Приложение к приказу
ГКУ «КЦСЗН» Забайкальского края
от 17.07.2017 №01-99

ПОЛИТИКА
информационной безопасности в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края

г. Чита
2017

Оглавление

I. Назначение

1.1. В соответствии с:

- 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 Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края (далее- Политики) является определение основных правил обеспечения безопасности объектов защиты ГКУ «КЦСЗН» Забайкальского края от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также минимизации ущерба от

[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.

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 информационной безопасности в организациях роль основного внутреннего документа органа (организации), 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.

II. Область применения

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

2.2. В Политике определены объекты защиты, общий замысел защиты информации ГКУ «КЦСЗН» 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 ГКУ «КЦСЗН» Забайкальского края.

2.3. Требования Политики обязательны для всех работников ГКУ «КЦСЗН» Забайкальского края, представителей контрольно- надзорных органов,

---

[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;
- 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 (ред. от 22.02.2017) «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).

допущенных к защищаемой информации на законных основаниях, а также индивидуальных лиц и сотрудников иных органов (организаций) допущенных к защищаемой информации для проведения работ по государственным контрактам или иным гражданско- правовым договорам[5].

Нормативные ссылки

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

- Конституции Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ, от 05.02.2014 №2-ФКЗ, от 21.07.2014 №11-ФКЗ);
- Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных";
- Трудового кодекса Российской Федерации от 30.12.2001 №197-ФЗ (ред. от 01.05.2017);
- Указа Президента Российской Федерации от 06.03.97 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера»;
- Указа Президента РФ от 17.03.2008 №351 (ред. от 22.05.2015) "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";

[5] Заключенным на основании и условиях:

- ч.3 ст.6 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «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 Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-101;
- п.6.2.7 Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

- Постановления Правительства Российской Федерации от 21.03.2012 №211 (ред. от 06.09.2014) "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 (ред. от 21.04.2010)"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);
- 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 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[6].

4.1.2. **Автоматизированная система** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[7].

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[8].

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[9].

4.1.5. **Аттестация объектов информатизации** – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации[10].

4.1.6. **Аутентификация -** проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе)[11].

---

[6] См.: ч.4.ст.3 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных".

[7] 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.

[8] 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 30.08.2002 № 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).

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

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

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

4.1.7. **Безопасность информации [данных]** - 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность[12]; 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[13].

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[14].

4.1.9. **Вредоносная программа** - программа, используемая для несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы[15].

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[16]. В ГКУ «КЦСЗН» Забайкальского края к государственной информационной системе относится ГИС «АС «АСП», собственником которой является Министерство труда и социальной защиты населения Забайкальского края[17], передавшее некоторые права управления указанной ГИС ГКУ «КЦСЗН» Забайкальского края как уполномоченному лицу[18] в целях обеспечения реализации предусмотренных законодательством Российской

---

[12] 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».

[13] См. п. 1.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 №282.

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

[15] 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».

[16] См.: п.1) ч.1 ст.13 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) "Об информации, информационных технологиях и о защите информации". ГИС «Автоматизированная система «Адресная социальная помощь РКО» (ГИС «АС «АСП») является региональной государственной информационной системой. Сегмент ГИС «АС «АСП» передан в оперативное управление ГКУ «КЦСЗН» Забайкальского края

[17] В соответствии с п.1.1 приказа Министерства социальной защиты населения Забайкальского края от 08.07.2016 №953 «О государственных информационных системах Министерства социальной защиты населения Забайкальского края».

[18] См.: п.4.1.52 настоящей Политики.

Федерации полномочий Министерства труда и социальной защиты населения Забайкальского края[19].

4.1.11. **Документооборот** - движение документов в организации с момента их создания или получения до завершения исполнения или отправления[20].

4.1.12. **Должностное лицо** – работник ГКУ «КЦСЗН» Забайкальского края, правомочный от имени ГКУ «КЦСЗН» Забайкальского края исполнять определенные, предусмотренные должностными обязанностями действия.

4.1.13. **Доступность (санкционированная доступность) информации** - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия[21].

4.1.14. **Жизненный цикл СКЗИ** - разработка (модернизация) указанных средств, их производство, хранение, транспортировка, ввод в эксплуатацию (пусконаладочные работы), эксплуатация.[22]

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[23].

4.1.16. **Идентификатор** - представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе[24].

4.1.17. **Идентификация** - присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов[25].

4.1.18. **Информационная система (ИС)** - совокупность содержащейся в

---

[19] См.: п.1.6 , п.2.1- п.2.2 Устава Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом Министерства труда и социальной защиты населения Забайкальского края от 13.03.2017 №417.

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

[21] См.:

- п.1.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п.3.1.9 «Рекомендации по стандартизации Р.50.1.053 – 2005. Информационная технология. Основные термины и определения в области защиты информации».

[22] 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).

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

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

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

базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.[26]

4.1.19. **Информационная система персональных данных (ИСПДн)** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств[27].

4.1.20. **Информационные системы ГКУ «КЦСЗН» Забайкальского края** – находящиеся на правах собственности ГКУ «КЦСЗН» Забайкальского края, или на правах его управления, или других законных основаниях информационные системы[28], представляющие собой совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий и 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)[29].

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[30].

4.1.23. **Контролируемая зона** – это пространство, в котором исключено неконтролируемое пребывание работников и посетителей оператора и посторонних транспортных, технических и иных материальных средств[31].

---

[26] См.: ч.3 ст.2 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «Об информации, информационных технологиях и о защите информации».

[27] См.:

- ч.10 ст.3 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «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.

[28] включая информационные системы персональных данных и государственную информационную систему ГИС «АСП»

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

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

[31] 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

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[32].

