---

316 См.: разд. «Требования к реализации РСБ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.68-л.69.

317 См.:

- АНЗ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации АНЗ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.78-л.79.

318 См.:

- СОВ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации СОВ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.75-л.76.

319 См.: разд. «Требования к реализации РСБ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675л.69.

событий безопасности в информационной системе достигается посредством применения внутренних системных часов информационной системы.

8.5.6.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по генерированию надежных меток времени и (или) синхронизации системного времени[320]:

8.5.6.2.1. Оператором информационной системы должен быть определен источник надежных меток времени; в информационной системе должна выполняться синхронизация системного времени с периодичностью, определенной оператором.

8.5.7. Защита информации о событиях безопасности

8.5.7.1. Должны выполняться следующие требования Регуляторов к реализации защиты информации о событиях безопасности:[321]

8.5.7.1.1. В информационной системе должна обеспечиваться защита информации о событиях безопасности.

8.5.7.1.2. Защита информации о событиях безопасности (записях регистрации (аудита) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в соответствии с настоящим методическим документом, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

8.5.7.1.3. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

8.5.7.2. Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

8.5.7.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по защите информации о событиях безопасности:

8.5.7.3.1. В информационной системе обеспечивается резервное копирование записей регистрации (аудита).

8.5.7.3.2. В информационной системе обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (неперезаписываемые носители информации).

8.5.7.3.3. В информационной системе для обеспечения целостности информации о зарегистрированных событиях безопасности должны применяться в соответствии с законодательством Российской Федерации криптографические методы.

8.5.7.3.4. Оператор предоставляет доступ к записям регистрации событий безопасности (аудита) ограниченному кругу администраторов.

---

[320] См.: разд. «Требования к реализации РСБ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675л.69.

[321] См.: разд. «Требования к реализации РСБ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675л.70.

8.6. Политика антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края

Применяемая в Департаменте ЗАГС Забайкальского края политика антивирусной защиты в информационных системах устанавливает требования к:

- реализации антивирусной защиты;[322]
- обновлению базы данных признаков вредоносных компьютерных программ (вирусов)[323].

8.6.1. Реализация антивирусной защиты

8.6.1.1. Должны выполняться следующие требования Регуляторов к реализации антивирусной защиты в информационных системах:[324]

8.6.1.1.1. Оператором должна обеспечиваться антивирусная защита информационной системы, включающая обнаружение компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

8.6.1.1.2. Реализация антивирусной защиты должна предусматривать:

- применение средств антивирусной защиты на автоматизированных рабочих местах, серверах, периметральных средствах защиты информации (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других средствах защиты информации), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы);
- установку, конфигурирование и управление средствами антивирусной защиты;
- предоставление доступа средствам антивирусной защиты к объектам информационной системы, которые должны быть подвергнуты проверке средством антивирусной защиты;
- проведение периодических проверок компонентов информационной системы (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов);
- проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных машинных носителей информации, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при

[322] См.: разд. 8.6.1 настоящей Политики.

[323] См.: разд. 8.6.2 настоящей Политики.

[324] См.: разд. «Требования к реализации АВЗ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675л.72-л.73.

загрузке, открытии или исполнении таких файлов;

- оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов);
- определение и выполнение действий по реагированию на обнаружение в информационной системе объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами).

8.6.1.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по реализации антивирусной защиты[325]:

8.6.1.2.1. В информационной системе должно обеспечиваться предоставление прав по управлению (администрированию) средствами антивирусной защиты администратору безопасности.

8.6.1.2.2. В информационной системе должно обеспечиваться централизованное управление (установка, удаление, обновление, конфигурирование и контроль актуальности версий программного обеспечения средств антивирусной защиты) средствами антивирусной защиты, установленными на компонентах информационной системы (серверах, автоматизированных рабочих местах).

8.6.1.2.3. Оператором должен обеспечиваться запрет использования съемных машинных носителей информации, которые могут являться источниками вредоносных компьютерных программ (вирусов).

8.6.1.2.4. В информационной системе должно обеспечиваться использование на разных уровнях информационной системы средств антивирусной защиты разных производителей.

8.6.1.2.5. В информационной системе должны обеспечиваться проверка работоспособности, актуальность базы данных признаков компьютерных вирусов и версии программного обеспечения средств антивирусной защиты.

8.6.1.2.6. В информационной системе должна обеспечиваться проверка объектов файловой системы средством антивирусной защиты до загрузки операционной системы.

8.6.1.2.7. В информационной системе должна обеспечиваться регистрация событий о неуспешном обновлении базы данных признаков вредоносных компьютерных программ (вирусов).

8.6.1.2.8. Оператором должна обеспечиваться антивирусная защита на этапе инициализации микропрограммного обеспечения средства вычислительной техники.

8.6.1.3. Правила и процедуры антивирусной защиты информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации[326], которые устанавливают:

8.6.1.3.1. Безопасность аппаратно- программного обеспечения в Департаменте ЗАГС Забайкальского края от разрушающего

[325] См.: разд. «Требования к реализации АВЗ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.73.

[326] См.: Инструкция по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденная приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

воздействия компьютерных вирусов достигается также проведением мероприятий по антивирусной защите[327], основанных на следующих принципах:

8.6.1.3.1.1. контроль состояния антивирусной защиты ИС Департамента ЗАГС Забайкальского края возлагается на администратора безопасности информации[328] или уполномоченное лицо[329];

8.6.1.3.1.2. к использованию в ИС допускаются только сертифицированные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств[330];

---

[327] Выполняется в соответствии с:

- п.18.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и разделом VI Приложения №2 к указанным Требованиям;
- п. А.10.4 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
- АВ3.1-АВ3.2 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- АВ3.1-АВ3.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[328] Выполняется в соответствии с:

- п.20.6 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п. АВ3.1 Приложения №2 к указанным Требованиям.
- п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.5.5 Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[329] Действующее по гражданско- правовому договору в соответствии с:

- ст. 3 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[330]Исполняется в соответствии с:

- п.3) ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п. в) ст.1 Указа Президента Российской Федерации от 17.03.2008 №351(в ред. Указа Президента РФ от 21.10.2008 № 1510) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно - телекоммуникационных сетей международного информационного обмена»;
- ст.25 и ст.26 Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного Постановлением Совета Министров — Правительства РФ от 15.09.1993 № 912-51;
- п. «г» ст.13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.11. Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013

8.6.1.3.1.3. в Департаменте ЗАГС Забайкальского края ежедневно в начале работы при загрузке компьютеров в автоматическом режиме обязан проводиться автоматический контроль всех дисков и файлов [331];

8.6.1.3.1.4. должно обеспечиваться автоматическое централизованное обновление вирусных сигнатур и антивирусного ПО на всех ПЭВМ, работающих в ИС[332];

8.6.1.3.1.5. обязательному автоматическому антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных (несъемных) носителях (магнитных дисках, CD-ROM, флэш и т.п.)[333];

8.6.1.3.1.6. разархивирование и контроль входящей информации обязан проводиться непосредственно после ее приема на выделенном автономном компьютере или на любом другом

№17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

- подпунктом г) п.5 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620);
- п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.6.3.1.2. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[331] См.: п.6.3.1.3. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[332] Исполняется в соответствии с:

- п. АВЗ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации АВЗ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.73- л.74;
- Приложением А ГОСТ Р 51188-98. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство
- п. АВЗ.2 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. АВЗ.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.6.3.1.4. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107;
- п.6.1.3.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[333] См. п.6.3.1.5. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

компьютере[334] (возможно применение другого способа антивирусного контроля входящей информации, обеспечивающей аналогичный уровень эффективности контроля)[335];

8.6.1.3.1.7. контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный машинный носитель информации)[336];

8.6.1.3.1.8. файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль[337];

8.6.1.3.1.9. периодические проверки электронных архивов должны проводиться не реже одного раза в месяц[338];

8.6.1.3.1.10. устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов[339].

8.6.2. Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

8.6.2.1. Должны выполняться следующие требования Регуляторов к

---

[334] При условии начальной загрузки ОС в оперативную память компьютера с системной дискеты, заведомо «чистой» (не зараженной вирусами) и защищенной от записи.

[335] См. п.6.3.1.6. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[336] См. п.6.3.1.7. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[337] См.:

- п. ЗИС.15 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд.3.13 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п. ЗИС.15 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ЗИС.15 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.6.3.1.8. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107;
- п.6.1.2.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[338] В соответствии с п.6.3.1.9. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[339] В соответствии с:

- п.6.1.3.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- п.6.3.1.10. Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

реализации обновления базы данных признаков вредоносных компьютерных программ (вирусов):[340]

8.6.2.1.1. Оператором должно быть обеспечено обновление базы данных признаков вредоносных компьютерных программ (вирусов). Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать[341]:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов);
- получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов);
- контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов).

8.6.2.2. Правила и процедуры обновления базы данных признаков вредоносных компьютерных программ (вирусов) регламентируются в организационно-распорядительных документах оператора по защите информации[342].

8.6.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обновлению базы данных признаков вредоносных компьютерных программ (вирусов)[343]:

8.6.2.3.1. В информационной системе должно обеспечиваться централизованное управление обновлением базы данных признаков вредоносных компьютерных программ (вирусов).

8.6.2.3.2. В информационной системе должно обеспечиваться автоматическое обновление базы данных признаков вредоносных компьютерных программ (вирусов) на всех компонентах информационной системы.

8.6.2.3.3. В информационной системе должен обеспечиваться запрет изменений настроек системы обновления базы данных признаков вредоносных компьютерных программ (вирусов) на автоматизированных рабочих местах и серверах.

8.6.2.3.4. В информационной системе должна обеспечиваться возможность возврата (отката) к предыдущим обновлениям базы данных признаков вредоносных компьютерных программ (вирусов).

---

[340] См.: разд. «Требования к реализации АВЗ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.73- л.74.

[341] См.: п.7.1.1 Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[342] См.: разд.VII Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[343] См.:

- разд. «Требования к реализации АВЗ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.74;
- п.7.3 Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

8.7. Политика обнаружения вторжений

Применяемая в Департаменте ЗАГС Забайкальского края политика антивирусной защиты в информационных системах устанавливает требования к:

- обнаружению вторжений[344];
- обновлению базы решающих правил[345].

8.7.1. Обнаружение вторжений[346]

8.7.1.1. Должны выполняться следующие требования Регуляторов к реализации обнаружения вторжений:[347]

8.7.1.1.1. Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак), направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений.

8.7.1.1.2. Применяемые системы обнаружения вторжений должны включать компоненты регистрации событий безопасности (датчики), компоненты анализа событий безопасности и распознавания компьютерных атак (анализаторы) и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

8.7.1.1.3. Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе информационной системы (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором.

8.7.1.1.4. Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам.

8.7.1.1.5. Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования

---

[344] См.: разд. 8.7.1 настоящей Политики.

[345] См.: разд. 8.7.2 настоящей Политики.

[346] Исполняется только для информационных систем 1 и 2 классов защищенности. См.:

- СОВ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- СОВ.1 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- СОВ.1 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[347] См.: разд. «Требования к реализации СОВ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.75- л.76.

информационных систем.

8.7.1.2. Правила и процедуры обнаружения (предотвращения) вторжений (компьютерных атак) регламентируются в организационно-распорядительных документах оператора по защите информации.

8.7.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обнаружению вторжений:

8.7.1.3.1. Оператором обеспечивается применение систем обнаружения вторжений уровня сети, обеспечивающих сбор и анализ информации об информационных потоках, передаваемых в рамках сегмента (сегментов) информационной системы.

8.7.1.3.2. В информационной системе обеспечивается централизованное управление (администрирование) компонентами системы обнаружения вторжений, установленными в различных сегментах информационной системы.

8.7.1.3.3. Обнаружение и реагирование (уведомление администратора безопасности, блокирование трафика и иные действия по реагированию) на компьютерные атаки в масштабе времени, близком к реальному.

8.7.1.3.4. Защита информации, собранной и сгенерированной системой обнаружения вторжений, от несанкционированного доступа, модификации и удаления.

8.7.1.3.5. Оператором информационной системы обеспечивается применение систем обнаружения вторжений уровня узла на автоматизированных рабочих местах и серверах информационной системы.

8.7.1.3.6. Оператором информационной системы обеспечивается применение систем обнаружения вторжений на прикладном уровне базовой эталонной модели взаимосвязи открытых систем.

8.7.2. Обновление базы решающих правил

8.7.2.1. Должны выполняться следующие требования Регуляторов к реализации обновления базы решающих правил:[348]

8.7.2.1.1. Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе.

8.7.2.1.2. Обновление базы решающих правил системы обнаружения вторжений должно предусматривать:

- получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил;
- получение из доверенных источников и установку обновлений базы решающих правил;
- контроль целостности обновлений базы решающих правил.

8.7.2.2. Правила и процедуры обновления базы решающих правил регламентируются в организационно-распорядительных документах оператора по защите информации.

8.7.2.3. Должны выполняться следующие требования Регуляторов к

[348] См.: разд. «Требования к реализации СОВ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.76- л.77.

усилению мероприятий по обновлению базы решающих правил[349]:

8.7.2.3.1. В информационной системе должно обеспечиваться централизованное управление обновлением базы решающих правил системы обнаружения вторжений.

8.7.2.3.2. В информационной системе должна обеспечиваться возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) со стороны уполномоченных должностных лиц (администраторов) для предотвращения определенных оператором компьютерных атак и (или) сокращения нагрузки на информационную систему, а также минимизации ложных срабатываний системы обнаружения вторжений.

8.7.2.3.3. Оператором информационной системы устанавливается порядок редактирования базы решающих правил.

8.7.2.3.4. В случае редактирования базы решающих правил запись об этом событии с указанием произведенных изменений фиксируется в соответствующем журнале регистрации событий безопасности[350].

8.8. Политика контроля (анализа) защищенности информации

Применяемая в Департаменте ЗАГС Забайкальского края политика контроля (анализа) защищенности информации устанавливает требования к:

- выявлению, анализу уязвимостей информационной системы и оперативному устранению вновь выявленных уязвимостей[351];
- контролю установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации[352];
- контролю работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации[353];
- контролю состава технических средств, программного обеспечения и средств защиты информации[354];
- контролю правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе[355].

8.8.1. Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей

8.8.1.1. Должны выполняться следующие требования Регуляторов к реализации выявлению, анализу уязвимостей информационной системы и оперативному устранению вновь выявленных

---

[349] См.: разд. «Требования к реализации СОВ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.76- л.77.

[350] См.: Приложение к Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111.

[351] См.: разд.8.8.1 настоящей Политики.

[352] См.: разд.8.8.2 настоящей Политики.

[353] См.: разд.8.8.3 настоящей Политики.

[354] См.: разд.8.8.4 настоящей Политики.

[355] См.: разд.8.8.5 настоящей Политики.

уязвимостей[356]:

8.8.1.1.1. Оператором должны осуществляться выявление (поиск), анализ и устранение уязвимостей в информационной системе.

8.8.1.1.2. При выявлении (поиске), анализе и устранении уязвимостей в информационной системе должны проводиться:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;
- разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;
- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации; устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;
- информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

8.8.1.1.3. В качестве источников информации об уязвимостях используются опубликованные данные разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств, а также другие базы данных уязвимостей.

8.8.1.1.4. Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы.

8.8.1.1.5. На этапе эксплуатации поиск и анализ уязвимостей проводится с периодичностью, установленной оператором.

8.8.1.1.6. При этом в обязательном порядке для критических уязвимостей проводится поиск и анализ уязвимостей в случае опубликования в общедоступных источниках информации о новых уязвимостях в средствах защиты информации, технических средствах и программном обеспечении, применяемом в информационной системе.

8.8.1.1.7. В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или

[356] См.: разд. «Требования к реализации АН3.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.78- л.80.

микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

8.8.1.1.8. Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей.

8.8.1.2. Правила и процедуры выявления, анализа и устранения уязвимостей регламентируются в организационно-распорядительных документах оператора по защите информации.

8.8.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по выявлению, анализу уязвимостей информационной системы и оперативному устранению вновь выявленных уязвимостей:

8.8.1.3.1. Оператором обеспечивается использование для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

8.8.1.3.2. Оператор должен уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях.

8.8.1.3.3. Оператором определяется информация об информационной системе, которая может стать известной нарушителям и использована ими для эксплуатации уязвимостей (в том числе уязвимостей «нулевого дня» - уязвимостей, описание которых отсутствует в базах данных разработчиков средств защиты информации, общесистемного, прикладного и специального программного обеспечения, технических средств), и принимаются меры по снижению (исключению) последствий от эксплуатации нарушителями неустранимых уязвимостей.

8.8.1.3.4. Оператором предоставляется доступ только администраторам к функциям выявления (поиска) уязвимостей (предоставление такой возможности только администраторам безопасности).

8.8.1.3.5. Оператором применяются автоматизированные средства для сравнения результатов сканирования уязвимостей в разные периоды времени для анализа изменения количества и классов (типов) уязвимостей в информационной системе.

8.8.1.3.6. Оператором применяются автоматизированные средства для обнаружения в информационной системе неразрешенного программного обеспечения (компонентов программного обеспечения) и уведомления об этом уполномоченных должностных лиц (администратора безопасности).

8.8.1.3.7. Оператором проводится анализ журналов регистрации

событий безопасности (журнала аудита) в целях определения, были ли выявленные уязвимости ранее использованы в информационной системе для нарушения безопасности информации.

8.8.1.3.8. Оператором обеспечивается проведение выявления уязвимостей «нулевого дня», о которых стало известно, но информация о которых не включена в сканеры уязвимостей.

8.8.1.3.9. Оператором обеспечивается проведение выявления новых уязвимостей, информация о которых не опубликована в общедоступных источниках.

8.8.1.3.10. Оператором должно осуществляться выявление (поиск) уязвимостей в информационной системе с использованием учетных записей на сканируемых ресурсах.

8.8.1.3.11. Оператором должно использоваться тестирование информационной системы на проникновение.

8.8.2. Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

8.8.2.1. Должны выполняться следующие требования Регуляторов к реализации контроля установки обновлений программного обеспечения:[357]

8.8.2.1.1. Оператором должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

8.8.2.1.2. Оператором должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

8.8.2.1.3. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений.

8.8.2.1.4. Контроль установки обновлений проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации, и фиксируется в соответствующих журналах[358].

---

[357] См.: разд. «Требования к реализации АН3.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.78- л.80.

[358] Исполняется для неаттестованных ИС. В аттестованных на соответствие требованиям по безопасности информации ИС администратор безопасности информации должен контролировать неизменность состава технических средств, программного обеспечения и средств защиты информации, а также осуществление эксплуатации объекта информатизации в соответствии с условиями и требованиями, установленными в выданном аттестате соответствия. См.:

– п.2.6 Положения "Аттестации объектов информатизации по требованиям безопасности информации", утвержденного председателем Государственной технической комиссии при Президенте Российской Федерации 25.11.1994.

8.8.2.1.5. При контроле установки обновлений осуществляются проверки установки обновлений баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты в соответствии с требованиями Регуляторов[359], баз решающих правил систем обнаружения вторжений в соответствии с требованиями Регуляторов[360], баз признаков уязвимостей средств анализа защищенности и иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

8.8.2.2. Правила и процедуры контроля установки обновлений программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

8.8.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю установки обновлений программного обеспечения[361]:

8.8.2.3.1. Оператором должна осуществляться проверка корректности функционирования обновлений в тестовой среде с обязательным оформлением результатов проверки в соответствующем журнале.

8.8.2.3.2. Оператором обеспечивается регламентация и контроль обновлений программного обеспечения базовой системы ввода-вывода (иного микропрограммного обеспечения).

8.8.3. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации

8.8.3.1. Должны выполняться следующие требования Регуляторов к реализации контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации:[362]

8.8.3.1.1. Оператором должен проводиться контроль

– п.6.4.2.4.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[359] См.:

– АВЗ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд. «Требования к реализации АВЗ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.73- л.74.

[360] См.:

– СОВ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд. «Требования к реализации СОВ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.75- л.76.

[361] См.: разд. «Требования к реализации АНЗ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.79- л.80.

[362] См.: разд. «Требования к реализации АНЗ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.81- л.82.

работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

8.8.3.1.2. При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации осуществляется:

- контроль работоспособности (неотключения) программного обеспечения и средств защиты информации;
- проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации, объем и содержание которой определяется оператором;
- контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации; восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

8.8.3.2. Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

8.8.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации[363]:

8.8.3.3.1. В информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации.

8.8.3.3.2. Оператором в случае обнаружения нарушений работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации должен обеспечиваться перевод информационной системы, сегмента или компонента информационной системы в режим ограничения обработки информации и (или) запрет обработки информации в информационной системе, сегменте или компоненте информационной системы до устранения нарушений.

8.8.3.3.3. Оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию параметров настройки программного обеспечения и средств защиты

[363] См.: разд. «Требования к реализации АНЗ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.82.

информации и восстановление параметров настройки программного обеспечения и средств защиты информации.

8.8.3.3.4. В информационной системе должно использоваться программное обеспечение, прошедшее контроль отсутствия недекларированных возможностей и отсутствия влияния на корректность работы средств защиты информации.

8.8.4. Контроль состава технических средств, программного обеспечения и средств защиты информации

8.8.4.1. Должны выполняться следующие требования Регуляторов к реализации контроля состава технических средств, программного обеспечения и средств защиты информации:[364]

8.8.4.1.1. Оператором должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационной системе (инвентаризация).

8.8.4.1.2. При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

8.8.4.2. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

8.8.4.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю состава технических средств, программного обеспечения и средств защиты информации[365]:

8.8.4.3.1. В информационной системе должна обеспечиваться

---

[364] См.: разд. «Требования к реализации АН3.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.83.

[365] См.: разд. «Требования к реализации АН3.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.83.

регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.

8.8.4.3.2. Оператором должны использоваться автоматизированные средства, обеспечивающие инвентаризацию технических средств, программного обеспечения и средств защиты информации.

8.8.5. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе

8.8.5.1. Должны выполняться следующие требования Регуляторов к реализации контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе:[366]

8.8.5.1.1. Оператором должен проводиться контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе.

8.8.5.1.2. При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

- контроль правил генерации и смены паролей пользователей в соответствии с требованиями Регуляторов[367];
- контроль заведения и удаления учетных записей пользователей в соответствии с требованиями Регуляторов[368];
- контроль реализации правил разграничения доступом в соответствии с требованиями Регуляторов[369];

---

366 См.: разд. «Требования к реализации АНЗ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.84-л.85.

367 См.:

- ИАФ.1 и ИАФ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1» и разд. «Требования к реализации ИАФ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.16-л.17, л.20-л.22.

368 См.:

- УПД.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.25-л.26.

369 См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом

- контроль реализации полномочий пользователей в соответствии с требованиями Регуляторов[370];
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора;
- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

8.8.5.2. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью, установленной оператором в организационно-распорядительных документах по защите информации.

8.8.5.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе[371]:

8.8.5.3.1. В информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

8.8.5.3.2. Оператором должны использоваться автоматизированные средства, обеспечивающие контроль правил генерации и смены паролей пользователей, учетных записей пользователей, правил разграничения доступом и полномочий пользователей.

8.9. Политика обеспечения целостности информационной системы и информации

Применяемая в Департаменте ЗАГС Забайкальского края политика обеспечения целостности информационной системы и информации устанавливает требования к:

- контролю целостности программного обеспечения, включая программное

ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.26-л.28.

[370] См.:

- УПД.4 и УПД.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.4» и разд. «Требования к реализации УПД.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.30-л.32.

[371] См.: разд. «Требования к реализации АНЗ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.84-л.85.

обеспечение средств защиты информации[372];

- обеспечению возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций[373];
- ограничению прав пользователей по вводу информации в информационную систему[374].

8.9.1. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации[375]

8.9.1.1. Должны выполняться следующие требования Регуляторов к реализации контроля целостности программного обеспечения, включая программное обеспечение средств защиты информации:[376]

8.9.1.1.1. В информационной системе должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации.

8.9.1.1.2. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать:

- контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы информационной системы;
- контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы информационной системы;
- контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы; тестирование с периодичностью установленной

---

[372] См.: разд.8.9.1 настоящей Политики.

[373] См.: разд.8.9.2 настоящей Политики.

[374] См.: разд.8.9.3 настоящей Политики.

[375] Исполняется для 1 и 2 класса защищенности информационной системы. См.:

- ОЦЛ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОЦЛ.1 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОЦЛ.1 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[376] См.: разд. «Требования к реализации ОЦЛ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.86-л.87.

оператором функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств, в соответствии с требованиями Регуляторов[377];

– обеспечение физической защиты технических средств информационной системы в соответствии с требованиями Регуляторов[378].

8.9.1.1.3. В случае если функциональные возможности информационной системы должны предусматривать применение в составе ее программного обеспечения средств разработки и отладки программ, оператором обеспечивается выполнение процедур контроля целостности программного обеспечения после завершения каждого процесса функционирования средств разработки и отладки программ.

8.9.1.2. Правила и процедуры контроля целостности программного обеспечения регламентируются в организационно-распорядительных документах оператора по защите информации.

8.9.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю целостности программного обеспечения, включая программное обеспечение средств защиты информации:

8.9.1.3.1. В информационной системе контроль целостности средств защиты информации должен осуществляться по контрольным суммам всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы.

8.9.1.3.2. В информационной системе должен обеспечиваться контроль целостности средств защиты информации с использованием криптографических методов в соответствии с законодательством Российской Федерации, всех компонентов средств защиты информации, как в процессе загрузки, так и динамически в процессе работы системы.

8.9.1.3.3. Оператором исключается возможность использования средств разработки и отладки программ во время обработки и (или) хранения информации в целях обеспечения целостности программной среды.

---

[377] См.:

– АН3.1 и АН3.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд. «Требования к реализации АН3.1» и разд. «Требования к реализации АН3.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.78-л.81.

[378] См.:

– ЗТС.2 и ЗТС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд. «Требования к реализации ЗТС.2» и разд. «Требования к реализации ЗТС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.117-л.119.

8.9.1.3.4. Оператором обеспечивается выделение рабочих мест с установленными средствами разработки и отладки программ в отдельный сегмент (тестовую среду).

8.9.1.3.5. В информационной системе должна обеспечиваться блокировка запуска программного обеспечения и (или) блокировка сегмента (компонента) информационной системы (автоматизированного рабочего места, сервера) в случае обнаружения фактов нарушения целостности.

8.9.2. Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций

8.9.2.1. Должны выполняться следующие требования Регуляторов к реализации обеспечению возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций:[379]

8.9.2.1.1. Оператором должна быть предусмотрена возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

8.9.2.1.2. Для обеспечения возможности восстановления программного обеспечения в информационной системе должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций.

8.9.2.1.3. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать:

- восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения;
- восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации; возврат информационной системы в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей информационной системы, определенных оператором, позволяющих решать задачи по обработке информации.

8.9.2.1.4. Оператором применяются компенсирующие меры защиты информации в случаях, когда восстановление работоспособности системы защиты информации невозможно.

8.9.2.2. Правила и процедуры восстановления (в том числе планы по действиям персонала порядок применения компенсирующих мер) отражаются в организационно-распорядительных документах оператора по защите информации.

---

[379] См.: разд. «Требования к реализации ОЦЛ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.88-л.89.

8.9.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обеспечению возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций[380]:

8.9.2.3.1. Оператором обеспечивается восстановление отдельных функциональных возможностей информационной системы с применением резервированного программного обеспечения зеркальной информационной системы (сегмента информационной системы, технического средства, устройства) в соответствии с требованиями Регуляторов[381].

8.9.3. Ограничение прав пользователей по вводу информации в информационную систему[382]

8.9.3.1. Должны выполняться следующие требования Регуляторов к реализации ограничения прав пользователей по вводу информации в информационную систему[383]:

8.9.3.1.1. В информационной системе должно осуществляться ограничение прав пользователей по вводу информации в информационную систему.

8.9.3.1.2. Ограничение прав пользователей по вводу информации предусматривает ограничение по вводу в определенные типы объектов доступа (объекты файловой системы, объекты баз данных, объекты прикладного и специального программного обеспечения) информации исходя из задач и полномочий, решаемых пользователем в информационной системе.

8.9.3.2. Ограничения прав пользователей по вводу информации в информационную систему должны фиксироваться в организационно-

---

[380] См.: разд. «Требования к реализации ОЦЛ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.89.

[381] См.:

- ОДТ.2 и ОДТ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ОДТ.2» и разд. «Требования к реализации ОДТ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.89.

[382] Исполняется только для 1 класса защищенности информационной системы. См.:

- ОЦЛ.6 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОЦЛ.6 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОЦЛ.6 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[383] См.: разд. «Требования к реализации ОЦЛ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.92-л.93.

распорядительных документах по защите информации (документироваться) и реализовываться в соответствии с требованиями Регуляторов[384].

8.9.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по ограничению прав пользователей по вводу информации в информационную систему[385]:

8.9.3.3.1. В информационной системе обеспечивается исключение возможности ввода пользователями информации в информационную систему, вследствие реализации ограничительных интерфейсов по вводу информации только через специальные формы прикладного программного обеспечения.

8.10. Политика обеспечения доступности информации

Применяемая в Департаменте ЗАГС Забайкальского края политика обеспечения доступности информации устанавливает требования к:

- использованию отказоустойчивых технических средств[386];
- резервированию технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы[387];
- контролю безотказного функционирования технических средств, обнаружению и локализации отказов функционирования, принятию мер по восстановлению отказавших средств и их тестированию[388];
- периодическому резервному копированию информации на резервные машинные носители информации[389];
- обеспечению возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала[390];
- контролю состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации[391].

8.10.1. Использование отказоустойчивых технических средств[392]

---

[384] См.:
- УПД.4 и УПД.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.4» и разд. «Требования к реализации УПД.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.30-л.32.

[385] См.: разд. «Требования к реализации ОЦЛ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.92-л.93.

[386] См. разд.8.10.1 настоящей Политики.

[387] См. разд.8.10.2 настоящей Политики.

[388] См. разд.8.10.3 настоящей Политики.

[389] См. разд.8.10.4 настоящей Политики.

[390] См. разд.8.10.5 настоящей Политики.

[391] См. разд.8.10.6 настоящей Политики.

[392] Исполняется только для 1 класса защищенности информационной системы. См.:
- ОДТ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом

8.10.1.1. Должны выполняться следующие требования Регуляторов к реализации использования отказоустойчивых технических средств:[393]

8.10.1.1.1. Оператором должно обеспечиваться использование отказоустойчивых технических средств, предусматривающее:

- определение сегментов информационной системы, в которых должны применяться отказоустойчивые технические средства, обладающие свойствами сохранять свою работоспособность после отказа одного или нескольких их составных частей, и перечня таких средств исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;
- определение предельных (пороговых) значений характеристик (коэффициента) готовности, показывающего, какую долю времени от общего времени работы информационной системы техническое средство (техническое решение) находится в рабочем состоянии, и характеристик надежности (требуемое значение вероятности отказа в единицу времени) исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;
- применение в информационной системе технических средств с установленными оператором характеристиками (коэффициентом) готовности и надежности, обеспечивающих требуемые условия непрерывности функционирования информационной системы и доступности информации;
- контроль с установленной оператором периодичностью за значениями характеристик (коэффициентов) готовности и надежности технических средств, и реагирование на ухудшение значений данных характеристик (инициализация плана восстановления работоспособности и иные методы реагирования);
- замена технических средств, характеристики (коэффициенты) готовности и надежности которых достигли предельного значения.

8.10.1.2. Оператором должно быть обеспечено определение требуемых характеристик (коэффициентов) надежности и готовности в соответствии с национальными стандартами.

8.10.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по использованию отказоустойчивых

ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

- ОДТ.1 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОДТ.1 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[393] См.: разд. «Требования к реализации ОДТ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.95-л.96.

технических средств[394]:

8.10.1.3.1. Оператор выводит из эксплуатации техническое средство путем передачи его функций другому (резервному) техническому средству до достижения первым предельных (пороговых) значений характеристик (коэффициентов) готовности и (или) надежности.

8.10.1.3.2. В информационной системе реализуется автоматическое оповещение (сигнализация) о достижения техническим средством предельных (пороговых) значений характеристик (коэффициентов) готовности и надежности (степень достижения предельных значений определяется оператором).

8.10.1.3.3. В информационной системе реализуется автоматическое оповещение (сигнализация) о достижения техническим средством предельных (пороговых) значений характеристик загрузки.

8.10.2. Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы[395]

8.10.2.1. Должны выполняться следующие требования Регуляторов к реализации резервирования технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы:[396]

8.10.2.1.1. Оператором должно обеспечиваться резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы, предусматривающее:

- определение сегментов информационной системы, в которых должно осуществляться резервирование технических средств, программного обеспечения, каналов передачи информации и средств обеспечения функционирования, а также перечня резервируемых средств исходя из требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации, установленных оператором;
- применение резервных (дублирующих) технических средств,

---

[394] См.: разд. «Требования к реализации ОДТ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.95-л.96.

[395] Исполняется только для 1 класса защищенности информационной системы. См.:

- ОДТ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОДТ.2 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОДТ.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[396] См.: разд. «Требования к реализации ОДТ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.96-л.98.

программного обеспечения, каналов передачи информации и (или) средств обеспечения функционирования информационной системы, обеспечивающих требуемые условия непрерывности функционирования информационной системы и доступности информации;

- ввод в действие резервного технического средства, программного обеспечения, канала передачи информации или средства обеспечения функционирования при нарушении требуемых условий непрерывности функционирования информационной системы и доступности информации.

8.10.2.1.2. Резервирование технических средств в зависимости от требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации включает ненагруженное («холодное») и (или) нагруженное («горячее») резервирование.

8.10.2.1.3. При резервировании программного обеспечения осуществляется создание резервных копий общесистемного, специального и прикладного программного обеспечения, а также программного обеспечения средств защиты информации, необходимых для обеспечения требуемых условий непрерывности функционирования информационной системы и доступности информации.

8.10.2.1.4. Резервирование каналов передачи информации включает:

- резервирование каналов связи, обеспечивающее снижение вероятности отказа в доступе к информационной системе;
- наличие у основных и альтернативных поставщиков телекоммуникационных услуг (провайдеров) информационной системы планов по восстановлению связи при авариях и сбоях, с указанием времени восстановления.

8.10.2.1.5. Резервирование средств обеспечения функционирования информационной системы включает:

- использование кратковременных резервных источников питания для обеспечения правильного (корректного) завершения работы сегмента информационной системы (технического средства, устройства) в случае отключения основного источника питания; использование долговременных резервных источников питания в случае длительного отключения основного источника питания и необходимости продолжения выполнения сегментом информационной системы (техническим средством, устройством) установленных функциональных (задач);
- определение перечня энергозависимых технических средств, которым необходимо обеспечить наличие резервных источников питания (кратковременных и долговременных).

8.10.2.2. Правила и процедуры резервирования регламентируются в организационно-распорядительных документах оператора по защите информации[397].

8.10.2.3. Должны выполняться следующие требования Регуляторов к

[397] См.: Инструкция по резервному копированию информационных ресурсов информационных систем Департамента ЗАГС Забайкальского края, утвержденная приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 112.

усилению мероприятий по резервированию технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы[398]:

8.10.2.3.1. В информационной системе должно обеспечиваться резервирование автоматизированных рабочих мест, на которых обрабатывается информация (совокупности технических средств, установленного программного обеспечения, средств защиты информации и параметров настройки), в том числе предусматривающее:

- пространственное (географическое) отделение резервных автоматизированных рабочих мест от основных мест обработки информации, с учетом возможных угроз нарушения доступности информации;
- конфигурацию резервных мест обработки информации, предусматривающую минимально требуемые эксплуатационные возможности рабочего места;
- разработку оператором процедур обеспечения требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации в случае нарушения функционирования (сбоев, аварий) резервных мест обработки информации;
- ограничение времени обработки информации на резервном рабочем месте до времени восстановления функционирования основного рабочего места.

8.10.2.3.2. В информационной системе должно обеспечиваться предоставление резервных каналов связи от альтернативных поставщиков телекоммуникационных услуг (провайдеров), отличных от поставщиков (провайдеров) основных каналов связи.

8.10.2.3.3. В информационной системе должно обеспечиваться использование резервных каналов связи, проходящих по трассам отличным, от трасс прохождения основных каналов связи.

8.10.2.3.4. В информационной системе должно обеспечиваться использование резервных (отделенных от основных) телекоммуникационных сервисов, обеспечивающих доступность информации, до восстановления доступности основных телекоммуникационных сервисов поставщиком телекоммуникационных услуг (провайдером).

8.10.3. Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование[399]

---

[398] См.: разд. «Требования к реализации ОДТ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.97-л.98.

[399] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ОДТ.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОДТ.3 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;

8.10.3.1. Должны выполняться следующие требования Регуляторов к реализации контроля безотказного функционирования технических средств, обнаружению и локализации отказов функционирования, принятию мер по восстановлению отказавших средств и их тестированию:[400]

8.10.3.1.1. Оператором должен осуществляться контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование.

8.10.3.1.2. Контроль безотказного функционирования проводится в отношении серверного и телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования информационной системы путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами).

8.10.3.1.3. При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств в соответствии с требованиями Регуляторов[401], их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах[402].

8.10.3.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование[403]:

8.10.3.2.1. В информационной системе должна быть обеспечена сигнализация (уведомление) о неисправностях, сбоях и отказах в функционировании программно-технических средств информационной системы.

8.10.3.2.2. Оператором должна обеспечиваться регистрация сбоев и

– ОДТ.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[400] См.: разд. «Требования к реализации ОДТ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.98-л.99.

[401] См.:

– ОЦЛ.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд. «Требования к реализации ОЦЛ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.88-л.89.

[402] См.: Приложение к Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111.

[403] См.: разд. «Требования к реализации ОДТ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.99.

отказов в функционировании технических средств информационной системы.

8.10.3.2.3. В информационной системе должны применяться программные средства мониторинга технического состояния информационной системы, осуществляющие мониторинг отказов программных и программно-технических средств в соответствии с перечнем, определенным оператором.

8.10.4. Периодическое резервное копирование информации на резервные машинные носители информации[404]

8.10.4.1. Должны выполняться следующие требования Регуляторов к реализации периодическому резервному копированию информации на резервные машинные носители информации:[405]

8.10.4.1.1. Оператором должно обеспечиваться периодическое резервное копирование информации на резервные машинные носители информации, предусматривающее:

- резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью;
- разработку перечня информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации;
- регистрацию событий, связанных с резервным копированием информации на резервные машинные носители информации;
- принятие мер для защиты резервируемой информации, обеспечивающих ее конфиденциальность, целостность и доступность.

8.10.4.2. Правила и процедуры резервного копирования информации регламентируются в организационно-распорядительных документах оператора по защите информации[406].

8.10.4.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по периодическому резервному копированию

---

[404] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ОДТ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОДТ.4 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОДТ.4 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[405] См.: разд. «Требования к реализации ОДТ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.99-л.100.

[406] См.: Инструкция по резервному копированию информационных ресурсов информационных систем Департамента ЗАГС Забайкальского края, утвержденная приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 112.

информации на резервные машинные носители информации[407]:

8.10.4.3.1. Оператором должна осуществляться с установленной им периодичностью проверка работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий (периодичность проверки работоспособности определяется оператором).

8.10.4.3.2. Оператором должно осуществляться хранение (размещение) резервных копий информации на отдельных (размещенных вне информационной системы) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.

8.10.4.3.3. Оператором должно осуществляться резервное копирование информации на зеркальную информационную систему (сегмент информационной системы, техническое средство, устройство).

8.10.4.3.4. Оператором должна обеспечиваться соответствующая пропускная способность каналов связи, используемых для передачи резервных копий в процессе их создания или восстановления информации, для достижения требуемых условий обеспечения непрерывности функционирования информационной системы и доступности информации.

8.10.4.3.5. Оператором должно осуществляться пространственное (географическое) разнесение мест хранения носителей резервных копий информации и мест расположения оригиналов этой информации.

8.10.5. Обеспечение возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала[408]

8.10.5.1. Должны выполняться следующие требования Регуляторов к реализации обеспечения возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала:[409]

8.10.5.1.1. Оператором должна быть обеспечена возможность восстановления информации с резервных машинных носителей

---

[407] См.: разд. «Требования к реализации ОДТ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.99-л.100.

[408] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ОДТ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОДТ.5 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОДТ54 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[409] См.: разд. «Требования к реализации ОДТ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.100-л.101.

информации (резервных копий) в течение установленного оператором временного интервала.

8.10.5.1.2. Восстановление информации с резервных машинных носителей информации (резервных копий) должно предусматривать:

- определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования информационной системы и доступности информации;
- восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного оператором временного интервала;
- регистрация событий, связанных восстановлением информации с резервных машинных носителей информации.

8.10.5.2. Правила и процедуры восстановления информации с резервных машинных носителей информации регламентируются в организационно-распорядительных документах оператора по защите информации[410].

8.10.5.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обеспечению возможности восстановления информации с резервных машинных носителей информации (резервных копий) в течение установленного временного интервала[411]:

8.10.5.3.1. Оператором должна обеспечиваться возможность восстановления информации с учетом нагруженного («горячего») резервирования технических средств в соответствии с требованиями Регуляторов.[412]

8.10.5.3.2. В информационной системе должно осуществляться предоставление пользователям резервных мест обработки информации в соответствии с требованиями Регуляторов[413] до восстановления из резервных копий информации и обеспечения ее доступности на основных местах обработки информации.

---

[410] См.: Инструкция по резервному копированию информационных ресурсов информационных систем Департамента ЗАГС Забайкальского края, утвержденная приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 112.

[411] См.: разд. «Требования к реализации ОДТ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.101.

[412] См.:

- ОДТ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ОДТ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.96-л.97.