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 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

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 30.08.2002 № 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;
- разд.А.9.1 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. 9.1.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
- разд.1, разд.5- 7, разд.11-12 ГОСТ Р ИСО/МЭК ТО 13335-5-2006. Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 5. Руководство по менеджменту безопасности сети.

[32] См.: п.11) ст.2 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «Об информации, информационных технологиях и о защите информации».

информации)[33].

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[34].

4.1.28. **Модель угроз** - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации[35].

4.1.29. **Несанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или информационными системами[36].

4.1.30. **Обработка информации** - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи хранения,

---

[33] 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(ред. от 18.05.2017);
- 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.

[34] См.:

- п.1.19. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 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 .

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

[36] См.: п.1.20. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282.

регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией[37].

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[38].

4.1.32. **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа[39].

4.1.33. **Объект защиты информации** - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации[40].

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[41].

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[42]. 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

[37] См.: п.3.1 ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования.
[38] См.: ч.3.ст.3 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных".
[39] См.: п.1.4 «Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. (Утверждено решением председателя Гостехкомиссии России от 30.03.1992).
[40] См.: п. 2.5.1 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
[41] См. п.3.2 ГОСТ РО 0043-003-2012. Защита информации. Аттестация объектов информатизации. Общие требования.
[42] См.: примечание 1 к п.2.2.4 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

обработка ПДн и (или) размещены СКЗИ[43]; разработка должностных инструкций по работе с персональными данными; установление персональной ответственности за нарушения правил обработки ПДн; определение продолжительности хранения ПДн и т.д.[44]

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[45].

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[46].

4.1.38. **Ответственный за организацию обработки персональных данных** - должностное лицо оператора ПДн (ГКУ «КЦСЗН» Забайкальского края), осуществляющее:

- внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников ГКУ «КЦСЗН» 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[47];
- контроль организации допуска работников ГКУ «КЦСЗН» Забайкальского края к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности[48].

4.1.39. **Персональные данные** - любая информация, относящаяся к

---

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

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

[45] См.: п.12) ст.2 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «Об информации, информационных технологиях и о защите информации»

[46] См.: ч.2.ст.3 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных".

[47] См.: ст.22.1 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных"

[48] См.: п. 7.1.2, п.7.2.2. Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100.

прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[49].

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[50].

4.1.41. **Пользователь (потребитель) информации** – 1) субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею; 2) работник ГКУ «КЦСЗН» 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] ГКУ «КЦСЗН» 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 ГКУ «КЦСЗН» 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

---

[49] См.: ч.1.ст. Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «О персональных данных».

[50] См.:
- 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».

[51] В соответствии с:
- разделом VII Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100;
- разделом IV Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

[52] См.:
- п.6.1.2 Политики информационной безопасности в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-99;
- раздела VI. Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109.

[53] См.:
- ч.1 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «О персональных данных»;
- ч.1 ст.16 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «Об информации, информационных технологиях и о защите информации».

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

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 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

---

[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 (ред. от 22.02.2017) «О персональных данных»;
- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «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 (ред. от 20.01.2015).

[57] Полномочия установлены в соответствии с:
- ч.9 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «О персональных данных»;
- ст.11.2, п. «и.1» ст.12 Федерального закона от 03.04.1995 №40-ФЗ (ред. от 06.07.2016) "О Федеральной службе безопасности";
- ст.5 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 (ред. от 18.05.2017).

[58] Полномочия установлены в соответствии с:
- ст.23 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «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 (ред. от 01.07.2016).

[59] См.: 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 (ред. от 22.02.2017) «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).

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, 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

---

[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).

[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 (ред. от 22.02.2017) "О персональных данных";
- Федеральном законе от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «Об информации, информационных технологиях и о 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.

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. **Уполномоченное лицо**- юридическое или физическое лицо, осуществляющее деятельность по гражданско- правовому договору или распорядительному акту вышестоящего органа (организации), и на которое 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),

возложены обязанности по обработке и (или) защите персональных данных.

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

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

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

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

4.2.В настоящем Положении используются следующие сокращения:

---

[67] См.: 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 30.08.2002 № 282.

[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.

4.2.1. **АС**- автоматизированная система;
4.2.2. **ИС**- информационная система;
4.2.3. **ИСПДн**- информационная система персональных данных;
4.2.4. **КЗ**- контролируемая зона;
4.2.5. **КСЗИ**- криптографическое средство защиты информации;
4.2.6. **МНИ**- машинные носители информации;
4.2.7. **МЭ**- межсетевой экран;
4.2.8. **НСД**- несанкционированный доступ;
4.2.9. **оргмеры**- организационные меры защиты персональных данных;
4.2.10. **ПДн**- персональные данные;
4.2.11. **СЗИ**- средства защиты информации;
4.2.12. **СЗИИС**- система защиты информации информационных систем;
4.2.13. **СЭД**- система электронного документооборота;
4.2.14. **Учреждение** - ГКУ «КЦСЗН» Забайкальского края.

V. Объекты и общий замысел защиты информации ГКУ «КЦСЗН» Забайкальского края

5.1. Объектами защиты ГКУ «КЦСЗН» Забайкальского края являются[73]:
5.1.1. информационные ресурсы, содержащие конфиденциальную информацию, а также открытая (общедоступная) информация[74], необходимая для работы ГКУ «КЦСЗН» Забайкальского края, независимо от формы и вида ее представления;
5.1.2. процессы обработки информации в информационных системах ГКУ «КЦСЗН» Забайкальского края, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий 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

[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.:
- ст.7, ч.3 ст.16 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «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).

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 ГКУ «КЦСЗН» Забайкальского края[77];
- информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей[78];
- должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных[79];

---

[75] См.:
- Техническое задание «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.

[76] Исполняется в соответствии с:
- п.6 ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "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.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);
- п.2.8. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282.

[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 раздел X 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 30.08.2002 № 282.

[79] Исполняется в соответствии с:
- п.6) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «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 30.08.2002 № 282;

– 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 информационной системы[81].

5.5. Основополагающим принципом построения системы защиты информации информационных систем ГКУ «КЦСЗН» Забайкальского края является следующее положение: в соответствии с положениями нормативных правовых актов Регуляторов[82] и внутренних распорядительных актов[83] в ГКУ «КЦСЗН» Забайкальского края применяются требования для защиты информации, содержащейся в государственных информационных систем.

– п.6.3. ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью».

[80] Исполняется в соответствии с:

– п.7) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «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.3 Приложения №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 30.08.2002 №282;
– п.ЗИС.3 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п.ЗИС.3Таблицы 1. «Принятые в техническом проекте решения по защите информации Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР.

[81] См.:

– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 2. Паспорт ГИС «АС «АСП». СЗИИС-КЦСЗН.ПС.01-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 3. Паспорт ИСПДн «Зарплата». СЗИИС-КЦСЗН.ПС.02-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 4. Паспорт ИСПДн «Бухгалтерия». СЗИИС-КЦСЗН.ПС.03-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 5. Паспорт ИСПДн «Кадры». СЗИИС-КЦСЗН.ПС.04-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 6. Паспорт ИСПДн «Официальный сайт». СЗИИС-КЦСЗН.ПС.05-ОР.

[82] 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).

[83] См.: п.3 приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-99 «Об утверждении Политики информационной безопасности в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края».

Цели, задачи и принципы обеспечения информационной безопасности в ГКУ «КЦСЗН» Забайкальского края

6.1. Цели обеспечения информационной безопасности в ГКУ «КЦСЗН» 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 (ред. от 07.06.2017) «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 ГКУ «КЦСЗН» 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:

- п.1 и п. 3 ч.1 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «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 ГКУ «КЦСЗН» 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 ГКУ «КЦСЗН» Забайкальского края

6.2.1. Для достижения целей защиты информации, указанных в разделе 6.1 настоящей Политики в ГКУ «КЦСЗН» 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 ГКУ «КЦСЗН» Забайкальского края призвана решать задачи[85]:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управления доступом субъектов доступа к объектам доступа;
- ограничения программной среды;
- защиты машинных носителей информации;
- регистрации событий безопасности;
- антивирусной защиты;
- обнаружения (предотвращения) вторжений;
- контроля (анализа) защищенности информации;
- целостности информационной системы и информации;
- доступность информации;
- защиты технических средств;
- защиты среды виртуализации;
- защиты информационной системы, ее средств, систем связи и передачи данных.

6.3. Принципы обеспечения информационной безопасности в ГКУ «КЦСЗН» Забайкальского края

6.3.1. Политика информационной безопасности в основана на принципах[86]:

---

[84] См.:

- Техническое задание «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.

[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.:

- 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;

- законности[87];
- системности[88];
- комплексности[89];
- непрерывности[90];
- своевременности[91];
- преемственности и непрерывности совершенствования[92];
- разумной достаточности (экономической целесообразности)[93];
- персональной ответственности[94];
- минимизации полномочий[95];
- исключения конфликта интересов[96];
- взаимодействия и сотрудничества[97];
- гибкости системы защиты[98];
- открытости алгоритмов и механизмов защиты[99];
- простоты применения средств защиты[100];
- обоснованности и технической реализуемости[101];
- специализации и профессионализма[102];
- обязательности контроля[103].

6.3.2. Принцип законности информационной безопасности в ГКУ «КЦСЗН» 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.

6.3.3. Принцип системности построения системы защиты информации в

- 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.

[87] См.: п. 6.3.2 настоящей Политики.
[88] См.: п. 6.3.3 настоящей Политики.
[89] См.: п. 6.3.4 настоящей Политики.
[90] См.: п. 6.3.5 настоящей Политики.
[91] См.: п. 6.3.6 настоящей Политики.
[92] См.: п. 6.3.7 настоящей Политики.
[93] См.: п. 6.3.8 настоящей Политики.
[94] См.: п. 6.3.9 настоящей Политики.
[95] См.: п. 6.3.10 настоящей Политики.
[96] См.: п. 6.3.11 настоящей Политики.
[97] См.: п. 6.3.12 настоящей Политики.
[98] См.: п. 6.3.13 настоящей Политики.
[99] См.: п. 6.3.14 настоящей Политики.
[100] См.: п.6.3.15 настоящей Политики.
[101] См.: п. 6.3.16 настоящей Политики.
[102] См.: п. 6.3.17 настоящей Политики.
[103] См.: п. 6.3.18 настоящей Политики.

ГКУ «КЦСЗН» 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 ГКУ «КЦСЗН» Забайкальского края. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационных систем ГКУ «КЦСЗН» 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.

6.3.4. 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, организационными и правовыми мерами.

6.3.5. 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)[104].

6.3.6. 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.

[104] 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).

6.3.7. 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 ГКУ «КЦСЗН» 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.

6.3.8. 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 ГКУ «КЦСЗН» Забайкальского края.

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

6.3.10. 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 должностных регламентов (обязанностей).[105]

6.3.11. Принцип исключения конфликта интересов (разделения функций) предполагает четкое разделение обязанностей работников ГКУ «КЦСЗН» Забайкальского края и исключение ситуаций, когда сфера ответственности работников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что ни один работник ГКУ «КЦСЗН» Забайкальского края не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение работников полномочиями, порождающими конфликт интересов, дает им возможность манипулировать информацией в корыстных целях или с тем, чтобы скрыть проблемы

[105] См.: п.6.2.4 и п.6.2.5. Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными работниками или подразделениями ГКУ «КЦСЗН» Забайкальского края. Необходимо проводить периодические проверки обязанностей, функций и деятельности 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 работниками.