[413] См.:

- ОДТ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ОДТ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.96-л.97.

8.10.6. Контроль состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации[414]

8.10.6.1. Должны выполняться следующие требования Регуляторов к реализации контроля состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации:[415]

8.10.6.1.1. Оператором должен осуществляться контроль состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей), в том числе по передаче информации, предусматривающий:

- контроль выполнения уполномоченным лицом требований о защите информации, установленных законодательством Российской Федерации и условиями договора (соглашения), на основании которого уполномоченное лицо обрабатывает информацию или предоставляет вычислительные ресурсы (мощности);
- мониторинг состояния и качества предоставления уполномоченным лицом (провайдером) вычислительных ресурсов (мощностей);
- мониторинг состояния и качества предоставления уполномоченным лицом (провайдером)услуг по передаче информации.

8.10.6.1.2. Условия, права и обязанности, содержание и порядок контроля должны определяться в договоре (соглашении), заключаемом между оператором и уполномоченным лицом на предоставление вычислительных ресурсов (мощностей) или передачу информации с использованием информационно-телекоммуникационных сетей связи.

8.10.6.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю состояния и качества предоставления уполномоченным лицом вычислительных ресурсов (мощностей), в том числе по передаче информации[416]:

8.10.6.2.1. Между оператором и поставщиком услуг

---

[414] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ОДТ.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОДТ.7 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ОДТ.7 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[415] См.: разд. «Требования к реализации ОДТ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.102-л.103.

[416] См.: разд. «Требования к реализации ОДТ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.102-л.103.

(телекоммуникационных, вычислительных) должно заключаться соглашение об уровне услуг, содержащее описание услуг, прав и обязанностей сторон и согласованный уровень качества предоставляемых услуг в соответствии с законодательством Российской Федерации.

8.11. Политика защиты среды виртуализации

Применяемая в Департаменте ЗАГС Забайкальского края политика защиты среды виртуализации устанавливает требования к:

- идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации[417];
- управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин[418];
- регистрации событий безопасности в виртуальной инфраструктуре[419];
- управлению (фильтрации, маршрутизации, контролю соединения, однонаправленной передаче) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры[420];
- управлению перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных[421];
- контролю целостности виртуальной инфраструктуры и ее конфигураций[422];
- резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры[423];
- реализации и управлению антивирусной защитой в виртуальной инфраструктуре[424];
- разбиению виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей[425].

8.11.1. Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

8.11.1.1. Должны выполняться следующие требования Регуляторов к реализации идентификации и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации:[426]

8.11.1.1.1. В информационной системе должны обеспечиваться

[417] См.: разд.8.11.1 настоящей Политики.
[418] См.: разд.8.11.2 настоящей Политики.
[419] См.: разд.8.11.3 настоящей Политики.
[420] См.: разд.8.11.4 настоящей Политики.
[421] См.: разд.8.11.5 настоящей Политики.
[422] См.: разд.8.11.6 настоящей Политики.
[423] См.: разд.8.11.7 настоящей Политики.
[424] См.: разд.8.11.8 настоящей Политики.
[425] См.: разд.8.11.9 настоящей Политики.
[426] См.: разд. «Требования к реализации ЗСВ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.104-л.105.

идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации, в соответствии с требованиями Регуляторов[427].

8.11.1.1.2. Виртуальная инфраструктура включает среду виртуализации (программное обеспечение, служебные данные компонентов виртуальной инфраструктуры) и аппаратное обеспечение (аппаратные средства, необходимые для функционирования среды виртуализации, в том числе средства резервного копирования и защиты информации).

8.11.1.1.3. В качестве компонентов виртуальной инфраструктуры необходимо, как минимум, рассматривать серверное оборудование, аппаратное обеспечение консолей управления, оборудование хранения данных, сетевое оборудование, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальное аппаратное обеспечение, виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенным для выполнения определенных функций в виртуальной инфраструктуре), программное обеспечение управления виртуальной инфраструктурой (в том числе гипервизором, настройками виртуальных машин, миграцией виртуальных машин, балансировкой нагрузки), служебные данные компонентов виртуальной инфраструктуры (настройки и иные служебные данные), средства резервного копирования компонентов среды виртуализации и средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

8.11.1.1.4. В качестве объектов доступа в виртуальной инфраструктуре необходимо, как минимум, рассматривать программное обеспечение управления виртуальной инфраструктурой, гипервизор, хостовую операционную систему (если применимо), виртуальные машины, программную среду виртуальных машин (в том числе их операционные системы и программное обеспечение), виртуальные контейнеры (зоны), виртуализированное программное обеспечение (виртуальные машины с предустановленным программным обеспечением, предназначенная для выполнения определенных функций в виртуальной инфраструктуре), средства защиты информации, используемые в рамках виртуальных машин и виртуальной инфраструктуры в целом.

8.11.1.1.5. При реализации мер по идентификации и аутентификации

---

[427] См.:

- ИАФ.1 - ИАФ.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1»- разд. «Требования к реализации ИАФ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.16-л.24.

субъектов доступа и объектов доступа в виртуальной инфраструктуре должны обеспечиваться:

- идентификация и аутентификация администраторов управления средствами виртуализации;
- идентификация и аутентификация субъектов доступа при их локальном и удалённом обращении к объектам доступа в виртуальной инфраструктуре;
- блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации;
- защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования;
- защита аутентификационной информации в процессе ее ввода для аутентификации в виртуальной инфраструктуре от возможного использования лицами, не имеющими на это полномочий;
- идентификация и аутентификация субъектов доступа при осуществлении ими попыток доступа к средствам управления параметрами аппаратного обеспечения виртуальной инфраструктуры.

8.11.1.1.6. Внутри развернутых на базе виртуальной инфраструктуры виртуальных машин должна быть также обеспечена реализация мер по идентификации и аутентификации субъектов и объектов доступа в соответствии с требованиями Регуляторов[428].

8.11.1.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации[429]:

8.11.1.2.1. В информационной системе должны обеспечиваться взаимная идентификация и аутентификация пользователя и сервера виртуализации (виртуальных машин) при удалённом доступе.

8.11.2. Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин

8.11.2.1. Должны выполняться следующие требования Регуляторов к реализации управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри

---

[428] См.:

- ИАФ.1 - ИАФ.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1»- разд. «Требования к реализации ИАФ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.16-л.24.

[429] См.: разд. «Требования к реализации ЗСВ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.105.

виртуальных машин:[430]

8.11.2.1.1. В информационной системе должно обеспечиваться управление доступом субъектов доступа к объектам доступа, в том числе внутри виртуальных машин, в соответствии с требованиями Регуляторов[431].

8.11.2.1.2. При реализации мер по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре должны обеспечиваться:

- контроль доступа субъектов доступа к средствам управления компонентами виртуальной инфраструктуры;
- контроль доступа субъектов доступа к файлам-образам виртуализированного программного обеспечения, виртуальных машин, файлам-образам, служебным данным, используемым для обеспечения работы виртуальных файловых систем, и иным служебным данным средств виртуальной среды;
- управление доступом к виртуальному аппаратному обеспечению информационной системы, являющимся объектом доступа;
- контроль запуска виртуальных машин на основе заданных оператором правил (режима запуска, типа используемого носителя и иных правил).

8.11.2.1.3. Кроме того, меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать:

- разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к объектам доступа, расположенным внутри виртуальных машин, в соответствии с правилами разграничения доступа пользователей данных виртуальных машин (потребителей облачных услуг);
- разграничение доступа субъектов доступа, зарегистрированных на виртуальных машинах, к ресурсам информационной системы, размещенным за пределами виртуальных машин, в соответствии с правилами разграничения доступа, принятыми в информационной системе в целом.

8.11.2.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри

---

[430] См.: разд. «Требования к реализации ЗСВ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.105-л.106.

[431] См.:

- УПД.1, УПД.2, УПД.4, УПД.5, УПД.6, УПД.9, УПД.10, УПД.11, УПД.12, УПД.13 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.1»- разд. «Требования к реализации УПД.13» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.25-л.40.

виртуальных машин[432]:

8.11.2.2.1. В информационной системе должен обеспечиваться доступ к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, останова, создания копий, удаления виртуальных машин, который должен быть разрешен только администраторам виртуальной инфраструктуры.

8.11.2.2.2. В информационной системе должен обеспечиваться доступ к конфигурации виртуальных машин только администраторам виртуальной инфраструктуры.

8.11.2.2.3. Администратор виртуальной инфраструктуры определяет ограничения по изменению состава устройств виртуальных машин, объема используемой оперативной памяти, подключаемых виртуальных и физических носителей информации.

8.11.2.2.4. В информационной системе должен обеспечиваться контроль доступа субъектов доступа к изолированному адресному пространству в памяти гипервизора, в памяти хостовой операционной системы, виртуальных машин и (или) иных объектов доступа.

8.11.3. Регистрация событий безопасности в виртуальной инфраструктуре

8.11.3.1. Должны выполняться следующие требования Регуляторов к реализации регистрации событий безопасности в виртуальной инфраструктуре:[433]

8.11.3.1.1. В информационной системе должна обеспечиваться регистрация событий безопасности в виртуальной инфраструктуре в соответствии с требованиями Регуляторов[434].

8.11.3.1.2. При реализации мер по регистрации событий безопасности в виртуальной инфраструктуре дополнительно к событиям, установленным в требованиях Регуляторов[435], должны подлежать регистрации следующие события:

---

[432] См.: разд. «Требования к реализации ЗСВ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.106.

[433] См.: разд. «Требования к реализации ЗСВ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.107-л.108.

[434] См.:

- РСБ.1- РСБ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации РСБ.1»- разд. «Требования к реализации РСБ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.62-л.69.

[435] См.:

- РСБ.1Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации РСБ.1методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.62-л.63.

- запуск (завершение) работы компонентов виртуальной инфраструктуры;
- доступ субъектов доступа к компонентам виртуальной инфраструктуры;
- изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;
- изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

8.11.3.1.3. При регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы указанных компонентов виртуальной инфраструктуры.

8.11.3.1.4. При регистрации входа (выхода) субъектов доступа в компоненты виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры.

8.11.3.1.5. При изменении в составе и конфигурации компонентов виртуальной инфраструктуры во время запуска, функционирования и в период её аппаратного отключения состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры.

8.11.3.1.6. При изменении правил разграничения доступа к компонентам виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому

оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры.

8.11.3.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по регистрации событий безопасности в виртуальной инфраструктуре[436]:

8.11.3.2.1. В информационной системе должен обеспечиваться централизованный сбор, хранение и анализ информации о зарегистрированных событиях безопасности виртуальной инфраструктуры.

8.11.3.2.2. В информационной системе при регистрации запуска (завершения) работы компонентов виртуальной инфраструктуры состав и содержание информации, подлежащей регистрации, должны включать дату и время запуска (завершения) программ и процессов в гипервизоре и хостовой операционной системе.

8.11.3.2.3. В информационной системе должна обеспечиваться регистрация событий безопасности, связанных с перемещением и размещением виртуальных машин.

8.11.4. Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры[437]

8.11.4.1. Должны выполняться следующие требования Регуляторов к реализации управления (фильтрации, маршрутизации, контроля соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры:[438]

8.11.4.1.1. В информационной системе должно осуществляться управление потоками информации между компонентами

---

[436] См.: разд. «Требования к реализации ЗСВ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.108.

[437] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗСВ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗСВ.4 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗСВ.4 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[438] См.: разд. «Требования к реализации ЗСВ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.109-л.110.

виртуальной инфраструктуры и по периметру виртуальной инфраструктуры в соответствии с требованиями Регуляторов[439].

8.11.4.1.2. При реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться:

- фильтрация сетевого трафика между компонентами виртуальной инфраструктуры, в том числе между внешними по отношению к серверу виртуализации сетями и внутренними по отношению к серверу виртуализации сетями, в том числе при организации сетевого обмена с сетями связи общего пользования;
- обеспечение доверенных канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и средствами защиты информации (функциями безопасности);
- контроль передачи служебных информационных сообщений, передаваемых в виртуальных сетях гипервизора, хостовой операционной системы, по составу, объёму и иным характеристикам;
- отключение неиспользуемых сетевых протоколов компонентами виртуальной инфраструктуры гипервизора, хостовой операционной системы, виртуальной вычислительной сети;
- обеспечение подлинности сетевых соединений (сеансов взаимодействия) внутри виртуальной инфраструктуры, в том числе для защиты от подмены сетевых устройств и сервисов;
- обеспечение изоляции потоков данных, передаваемых и обрабатываемых компонентами виртуальной инфраструктуры (гипервизором, хостовой операционной системой) и сетевых потоков виртуальной вычислительной сети; семантический и статистический анализ сетевого трафика виртуальной вычислительной сети.

8.11.4.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению (фильтрации, маршрутизации, контролю соединения, однонаправленной передаче) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры[440]:

8.11.4.2.1. В информационной системе, построенной с применением технологии виртуализации, должна быть обеспечена единая точка подключения к виртуальной инфраструктуре (при необходимости резервирования каналов связи, точка подключения должна

---

[439] См.:

- УПД.3, ЗИС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.3» и разд. «Требования к реализации ЗИС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.28-л.30, л.124.

[440] См.: разд. «Требования к реализации ЗСВ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.110.

рассматриваться как комплексное решение, включающее в себя средства взаимодействия с основным и резервными каналами связи).

8.11.4.2.2. В информационной системе должна обеспечиваться фильтрация сетевого трафика от (к) каждой гостевой операционной системы, в виртуальных сетях гипервизора и для каждой виртуальной машины.

8.11.4.2.3. В информационной системе должен обеспечиваться запрет прямого (с использованием механизмов, встроенных в средства виртуализации) взаимодействия виртуальных машин между собой; для служебных данных должен обеспечиваться контроль прямого взаимодействия виртуальных машин между собой.

8.11.4.2.4. В информационной системе в соответствии с законодательством Российской Федерации применяются криптографические методы защиты информации конфиденциального характера, передаваемой по виртуальным и физическим каналам связи гипервизора, хостовой операционной системы.

8.11.4.2.5. В информационной системе при реализации мер по управлению потоками информации между компонентами виртуальной инфраструктуры должны обеспечиваться семантический и статистический анализ сетевого трафика.

8.11.4.2.6. В информационной системе должно обеспечиваться определение перечня протоколов и портов (включая динамически выделяемые порты), необходимых для работы приложений и сервисов в рамках виртуальной инфраструктуры.

8.11.4.2.7. В информационной системе должно обеспечиваться определение перечня протоколов и портов (включая динамически выделяемые порты), необходимых для работы приложений и сервисов между виртуальной инфраструктурой и сетями, являющимися внешними по отношению к виртуальной инфраструктуре.

8.11.5. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных[441]

8.11.5.1. Должны выполняться следующие требования Регуляторов к реализации управления перемещением виртуальных машин

[441] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗСВ.6 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗСВ.6 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗСВ.6 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

(контейнеров) и обрабатываемых на них данных:[442]

8.11.5.1.1. Оператором должно обеспечиваться управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

8.11.5.1.2. При управлении перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных должны обеспечиваться:

- регламентирование порядка перемещения (определение ответственных за организацию процесса, объектов перемещения, ресурсов инфраструктуры, задействованных в перемещении, а также способов перемещения);
- управление размещением и перемещением файлов-образов виртуальных машин (контейнеров) между носителями (системами хранения данных);
- управление размещением и перемещением исполняемых виртуальных машин (контейнеров) между серверами виртуализации; управление размещением и перемещением данных, обрабатываемых с использованием виртуальных машин, между носителями (системами хранения данных).

8.11.5.1.3. Управление перемещением виртуальных машин (контейнеров) должно предусматривать:

- полный запрет перемещения виртуальных машин (контейнеров);
- ограничение перемещения виртуальных машин (контейнеров) в пределах информационной системы (сегмента информационной системы);
- ограничение перемещения виртуальных машин (контейнеров) между сегментами информационной системы.

8.11.5.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных[443]:

8.11.5.2.1. Оператором должно обеспечиваться перемещение виртуальных машин (контейнеров) и обрабатываемых на них данных в пределах информационной системы только на контролируемые им (или уполномоченным лицом) технические средства (сервера виртуализации, носители, системы хранения данных).

8.11.5.2.2. Оператором должна осуществляться обработка отказов перемещения виртуальных машин (контейнеров) и обрабатываемых на них данных.

8.11.5.2.3. В информационной системе должны использоваться механизмы централизованного управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

8.11.5.2.4. В информационной системе должна быть обеспечена

[442] См.: разд. «Требования к реализации ЗСВ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.111- л.112.

[443] См.: разд. «Требования к реализации ЗСВ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.112.

непрерывность регистрации событий безопасности в виртуальных машинах (контейнерах) в процессе перемещения.

8.11.5.2.5. В информационной системе должна осуществляться очистка освобождаемых областей памяти на серверах виртуализации, носителях, системах хранения данных при перемещении виртуальных машин (контейнеров) и обрабатываемых на них данных.

8.11.6. Контроль целостности виртуальной инфраструктуры и ее конфигураций[444]

8.11.6.1. Должны выполняться следующие требования Регуляторов к реализации контроля целостности виртуальной инфраструктуры и ее конфигураций:[445]

8.11.6.1.1. В информационной системе должен обеспечиваться контроль целостности компонентов виртуальной инфраструктуры в соответствии с требованиями Регуляторов[446].

8.11.6.1.2. При реализации мер по контролю целостности компонентов виртуальной инфраструктуры должны обеспечиваться:

- контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем и (или) обеспечения безопасности обрабатываемой в них информации (загрузчика, системных файлов, библиотек операционной системы и иных компонентов);
- контроль целостности состава и конфигурации виртуального оборудования; контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;
- контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-

---

[444] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗСВ.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗСВ.7 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗСВ7 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[445] См.: разд. «Требования к реализации ЗСВ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.112- л.113.

[446] См.:

- ОЦЛ.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный № 28608);
- разд. «Требования к реализации ОЦЛ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.86-л.87.

образов, используемых для обеспечения работы виртуальных файловых систем (контроль файлов-образов должен проводиться во время, когда файлы-образы не задействованы).

8.11.6.1.3. В информационной системе должен обеспечиваться контроль целостности резервных копий виртуальных машин (контейнеров).

8.11.6.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю целостности виртуальной инфраструктуры и ее конфигураций[447]:

8.11.6.2.1. В информационной системе должен обеспечиваться контроль целостности базовой системы ввода-вывода вычислительных серверов и консолей управления виртуальной инфраструктуры.

8.11.6.2.2. В информационной системе должен обеспечиваться контроль целостности микропрограмм и служебных данных элементов аппаратной части виртуальной инфраструктуры (в том числе загрузочных записей машинных носителей информации).

8.11.6.2.3. В информационной системе должен обеспечиваться контроль состава аппаратной части компонентов виртуальной инфраструктуры.

8.11.6.2.4. В информационной системе должен обеспечиваться контроль целостности программного обеспечения облачных клиентов.

8.11.7. Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры[448]

8.11.7.1. Должны выполняться следующие требования Регуляторов к реализации резервного копирования данных, резервирования технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры:[449]

8.11.7.1.1. В информационной системе должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры и каналов связи внутри виртуальной инфраструктуры в

---

[447] См.: разд. «Требования к реализации ЗСВ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.113.

[448] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗСВ.8 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗСВ.8 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;

  ЗСВ8 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[449] См.: разд. «Требования к реализации ЗСВ.8» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.113- л.114.

соответствии с требованиями Регуляторов[450].

8.11.7.1.2. При реализации мер по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры должны обеспечиваться:

- определение мест хранения резервных копий виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре;
- резервное копирование виртуальных машин (контейнеров);
- резервное копирование данных, обрабатываемых в виртуальной инфраструктуре;
- резервирование программного обеспечения виртуальной инфраструктуры;
- резервирование каналов связи, используемых в виртуальной инфраструктуре;
- периодическая проверка резервных копий и возможности восстановления виртуальных машин (контейнеров) и данных, обрабатываемых в виртуальной инфраструктуре с использованием резервных копий.

8.11.7.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по резервному копированию данных, резервированию технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры:[451]

8.11.7.2.1. В информационной системе должно выполняться резервное копирование конфигурации виртуальной инфраструктуры.

8.11.7.2.2. В информационной системе должно выполняться резервное копирование программного обеспечения серверов управления виртуализацией, автоматизированного рабочего места администратора управления средствами виртуализации.

8.11.7.2.3. В информационной системе должно выполняться резервирование дистрибутивов средств построения виртуальной инфраструктуры (в том числе средств управления виртуальной инфраструктурой).

8.11.7.2.4. В информационной системе должно обеспечиваться резервирование технических средств для серверов виртуализации, серверов управления виртуализацией, автоматизированного рабочего места администратора управления средствами виртуализации.

8.11.7.2.5. В информационной системе должно обеспечиваться резервирование технических средств систем хранения данных и

---

[450] См.:

- ОДТ.2, ОДТ.4, ОДТ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ОДТ.2», разд. «Требования к реализации ОДТ.4» и разд. «Требования к реализации ОДТ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.96- л.98, л.99-л.101.

[451] См.: разд. «Требования к реализации ЗСВ.8» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.114.

их компонент, используемых в виртуальной инфраструктуре.

8.11.7.2.6. В информационной системе должно обеспечиваться резервирование технических средств активного (коммутационного) и пассивного оборудования каналов связи, используемых в виртуальной инфраструктуре.

8.11.7.2.7. В информационной системе должно обеспечиваться применение технологий распределенного хранения информации и восстановления информации после сбоев для обеспечения отказоустойчивости виртуальной инфраструктуры.

8.11.8. Реализация и управление антивирусной защитой в виртуальной инфраструктуре

8.11.8.1. Должны выполняться следующие требования Регуляторов к реализации и управлению антивирусной защитой в виртуальной инфраструктуре[452]:

8.11.8.1.1. В информационной системе должны обеспечиваться реализация и управление антивирусной защитой в виртуальной инфраструктуре в соответствии с требованиями Регуляторов[453].

8.11.8.1.2. При реализации соответствующих мер должны обеспечиваться:

- проверка наличия вредоносных программ (вирусов) в хостовой операционной системе, включая контроль файловой системы, памяти, запущенных приложений и процессов;
- проверка наличия вредоносных программ в гостевой операционной системе, в процессе ее функционирования, включая контроль файловой системы, памяти, запущенных приложений и процессов.

8.11.8.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по реализации и управлению антивирусной защитой в виртуальной инфраструктуре[454]:

8.11.8.2.1. В информационной системе должно обеспечиваться разграничение доступа к управлению средствами антивирусной защиты.

8.11.8.2.2. В информационной системе должен обеспечиваться контроль функционирования средств антивирусной защиты в виртуальной инфраструктуре, в том числе маршрутизация потоков информации в виртуальной инфраструктуре через средство антивирусной защиты.

8.11.8.2.3. В информационной системе должна обеспечиваться

---

[452] См.: разд. «Требования к реализации ЗСВ.9» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.115.

[453] См.:

- АВЗ.1, АВЗ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- См.: разд. «Требования к реализации АВЗ.1» и разд. «Требования к реализации АВЗ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.72-л.74.

[454] См.: разд. «Требования к реализации ЗСВ.9» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.115.

реализация технологии обновления программного обеспечения и баз данных признаков компьютерных вирусов средств антивирусной защиты, предусматривающая однократную передачу обновлений на сервер виртуальной инфраструктуры для их последующего применения в виртуальных машинах.

8.11.8.2.4. В информационной системе должна обеспечиваться проверка наличия вредоносных программ (вирусов) в гипервизоре.

8.11.8.2.5. В информационной системе должна обеспечиваться проверка наличия вредоносных программ в файлах конфигурации виртуального оборудования.

8.11.8.2.6. В информационной системе должна обеспечиваться проверка наличия вредоносных программ в файлах-образах виртуализированного программного обеспечения и виртуальных машин.

8.11.9. Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей

8.11.9.1. Должны выполняться следующие требования Регуляторов к реализации разбиения виртуальной инфраструктуры на сегменты:[455]

8.11.9.1.1. В информационной системе должно обеспечиваться разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей в соответствии с требованиями Регуляторов[456].

8.11.9.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по разбиению виртуальной инфраструктуры на сегменты[457]:

8.11.9.2.1. В информационной системе должно обеспечиваться логическое сегментирование виртуальной инфраструктуры, предусматривающее выделение группы виртуальных машин, хранилищ информации и информационных потоков, предназначенных для решения выделенных (обособленных) задач.

8.11.9.2.2. В информационной системе должно обеспечиваться выделение в отдельный сегмент (отдельные сегменты) серверов управления виртуализацией (автоматизированного рабочего места администратора управления средствами виртуализации).

8.11.9.2.3. В информационной системе должно обеспечиваться

---

[455] См.: разд. «Требования к реализации ЗСВ.10» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.116.

[456] См.:

- ЗИС.17 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ЗИС.17» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.136-л.137.

[457] См.: разд. «Требования к реализации ЗСВ.10» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.116.

физическое сегментирование виртуальной инфраструктуры для решения выделенных (обособленных) задач.

8.12. Политика защиты информационной системы и ее средств

Применяемая в Департаменте ЗАГС Забайкальского края политика защиты информационной системы и ее средств устанавливает требования к:

- разделению в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы[458];
- защите архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации[459];
- разбиению информационной системы на сегменты (сегментированию информационной системы) и обеспечению защиты периметров сегментов информационной системы[460];
- исключению доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы[461];
- защите информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы[462];
- защите периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями[463].

8.12.1. Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы[464]

8.12.1.1. Должны выполняться следующие требования Регуляторов к реализации разделения в информационной системе функций по управлению (администрированию) информационной системой,

---

[458] См.: разд.8.12.1 настоящей Политики.
[459] См.: разд.8.12.2 настоящей Политики.
[460] См.: разд.8.12.3 настоящей Политики.
[461] См.: разд.8.12.4 настоящей Политики.
[462] См.: разд.8.12.5 настоящей Политики.
[463] См.: разд.8.12.6 настоящей Политики.
[464] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.1 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.1 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы:[465]

8.12.1.1.1. В информационной системе должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации(функций безопасности) и функциональных возможностей пользователей по обработке информации.

8.12.1.1.2. Функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации включают функции по управлению базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями, серверами, средствами защиты информации и иные функции, требующие высоких привилегий.

8.12.1.1.3. Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств информационной системы, реализующих функциональные возможности по управлению (администрированию) информационной системой и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами.

8.12.1.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по разделению в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы:[466]

8.12.1.2.1. В информационной системе должно обеспечиваться исключение отображения функциональных возможностей по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации в интерфейсе пользователя.

8.12.1.2.2. В информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов информационной системы.

8.12.1.2.3. В информационной системе должно обеспечиваться выделение автоматизированных рабочих мест для администраторов безопасности.

8.12.1.2.4. Оператором должно обеспечиваться исключение возможности

[465] См.: разд. «Требования к реализации ЗИС.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.122.

[466] См.: разд. «Требования к реализации ЗИС.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.122.

управления (администрирования) информационной системой, управления (администрирования) системой защиты информации из-за пределов контролируемой зоны.

8.12.2. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации[467]

8.12.2.1. Должны выполняться следующие требования Регуляторов к реализации защиты архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации[468]:

8.12.2.1.1. В информационной системе должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации.

8.12.2.1.2. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором в соответствии с настоящим методическим документом, направленных на обеспечение их конфиденциальности и целостности.

8.12.2.1.3. Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в информационной системе.

8.12.2.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по защите архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации: [469]

8.12.2.2.1. Оператором для обеспечения конфиденциальности и целостности архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных

---

[467] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.15 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.15 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.15 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[468] См.: разд. «Требования к реализации ЗИС.15» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.135.

[469] См.: разд. «Требования к реализации ЗИС.15» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.135.

данных, не подлежащих изменению в процессе обработки информации, в соответствии с законодательством Российской Федерации применяются криптографические (шифровальные) средства защиты информации (данных).

8.12.2.2.2. Использование неперезаписываемых носителей или носителей с защищенной областью памяти для размещения (хранения) параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации.

8.12.3. Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы

8.12.3.1. Должны выполняться следующие требования Регуляторов к реализации разбиения информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы:[470]

8.12.3.1.1. Оператором должно осуществляться разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечиваться защита периметров сегментов информационной системы.

8.12.3.1.2. Сегментирование информационной системы проводится с целью построения многоуровневой (эшелонированной) системы защиты информации путем построения сегментов на различных физических доменах или средах.

8.12.3.1.3. Принципы сегментирования информационной системы определяются оператором с учетом функциональных и технологических особенностей процесса обработки информации и анализа угроз безопасности информации и должны заключаться в снижении вероятности реализации угроз и (или) их локализации в рамках одного сегмента.

8.12.3.1.4. Сегментирование информационной системы также может проводиться с целью разделения информационной системы на сегменты, имеющие различные классы защищенности информационной системы.

8.12.3.1.5. При сегментировании информационной системы должна быть обеспечена защита периметров сегментов информационной системы в соответствии с требованиями Регуляторов[471].

8.12.3.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по разбиению информационной системы на сегменты (сегментирование информационной системы) и обеспечению

---

[470] См.: разд. «Требования к реализации ЗИС.17» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.136-л.137.

[471] См.:

- УПД.3 и ЗИС.23 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.3» и разд. «Требования к реализации ЗИС.23» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.28-л.30, л.142- л.145.

защиты периметров сегментов информационной системы[472]:

8.12.3.2.1. Оператором осуществляется выделение сегментов информационной системы для размещения общедоступной (публичной) информации:

а) путем выделения отдельных физических сетевых интерфейсов коммуникационного оборудования и (или) средств защиты периметра;

б) путем физической изоляции сегментов информационной системы для размещения общедоступной (публичной) информации.

8.12.4. Исключение доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы[473]

8.12.4.1. Должны выполняться следующие требования Регуляторов к реализации исключения доступа пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы:[474]

8.12.4.1.1. В информационной системе должен быть исключен доступ пользователя к информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства, ресурсы файловой системы и иные общие для пользователей ресурсы информационной системы.

8.12.4.1.2. Исключение доступа к информации через общие для пользователей ресурсы должно обеспечивать запрет доступа текущему пользователю (учетной записи) или текущему процессу к системным ресурсам (реестрам, оперативной памяти, внешним запоминающим устройствам) при их повторном использовании, в которых хранится информация другого (предыдущего) пользователя.

8.12.4.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по исключению доступа пользователя к

---

[472] См.: разд. «Требования к реализации ЗИС.17» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.137.

[473] Исполняется только для 1 класса защищенности информационной системы. См.:

- ЗИС.15 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.15 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.15 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[474] См.: разд. «Требования к реализации ЗИС.21» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.140-л.141.

информации, возникшей в результате действий предыдущего пользователя через реестры, оперативную память, внешние запоминающие устройства и иные общие для пользователей ресурсы информационной системы[475]:

8.12.4.2.1. В информационной системе должна быть исключена возможность использования в качестве общих для пользователей ресурсов информационной системы, которые используются как интерфейс (память, однонаправленные интерфейсы (устройства) и сетевые карты) взаимодействия (связи) с системами, имеющими другие классы защищенности.

8.12.5. Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы[476]

8.12.5.1. Должны выполняться следующие требования Регуляторов к реализации защиты информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы:[477]

8.12.5.1.1. В информационной системе должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы.

8.12.5.1.2. Оператором должен быть определен перечень угроз (типов угроз) безопасности информации, направленных на отказ в обслуживании.

8.12.5.1.3. Защита от угроз безопасности информации, направленных на отказ в обслуживании, осуществляется посредством реализации в информационной системе мер защиты информационной системы в соответствии с требованиями Регуляторов[478] и повышенными характеристиками производительности телекоммуникационного

---

[475] См.: разд. «Требования к реализации ЗИС.21» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.141.

[476] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.22 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.22 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.22 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[477] См.: разд. «Требования к реализации ЗИС.22» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.141-л.142.

[478] См.:

- ЗИС.23 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ЗИС.23» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.142-л.145.

оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с требованиями Регуляторов[479].

8.12.5.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по защите информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы[480]:

8.12.5.2.1. В информационной системе обеспечивается ограничение возможностей пользователей по реализации угроз безопасности информации, направленных на отказ в обслуживании, в отношении отдельных сегментов информационной системы и других информационных систем.

8.12.5.2.2. В информационной системе обеспечивается управление характеристиками производительности телекоммуникационного оборудования и каналов передачи информации в зависимости от интенсивности реализации угроз безопасности информации, направленных на отказ в обслуживании.

8.12.5.2.3. Оператором в установленном порядке обеспечивается использование услуг сторонних организаций (провайдеров) по «очистке» входящего трафика (для сброса потока пакетов, используемых нарушителем для реализации угроз безопасности, направленных на отказ в обслуживании этой информационной системы).

8.12.5.2.4. Оператором обеспечивается применение средств защиты информации, предназначенных для нейтрализации угроз безопасности, направленных на отказ в обслуживании.

8.12.5.2.5. В информационной системе меры защиты от угроз безопасности информации, направленных на отказ в обслуживании, должны обеспечить возможность защиты от соответствующих атак на информационную систему без воздействия на трафик сети (подсети), в которой функционирует информационная система.

8.12.5.2.6. Оператором обеспечивается возможность взаимодействия по вопросам защиты информации от угроз, направленных на отказ в обслуживании, со специальными системами уполномоченных органов с учетом требований по защите информации.

8.12.6. Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-

---

[479] См.:

- ОДТ.2, ОДТ.4 и ОДТ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ОДТ.2» , разд. «Требования к реализации ОДТ.4» и разд. «Требования к реализации ОДТ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.96-л.98, л.99-л.101.

[480] См.: разд. «Требования к реализации ЗИС.22» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.142.

телекоммуникационными сетями[481]

8.12.6.1. Должны выполняться следующие требования Регуляторов к реализации защиты периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями:[482]

8.12.6.1.1. В информационной системе должна осуществляться защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, предусматривающая:

- управление (контроль) входящими в информационную систему и исходящими из информационной системы информационными потоками на физической и (или) логической границе информационной системы (сегментов информационной системы);
- обеспечение взаимодействия информационной системы и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации).

8.12.6.2. Правила и процедуры защиты периметра информационной системы регламентируются в организационно-распорядительных документах оператора по защите информации[483].

8.12.6.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии

---

[481] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.23 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.23 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.23 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[482] См.: разд. «Требования к реализации ЗИС.23» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.142-л.145.

[483] См.: Инструкция по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденная приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109.

с иными информационными системами и информационно-телекоммуникационными сетями[484]:

8.12.6.3.1. В информационной системе должна быть обеспечена возможность размещения публичных общедоступных ресурсов (в частности общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы.

8.12.6.3.2. В информационной системе должно быть обеспечено предоставление доступа во внутренние сегменты информационной системы (демилитаризованную зону) из внешних информационных систем и сетей только через средства защиты периметра (за исключением внутренних сегментов, которые специально выделены для такого взаимодействия).

8.12.6.3.3. Оператор должен ограничить количество точек доступа в информационную систему из внешних информационных систем и сетей до минимально необходимого числа для решения постановленных задач, а также обеспечивающего постоянный и всесторонний контроль входящих и исходящих информационных потоков.

8.12.6.3.4. Оператором в информационной системе:

а) должен применяться отдельный физический управляемый (контролируемый) сетевой интерфейс для каждого внешнего телекоммуникационного сервиса;

б) должны быть установлены правила управления информационными потоками для каждого физического управляемого (контролируемого) сетевого интерфейса;

в) должна обеспечиваться защита информации при ее передаче по каналам связи, имеющим выход за пределы контролируемой зоны (при необходимости), путем применения организационно-технических мер или криптографических методов в соответствии с законодательством Российской Федерации;

г) должно обеспечиваться обоснование и документирование всех исключений из правил управления информационными потоками, связанных с решением определенных задач в информационной системе, и определение продолжительности потребности таких исключений;

д) должно обеспечиваться удаление введенных исключений из правил управления информационными потоками после истечения установленного времени.

8.12.6.3.5. В информационной системе должен быть исключен выход (вход) через управляемые (контролируемые) сетевые интерфейсы информационных потоков по умолчанию (реализация принципа «запрещено все, что не разрешено»).

8.12.6.3.6. Оператором обеспечивается запрет передачи информации за пределы периметра информационной системы при отказе (сбое) функционирования средств защиты периметра.

8.12.6.3.7. В информационной системе должна быть исключена

[484] См.: разд. «Требования к реализации ЗИС.23» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.143-л.145.

возможность информационного взаимодействия мобильных и иных технических средств (устройств) с внешними информационными системами и информационно-телекоммуникационным сетям в процессе их удаленного подключения к защищаемой информационной системе с использованием средств построения виртуальных частных сетей.

8.12.6.3.8. В информационной системе обеспечивается сетевое соединение внутренних сегментов информационной системы (отдельных средств вычислительных техники), определенных оператором, с установленными им внешними информационными системами и сетями через прокси-серверы, размещенные совместно со средствами защиты периметра, обеспечивающие логирование (отслеживание) TCP-сессий, блокирование конкретных URL, доменных имен, IP-адресов и другим параметрам запросов к внешним информационным ресурсам.

8.12.6.3.9. В информационной системе исключается возможность выхода через управляемые (контролируемые) сетевые интерфейсы информационных потоков, содержащих вредоносное программное обеспечение (вирусы) или признаки компьютерных атак, представляющих угрозу внешним информационным системам и сетям.

8.12.6.3.10. В информационной системе исключается возможность утечки информации через управляемые (контролируемые) сетевые интерфейсы путем точного соблюдения форматов протоколов, контроля использования стеганографии, отключения внешних сетевых интерфейсов, разборки и сборки пакетов данных, контроля отклонения типа и объема информационного потока от установленного профиля.

8.12.6.3.11. В информационной системе должна быть обеспечена проверка адреса источника информационного потока и адреса получателя информационного потока с целью подтверждения того, что информационное взаимодействие между этими адресами разрешено.

8.12.6.3.12. В информационной системе обеспечивается защита периметра с использованием шлюза безопасности на уровне узлов (хостов) для серверов, рабочих станций и мобильных технических средств.

8.12.6.3.13. В информационной системе обеспечивается сокрытие сетевых адресов, используемых для управления средствами защиты периметра, информация о которых может быть получена через технологии определения устройств в сети (в частности систему доменных имен).

8.12.6.3.14. Оператором обеспечивается отделение через отдельный физический управляемый (контролируемый) сетевой интерфейс функций безопасности и управления (администрирования) информационной системы, определенных оператором, от других (внутренних) компонентов информационной системы.

8.12.6.3.15. Оператором обеспечивается исключение возможности несанкционированного физического сетевого подключения к управляемым (контролируемым) сетевым интерфейсам (сетевым интерфейсам средств защиты периметра).

8.12.6.3.16. В информационной системе для контроля (анализа)

защищенности доступ администраторов обеспечивается через выделенный отдельный физический управляемый (контролируемый) сетевой интерфейс.

8.12.6.3.17. Оператором применяются автоматизированные средства, обеспечивающие строгое соблюдение формата сетевых протоколов на уровне приложений (проверка пакетов на предмет соблюдения спецификаций протокола на уровне приложений).

8.12.6.3.18. В информационной системе обеспечивается корректное завершение ее функционирования в случае нарушения функционирования (сбоя, отказов) средств защиты периметра.

8.12.6.3.19. В информационной системе при необходимости предоставлять доступ к ресурсам информационной системы должна быть организована демилитаризованная зона, содержащая доступные ресурсы.

8.12.6.3.20. В информационной системе должна быть обеспечена возможность размещения публичных общедоступных ресурсов (например, общедоступный веб-сервер), взаимодействующих с информационной системой через отдельные физические управляемые (контролируемые) сетевые интерфейсы.

IX. Политика обеспечения телекоммуникационной безопасности Департамента ЗАГС Забайкальского края

Политика обеспечения телекоммуникационной безопасности Департамента ЗАГС Забайкальского края строится на осуществлении политик более низкого уровня[485]:

- политики в отношении использования сетевых служб[486];
- политики обеспечения безопасности систем связи и информации, передаваемой по сетям общего пользования[487];
- политики обеспечения безопасности информации при беспроводных соединениях[488].

9.1.Политика в отношении использования сетевых служб

9.1.1. В Департаменте ЗАГС Забайкальского края установлен разрешительный режим доступа к сетевым службам[489].

---

[485] См.: аналогичный методический подход применительно к п. ИАФ.0, п. УПД.0, п. ОПС.0, п. ЗНИ.0, п. АУД.0, п. АВЗ.0, п. СОВ.0, п. ОЦЛ.0, п. ОДТ.0, п. ЗТС.0, п. ЗИС.0, п. ИНЦ.0, п. УКФ.0, п. ОПО.0, п. ПЛН.0, п. ДНС.0, п. ИПО.0 Приложения к Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСТЭК России от 25.12.2017 №239 (Зарегистрировано в Минюсте России 26.03.2018 №50524).

[486] См.: разд.9.1 настоящей Политики.

[487] См.: разд.9.2 настоящей Политики.

[488] См.: разд.9.3 настоящей Политики.

[489] См.:

- п.8 ч.2 ст.19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»»;
- п. «в» ст.13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.12 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608;
- разд.3.2 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);

9.1.2. В связи с тем, что несанкционированные подключения к сетевым службам могут нарушать информационную безопасность Департамента ЗАГС Забайкальского края, пользователям должен обеспечиваться непосредственный доступ только к тем сервисам, в которых они были авторизованы[490].

9.1.3. В целях контроля сетевого доступа должны определяться:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ;
- мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.