6.3.12. Принцип взаимодействия и сотрудничества предполагает создание благоприятной атмосферы в коллективах структурных подразделений ГКУ «КЦСЗН» Забайкальского края. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие деятельности лицам, ответственным за безопасность информации[106].

6.3.13. Принцип гибкости системы защиты заключается в том, что система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления ГКУ «КЦСЗН» Забайкальского края своей деятельности. В число таких изменений входят:

- изменения организационной и штатной структуры ГКУ «КЦСЗН» 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.

6.3.14. 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[107].

6.3.15. Принцип простоты применения средств защиты заключается в том, что механизмы и методы защиты должны быть понятны и просты в

[106] См.: п.3 и п.4 приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103 «Об утверждении Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края».

[107] См.: Приложение №1 к Положению о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденному приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100.

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.

6.3.16. 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[108]) и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности информации.

6.3.17. 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 ГКУ «КЦСЗН» Забайкальского края [109] или уполномоченными лицами[110]).

6.3.18. Принцип обязательности контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения

---

[108] 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).

[109] Во исполнение :

- 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 30.08.2002 № 282.

[110] 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).

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 ГКУ «КЦСЗН» Забайкальского края

7.1. Организация информационной безопасности в ГКУ «КЦСЗН» Забайкальского края

Организация информационной безопасности в ГКУ «КЦСЗН» Забайкальского края заключается в:

- определении лиц, ответственных за организацию и поддержание информационной безопасности в ГКУ «КЦСЗН» Забайкальского края;
- регламентации оборота конфиденциальной информации на бумажных и электронных носителях;
- построении, аттестации и вводе в эксплуатацию системы защиты информационных систем;
- обучении пользователей по вопросам информационной безопасности[111].

7.1.1. Лица, ответственные за организацию и поддержание информационной безопасности в ГКУ «КЦСЗН» Забайкальского края

7.1.1.1. Директор ГКУ «КЦСЗН» Забайкальского края как первый руководитель несет персональную ответственность за регламентацию порядка безопасной обработки конфиденциальной информации и обеспечение требований по технической защите конфиденциальной информации[112].

---

[111] См.: п.13.4.4 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

[112] В соответствии с:

- п.2.18 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п.5.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

7.1.1.2. Начальник отдела автоматизации, на который возложены функции по обеспечению информационной безопасности[113], несет ответственность за контроль поддержания уровня защищенности информационных систем ГКУ «КЦСЗН» Забайкальского края.

7.1.1.3. Администратор безопасности информации[114], или уполномоченное лицо[115] 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[116].

---

[113] См.:

- п/п б) 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.3 приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103 «Об утверждении Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края».

[114] 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 30.08.2002 № 282;
- п.13 Требований о защите информации, содержащейся в информационных системах общего пользования, утвержденных приказом ФСБ России, ФСТЭК России от 31.08.2010 №489.

В ГКУ «КЦСЗН» Забайкальского края в настоящее время обязанности администратора безопасности информации возложены на начальника отдела автоматизации. При необходимости обязанности администратора безопасности информации могут быть возложены и на иного работника. Поэтому функции, обязанности и ответственность администратора безопасности информации в настоящей Политике отделены от функций, обязанностей и ответственности начальника отдела автоматизации.

[115] 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).

[116] 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 30.08.2002 № 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 об администраторе информационной системы Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-104.

7.1.1.4. Системные администраторы (администраторы информационных систем)[117] несут ответственность за поддержание уровня защищенности информационных систем ГКУ «КЦСЗН» Забайкальского края.

7.1.1.5. Лицо, ответственное за организацию обработки персональных данных,[118] несет ответственность за:

- осуществление внутреннего контроля за соблюдением работниками законодательства Российской Федерации о защите персональных данных, в том числе требований к защите персональных данных[119];
- доведение до сведения работников ГКУ «КЦСЗН» Забайкальского края положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных[120];
- 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[121];
- осуществление контроля организации допуска работников ГКУ «КЦСЗН» Забайкальского края к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности[122].

---

[117] См.:п.3 приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103 «Об утверждении Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края».

[118] В соответствии с:

- ч.4 ст.22.1 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "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 (ред. от 06.09.2014);
- п.3 приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-102 «Об утверждении Положения об ответственном за организацию обработки персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края».

[119] Осуществляется в соответствии с:

- п.4) ч.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных";
- разделом IX Политики в отношении обработки персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-101;
- Планом проведения периодических проверок условий обработки персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденным приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-124.

[120] В соответствии с п.6) ч.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных".

[121] См.: ст.22.1 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «О персональных данных».

[122] См.: п.7.1.2 и п. 7.2.2 Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100.

7.1.2. Регламентация оборота конфиденциальной информации на бумажных и электронных носителях в ГКУ «КЦСЗН» Забайкальского края

7.1.2.1. В ГКУ «КЦСЗН» Забайкальского края оборот конфиденциальной информации на бумажных носителях регламентирован требованиями следующих внутренних организационно-распорядительных актов:

- Политики информационной безопасности в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-99;
- Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100;
- разделом 6.6 Политики в отношении обработки персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-101;
- Положения об архиве Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-119;
- Положения о Постоянно действующей экспертной комиссии Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-120;
- Инструкции по обеспечению физической защиты помещений контролируемой зоны Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-115;
- приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-121 «О регистрации обращений граждан в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края»;
- приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-122 «Об утверждении сроков и мест хранения материальных носителей персональных данных в

Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края».