9.2. Политика обеспечения безопасности систем связи и информации, передаваемой по сетям общего пользования

Применяемая в Департаменте ЗАГС Забайкальского края политика защиты систем связи и передачи данных устанавливает требования к:

- управлению взаимодействием с информационными системами сторонних организаций (внешние информационные системы)[491];
- обеспечению защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой

- п.3.6 и п.3.15, п.5.1.3., п.5.2.7, п.5.3.6., п.5.4.., п.5.6.3 и п.6.3.14. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282»;
- разделом VII Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91;
- разделом VI Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

[490] Исполняется в соответствии с:

- п.16.3, п.18.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п.ОЦЛ.6 Приложения №2 к указанным Требованиям;
- п.5.1.3 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п. А.11.4.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.ОЦЛ.6 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п.ОЦЛ.6 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.8.1.4. Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100;
- разд. VII. Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

[491] См.: разд.9.2.1 настоящей Политики.

зоны, в том числе беспроводным каналам связи[492];

- управлению (фильтрации, маршрутизации, контролю соединений, однонаправленной передаче и иным способам управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами[493];
- реализации защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети[494];
- запрету несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств[495];
- контролю санкционированного и исключению несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи[496];
- контролю санкционированной и исключению несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации[497];
- обеспечению подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов[498];
- исключению возможности отрицания пользователем факта отправки информации другому пользователю[499];
- исключению возможности отрицания пользователем факта получения информации от другого пользователя[500];
- выявлению, анализу и блокированию в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов[501];
- прекращения сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения[502];
- обнаружению и реагированию на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)[503].

9.2.1. Управление взаимодействием с информационными системами

[492] См.: разд.9.2.2 настоящей Политики.
[493] См.: разд.9.2.3 настоящей Политики.
[494] См.: разд.9.2.4 настоящей Политики.
[495] См.: разд.9.2.5 настоящей Политики.
[496] См.: разд.9.2.6 настоящей Политики.
[497] См.: разд.9.2.7 настоящей Политики.
[498] См.: разд.9.2.8 настоящей Политики.
[499] См.: разд.9.2.9 настоящей Политики.
[500] См.: разд.9.2.10 настоящей Политики.
[501] См.: разд.9.2.11 настоящей Политики.
[502] См.: разд.9.2.12 настоящей Политики.
[503] См.: разд.9.2.13 настоящей Политики.

сторонних организаций (внешние информационные системы)

9.2.1.1. Должны выполняться следующие требования Регуляторов к реализации управлению взаимодействием с информационными системами сторонних организаций (внешними информационными системами):[504]

9.2.1.1.1. Оператором должно быть обеспечено управление взаимодействием с внешними информационными системами, включающими информационные системы и вычислительные ресурсы (мощности) уполномоченных лиц, информационные системы, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными информационными системами, информационное взаимодействие с которыми необходимо для функционирования информационной системы.

9.2.1.1.2. Управление взаимодействием с внешними информационными системами должно включать:

- предоставление доступа к информационной системе только авторизованным (уполномоченным) пользователям в соответствии с требованиями Регуляторов[505];
- определение типов прикладного программного обеспечения информационной системы, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;
- определение системных учетных записей, используемых в рамках данного взаимодействия;
- определение порядка предоставления доступа к информационной системе авторизованными (уполномоченным) пользователями из внешних информационных систем;
- определение порядка обработки, хранения и передачи информации с использованием внешних информационных систем.

9.2.1.1.3. Управление взаимодействием с внешними информационными системами в целях межведомственного электронного взаимодействия, исполнения государственных и муниципальных функций, формирования базовых государственных информационных ресурсов осуществляется в том числе с использованием единой системы идентификации и аутентификации, созданной в соответствии с постановлением Правительства Российской Федерации от 28.11.2011 № 977[506].

---

[504] См.: разд. «Требования к реализации УПД.16» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.44- л.45.

[505] См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.26- л.28.

[506] См.: Постановление Правительства РФ от 28.11.2011 №977 "О федеральной государственной

9.2.1.2. Правила и процедуры управления взаимодействием с внешними информационными системами регламентируются в организационно-распорядительных документах оператора по защите информации.

9.2.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению взаимодействием с информационными системами сторонних организаций (внешние информационные системы)[507]:

9.2.1.3.1. Оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий:

а) при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

б) при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

9.2.2. Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

9.2.2.1. Должны выполняться следующие требования Регуляторов к реализации обеспечения защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи:[508]

9.2.2.1.1. Оператором должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны.

9.2.2.1.2. Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации или иными методами.

9.2.2.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обеспечению защиты информации от раскрытия, модификации и навязывания (ввода ложной информации)

информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме" (с изменениями и дополнениями).

[507] См.: разд. «Требования к реализации УПД.16» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.44- л.45.

[508] См.: разд. «Требования к реализации ЗИС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.124.

при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи[509]:

9.2.2.2.1. Оператор обеспечивает защиту от модификации и навязывания (ввода ложной информации) видеоинформации (звуковой информации) путем ее маркирования и контроля (в том числе с использованием цифровых водяных знаков) в различных точках тракта ее формирования и распространения.

9.2.2.2.2. Оператор обеспечивает защиту от модификации и навязывания (ввода ложной информации) передаваемой видеоинформации путем выявления и удаления скрытых вставок.

9.2.3. Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами

9.2.3.1. Должны выполняться следующие требования Регуляторов к реализации управления (фильтрации, маршрутизации, контроля соединений, однонаправленной передачи и иных способов управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами:[510]

9.2.3.1.1. В информационной системе должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

- фильтрацию информационных потоков в соответствии с правилами управления потоками, установленными оператором; разрешение передачи информации в информационной системе только по маршруту, установленному оператором; изменение (перенаправление) маршрута передачи информации в случаях, установленных оператором;
- запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных оператором.

9.2.3.1.2. Управление информационными потоками должно обеспечивать разрешенный (установленный оператором) маршрут прохождения информации между пользователями, устройствами, сегментами в рамках информационной системы, а также между информационными системами или при взаимодействии с сетью Интернет(или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой

[509] См.: разд. «Требования к реализации ЗИС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.124.

[510] См.: разд. «Требования к реализации УПД.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.28-л.30.

информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации).

9.2.3.1.3. Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из информационной системы и (или) входящие в информационную систему.

9.2.3.2. Правила и процедуры управления информационными потоками регламентируются в организационно-распорядительных документах оператора по защите информации.

9.2.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по управлению (фильтрации, маршрутизации, контролю соединений, однонаправленной передаче и иным способам управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами[511]:

9.2.3.3.1. В информационной системе должно обеспечиваться управление информационными потоками на основе атрибутов (меток) безопасности, связанных с передаваемой информацией, источниками и получателями информации.

9.2.3.3.2. В информационной системе должно обеспечиваться динамическое управление информационными потоками, запрещающее и (или) разрешающее передачу информации на основе анализа изменения текущего состояния информационной системы или условий ее функционирования.

9.2.3.3.3. В информационной системе должен исключаться обход правил управления информационными потоками за счет преобразования передаваемой информации.

9.2.3.3.4. В информационной системе должен исключаться обход правил управления информационными потоками за счет встраивания одних данных в другие данные информационного потока.

9.2.3.3.5. В информационной системе должен обеспечиваться контроль соединений между техническими средствами (устройствами), используемыми для организации информационных потоков.

9.2.3.3.6. В информационной системе при передаче информации между сегментами информационной системы и (или) информационными системами разных классов защищенности должна обеспечиваться однонаправленная передача информации с использованием аппаратных средств.

9.2.3.3.7. В информационной системе должно обеспечиваться управление информационными потоками на основе структуры передаваемых данных (текст, таблицы, видео, аудиоинформация);

9.2.3.3.8. В информационной системе должно обеспечиваться управление информационными потоками на основе используемых сетевых протоколов.

9.2.3.3.9. В информационной системе должно обеспечиваться

[511] См.: разд. «Требования к реализации УПД.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.29-л.30.

управление информационными потоками на основе типов (расширений) файлов и (или) имен файлов.

9.2.3.3.10. В информационной системе должна обеспечиваться возможность запрета, разрешения и изменения маршрута передачи информации только администраторами.

9.2.3.3.11. В информационной системе должно обеспечиваться разделение информационных потоков, содержащих различные виды (категории) информации, а также отделение информации управления от пользовательской информации.

9.2.3.3.12. В информационной системе должна обеспечиваться возможность автоматического блокирования передачи информации при выявлении в передаваемой информации вредоносных компьютерных программ.

9.2.3.3.13. В информационной системе должно осуществляться управление информационными потоками при передаче информации между информационными системами.

9.2.3.3.14. В информационной системе должна обеспечиваться возможность фильтрации информационных потоков на уровне прикладного программного обеспечения (приложений).

9.2.3.3.15. В информационной системе должна осуществляться накопление статистических данных, проверка и фильтрация сетевых пакетов по их содержимому (технология DPI).

9.2.3.3.16. Наделение трафика конкретными параметрами (в частности включение уведомлений пользователей, исключение или замена элементов трафика) в зависимости от получателя информации.

9.2.4. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети

9.2.4.1. Должны выполняться следующие требования Регуляторов к реализации защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети:[512]

9.2.4.1.1. Оператором должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств (защита удаленного доступа).

9.2.4.1.2. Защита удаленного доступа должна обеспечиваться при всех видах доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа) и включает:

- установление (в том числе документальное) видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы;
- ограничение на использование удаленного доступа в соответствии с задачами (функциями) информационной

[512] См.: разд. «Требования к реализации УПД.13» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.39-л.40.

системы, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с требованиями Регуляторов[513];

- предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа информационной системы;
- контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой (передачи защищаемой информации).

9.2.4.2. Правила и процедуры применения удаленного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

9.2.4.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по реализации защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети[514]:

9.2.4.1.3. В информационной системе для мониторинга и контроля удаленного доступа должны применяться автоматизированные средства (дополнительные программные или программно-технические средства).

9.2.4.1.4. В информационной системе используется ограниченное (минимально необходимое) количество точек подключения к информационной системе при организации удаленного доступа к объектам доступа информационной системы.

9.2.4.1.5. В информационной системе исключается удаленный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации.

9.2.4.1.6. В информационной системе при удаленном доступе обеспечивается применение в соответствии с законодательством Российской Федерации криптографических методов защиты информации.

9.2.4.1.7. В информационной системе обеспечивается мониторинг и контроль удаленного доступа на предмет выявления установления

---

[513] См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.27- л.28.

[514] См.: разд. «Требования к реализации УПД.13» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.40.

несанкционированного соединения технических средств (устройств) с информационной системой.

9.2.4.1.8. В информационной системе должен обеспечиваться запрет удаленного доступа с использованием сетевых технологий и протоколов, определенных оператором по результатам анализа защищенности в соответствии с требованиями Регуляторов[515] как небезопасных.

9.2.5. Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств

9.2.5.1. Должны выполняться следующие требования Регуляторов к реализации запрета несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств:[516]

9.2.5.1.1. В информационной системе должны осуществляться запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств, в том числе путем сигнализации, индикации.

9.2.5.1.2. Запрет несанкционированной удаленной активации должен осуществляться в отношении всех периферийных устройств ввода (вывода) информации, которые имеют возможность управления (запуска, включения, выключения) через компоненты программного обеспечение, установленные на рабочем месте пользователя, коммуникационных сервисов сторонних лиц (провайдеров) (ICQ, Skype и иные сервисы).

9.2.5.1.3. Запрет несанкционированной удаленной активации должен осуществляться через физическое исключение такой возможности и (или) путем управления программным обеспечением.

9.2.5.1.4. В исключительных случаях для решения установленных оператором отдельных задач, решаемых информационной системой, допускается возможность удаленной активации периферийных устройств.

9.2.5.1.5. При этом должно быть обеспечено определение и фиксирование в организационно-распорядительных документах по защите информации (документирование) перечня периферийных устройств, для которых допускается возможность удаленной активации и обеспечен контроль за активацией таких

---

[515] См.:

- АН3.1 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации АН3.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.78-л.80.

[516] См.: разд. «Требования к реализации ЗИС.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.125-л.126.

устройств.

9.2.5.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по запрету несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещению пользователей об активации таких устройств[517]:

9.2.5.2.1. В информационной системе должна обеспечиваться возможность физического отключения периферийных устройств (например, отключение при организации и проведении совещаний в помещениях, где размещены видеокамеры и микрофоны).

9.2.5.2.2. В информационной системе должна обеспечиваться возможность блокирования входящего и исходящего трафика от пользователей систем, предоставляющих внешние сервисы (например, системы видеоконференцсвязи), в которых конфигурации (настройки) сервисов для конечных пользователей устанавливаются провайдерами или самими пользователями.

9.2.5.2.3. Оператором обеспечивается удаление (отключение) из информационной системы (отдельных сегментов, например, расположенных в защищаемых и выделенных помещениях) периферийных устройств, перечень которых определяется оператором.

9.2.5.2.4. Оператором обеспечивается запись и хранение в течение установленного времени информации, переданной (полученной) периферийными устройствами ввода (вывода) информации при разрешенной удаленной активации периферийных устройств ввода (вывода) информации.

9.2.6. Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи[518]

9.2.6.1. Должны выполняться следующие требования Регуляторов к реализации контроля санкционированного и исключению несанкционированного использования технологий передачи речи, в том числе регистрации событий, связанных с использованием

---

[517] См.: разд. «Требования к реализации ЗИС.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.125-л.126.

[518] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.8 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.8 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.8 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

технологий передачи речи, их анализу и реагированию на нарушения, связанные с использованием технологий передачи речи:[519]

9.2.6.1.1. Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи речи в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи.

9.2.6.1.2. При контроле использования технологий передачи речи должно быть обеспечено:

- определение перечня технологий (сервисов) передачи речи разрешенных и (или) запрещенных для использования в информационной системе;
- определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи речи в соответствии с установленными ролями;
- реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи речи;
- регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи речи;
- исключение возможности использования запрещенной технологии передачи речи в информационной системе, а также разработки, приобретения и внедрения технологий передачи речи субъектам доступа (пользователям), которым не разрешено ее использование.

9.2.6.1.3. Технология передачи речи включает, в том числе, передачу речи через Интернет (в частности VoIP).

9.2.6.2. Правила и процедуры контроля использования технологий передачи речи регламентируются в организационно-распорядительных документах оператора по защите информации.

9.2.7. Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации[520]

---

[519] См.: разд. «Требования к реализации ЗИС.8» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.128-л.129.

[520] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.9 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.9 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.9 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

9.2.7.1. Должны выполняться следующие требования Регуляторов к реализации контроля санкционированной и исключения несанкционированной передачи видеоинформации, в том числе регистрации событий, связанных с передачей видеоинформации, их анализа и реагирования на нарушения, связанные с передачей видеоинформации:[521]

9.2.7.1.1. Оператором должны осуществляться контроль санкционированного и исключение несанкционированного использования технологий передачи видеоинформации в информационной системе, в том числе регистрация событий, связанных с использованием технологий передачи видеоинформации, их анализ и реагирование на нарушения, связанные с использованием технологий передачи видеоинформации.

9.2.7.1.2. При контроле использования технологий передачи видеоинформации должно быть обеспечено:

- определение перечня технологий (сервисов) передачи видеоинформации разрешенных и (или) запрещенных для использования в информационной системе;
- определение субъектов доступа (категорий пользователей), которым разрешены разработка, приобретение или внедрение технологий передачи видеоинформации в соответствии с установленными ролями;
- реализация параметров настройки, исключающих возможность удаленной конфигурации устройств передачи видеоинформации;
- регистрация и анализ событий, связанных с разработкой, приобретением и внедрением технологий передачи видеоинформации;
- исключение возможности использования запрещенной технологии передачи видеоинформации в информационной системе, а также разработки, приобретения и внедрения технологий передачи видеоинформации субъектов доступа (пользователям), которым не разрешено ее использование.

9.2.7.1.3. Технология передачи видеоинформации включает, в том числе, применение технологий видеоконференцсвязи.

9.2.7.2. Правила и процедуры контроля передачи видеоинформации регламентируются в организационно-распорядительных документах оператора по защите информации.

9.2.7.3. Требования к усилению мероприятий по контролю санкционированной и исключению несанкционированной передачи видеоинформации, в том числе регистрации событий, связанных с передачей видеоинформации, их анализу и реагированию на нарушения, связанные с передачей видеоинформации Регуляторами не установлены[522].

---

[521] См.: разд. «Требования к реализации ЗИС.9» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.129-л.130.

[522] См.: разд. «Требования к реализации ЗИС.9» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.130.

9.2.8. Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов[523]

9.2.8.1. Должны выполняться следующие требования Регуляторов к реализации обеспечения подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов:[524]

9.2.8.1.1. В информационной системе должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»).

9.2.8.1.2. Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация в соответствии с требованиями Регуляторов[525].

9.2.8.1.3. Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов (в соответствии с требованиями Регуляторов[526]).

9.2.8.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обеспечению подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов[527]:

---

[523] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.11 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.11 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.11 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[524] См.: разд. «Требования к реализации ЗИС.11» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.131-л.132.

[525] См.:

- ИАФ.2 и ЗИС.10 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.2» и разд. «Требования к реализации ЗИС.10» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.18, л.130-л.131.

[526] См.:

- ЗИС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ЗИС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.124.

[527] См.: разд. «Требования к реализации ЗИС.11» методического документа «Меры защиты информации в

9.2.8.2.1. В информационной системе должно обеспечиваться признание идентификатора сеанса связи недействительным после окончания сетевого соединения.

9.2.8.2.2. В информационной системе должна осуществляться регистрация установления и разрыва сетевых соединений (сеансов взаимодействия) в целях выявления возможных инцидентов (событий безопасности).

9.2.8.2.3. В информационной системе должна осуществляться генерация и присвоение уникальных идентификаторов (одноразовых) для каждого сетевого соединения (сеанса взаимодействия) и контроль их подлинности (восприниматься должны только идентификаторы, сгенерированные информационной системой).

9.2.8.2.4. В информационной системе должно обеспечиваться обнаружение попыток повторного использования идентификаторов сетевых соединений и реагирование на эти попытки.

9.2.8.2.5. В информационной системе должна осуществляться защита от подбора идентификаторов, присваиваемых будущим сетевым соединениям (сеансам взаимодействия).

9.2.9. Исключение возможности отрицания пользователем факта отправки информации другому пользователю[528]

9.2.9.1. Должны выполняться следующие требования Регуляторов к реализации исключения возможности отрицания пользователем факта отправки информации другому пользователю[529]:

9.2.9.1.1. Оператором должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю.

9.2.9.1.2. Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться:

- определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки (например, сообщения электронной почты);
- обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи в

государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.131-л.132.

[528] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.12 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.12 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.12 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[529] См.: разд. «Требования к реализации ЗИС.12» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.132-л.133.

соответствии с требованиями Регуляторов[530];

- регистрация событий, связанных с отправкой информации другому пользователю в соответствии с требованиями Регуляторов[531].

9.2.9.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по исключению возможности отрицания пользователем факта отправки информации другому пользователю[532]:

9.2.9.2.1. В информационной системе должна обеспечиваться генерация свидетельства отправления информации (например, электронной подписи).

9.2.9.2.2. В информационной системе должна обеспечиваться связь атрибутов отправителя информации в соответствии с учетом требований Регуляторов[533] с полями отправляемой информации (текстом сообщения).

9.2.9.2.3. В информационной системе должна быть обеспечена возможность верификации (проверки) свидетельства отправления информации.

9.2.9.2.4. В информационной системе должна быть обеспечена возможность записи и защищенного хранения в течение установленного оператором времени информации, отправленной пользователем другому пользователю.

9.2.10. Исключение возможности отрицания пользователем факта получения информации от другого пользователя

9.2.10.1. Должны выполняться следующие требования Регуляторов к реализации исключения возможности отрицания пользователем факта

---

[530] См.:

- ЗИС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ЗИС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.124.

[531] См.:

- РСБ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации РСБ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.63-л.65.

[532] См.: разд. «Требования к реализации ЗИС.12» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.132-л.133.

[533] См.:

- ИАФ.1 и ИАФ.6 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1» и разд. «Требования к реализации ИАФ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675,л.16-л.17, л.23.

получения информации от другого пользователя:[534]

9.2.10.1.1. Оператором должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя.

9.2.10.1.2. Для исключения возможности отрицания пользователем факта получения информации должны осуществляться:

- определение объектов или типов информации, для которых требуется обеспечение неотказуемости получения (сообщения электронной почты);
- обеспечение целостности полученной информации в соответствии с требованиями Регуляторов[535];
- регистрация событий, связанных с получением информации от другого пользователя в соответствии с требованиями Регуляторов[536].

9.2.10.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по исключению возможности отрицания пользователем факта получения информации от другого пользователя[537]:

9.2.10.2.1. В информационной системе должна обеспечиваться генерация свидетельства получения информации (запрос подтверждения получения или электронная подпись).

9.2.10.2.2. В информационной системе должна быть обеспечена связь атрибутов получателя информации в соответствии с требованиями Регуляторов[538] с полями отправляемой информации (текстом сообщения).

---

[534] См.: разд. «Требования к реализации ЗИС.13» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.133.

[535] См.:

- ЗИС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ЗИС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.124.

[536] См.:

- РСБ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации РСБ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.63-л.65.

[537] См.: разд. «Требования к реализации ЗИС.13» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.133.

[538] См.:

- ИАФ.1 и ИАФ.6 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1» и разд. «Требования к реализации ИАФ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675,л.16-л.17, л.23.

9.2.10.2.3. В информационной системе должна быть обеспечена возможность верификации (проверки) свидетельства получения информации.

9.2.10.2.4. В информационной системе должна быть обеспечена возможность записи и защищенного хранения в течение установленного оператором времени информации, полученной пользователем от другого пользователя.

9.2.11. Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов

9.2.11.1. Должны выполняться следующие требования Регуляторов к реализации выявления, анализа и блокирования в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов:[539]

9.2.11.1.1. Оператором должны выполняться мероприятия по выявлению и анализу скрытых каналов передачи информации для определения параметров передачи информации, которые могут использоваться для скрытого хранения информации и скрытой передачи информации за пределы информационной системы.

9.2.11.1.2. Выявление, анализ и блокирование скрытых каналов передачи информации выполняется с учетом национальных стандартов:

- ГОСТ Р 53113-2008 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения;
- ГОСТ Р 53113.2-2009 Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов.

9.2.11.1.3. Выявление и анализ скрытых каналов передачи информации осуществляется на этапах разработки и реализации системы защиты информации.

9.2.11.2. Требования к усилению мероприятий по выявлению, анализу и блокированию в информационной системе скрытых каналов передачи информации в обход реализованных мер защиты информации или внутри разрешенных сетевых протоколов Регуляторами не установлены[540].

9.2.12. Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого

[539] См.: разд. «Требования к реализации ЗИС.16» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.136.

[540] См.: разд. «Требования к реализации ЗИС.16» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.136.

соединения[541]

9.2.12.1. Должны выполняться следующие требования Регуляторов к реализации прекращения сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения[542]:

9.2.12.1.1. В информационной системе должно осуществляться завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения.

9.2.12.2. Требования к усилению мероприятий по прекращению сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения Регуляторами не установлены.[543]

9.2.13. Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)[544]

9.2.13.1. Должны выполняться следующие требования Регуляторов к реализации обнаружения и реагирования на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к

---

[541] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:
- ЗИС.24 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.24 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.24 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[542] См.: разд. «Требования к реализации ЗИС.24» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.145.

[543] См.: разд. «Требования к реализации ЗИС.24» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.145.

[544] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:
- ОЦЛ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ОЦЛ.4 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
  ОЦЛ.4 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

функционированию информационной системы (защита от спама)[545]:

9.2.13.1.1. Оператором должно обеспечиваться обнаружение и реагирование на поступление незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама).

9.2.13.1.2. Защита от спама реализуется на точках входа в информационную систему (выхода) информационных потоков (межсетевые экраны, почтовые серверы, Web-серверы, прокси-серверы и серверы удаленного доступа), а также на автоматизированных рабочих местах, серверах и (или) мобильных технических средствах, подключенных к сетям связи общего пользования, для обнаружения и реагирования на поступление по электронной почте незапрашиваемых электронных сообщений (писем, документов) или в приложениях к электронным письмам.

9.2.13.1.3. Защита от спама обеспечивается применением специализированных средств защиты, реализующих следующие механизмы защиты:

- фильтрация по содержимому электронных сообщений (писем, документов) с использованием критериев, позволяющих относить сообщения к спаму сигнатурным и (или) эвристическим методами;
- фильтрация на основе информации об отправителе электронного сообщения (в том числе с использованием «черных» списков (запрещенные отправители) и (или) «белых» списков (разрешенные отправители).

9.2.13.1.4. Оператором должно осуществляться обновление базы «черных» («белых») списков и контроль целостности базы «черных» («белых») списков.

9.2.13.2. Правила и процедуры обнаружения и реагирования на поступление незапрашиваемой информации регламентируются в организационно-распорядительных документах оператора по защите информации.

9.2.13.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по обнаружению и реагированию на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)[546]:

9.2.13.3.1. Оператором обеспечивается централизованное управление средствами защиты от спама.

9.2.13.3.2. В информационной системе должна обеспечиваться фильтрация на основе информации об отправителе электронного сообщения с использованием эвристических методов (например, «серые» списки серверов электронной почты, распознавание автоматически генерируемых имен отправителей и другие).

---

[545] См.: разд. «Требования к реализации ОЦЛ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.90-л.91.

[546] См.: разд. «Требования к реализации ОЦЛ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.90-л.91.

9.2.13.3.3. В информационной системе должна обеспечиваться аутентификация отправителей электронных сообщений в соответствии с требованиями Регуляторов[547].

9.2.13.3.4. В информационной системе должна обеспечиваться аутентификация серверов электронной почты (в том числе в соответствии с требованиями Регуляторов[548]).

9.2.13.3.5. В информационной системе должен обеспечиваться контроль поступления в информационную систему информационных сообщений и документов на основе контентного анализа.

9.3.Политика обеспечения безопасности информации при беспроводных соединениях

Применяемая в Департаменте ЗАГС Забайкальского края политика обеспечения безопасности информации при беспроводных соединениях устанавливает требования к:

- регламентации и контролю использования в информационной системе технологий беспроводного доступа;
- регламентации и контролю использования в информационной системе мобильных технических средств;
- контролю санкционированного и исключению несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода;
- защите беспроводных соединений, применяемых в информационной системе;
- защите мобильных технических средств, применяемых в информационной системе.

9.3.1. Регламентация и контроль использования в информационной системе технологий беспроводного доступа

9.3.1.1. Должны выполняться следующие требования Регуляторов к реализации регламентации и контролю использования в информационной системе технологий беспроводного доступа:[549]

---

[547] См.:

- ИАФ.1, ИАФ.6, ИАФ.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1», разд. «Требования к реализации ИАФ.6» и разд. «Требования к реализации ИАФ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.16-л.17, л.23-л.24.

[548] См.:

- ИАФ.2, ИАФ.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.2» и разд. «Требования к реализации ИАФ.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.16-л.17л.24.

[549] См.: разд. «Требования к реализации УПД.14» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014),

9.3.1.1.1. Оператором должны обеспечиваться регламентация и контроль использования в информационной системе технологий беспроводного доступа пользователей к объектам доступа (стандарты коротковолновой радиосвязи, спутниковой и пакетной радиосвязи), направленные на защиту информации в информационной системе.

9.3.1.1.2. Регламентация и контроль использования технологий беспроводного доступа должны включать:

- ограничение на использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) информационной системы, для решения которых такой доступ необходим, и предоставление беспроводного доступа в соответствии с требованиями Регуляторов[550];
- предоставление технологий беспроводного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- мониторинг и контроль применения технологий беспроводного доступа на предмет выявления несанкционированного использования технологий беспроводного доступа к объектам доступа информационной системы;
- контроль беспроводного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа информационной системы до начала информационного взаимодействия с информационной системой.

9.3.1.2. Правила и процедуры применения технологий беспроводного доступа регламентируются в организационно-распорядительных документах оператора по защите информации.

9.3.1.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по регламентации и контролю использования в информационной системе технологий беспроводного доступа[551]:

9.3.1.3.1. В информационной системе обеспечивается аутентификация подключаемых с использованием технологий беспроводного доступа устройств в соответствии с требованиями Регуляторов[552].

---

https://fstec.ru/component/attachments/download/675 л.40-л.41.

[550] См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.26-л.28.

[551] См.: разд. «Требования к реализации УПД.14» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.40-л.41.

[552] См.:

- ИАФ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом

9.3.1.3.2. В информационной системе обеспечивается мониторинг точек беспроводного подключения устройств к информационной системе на предмет выявления несанкционированного беспроводного подключения устройств.

9.3.1.3.3. В информационной системе исключается возможность изменения пользователем точек беспроводного доступа информационной системы.

9.3.1.3.4. Оператором одолжен быть предусмотрен запрет беспроводного доступа к информационной системе из-за пределов контролируемой зоны.

9.3.1.3.5. В информационной системе должен быть запрещен беспроводный доступ от имени привилегированных учетных записей (администраторов) для администрирования информационной системы и ее системы защиты информации.

9.3.1.3.6. В информационной системе исключается возможность изменения пользователем устройств и настроек беспроводного доступа.

9.3.1.3.7. Оператором обеспечивается определение местонахождения несанкционированного беспроводного устройства.

9.3.1.3.8. Оператором обеспечивается блокирование функционирования несанкционированного беспроводного устройства.

9.3.2. Регламентация и контроль использования в информационной системе мобильных технических средств

9.3.2.1. Должны выполняться следующие требования Регуляторов к реализации регламентации и контроля использования в информационной системе мобильных технических средств:[553]

9.3.2.1.1. Оператором должны обеспечиваться регламентация и контроль использования в информационной системе мобильных технических средств, направленные на защиту информации в информационной системе.

9.3.2.1.2. В качестве мобильных технических средств рассматриваются съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства), портативные вычислительные устройства и устройства связи с возможностью обработки информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные устройства).

9.3.2.1.3. Регламентация и контроль использования мобильных технических средств должны включать:

- установление (в том числе документальное) видов доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа информационной системы с

ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

- разд. «Требования к реализации ИАФ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.16-л.17.

[553] См.: разд. «Требования к реализации УПД.15» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.42-л.43.

использованием мобильных технических средств, входящих в состав информационной системы;

- использование в составе информационной системы для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации в соответствии с требованиями Регуляторов[554];
- ограничение на использование мобильных технических средств в соответствии с задачами (функциями) информационной системы, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств в соответствии с требованиями Регуляторов[555];
- мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы;
- запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством.

9.3.2.2. Правила и процедуры применения мобильных технических средств, включая процедуры выдачи и возврата мобильных технических средств, а также их передачи на техническое обслуживание (процедура должна обеспечивать удаление или недоступность информации), регламентируются в организационно-распорядительных документах оператора по защите информации.

9.3.2.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по регламентации и контролю использования в информационной системе мобильных технических средств[556]:

9.3.2.3.1. Оператором обеспечивается запрет использования в информационной системе, не входящих в ее состав (находящихся в личном использовании) съемных машинных носителей информации.

---

[554] См.:

- ЗИС.30 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ЗИС.30» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.151-л.152.

[555] См.:

- УПД.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.26-л.28.

[556] См.: разд. «Требования к реализации УПД.15» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.43.

9.3.2.3.2. Оператором обеспечивается запрет использования в информационной системе съемных машинных носителей информации, для которых не определен владелец (пользователь, организация, ответственные за принятие мер защиты информации).

9.3.2.3.3. Оператором обеспечивается (в соответствии с процедурами, зафиксированными в организационно-распорядительных документах) очистка машинного носителя информации мобильного технического средства, переустановка программного обеспечения и выполнение иных мер по защите информации мобильных технических средств, после их использования за пределами контролируемой зоны.

9.3.2.3.4. Оператором обеспечивается предоставление доступа с использованием мобильных технических средств к объектам доступа информационной системы только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций).

9.3.2.3.5. В информационной системе обеспечивается запрет использования мобильных технических средств, на которые в информационной системе может быть осуществлена запись информации (перезаписываемых съемных машинных носителей информации).

9.3.3. Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода[557]

9.3.3.1. Должны выполняться следующие требования Регуляторов к реализации контроля санкционированного и исключения несанкционированного использования технологий мобильного кода, в том числе регистрации событий, связанных с использованием технологий мобильного кода, их анализа и реагирования на нарушения, связанные с использованием технологий мобильного кода:[558]

9.3.3.1.1. Оператором должны осуществляться контроль санкционированного и исключение несанкционированного

[557] Исполняется только для 1 и 2 классов защищенности информационной системы. См.:

- ЗИС.7 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗИС.7 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗИС.7 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[558] См.: разд. «Требования к реализации ЗИС.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.127-л.128.

использования технологий мобильного кода (активного контента) в информационной системе, в том числе регистрация событий, связанных с использованием технологии мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологии мобильного кода.

9.3.3.1.2. Технология мобильного кода включает, в том числе использование Java, JavaScript, ActiveX, PDF, Postscript, Flash-анимация и VBScript и иных технологий.

9.3.3.1.3. При контроле использования технологий мобильного кода должно быть обеспечено:

- определение перечня мобильного кода и технологий мобильного кода разрешенных и (или) запрещенных для использования в информационной системе;
- определение разрешенных мест распространения (серверы информационной системы) и использования мобильного кода (автоматизированные рабочие места, мобильные технические средства информационной системы) и функций информационной системы, для которых необходимо применение технологии мобильного кода;
- регистрация и анализ событий, связанных с разработкой, приобретением или внедрением технологии мобильного кода;
- исключение возможности использования запрещенного мобильного кода в информационной системе, а также внедрение мобильного кода в местах, не разрешенных для его установки.

9.3.3.2. Правила и процедуры контроля использования технологий мобильного кода регламентируются в организационно-распорядительных документах оператора по защите информации.

9.3.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю санкционированного и исключению несанкционированного использования технологий мобильного кода, в том числе регистрации событий, связанных с использованием технологий мобильного кода, их анализу и реагированию на нарушения, связанные с использованием технологий мобильного кода[559]:

9.3.3.3.1. В информационной системе должны быть реализованы механизмы обнаружения и анализа мобильного кода для выявления фактов несанкционированного использования мобильного кода и выполнения действий по реагированию (оповещение администраторов, изоляция мобильного кода (перемещение в карантин), блокирование мобильного кода, удаление мобильного кода) и иные действия, определяемые оператором.

9.3.3.3.2. В информационной системе должен осуществляться запрет загрузки и выполнения запрещенного мобильного кода.

В информационной системе для приложений, определяемых оператором, должен осуществляться запрет автоматического выполнения разрешенного мобильного кода (уведомление

[559] См.: разд. «Требования к реализации ЗИС.7» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.127-л.128.

пользователя о получении мобильного кода и запрос разрешения на запуск или иные действия, определяемые оператором).

В информационной системе должен осуществляться контроль подлинности источника мобильного кода и контроль целостности мобильного кода.

9.3.4. Защита беспроводных соединений, применяемых в информационной системе

9.3.4.1. Должны выполняться следующие требования Регуляторов к реализации защиты беспроводных соединений, применяемых в информационной системе:[560]

9.3.4.1.1. Оператором должна быть обеспечена защита беспроводных соединений, применяемых в информационной системе.

9.3.4.1.2. Защита беспроводных соединений включает:

- ограничение на использование в информационной системе беспроводных соединений (в частности, 802.11xWi-Fi, 802.15.1 Bluetooth, 802.22WRAN, IrDA и иных беспроводных соединений) в соответствии с задачами (функциями) информационной системы, для решения которых такие соединения необходимы;
- предоставление доступа к параметрам (изменению параметров) настройки беспроводных соединений только администраторам информационной системы;
- обеспечение возможности реализации беспроводных соединений только через контролируемые интерфейсы (в том числе, путем применения средств защиты информации);
- регистрация и анализ событий, связанных с использованием беспроводных соединений, в том числе для выявления попыток несанкционированного подключения к информационной системе через беспроводные соединения.

9.3.4.1.3. При обеспечении защиты беспроводных соединений в зависимости от их типов должны реализовываться меры по идентификации и аутентификации в соответствии с требованиями Регуляторов[561].

9.3.4.1.4. При невозможности исключения установления беспроводных соединений из-за пределов контролируемой зоны должны приниматься меры защищенного удаленного доступа в соответствии с требованиями Регуляторов[562].

---

[560] См.: разд. «Требования к реализации ЗИС.20» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.139-л.140.

[561] См.:

- ИАФ.1, ИАФ.2 и ИАФ.6 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1», разд. «Требования к реализации ИАФ.2» и разд. «Требования к реализации ИАФ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675,л.16-л.18, л.23.

[562] См.:

- УПД.13 и ЗИС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных

9.3.4.2. Правила и процедуры применения беспроводных соединений регламентируются в организационно-распорядительных документах оператора по защите информации.

9.3.4.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по защите беспроводных соединений, применяемых в информационной системе:

9.3.4.3.1. Оператором для защиты беспроводных соединений в соответствии с законодательством Российской Федерации должны применяться средства криптографической защиты информации.

9.3.4.3.2. В информационной системе должны применяться программно-технические средства обнаружения, анализа и блокирования несанкционированного использования беспроводных технологий и подключений к информационной системе.

9.3.4.3.3. Оператором должно обеспечиваться блокирование несанкционированных беспроводных подключений к информационной системе.

9.3.4.3.4. Оператором должна быть исключена возможность установления беспроводных соединений из-за пределов контролируемой зоны.

9.3.5. Защита мобильных технических средств, применяемых в информационной системе

9.3.5.1. Должны выполняться следующие требования Регуляторов к реализации защиты мобильных технических средств, применяемых в информационной системе:[563]

9.3.5.1.1. Оператором должна осуществляться защита применяемых в информационной системе мобильных технических средств.

9.3.5.1.2. К мобильным техническим средствам относятся съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные носители), а также портативные вычислительные устройства и устройства связи с возможностью обработки информации (например, ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные средства).

9.3.5.1.3. Защита мобильных технических средств включает:

– реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по идентификации и аутентификации в соответствии с требованиями Регуляторов[564], управлению доступом в

приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

– разд. «Требования к реализации УПД.13» и разд. «Требования к реализации ЗИС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.39-л.40, л.124.

563 См.: разд. «Требования к реализации ЗИС.30» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.151-л.152.

564 См.:

– ИАФ.1 и ИАФ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

соответствии с требованиями Регуляторов[565], ограничению программной среды в соответствии с требованиями Регуляторов[566], защите машинных носителей информации в соответствии с требованиями Регуляторов[567], регистрации событий безопасности в соответствии с требованиями Регуляторов[568], антивирусной защите в соответствии с требованиями Регуляторов[569], контролю (анализу) защищенности в соответствии с требованиями Регуляторов[570],

---

– разд. «Требования к реализации ИАФ.1» и разд. «Требования к реализации ИАФ.1» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.16 и л.22.

[565] См.:
– УПД.2, УПД.5, УПД.13 и УПД.15 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации УПД.2», разд. «Требования к реализации УПД.5», разд. «Требования к реализации УПД.13» и разд. «Требования к реализации УПД.15» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.26- л.28, л.31-л.32, л.39-л.40, и л.42-л.43.

[566] См.:
– ОПС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации ОПС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.50.

[567] См.:
– ЗНИ.1, ЗНИ.2, ЗНИ.4, ЗНИ.8 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации ЗНИ.1», разд. «Требования к реализации ЗНИ.2», разд. «Требования к реализации ЗНИ.4» и разд. «Требования к реализации ЗНИ.8» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.52- л.54, л.55-56, л.59-л.60.

[568] См.:
– РСБ.1, РСБ.2, РСБ.3 и РСБ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации РСБ.1», разд. «Требования к реализации РСБ.2», разд. «Требования к реализации РСБ.3» и разд. «Требования к реализации РСБ.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.62- л.67, л.68-69.

[569] См.:
– АВЗ.1 и АВЗ.2 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– разд. «Требования к реализации АВЗ.1» и разд. «Требования к реализации АВЗ.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.72- л.74.

[570] См.:
– АНЗ.1, АНЗ.2 и АНЗ.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных

обеспечению целостности в соответствии с требованиями Регуляторов[571] очистку (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации;

- уничтожение съемных машинных носителей информации, которые не подлежат очистке;
- выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации);
- запрет возможности автоматического запуска (без команды пользователя) в информационной системе программного обеспечения на мобильных технических средствах.

9.3.5.2. Правила и процедуры защиты мобильных технических средств регламентируются в организационно-распорядительных документах оператора по защите информации.

9.3.5.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по защите мобильных технических средств, применяемых в информационной системе[572]:

9.3.5.3.1. Оператором должны применяться средства ограничения доступа к информации на съемных машинных носителях информации с использованием специализированных съемных машинных носителей информации и средств контроля съемных машинных носителей информации с учетом требований Регуляторов[573].

9.3.5.3.2. Оператором должна обеспечиваться очистка (удаление) информации в мобильном техническом средстве:

приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);

- разд. «Требования к реализации АНЗ.1», разд. «Требования к реализации АНЗ.2» и разд. «Требования к реализации АНЗ.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.78- л.82.

[571] См.:

- ОЦЛ.1. Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ОЦЛ.1.» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.86- л.87.

[572] См.: разд. «Требования к реализации ЗИС.30» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.152.

[573] См.:

- ЗНИ.4 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ЗНИ.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675 л.55-56.

а) при превышении допустимого числа неуспешных попыток входа в информационную систему под конкретной учетной записью (доступа к информационной системе), осуществляемых с мобильного устройства;

б) при превышении допустимого интервала времени с начала осуществления попыток входа в информационную систему под конкретной учетной записью, осуществляемых с мобильного устройства.

9.3.5.3.3. Оператором должно обеспечиваться применение технических средств защиты периметра уровня узла, устанавливаемых на портативные вычислительные устройства.

9.3.5.3.4. Оператором должно обеспечиваться использование радиометок (RFID меток) для контроля вноса или выноса мобильных технических устройств из помещения и (или) контролируемой зоны в целом.

9.3.5.3.5. Оператором обеспечивается шифрование хранимой на носителе мобильного технического средства информации с применением криптографических методов защиты информации в соответствии с законодательством Российской Федерации.