7.1.2.2. В ГКУ «КЦСЗН» Забайкальского края оборот конфиденциальной информации на электронных носителях регламентирован требованиями следующих внутренними организационно-распорядительных актов[123]:

- Политики информационной безопасности в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-99;
- Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105;
- Положения о порядке организации и проведении работ по защите конфиденциальной информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-106;
- приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-107 «О контролируемой зоне Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108;
- Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109;
- Инструкции по учету, маркировке, очистке и утилизации

[123] Во исполнение п.7 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных Постановлением Правительства РФ от 06.07.2015 №676 (ред. от 14.11.2015).

машинных носителей информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-110;

- Инструкции по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования, утвержденной приказом Забайкальского края от 17.07.2017 №01-111;
- Регламента безопасного функционирования подсистемы криптографической защиты информации СЗИИС Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-112;
- Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113;
- Инструкции по организации парольной защиты информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-114;
- Инструкции по внесению изменений в конфигурацию информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-116;
- Инструкции о порядке действий в нештатных ситуациях в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-117;
- Инструкции по резервному копированию информационных ресурсов информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-118;
- Инструкции по обеспечению физической защиты помещений контролируемой зоны Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-115;

- Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100;
- Политики в отношении обработки персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-101;
- приказа ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-122 «Об утверждении сроков и мест хранения материальных носителей персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края».

7.1.3. Система защиты информации информационных систем в ГКУ «КЦСЗН» Забайкальского края

7.1.3.1. Система защиты информации информационных систем[124] в ГКУ «КЦСЗН» Забайкальского края должна строиться на основании применения правовых[125], организационных[126] и технических[127] 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 ГКУ «КЦСЗН» Забайкальского края. На основании анализа актуальных угроз безопасности информации, описанного в Модели угроз[128], сделано заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности защищаемой информации. Выбранные необходимые технические мероприятия отражены в Техническом проекте[129] и в

---

[124] См.:
- п.3) ч.1. ст.18.1 , ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «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).

[125] См.: п.4.1.41 настоящей Политики.

[126] См.: п.4.1.34 настоящей Политики

[127] См.: п.4.1.48 настоящей Политики

[128] См.: Техническое задание «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края».

[129] См.: Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.

Плане мероприятий по защите информации информационных систем[130].

7.1.3.3. Для каждой информационной системы в разработанном Паспорте информационной системы[131] составлен список используемых технических средств защиты, а так же 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[132] 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[133].

---

[130] См.: План проведения периодических проверок условий обработки персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденный приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-124.

[131] См.:

- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 2. Паспорт ГИС «АС «АСП» . СЗИИС-КЦСЗН.ПС.01-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 3. Паспорт ИСПДн «Зарплата». СЗИИС-КЦСЗН.ПС.02-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 4. Паспорт ИСПДн «Бухгалтерия». СЗИИС-КЦСЗН.ПС.03-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 5. Паспорт ИСПДн «Кадры». СЗИИС-КЦСЗН.ПС.04-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 6. Паспорт ИСПДн «Официальный сайт». СЗИИС-КЦСЗН.ПС.05-ОР.

[132] См.:

- ч.3 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «О персональных данных»;
- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «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).

[133] 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

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[134]:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных [135].

7.1.3.6. Список используемых технических средств отражается в Техническом проекте на создание системы защиты информации информационных систем[136]. Список используемых средств должен

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).

[134] 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).

[135] См.: Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.

[136] См.:

- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 2. Паспорт ГИС «АС «АСП» . СЗИИС-КЦСЗН.ПС.01-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 3. Паспорт ИСПДн «Зарплата». СЗИИС-КЦСЗН.ПС.02-ОР;

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[137].

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, 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

- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 4. Паспорт ИСПДн «Бухгалтерия». СЗИИС-КЦСЗН.ПС.03-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 5. Паспорт ИСПДн «Кадры». СЗИИС-КЦСЗН.ПС.04-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 6. Паспорт ИСПДн «Официальный сайт». СЗИИС-КЦСЗН.ПС.05-ОР.

[137] Исполняется в соответствии с п.5.4.2. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282, а также п.5. Приложения 2 к указанным Специальным требованиям.

который возложены обязанности по защите информации) или иным образом обучены правилам обращения с конфиденциальной информацией и средствами защиты информации[138].

7.2. Инфраструктура информационной безопасности в ГКУ «КЦСЗН» Забайкальского края

Инфраструктура информационной безопасности заключается в[139]:

- определении ролей и обязанностей должностных лиц по обеспечению информационной безопасности[140];
- регулярной проверке согласованности мер защиты информации[141];
- обработке инцидентов, связанных с нарушением безопасности[142].

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

7.2.1.1. В Техническом проекте определены следующие категории лиц,

[138] 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 (ред. от 22.02.2017) "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;
- п.5.2 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109;
- п.6.2.6, п.7.3. Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105;
- п.5.6. Регламента безопасного функционирования подсистемы криптографической защиты информации СЗИИС Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-112.

[139] 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.

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

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

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

допущенных к работе в информационных системах ГКУ «КЦСЗН» Забайкальского края[143]:

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

7.2.1.2. В Паспорте информационной системы указанного Технического проекта разработаны матрицы доступа[144] 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 Положении о разрешительной системе допуска пользователей к информационным системам ГКУ «КЦСЗН» Забайкальского края [145].

7.2.1.4. Администратор информационной системы:

7.2.1.4.1. Администратор информационной системы – должностное лицо ГКУ «КЦСЗН» Забайкальского края или уполномоченное лицо (сотрудник уполномоченного лица)[146], ответственное за настройку, внедрение и сопровождение информационных

---

[143] См.:

- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 2. Паспорт ГИС «АС «АСП» . СЗИИС-КЦСЗН.ПС.01-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 3. Паспорт ИСПДн «Зарплата». СЗИИС-КЦСЗН.ПС.02-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 4. Паспорт ИСПДн «Бухгалтерия». СЗИИС-КЦСЗН.ПС.03-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 5. Паспорт ИСПДн «Кадры». СЗИИС-КЦСЗН.ПС.04-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 6. Паспорт ИСПДн «Официальный сайт». СЗИИС-КЦСЗН.ПС.05-ОР.

В данном случае речь идет не о конкретных должностях, а о ролях при осуществлении прав доступа к защищаемым ресурсам. Поэтому начальник отдела автоматизации как руководитель подразделения, ответственного за безопасность информации в информационных системах Учреждения, наделяется правами администратора безопасности информации, а как начальник отдела автоматизации как такового наделяется правами администратора ИС.

[144] 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 30.08.2002 № 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).

[145] См.: раздел VII Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

[146] Осуществляющее свои функциональные обязанности по гражданско - правовому договору, заключенному в соответствии с ч.3 ст.6 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «О персональных данных».

систем. 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 ГКУ «КЦСЗН» Забайкальского края или уполномоченное лицо (сотрудник уполномоченного лица)[147], 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;

[147] 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).

- устанавливать доверительные отношения своей защищенной сети с сетями других органов власти и организаций.

7.2.1.6. Пользователь:

7.2.1.6.1. Пользователь[148] - должностное лицо ГКУ «КЦСЗН» Забайкальского края или иного государственного (муниципального) органа (организации), допущенный в установленном порядке к работе с защищаемой информацией[149], полномочия которого регламентированы внутренними организационно - распорядительными актами[150] ГКУ «КЦСЗН» 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 обязанностях лиц, допущенных к работе в ИС.

7.2.2. Регулярная проверка согласованности мер защиты информации

7.2.2.1. В ГКУ «КЦСЗН» Забайкальского края должны проводиться следующие мероприятия по проверке согласованности мер защиты информации:

- поддержание в актуальном состоянии организационных

---

[148] См.: определение в п.4.1.40 настоящей Политики.

[149] В соответствии с:

- разделом VII Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100;
- разделом IV Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

[150] См.:

- п.3.2.1 Политики информационной безопасности в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-99;
- разд. VI Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109.

мер защиты информации[151];
- контроль неизменности защищаемой инфраструктуры[152];
- контроль работоспособности средств защиты информации[153];
- выявление и анализ уязвимостей ИС[154].

7.2.3. Обработка инцидентов, связанных с нарушением безопасности информации[155]

7.2.3.1. В ГКУ «КЦСЗН» 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;
- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их

[151] См.: п.8.5 и п.8.6. Положения о порядке организации и проведении работ по защите конфиденциальной информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-106.

[152] См.:п.6.2.4 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[153] См.: п.6.4.2 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[154] 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 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608)

[155] 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 Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

последствий[156];

- 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, 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.

VIII. Безопасность аппаратно-программного обеспечения в ГКУ «КЦСЗН» Забайкальского края

Безопасность аппаратно- программного обеспечения в ГКУ «КЦСЗН» Забайкальского края должна достигаться проведением следующих мероприятий:

- идентификацией и аутентификацией субъектов доступа[157];
- управлением доступом субъектов доступа к объектам доступа[158];
- мониторингом (просмотром, анализом) результатов регистрации событий безопасности и реагирование на них[159];
- уничтожением (стиранием) данных и остаточной информации с машинных носителей информации и (или) уничтожением машинных носителей информации[160];
- антивирусной защитой[161];
- обеспечением безопасности персональных компьютеров[162];
- обеспечением безопасности среды виртуализации;[163]
- регламентацией и контролем использования в информационной системе мобильных технических средств[164]
- установкой (инсталляцией) только разрешенного к использованию программного обеспечения и (или) его компонентов[165].

8.1.Идентификация и аутентификация субъектов доступа

[156] См.: п.13.4.2 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.
[157] См.: п.8.1 настоящей Политики.
[158] См.: п.8.2 настоящей Политики.
[159] См.: п.8.3 настоящей Политики.
[160] См.: п.8.4 настоящей Политики.
[161] См.: п.8.5 настоящей Политики.
[162] См.: п.8.6 настоящей Политики.
[163] См.: п.8.7 настоящей Политики.
[164] См.: п.8.8 настоящей Политики.
[165] См.: п.8.9 настоящей Политики.

8.1.1. Меры по идентификации и аутентификации субъектов доступа и объектов доступа в информационные системы ГКУ «КЦСЗН» 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)[166].

8.1.2. При идентификации и аутентификации субъектов доступа и объектов доступа в ИС ГКУ «КЦСЗН» Забайкальского края должны проводиться следующие мероприятия:

8.1.2.1. реализуемые встроенными в СЗИ Dallas Lock 8.0-К средствами идентификация и аутентификация пользователей, являющихся работниками оператора[167];

8.1.2.2. реализуемые криптографическими механизмами ПАК «ViPNet Custom 4.0» идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных[168];

---

[166] 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);
- 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).

[167] См.:

- п. ИАФ.1 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.1 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. ИАФ.1 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.3.1. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[168] Применяется только для ГИС «АС «АСП». 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 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. ИАФ.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;

8.1.2.3. реализуемое администратором безопасности информации при помощи средств управления СЗИ управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов[169];

8.1.2.4. реализуемое администратором безопасности информации при помощи средств управления СЗИ управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации[170];

8.1.2.5. защита обратной связи при вводе аутентификационной информации, реализуемая встроенными в СЗИ Dallas Lock 8.0-К[171];

– п.9.3.2. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[169] См.:

– п. ИАФ.3 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.3 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. ИАФ.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.9.3.3. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103;
– п.6.1.5.2.1. Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[170] См.:

– п. ИАФ.4 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.4 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. ИАФ.4 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.9.3.4. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[171] См.:

– п. ИАФ.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. ИАФ.5 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. ИАФ.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;

8.1.2.6. реализуемые встроенными в СЗИ Dallas Lock 8.0-К идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)[172].