X. Политика обеспечения физической безопасности технических средств, систем и информации в Департаменте ЗАГС Забайкальского края [574]

Политика обеспечения физической безопасности технических средств, систем и информации в Департаменте ЗАГС Забайкальского края строится на осуществлении политик более низкого уровня:

- политики защиты технических средств Департаменте ЗАГС Забайкальского края
- политики обеспечения безопасности документов и носителей информации Департамента ЗАГС Забайкальского края.

10.1. Политика защиты технических средств Департаменте ЗАГС Забайкальского края

Применяемая в Департаменте ЗАГС Забайкальского края политика защиты технических средств устанавливает требования к проведению мероприятий, касающихся как внешних[575], так и внутренних[576] аспектов. К мероприятиям по обеспечению физической защиты технических средств информационных систем от внешних факторов относятся:

- организации контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования[577];
- защите от внешних воздействий (воздействий окружающей среды,

[574] См.:
- п.8 Приложения А ГОСТ Р ИСО/МЭК ТО 13335-3—2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий;
- разд. А.9 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[575] Например, окружающей обстановки вокруг здания, возможности проникновения через крышки люков.

[576] Например, прочности конструкции здания, замков, системы пожарной сигнализации и защиты, системы сигнализации при затоплении водой/жидкостью, отказов в энергоснабжении и т.д.

[577] См.: разд. 10.1.1 настоящей Политики.

нестабильности электроснабжения, кондиционирования и иных внешних факторов)[578].

К мероприятиям по обеспечению физической защиты технических средств информационных систем от внутренних факторов относятся:

- контролю и управлению физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены[579].
- размещению устройств вывода (отображения) информации, исключающему ее несанкционированный просмотр[580];

10.1.1. Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования

10.1.1.1. Должны выполняться следующие требования Регуляторов к реализации организации контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования:[581]

10.1.1.1.1. Оператором должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования.

10.1.1.1.2. Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска на объекты информационной системы (не являющихся работниками оператора), а также транспортных, технических и иных материальных средств.

10.1.1.1.3. Границами контролируемой зоны могут являться периметр охраняемой территории, ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

10.1.1.1.4. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации.[582]

---

[578] См.: разд. 10.1.2 настоящей Политики.

[579] См.: разд. 10.1.3 настоящей Политики.

[580] См.: разд. 10.1.4 настоящей Политики.

[581] См.:

- разд. «Требования к реализации ЗТС.2» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.117-л.118;
- п.1.16, п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.

[582] См.: приказ Департамента ЗАГС Забайкальского края от 02.09.2019 № 98 «О контролируемой зоне Департамента ЗАГС Забайкальского края».

10.1.1.1.5. Для одной информационной системы (ее сегментов) может быть организовано несколько контролируемых зон.

10.1.2. Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)[583]

10.1.2.1. Должны выполняться следующие требования Регуляторов к реализации защиты от внешних воздействий:[584]

10.1.1.3.1. Оператором должна осуществляться защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

10.1.1.3.2. Защита от внешних воздействий в соответствии с требованиями законодательства Российской Федерации (национальных стандартов, технических регламентов) должна предусматривать:

- прочностью строительных конструкций здания[585];
- выполнение норм и правил пожарной безопасности, противопожарной защитой и пожарной сигнализацией[586];
- выполнение норм и правил устройства и технической

---

[583] Исполняется только для 1 класса защищенности информационной системы. См.:

- ЗТС.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- ЗТС.5 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- ЗТС.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР.

[584] См.: разд. «Требования к реализации ЗТС.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.120.

[585] См.:

- п.А.9.1.3Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;
- разд. 9.1.3 Безопасность зданий, производственных помещений и оборудования ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.5.3. Инструкции по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109.

[586] См.:

- п.А.9.1.4 Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;
- разд. 9.1.4 Защита от внешних угроз и угроз со стороны окружающей среды ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.5.3. Инструкции по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109.

эксплуатации электроустановок, а также соблюдение параметров электропитания и заземления технических средств; обеспечение необходимых для эксплуатации технических средств температурно-влажностного режима и условий по степени запыленности воздуха;

- регламентацией действий персонала при возгорании, предотвращении и (или) минимизации ущерба при затоплении водой/жидкостью, отключении электроэнергии[587];
- защитой коммуникаций и систем обеспечения энергоносителями в зданиях[588].

10.1.2.2. Требования к усилению мероприятий по защите от внешних воздействий Регуляторами не установлены[589].

10.1.3. Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и

---

[587] См.:

- п.6.3.7. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.2002 № 282;
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;
- п.А.8.1.1 Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;
- п.5.3., разделы VIII, X, XI и XIII Инструкции по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109;
- разд.3.5 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119;
- п.6.1.5.4.2, п.6.2.4.2.1, п.6.4.3.8 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[588] См.:

- п.А.9.2.3 Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;
- разд. 9.2.3 Безопасность кабельной сети ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.5.3. Инструкции по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109;
- разд.3.1 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119;
- п.8.2. Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111.

[589] См.: разд. «Требования к реализации ЗТС.5» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.120.

средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены

10.1.3.1. Должны выполняться следующие требования Регуляторов к реализации контроля и управления физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены:[590]

10.1.3.1.1. Оператором должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.

10.1.3.1.2. Контроль и управление физическим доступом должны предусматривать:

- определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены;
- учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

10.1.3.2. Правила и процедуры контроля и управления физическим доступом регламентируются в организационно-распорядительных документах оператора по защите информации[591].

10.1.3.3. Должны выполняться следующие требования Регуляторов к усилению мероприятий по контролю и управлению физическим доступом[592]:

10.1.3.3.1. Оператором должны применяться автоматизированные

---

[590] См.:

- п.ЗТС.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.3.1.6, п.5.1.3 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- разд. «Требования к реализации ЗТС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.118-л.119.

[591] См.: Инструкция по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденная приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109.

[592] См.: разд. «Требования к реализации ЗТС.3» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.119.

системы контроля и управления доступом (СКУД), обеспечивающие контроль и учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены с учетом национальных стандартов[593].

10.1.3.3.2. Оператором должны применяться средства видеонаблюдения, обеспечивающие регистрацию доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены.

10.1.3.3.3. Оператором обеспечивается интеграция системы контроля и управления доступом (СКУД) со средствами идентификации и аутентификации пользователей в информационной системе в соответствии с требованиями Регуляторов[594] и средствами управления доступом в соответствии с требованиями Регуляторов[595].

10.1.4. Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

10.1.4.1. Должны выполняться следующие требования Регуляторов к реализации размещения устройств вывода (отображения) информации, исключающем ее несанкционированный просмотр:[596]

10.1.4.1.1. Оператором должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

10.1.4.1.2. В качестве устройств вывода (отображения) информации в информационной системе следует рассматривать экраны

---

[593] См.: ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний

[594] См.:

- ИАФ.1, ИАФ.6 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации ИАФ.1» и разд. «Требования к реализации ИАФ.6» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.16-л.17, л.23.

[595] См.:

- УПД.2, УПД.10 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. «Требования к реализации УПД.2» и разд. «Требования к реализации УПД.10» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.26-л.28, л.36-л.37.

[596] См.:

- п.5.4.2 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 №282;
- раздел 4.2. «Угрозы утечки видовой информации» Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Федеральной службой по техническому и экспортному контролю 15.02.2008;
- разд. «Требования к реализации ЗТС.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.119-л.120.

мониторов автоматизированных рабочих мест пользователей, мониторы консолей управления технических средств (серверов, телекоммуникационного оборудования и иных технических средств), видео-панели, видеостены и другие средства визуального отображения защищаемой информации, печатающие устройства (принтеры, плоттеры и иные устройства), аудиоустройства, многофункциональные устройства.

10.1.4.1.3. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны.

10.1.4.1.4. Не следует размещать устройства вывода (отображения, печати) информации напротив оконных проемов, входных дверей, технологических отверстий, в коридорах, холлах и иных местах, доступных для несанкционированного просмотра.

10.1.4.2. Должны выполняться следующие требования Регуляторов к усилению мероприятий по размещению устройств вывода (отображения) информации, исключающем ее несанкционированный просмотр[597]:

10.1.4.2.1. Оператором обеспечивается установка на окна помещений информационной системы средств, ограничивающих возможность визуального ознакомления с защищаемой информацией извне помещений (жалюзи, плотные шторы и иные средства), если в этих помещениях размещены устройства вывода информации на печать и (или) осуществляется отображение информации на видеоустройства.

10.2. Политика обеспечения безопасности документов и носителей информации Департамента ЗАГС Забайкальского края

10.2.1. В Департаменте ЗАГС Забайкальского края в целях информационной безопасности регламентирован полный цикл обращения конфиденциальных документов, в том числе и на электронных носителях (создание или получение, регистрация, пересылка, исполнение, хранение, уничтожение)[598].

10.3. Контроль выполнения правил документооборота (в том числе и конфиденциального) в Департаменте ЗАГС Забайкальского края должна

---

[597] См.: разд. «Требования к реализации ЗТС.4» методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014), https://fstec.ru/component/attachments/download/675, л.120.

[598] См.:

- раздел VIII Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91;
- раздел VII Положения об архиве Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 113;
- раздел V и раздел VI Положения об экспертной комиссии Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 114;
- приказ Департамента ЗАГС Забайкальского края от 02.09.2019 № 116 «Об утверждении сроков и мест хранения материальных носителей персональных данных в Департаменте ЗАГС Забайкальского края».

осуществлять экспертная комиссия[599].

10.4. Контроль за оборотом[600] (учетом, выдачей, использованием, передачей, хранением и уничтожением) машинных носителей информации[601] должен осуществляться администратором безопасности информации[602].

XI. Политика обеспечения безопасности персонала Департамента ЗАГС Забайкальского края[603]

[599] Создается в соответствии с требованиями:
- Примерного положения об экспертной комиссии организации, утвержденного приказом Федерального архивного агентства от 11.04.2018 №43 (Зарегистрировано в Министерстве юстиции Российской Федерации 15.06.2018, регистрационный №51357);
- Положения об экспертной комиссии Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 114.

[600] Исполняется в соответствии с:
- п.5) ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п. «б» ст.13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.1 и п.2. гл.1 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного Постановлением Правительства РФ от 15.09.2008 №687;
- п.19.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.5.1.3., п.5.3.6., п.5.4.3.- п.5.4.5., п.5.6.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России;
- п. А.10.7.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п. 10.7.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.6.1.1. Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 101;
- п.9.6.1. Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[601] См.: п.4.1.26 настоящей Политики

[602] См.:
- п.20.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), и п. ЗНИ.1 и п. ЗНИ.8 Приложения №2 к указанным Требованиям;
- п. ЗНИ.1 и п. ЗНИ.8 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ЗНИ.1 и п. ЗНИ.8 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.6.2.1, п.6.3.1, п.6.4.2, п.7.2.1, п.7.3.2 Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 101;
- разд.9.6 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[603] См.: п.8 Приложения А ГОСТ Р ИСО/МЭК ТО 13335-3—2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

Политика обеспечения безопасности персонала Департамента ЗАГС Забайкальского края строится на осуществлении политик более низкого уровня:

- политики организации работы с личным составом (персоналом)[604];
- политики информирования и обучения персонала[605];
- политики организации реагирования персонала на инциденты нарушения информационной безопасности и сбои[606].

11.1. Политика организации работы с личным составом (персоналом)

Применяемая в ТФОМС Кемеровской области политика работы с личным составом (персоналом) устанавливает требования к:

- учету вопросов безопасности при найме персонала[607];
- включению вопросов информационной безопасности в должностные регламенты/должностные обязанности[608];
- соглашениям о конфиденциальности[609];
- условиям служебного контракта /трудового договора[610].

11.1.1. Учет вопросов безопасности при найме персонала[611]

11.1.1.1. В Департаменте ЗАГС Забайкальского края осуществляются проверки кандидатов[612], принимаемых в постоянный штат по мере подачи заявлений о приеме на службу/ работу. Среди прочего указанные проверки включают следующее:

- наличие положительных рекомендаций, в частности, в отношении деловых и личных качеств претендента;
- проверка (на предмет полноты и точности) резюме претендента;
- подтверждение заявляемого образования и профессиональных квалификаций;
- независимая проверка подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа);
- наличие личных или финансовых проблем у кандидата или уже принятого гражданского служащего или работника[613].

11.1.1.2. В случаях, когда новому гражданскому служащему (или работнику)

---

[604] См.: разд.11.1 настоящей Политики.
[605] См.: разд.11.2 настоящей Политики.
[606] См.: разд.11.3 настоящей Политики.
[607] См.: п. 11.1.1 настоящей Политики.
[608] См.: п. 11.1.2 настоящей Политики.
[609] См.: п. 11.1.3 настоящей Политики.
[610] См.: п. 11.1.4 настоящей Политики.
[611] См.: разд.8.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
[612] См.:

- п.2) ч.2 ст.32 и п.16)- п.18) ч.1 ст.44 Федерального закона от 27.07.2004 №79-ФЗ "О государственной гражданской службе Российской Федерации";
- п.А.8.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- разд.8.1.2 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[613] См.: абзац 5 п.6.1.2 ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью»: «Личные или финансовые проблемы сотрудников, изменения в их поведении или образе жизни, периодическая рассеянность и признаки стресса или депрессии могут быть причинами мошенничества, воровства, ошибок или других нарушений безопасности. Эту информацию следует рассматривать в соответствии с действующим законодательством».

непосредственно после приема на службу (работу) или в ее процессе предстоит доступ к средствам обработки важной информации, например, финансовой или иной информации, доступ к которой ограничен законом, перечень вопросов проверки может быть расширен. В отношении сотрудников, имеющих значительные полномочия, эта проверка должна проводиться периодически.

11.1.2. Включение вопросов информационной безопасности в должностные регламенты (должностные обязанности)[614]

11.1.2.1. Функции (роли) и ответственность в области информационной безопасности следует документировать. В должностные регламенты гражданских служащих (должностные обязанности работников) Департамента ЗАГС Забайкальского края должны включаться как общие обязанности по внедрению или соблюдению политики безопасности, так и специфические особенности по защите определенных активов или действий, касающихся безопасности.

11.1.3. Соглашение о конфиденциальности[615]

11.1.3.1. В Департаменте ЗАГС Забайкальского края регламентирован порядок доступа сотрудников Департамента и сотрудников иных органов и организаций к конфиденциальной информации[616]. Соглашение о конфиденциальности заключается в форме Обязательства гражданского служащего (работника) о неразглашении конфиденциальной информации Департамента ЗАГС Забайкальского края[617] и Соглашения о неразглашении конфиденциальной информации Департамента ЗАГС Забайкальского края, заключаемого с сотрудниками иных органов и организаций, допускаемых к конфиденциальной информации на основании государственных контрактов или гражданско- правовых договоров[618].

---

[614] См.:
- п. б) ст.1 Постановление Правительства РФ 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";
- п. А.6.1.2 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования ;
- 6.1.2 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.2 ст.8.1.4 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.

[615] См.:
- А.6.1.5 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.6.1.5 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[616] В соответствии с:
- разделом VII Положения о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91;
- разделом VI Положения о разрешительной системе допуска пользователей к информационным системам Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 96.

[617] См.: Приложение №2 к Положению о конфиденциальной информации Департамента ЗАГС Забайкальского края, утвержденному приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91.

[618] См.: Приложение №2-1 к Положению о конфиденциальной информации Департамента ЗАГС

11.1.3.2. В государственные контракты и гражданско- правовые договоры, заключаемые Департаментом ЗАГС Забайкальского края с подрядчиками, которым для выполнения условий контракта (договора) необходим доступ к служебной информации, в соответствии с нормами действующего законодательства включаются положения о соблюдении конфиденциальности.

11.1.4. Условия служебного контракта (трудового договора)[619]

11.1.4.1. В Департаменте ЗАГС Забайкальского края в соответствии с действующим законодательством устанавливаются условия служебного контракта (трудового договора)[620], определяющего ответственность гражданского служащего (работника) в отношении информационной безопасности. Указанная ответственность сохраняться и в течение неопределенного срока после увольнения со службы. До гражданского служащего (работника) доводятся меры ответственности, которые будут применимы в случае нарушения требований безопасности.

11.2. Политика информирования и обучения персонала

11.2.1. Разработка политики информирования и обучения персонала является обязательным требованием действующего законодательства и Регуляторов, а также внутренних организационно- распорядительных актов[621].

Забайкальского края, утвержденному приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 91.

[619] См.: п.8.1.3 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[620] В соответствии с:

- п.7) ч.2 ст.15 Федерального закона от 27.07.2004 №79-ФЗ "О государственной гражданской службе Российской Федерации";
- ч.4 ст.57 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ;
- п.6 Примерной форме служебного контракта о прохождении государственной гражданской службы Российской Федерации и замещении должности государственной гражданской службы Российской Федерации, утвержденной Указом Президента РФ от 16.02.2005 №159.

[621] Проводится в соответствии с:

- п.6) ч.1 ст.18.1, п.2) ч.4. ст.22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- п.18.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.3.16. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.2002 № 282;
- п.21 «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденную приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06. 2001 № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
- п.2.3. «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;
- разд. 8.2.2. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

11.2.2. Обучение гражданских служащих и работников должно проводиться с целью обеспечения уверенности в их осведомленности об угрозах и проблемах, связанных с информационной безопасностью, и их оснащенности всем необходимым для соблюдения требований политики информационной безопасности при выполнении должностных обязанностей[622].

11.2.3. Применяемая в ТФОМС Кемеровской области политика информирования и обучения персонала устанавливает требования к:

- информированию персонала об угрозах безопасности информации и о правилах безопасной работы;
- обучению персонала правилам безопасной работы;
- проведению практических занятий с персоналом по правилам безопасной работы;
- контролю осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы.

11.3. Политика организации реагирования персонала на инциденты нарушения информационной безопасности и сбои[623]

- п. А.8.2.2 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.10.4 ГОСТ Р ИСО/МЭК ТО 13335-3- 2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий;
- п.3 ст.8.1.4 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер;
- разд.9.2 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п.5.2 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100.

[622] См.: п.3.1.2.4.5- п. 3.1.2.4.6 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[623] Осуществляется в соответствии с:

- п.6) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п16.2, п.18, п.18.2, п.20.5-п.20.7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608), а также п. РСБ.4 , п. РСБ.5, п. ОЦЛ.4 , п. ЗИС.7 - п. ЗИС.9 Приложения №2 к указанным Требованиям;
- п. 3.24. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- разд.13.2 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п. 4.2.2, п. А.13.2.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п. РСБ.4, п. РСБ.5, п. ОЦЛ.4 , п. ЗИС.7 - п. ЗИС.9 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. РСБ.4 , п. РСБ.5, п. ОЦЛ.4 , п. ЗИС.7 - п. ЗИС.9 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;

Применяемая в ТФОМС Кемеровской области политика организации реагирования персонала на инциденты нарушения информационной безопасности и сбои осуществляется с целью сведения к минимуму ущерба от инцидентов нарушения информационной безопасности и сбоев[624] устанавливает требования к:

- информированию об инцидентах нарушения информационной безопасности[625];
- информированию о проблемах безопасности[626];
- информированию о сбоях программного обеспечения[627];
- извлечении уроков из инцидентов нарушения информационной безопасности[628];
- процессу установления дисциплинарной ответственности[629].

11.3.1. Информирование об инцидентах нарушения информационной безопасности[630]

11.3.1.1. В Департаменте ЗАГС Забайкальского края должны предусматриваться формализованные процедуры информирования об инцидентах, а также процедуры реагирования на инциденты, устанавливающие действия, которые должны быть предприняты после получения сообщения об инциденте[631].

- разд.9.16, п.9.7.4 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- разд. 6.2 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[624] См.: п.3.6, п. А.9.2.2 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[625] См.: п.11.3.1 настоящей Политики.

[626] См.: п.11.3.2 настоящей Политики.

[627] См.: п.11.3.3 настоящей Политики.

[628] См.: п.11.3.4 настоящей Политики.

[629] См.: п.11.3.5 настоящей Политики.

[630] Осуществляется в соответствии с:

- п.6) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»;
- п.18.2Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п. 3.24. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- разд.13.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- разд.А.13.1. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[631] См.:

- п.18.1 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.5.3. Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100;
- разд.6.2.3 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;

11.3.1.2. Все пользователи должны быть ознакомлены с процедурой информирования об инцидентах нарушения информационной безопасности, а также проинформированы о необходимости незамедлительного сообщения об инцидентах.

11.3.1.3. В Департаменте ЗАГС Забайкальского края предусматриваются процедуры обратной связи по результатам реагирования на инциденты нарушения информационной безопасности[632].

11.3.1.4. Информация об инцидентах может использоваться с целью повышения осведомленности пользователей, поскольку позволяет демонстрировать на конкретных примерах возможные последствия инцидентов, реагирование на них, а также способы их исключения в будущем[633].

11.3.2. Информирование о проблемах безопасности[634]

11.3.2.1. В обязанностях пользователей информационных сервисов предусматривается[635], что они должны:

– обращать внимание и сообщать о любых замеченных или предполагаемых недостатках и угрозах в области безопасности в системах или сервисах[636];

– п.10.3 Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111;
– п.7.15, п.8.28- п.8.29 Регламента безопасного функционирования подсистемы криптографической защиты информации системы защиты информации информационных систем Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 103.