8.2. Управление доступом субъектов доступа к объектам доступа

8.2.1. Меры по управлению доступом субъектов доступа к объектам доступа в информационные системы ГКУ «КЦСЗН» 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[173].

8.2.2. При управлении доступом субъектов доступа к объектам доступа в информационные системы ГКУ «КЦСЗН» Забайкальского края должны проводиться следующие мероприятия:

8.2.2.1. реализуемое администратором безопасности информации при помощи средств управления СЗИ управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей[174];

– п.9.3.5. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[172] Применяется только для ГИС «АС «АСП. См.:

– п. ИАФ.6 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.6 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. ИАФ.6 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.9.3.6. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[173] 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);
– п.2.3, п.3.2, п. методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014).

[174] См.:

– п. УПД.1 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.1 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. УПД.1 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного

8.2.2.2. реализация средствами СЗИ Dallas Lock 8.0-К на основании матрицы доступа необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) правил разграничения доступа[175];

8.2.2.3. управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами, реализуемые межсетевым экранированием ПО ViPNet Client 4 (КС2)[176];

8.2.2.4. разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы[177];

казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;

- п.9.4.1. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[175] См.:

- п. УПД.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. УПД.2 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.2 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.4.2. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[176] Применяется только для ГИС «АС «АСП». См.:

- п. УПД.3 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.3 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.4.3. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[177] См:

- п. УПД.4 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.4 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.4 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного

8.2.2.5. назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы, реализуемое администратором безопасности информации разграничительными механизмами СЗИ Dallas Lock 8.0-К на основании матрицы доступа[178];

8.2.2.6. ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе), реализуемое администратором безопасности информации разграничительными механизмами СЗИ Dallas Lock 8.0-К на основании матрицы доступа[179];

8.2.2.7. ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы, реализуемое администратором безопасности информации разграничительными механизмами СЗИ Dallas Lock 8.0-К [180];

казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;

- п.9.4.4. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[178] 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 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.4.5. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[179] См:

- п. УПД.6 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.6 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.6 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.4.6. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[180] Применяется только для ГИС «АС «АСП». См.:

- п. УПД.9 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);

8.2.2.8. реализуемое средствами ОС Windows блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу[181];

8.2.2.9. запрет любых действий пользователей до аутентификации в СЗИ Dallas Lock 8.0-К [182];

8.2.2.10. реализация путем создания защищенных каналов связи средствами ПАК «ViPNet Custom 4.0» защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно телекоммуникационные сети[183];

– п. УПД.9 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. УПД.9 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.9.4.7. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[181] См:
– п. УПД.10 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.10 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. УПД.10 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.9.4.8. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[182] См:
– п. УПД.11 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.11 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. УПД.11 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.9.4.9. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[183] См.:
– п. УПД.13 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.13 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. УПД.13 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного

8.2.2.11. регламентация и контроль использования в информационной системе технологий беспроводного доступа, заключающихся в применении одинакового набора средств защиты информации для всех узлов независимо от каналов связи[184];

8.2.2.12. регламентация и контроль использования в информационной системе мобильных технических средств, заключающихся в применении одинакового набора средств защиты информации для всех узлов независимо от каналов связи[185];

8.2.2.13. управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)[186];

казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;

- п.9.4.10. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[184] См:

- п. УПД.14 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.14 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.14 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.4.11. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[185] См:

- п. УПД.15 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.15 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.15 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.4.12. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[186] См.:

- п. УПД.16 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.16 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.16 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;

8.2.2.14. обеспечение доверенной загрузки средств вычислительной техники[187].

8.3. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

8.3.1. Мониторинг результатов регистрации событий безопасности должен проводиться в форме анализа системных журналов[188] и журналов СЗИ, проводимого администратором безопасности информации с целью своевременного выявления факта попыток несанкционированного доступа к информационным ресурсам в информационные системы ГКУ «КЦСЗН» Забайкальского края[189].

8.3.2. Анализ журналов должен производиться ежедневно[190].

– п.9.4.13. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[187] См.:

– п. УПД.17 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.17 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. УПД.17 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.9.4.14. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[188] См.: п.А.10.10 ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования.

[189] 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 30.08.2002 № 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;
– п. 8.7 Положения об администраторе информационной системы Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-104.

[190] В соответствии с пунктом 15 Требований к защите персональных данных для обеспечения 2 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 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

8.3.3. При анализе журналов СЗИ НСД проверяются:

- журналы контроля целостности программных частей СЗИ[191];
- журналы контроля целостности программного обеспечения ИС[192];
- журналы доступа пользователей и процессов к защищаемым объектам[193];
- журналы создания новых пользователей в СЗИ и изменения полномочий пользователей[194].

8.4. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации

8.4.1. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации в ГКУ «КЦСЗН» Забайкальского края должно производиться при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения[195].

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

[191] 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 30.08.2002 № 282.

[192] 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 30.08.2002 № 282.

[193] 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 30.08.2002 № 282.

[194] 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.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 30.08.2002 № 282.

[195] См.:

- 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), а также п. ЗНИ.8 Приложения №2 к указанным Требованиям;
- п. ЗНИ.8 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. ЗНИ.8 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- разд.7.3 Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-110;

8.4.2. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, в установленном порядке должно осуществляться физическое уничтожение этих машинных носителей информации.[196]

8.5. Антивирусная защита в информационных системах ГКУ «КЦСЗН» Забайкальского края

8.5.1. Безопасность аппаратно- программного обеспечения в ГКУ «КЦСЗН» Забайкальского края от разрушающего воздействия компьютерных вирусов достигается также проведением мероприятий по антивирусной защите[197], основанных на следующих принципах:

8.5.1.1. Контроль состояния антивирусной защиты ИС ГКУ «КЦСЗН» Забайкальского края возлагается на администратора безопасности информации[198] или уполномоченное лицо[199].