[632] См.: п.3.5.1.1.2, п.3.5.2.1.1 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[633] См.: п.6.2.4.2.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[634] См.:
– разд.13.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
– разд.А.13.1. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
– п.6.2.4.2.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

[635] См.: раздел VII Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100.

[636] Исполняется в соответствии:
– п.18.2 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
– п.20 Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001. № 152(Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
– п.2.5; п.2.8; п.3.24 «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для

– немедленно сообщать об этих причинах для принятия решений своему руководству или непосредственно поставщику услуг[637].

11.3.2.2. Требования информационной безопасности предусматривают, что пользователи не должны ни при каких обстоятельствах самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности. Это требование предъявляется в интересах самих пользователей, поскольку тестирование слабых мест защиты может быть интерпретировано как неправомочное использование системы[638].

11.3.3. Информирование о сбоях программного обеспечения[639]

11.3.3.1. Для информирования о сбоях программного обеспечения в Департаменте ЗАГС Забайкальского края регламентированы соответствующие процедуры, при которых должны предусматриваться следующие действия:

– симптомы проблемы и любые сообщения, появляющиеся на экране, должны фиксироваться;
– по возможности, компьютер необходимо изолировать и пользование им прекратить;
– о факте сбоя программного обеспечения немедленно должен извещаться администратор безопасности информации.

11.3.3.2. Пользователи не должны пытаться самостоятельно удалить подозрительное программное обеспечение, если они не уполномочены на это. Ликвидировать последствия сбоев должен соответственно обученный персонал[640].

11.3.4. Извлечение уроков из инцидентов нарушения информационной безопасности[641]

обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622.

[637] См.: п.7.1.3 и п. 7.1.4 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100.

[638] См.: п.8.1.6 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100.

[639] См.:

– п. А.13.1.1 Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;
– раздел 13.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[640] См.:

– п.8.1.8. Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 100;
– п.8.3 Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[641] См.:

– А.13.2.2 Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;

11.3.4.1. По закрытию инцидентов информационной безопасности при руководителе Департамента ЗАГС Забайкальского края должно проводиться оперативное совещание, на котором должны анализироваться действия должностных лиц при кризисном управлении и намечаться профилактические мероприятия по предотвращению подобных инцидентов[642].

11.3.4.2. В Департаменте ЗАГС Забайкальского края должен быть установлен порядок мониторинга и регистрации инцидентов и сбоев в отношении их числа, типов, параметров, а также связанных с этим затрат[643]. Данная информация должна использоваться для:

- идентификации повторяющихся или значительных инцидентов или сбоев;
- анализа необходимости совершенствования существующих или внедрении дополнительных мероприятий по управлению информационной безопасностью с целью минимизации вероятности появления инцидентов нарушения информационной безопасности, снижения возможного ущерба и расходов в будущем[644];

- разд. 13.2.2. «Извлечение уроков из инцидентов информационной безопасности» ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п.9.1 ГОСТ Р ИСО/МЭК 18044. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности;
- п.73 Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001. № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
- п.6.2.4.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

642 См.: п.3.1.2.4.3 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

643 См.:

- п. РСБ.5 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- разд. 3.5 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п. РСБ.5 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. РСБ.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.6.1.5.3.5, п. 6.1.5.5 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99.

644 См.: п.6.1.5.3.5 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99

– возможного пересмотра политики информационной безопасности.

11.3.5. Процесс установления дисциплинарной ответственности[645]

11.3.5.1. По каждому выявленному факту нарушения информационной безопасности в Департаменте ЗАГС Забайкальского края регламентировано проведение служебной проверки и привлечение виновных к ответственности[646].

XII. Политика обеспечения непрерывности деятельности Департамента ЗАГС Забайкальского края при чрезвычайных ситуациях и восстановления средств и систем после аварий[647]

---

[645] См.:
- п.8.2, п. 8.2.3 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п. А.8.2.3 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[646] Исполняется в соответствии с:
- п.7 Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001. № 152 (Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. № 34);
- п.2.3. и п. 3.24. «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622;
- п.5.1.4, п.7.3.4 ГОСТ Р ИСО/МЭК 18044. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности и Приложение А к указанному ГОСТ;
- п.6.2.5.4, п.6.4.1.4 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- п.3.3.2.3, п.3.5.2.3.3, п.3.1.2.4.1 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119;
- п.9.4.5 Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111;
- п.12.1.6, 13.3.3. Инструкции по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109.

[647] Исполняется в соответствии с:
- п. ОЦЛ.3 Приложения №2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.11 Приложения А ГОСТ Р ИСО/МЭК ТО 13335-3—2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий;
- раздела 8.3 ГОСТ Р 53647.1-2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство;
- п.4.3.3 ГОСТ Р 53647.2-2009. Менеджмент непрерывности бизнеса. Часть 2. Требования;
- раздела 10 ГОСТ Р 53647.3-2010 Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению;

12.1. В Департаменте ЗАГС Забайкальского края должно обеспечиваться управление непрерывностью деятельности с целью минимизации отрицательных последствий, вызванных бедствиями и нарушениями безопасности (которые могут быть результатом природных бедствий, несчастных случаев, отказов оборудования и преднамеренных действий), до приемлемого уровня с помощью комбинирования профилактических и восстановительных мероприятий по управлению информационной безопасностью. Проведение указанных мероприятий регламентировано внутренними организационно - распорядительными актами[648].

12.2. В случае чрезвычайных ситуаций, инцидентов информационной безопасности, способных повлиять на непрерывность информационных процессов Департамента ЗАГС Забайкальского края, создается (собирается) оперативный штаб и рабочая группа оперативного штаба[649].

- раздела 6 ГОСТ Р 53647.4-2011/ISO/PAS 22399:2007 Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности;
- ГОСТ Р 53647.5-2012. Менеджмент непрерывности бизнеса. Готовность к опасным ситуациям и инцидентам;
- раздела 3 ГОСТ Р 53647.6-2012. Менеджмент непрерывности бизнеса. Требования к системе менеджмента персональной информации для обеспечения защиты данных;
- раздела А.14 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- раздела 14 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п. ОЦЛ.3 Таблицы 1. «Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы» Технического задания «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»;
- п. ОЦЛ.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края» СЗ- ЗАГС.П2.01-ОР;
- п.7.2. Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111;
- п.6.1.2.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- разд.III Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[648] См. требования:

- Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111;
- Инструкции по резервному копированию информационных ресурсов информационных систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 112;
- разделы VIII-XIV Инструкции по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109;
- Планом обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденным приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[649] См.:

- п.10.4.6 ГОСТ Р 53647.3-2010 Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению;
- Приложение №2 к приказу Департамента ЗАГС Забайкальского края от 02.09.2019 № 119 «Об утверждении Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края»»;

12.3. Оперативный штаб возглавляет руководитель Департамента ЗАГС Забайкальского края. Место сбора оперативного штаба- рабочий кабинет руководителя Департамента ЗАГС Забайкальского края.

12.4. В состав оперативного штаба входят руководители подразделений Департамента ЗАГС Забайкальского края[650].

12.5. Рабочую группу оперативного штаба возглавляет заместитель руководителя Департамента - начальник отдела административной, методической работы и информатизации как руководитель подразделения, на которое возложены функции за обеспечение безопасности конфиденциальной информации в информационных системах[651]. Место сбора рабочей группы оперативного штаба – кабинет заместителя руководителя - начальника отдела административной, методической работы и информатизации.

12.6. В состав рабочей группы оперативного штаба входят администратор безопасности информации и системный администратор, а также иные должностные лица[652].

12.7. Задача оперативного штаба: активация Плана обеспечения непрерывности и восстановления управления информационных систем Департамента ЗАГС Забайкальского края[653], организация кризисного управления, проведение разбора недостатков кризисного управления после ликвидации ЧП, закрытия инцидента информационной безопасности.

12.8. Задача рабочей группы оперативного штаба: документирование решений оперативного штаба при кризисном управлении, проведение мероприятий кризисного управления, проведение анализа по результатам кризисного

- п.3.1.3.2, п.3.5.2.3.1 План обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденный приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119;
- п.6.4 и п. 6.5 Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111.

[650] См.: Приложение №2 к приказу Департамента ЗАГС Забайкальского края от 02.09.2019 № 119 «Об утверждении Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края».

[651] См.:

- п.16 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.9 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п/п. б) п.22 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, утвержденных приказом ФСБ России от 10.07.2014 №378 (зарегистрировано в Минюсте России 18.08.2014 №33620);
- п.3 приказа Департамента ЗАГС Забайкальского края от 02.09.2019 № 94 «Об утверждении Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края».

[652] См.: Приложение №2 к приказу Департамента ЗАГС Забайкальского края от 02.09.2019 № 119 «Об утверждении Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края».

[653] См.: План обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденный приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

управления[654], подготовка материалов для заседаний оперативного штаба[655], в том числе и по подведению итогов кризисного управления.

12.9. Последствия от бедствий, нарушений безопасности и отказов в обслуживании должны анализироваться должностными лицами, ответственными за обеспечение безопасности информации[656]. На основе проведенного анализа должно проводиться обучение персонала[657] и разрабатываться планы профилактических и восстановительных мероприятий[658] по управлению информационной безопасностью. Данные планы являются составной частью всех процессов управления. Обучение персонала может проводиться в форме учений с имитацией инцидента информационной безопасности[659].

---

[654] См.:
- п.6.4., п.6.5 Инструкции о порядке действий в нештатных ситуациях в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 111;
- п.3.1.2.2, п.3.1.3.2, п.3.1.4.2, п.3.5.2.3.1 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[655] См.:
- п.13.3.5 Инструкции по обеспечению физической защиты помещений контролируемой зоны Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 109
- п.3.1.2.4.3 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[656] См.:
- раздел 6.2.2, раздел 6.2.5, п. 6.2.6.2.1, п.6.2.4.1.6 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- п.7.1.1, п. 8.1.1 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94;
- п.3.1.2.4.2, п.3.1.5 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119;
- разд.6.1.5 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- п.8.4.2 Инструкции по организации антивирусной защиты в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 107.

[657] См.: п.3.1.2.4.5 и п.3.1.2.4.6 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

[658] См.:
- План обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденный приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119;
- План проведения периодических проверок условий обработки персональных данных в Департаменте ЗАГС Забайкальского края, утвержденный приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 118;
- План мероприятий по защите конфиденциальной информации информационных систем Департамента ЗАГС Забайкальского края, утвержденный приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 117.

[659] См.: п. 3.1.2.4.6 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 119.

XIII. Политика аутсорсинга в Департаменте ЗАГС Забайкальского края [660]

13.1. В соответствии с требованиями действующего законодательства Департамент ЗАГС Забайкальского края вправе поручить на договорной основе уполномоченным лицам исполнять следующие функции обеспечения безопасности:

- физическая защита[661] (охрана помещений, пропускной режим, обслуживание охранно- пожарной сигнализации);
- администрирование информационных систем[662];
- администрирование информационной безопасности[663] и др.

13.2. Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению Департамента ЗАГС Забайкальского края и (или) предоставляющее Департаменту ЗАГС Забайкальского края вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации[664]. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии требованиями по защите информации[665] и настоящей Политикой.

XIV. Политика управления изменениями в информационных системах Департамента ЗАГС Забайкальского края [666]

---

[660] См.: п.13 Приложения А ГОСТ Р ИСО/МЭК ТО 13335-3—2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

[661] См.:

- п.15) ч.1 ст12 Федерального закона от 04.05.2011 № 99-ФЗ "О лицензировании отдельных видов деятельности";
- раздел III Закона РФ от 11.03.1992 №2487-1"О частной детективной и охранной деятельности в Российской Федерации";
- Постановление Правительства РФ от 14.08.1992 №587 "Вопросы частной детективной (сыскной) и частной охранной деятельности";
- Постановление Правительства РФ от 30.12.2011 №1225 "О лицензировании деятельности по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений" (вместе с "Положением о лицензировании деятельности по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений").

[662] В соответствии с ч.3 ст.6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных».

[663] В соответствии с:

- ст.3Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119;
- п.10 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[664] См.: п.3) ч.2 ст.6, ч.1 ст.16 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации".

[665] См.:

- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[666] См.:

- п.16.2, п.16.3, п.18.3 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК

14.1. Для поддержания информационной безопасности в актуальном состоянии по мере необходимости могут вноситься изменения в:
- конфигурацию информационных систем;
- конфигурацию системы защиты информационных систем;
- внутренние организационно- распорядительные акты по вопросам обеспечения информационной безопасности;
- техническую документацию (технический проект) на создание системы защиты информации информационных систем персональных данных.

14.2. При внесении изменений конфигурацию информационных систем и конфигурацию системы защиты информации информационных систем Департамента ЗАГС Забайкальского края должны соблюдаться следующие требования[667]:

14.2.1. Изменения в конфигурацию ИС и СЗИИС вносятся уполномоченными сотрудниками Департамента ЗАГС Забайкальского края (или уполномоченным лицом[668]) по согласованию со специализированной организацией - лицензиатом ФСТЭК, аттестовавшей ранее данную информационную систему[669].

14.2.2. При изменении состава технических средств защиты или элементов ИС, соответствующие изменения должны быть внесены в Технический проект по согласованию с разработчиком[670].

14.2.3. Информация об изменениях конфигурации ИС и СЗИИС вносится в

России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.14 Приложения А ГОСТ Р ИСО/МЭК ТО 13335-3—2007. Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

[667] См.:
- разделы 6.3.2 и 6.3.3 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- разделы.6.2 и 6.3 Инструкции по внесению изменений в конфигурацию информационных систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 110

[668] Действующее по гражданско- правовому договору в соответствии с:
- ст. 3 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[669] См.:
- п.5.4.2., п.6.3.19 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282, а также п.5. Приложения 2 к указанным Специальным требованиям;
- п.6.3.2.1 Инструкции по администрированию безопасности информации в информационных системах Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 99;
- п.6.2.1 Инструкции по внесению изменений в конфигурацию информационных систем Департамента ЗАГС Забайкальского края, утвержденной приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 110.

[670] Исполняется в соответствии с п.5.4.2. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 №282, а также п.5. Приложения 2 к указанным Специальным требованиям.

проектную[671] и эксплуатационную документацию[672] в соответствии с положениями национальных стандартов[673].

14.2.4. Внесение изменений в информационной системы осуществляет администратор ИС по согласованию и под контролем руководителя подразделения безопасности информации и администратора безопасности информации (или уполномоченного лица[674]), т.к. неудачно и (или) неправильно конфигурированные операционные системы по причине неконтролируемых изменений в системе могут являться факторами, приводящими к инцидентам информационной безопасности[675]. Выбор правильной конфигурации и форм администрирования сетей являются эффективными средствами снижения уровня риска информационной безопасности[676].

14.2.5. Системный администратор выполняет конфигурирование и управление программным обеспечением (ПО) и оборудованием, администратор безопасности информации (уполномоченное лицо) выполняет конфигурирование оборудования, отвечающего за безопасность защищаемого объекта: средства криптографической защиты информации, мониторинга, регистрации, архивации, защиты от НСД[677].

14.2.6. При внесении изменений в конфигурацию информационных систем и (или) конфигурацию системы защиты информации информационных систем должны быть рассмотрены следующие мероприятия[678]:

---

[671] См.:
- Техническое задание «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». СЗ-ЗАГС.

[672] См.: п.3.1.1. и п. 5.1.2 ГОСТ 2.601-2006. Единая система конструкторской документации. Эксплуатационные документы.

[673] См.:
- ГОСТ 2.503-90. ЕСКД. Правила внесения изменений (взамен ГОСТ 2.503-74, ГОСТ 2.505-82, ГОСТ 2.506-84);
- ГОСТ 19.603-78 (СТ СЭВ 2089-80). Единая система программной документации. Общие правила внесения изменений;
- ГОСТ 19.604-78 (СТ СЭВ 2089-80) Единая система программной документации. ПРАВИЛА ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПРОГРАММНЫЕ ДОКУМЕНТЫ, ВЫПОЛНЕННЫЕ ПЕЧАТНЫМ СПОСОБОМ.

[674] Действующего по гражданско- правовому договору в соответствии с:
- ст. 3 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 №1119;
- п.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[675] См.: п.6.2, п.6.3 ГОСТ Р ИСО/МЭК 18044. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

[676] См.: п.8.2.4 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.

[677] См.: п. 5.1 Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной Федеральной службой по техническому и экспортному контролю 15.02.2008.

[678] См.:
- А.10.1.2 Таблицы А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;

- определение и регистрация существенных изменений;
- оценка возможных последствий таких изменений;
- формализованная процедура утверждения предлагаемых изменений;
- подробное информирование об изменениях всех заинтересованных лиц;
- процедуры, определяющие обязанности по прерыванию и восстановлению работы средств и систем обработки информации, в случае неудачных изменений программного обеспечения.

14.2.7. Данные о конфигурации сети и компоновочном плане должны резервироваться для обеспечения их доступности в аварийных ситуациях[679].

14.2.8. После изменений конфигурации информационной системы необходимо проводить повторную переаттестацию ИС или дополнительные аттестационные испытания в рамках действующего аттестата соответствия. Повторная аттестация информационной системы осуществляется в случае окончания срока действия аттестата соответствия или повышения класса защищенности информационной системы. При увеличении состава угроз безопасности информации или изменения проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия[680].

14.3. При внесении изменений во внутренние организационно- распорядительные акты в области информационной безопасности должны соблюдаться следующие требования:

- внесенные изменения должны соответствовать действующему законодательству на момент внесения указанных изменений;
- внесенные изменения не должны вступать в противоречие с политикой информационной безопасности, технической документацией на СЗИИС.

14.4. При внесении изменений в техническую документацию[681] должны соблюдаться следующие требования:

14.4.1. Изменения в техническую документацию (технический проект) на создание СЗИИС вносятся разработчиком проекта или по предварительному согласованию с разработчиком проекта.

14.4.2. Изменения в техническую документацию (технический проект) на создание СЗИИС вносятся в соответствии с положениями национальных

- разд.10.1.2 «Управление изменениями» ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[679] См.:

- п.10.4.3 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.;
- п.9.3. Технического задания «Система защиты персональных данных информационных систем персональных данных Общества с ограниченной ответственностью «Энергосбытовая компания Кузбасса»;
- п.9.12.4 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[680] В соответствии с п. 17.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[681] См.:

- Техническое задание «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края»
- Проект «Система защиты государственной информационной системы и иных информационных систем Департамента записи актов гражданского состояния Забайкальского края». СЗ-ЗАГС.

стандартов[682].

14.4.3. При изменении проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия[683].

XV. Ответственность и полномочия

15.1. Ответственность персонала

15.1.1. За нарушение требований настоящей Политики должностные лица Департамента ЗАГС Забайкальского края несут ответственность в соответствии с действующим законодательством.

15.1.2. Должностное лицо Департамента ЗАГС Забайкальского края, разработавшее проект организационно- распорядительного акта Департамента ЗАГС Забайкальского края в области защиты информации, несет ответственность за соответствие данного акта положениям настоящей Политики.

15.1.3. Должностные лица Департамента ЗАГС Забайкальского края, вносящие изменения в конфигурацию информационных систем и СЗИИС, несут ответственность за соответствие своих действий процедурам, регламентированным настоящей Политикой.

15.2. Полномочия персонала

15.2.1. Сотрудники Департамента ЗАГС Забайкальского края имеют право выходить с предложениями к руководству Департамента по вопросам защиты конфиденциальной информации.

XVI. Заключительные положения

16.1. Изменения в настоящую Политику вносятся приказом Департамента ЗАГС Забайкальского края после обязательного согласования вносимых изменений с заместителем руководителя - начальником отдела административной, методической работы и информатизации, отвечающим за контроль соответствия издаваемых Департаментом ЗАГС Забайкальского края организационно - правовых актов в области защиты информации требованиям Регуляторов[684], а также согласования с ответственным за организацию обработки персональных данных в Департаменте ЗАГС Забайкальского края[685].

---

[682] См.:
- ГОСТ 2.503-90. ЕСКД. Правила внесения изменений (взамен ГОСТ 2.503-74, ГОСТ 2.505-82, ГОСТ 2.506-84);
- ГОСТ 19.603-78 (СТ СЭВ 2089-80). Единая система программной документации. Общие правила внесения изменений;
- ГОСТ 19.604-78 (СТ СЭВ 2089-80) Единая система программной документации. ПРАВИЛА ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПРОГРАММНЫЕ ДОКУМЕНТЫ, ВЫПОЛНЕННЫЕ ПЕЧАТНЫМ СПОСОБОМ.

[683] В соответствии с п. 17.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[684] См.: п.8.1.4 Положения о подразделении, ответственном за обеспечение безопасности информации Департамента ЗАГС Забайкальского края, утвержденного приказом Департамента ЗАГС Забайкальского края от 02.09.2019 № 94.

[685] См.п.3 приказа Департамента ЗАГС Забайкальского края от 02.09.2019 № 93 «Об утверждении Положения об ответственном за организацию обработки персональных данных в Департаменте ЗАГС Забайкальского края».