8.5.1.2. К использованию в ИС допускаются только сертифицированные и (или) лицензионные[200] антивирусные средства, централизованно

– раздел 8.2 Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100.

[196] См.:
– 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), а также п. ЗНИ.8 Приложения №2 к указанным Требованиям;
– п. ЗНИ.8 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. ЗНИ.8 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР.;
– раздел 7.3 Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-110;
– раздел 8.2 Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100.

[197] 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.

[198] Выполняется в соответствии с п.5.5 Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[199] 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).

[200] См.: п.4.6.11, п.4.7.5 Регламента работы в корпоративной сети передачи данных Министерства труда и

закупленные у разработчиков (или официальных поставщиков) указанных средств[201].

8.5.1.3. В ГКУ «КЦСЗН» Забайкальского края ежедневно в начале работы при загрузке компьютеров в автоматическом режиме обязан проводиться автоматический контроль всех дисков и файлов[202].

8.5.1.4. Должно обеспечиваться автоматическое централизованное обновление вирусных сигнатур и антивирусного ПО на всех ПЭВМ, работающих в ИС[203].

социальной защиты населения Забайкальского края и ее локальных сегментах, утвержденного приказом Министерства труда и социальной защиты населения Забайкальского края от 31.05.2017 №947.

[201] Исполняется в соответствии с:

- п.3) ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных";
- п. в) ст.1 Указа Президента Российской Федерации от 17.03.2008 №351(ред. от 22.05.2015) «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 №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 30.08.2002 № 282;
- п.5.2. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[202] См.:

- п.5.3.1. Регламента работы в корпоративной сети передачи данных Министерства труда и социальной защиты населения Забайкальского края и ее локальных сегментах, утвержденного приказом Министерства труда и социальной защиты населения Забайкальского края от 31.05.2017 №947;
- п.6.1. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[203] 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);
- Приложением А ГОСТ Р 51188-98. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство;
- п. АВЗ.2 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. АВЗ.2. Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.6.2. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113;

8.5.1.5. 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.)[204].

8.5.1.6. Разархивирование и контроль входящей информации обязан проводиться непосредственно после ее приема на выделенном автономном компьютере или на любом другом компьютере[205]. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающей аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный машинный носитель информации)[206].

8.5.1.7. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль[207]. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

8.5.1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов[208].

– п.6.1.3.1 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108;
– п.9.8.2 Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[204] См.п.6.3. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[205] При условии начальной загрузки ОС в оперативную память компьютера с системной дискеты, заведомо «чистой» (не зараженной вирусами) и защищенной от записи.

[206] См.: п.6.3. и п. 6.4 Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[207] 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);
– п. ЗИС.15 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п. ЗИС.15 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– п.6.4. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[208] В соответствии с:
– разделы 6.2.2. и 6.2.5 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108;
– п. 6.5. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

8.6. Обеспечение безопасности персональных компьютеров ГКУ «КЦСЗН» Забайкальского края

8.6.1. Безопасность персональных компьютеров в ГКУ «КЦСЗН» Забайкальского края должна достигаться осуществлением мер физического и логического контроля доступа.

8.6.2. Меры физического контроля доступа к средствам вычислительной техники (физическая защита) регламентируются нормативными правовыми актами Регуляторов[209] и внутренними организационно - распорядительными актами[210].

8.6.3. Политика в отношении логического доступа к компьютерам заключается в:

- установлении правил разграничения доступа и контроля соблюдения этих правил [211];
- контроле доступа пользователей к СВТ информационной системы с целью предотвращения неавторизованного доступа к информационным системам (контроле регистрации пользователей[212],

---

[209] См.:

- подпункт а) п.5 Состава и содержания организационных и технических мер по обес-печению 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);
- п.ЗТС.3 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.ЗТС.3 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п.ЗТС.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР.

[210] См.: Инструкцию по обеспечению физической защиты помещений контролируемой зоны Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденную приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-115.

[211] 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 раздел II Приложения №2 к указанным Требованиям;
- п.А.11. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.7.1.1, п.8.6. Положения о порядке организации и проведении работ по защите конфиденциальной информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-106.

[212] 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);

управлении привилегиями доступа[213], контроле в отношении паролей пользователей[214], пересмотре прав доступа пользователей[215]

- п.5.1.3, п.5.9.2, п.6.3.9, п.6.3.15 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п. А.11.2.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения без-опасности. Системы менеджмента информационной безопасности. Требования;
- п.6.1.1.3, п.6.1.5.2 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[213] 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), а также п. УПД.5 Приложения №2 к указанным Требованиям;
- п.5.7.5, п. 5.7.6, п.5.9.2 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п.А.11.2.2. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.6.4.2.5 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[214] 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), а также п. АН3.5 Приложения №2 к указанным Требованиям;
- п.5.4.2, п.5.7.7. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п. А.11.2.3 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.6.4.2.5 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108;
- п.6.16 Инструкции по организации парольной защиты информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-114.

[215] 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), а также п. АН3.5 Приложения №2 к указанным Требованиям;
- п. АН3.5 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. АН3.5 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.5.4.2, п.5.7.7. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п. А.11.2.3 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- п.6.4.2.5 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108;

и др.).

8.7. Обеспечение безопасности среды виртуализации

8.7.1. Для обеспечения безопасности виртуальной среды должны применяться меры защиты аналогичные применяемым в физической среде, но с учетом специфических особенностей виртуальной среды, а именно[216]:

- идентификация и аутентификация субъектов доступа как внутри виртуальной среды, так и при доступе к средствам управления виртуальной инфраструктурой;
- управления доступом субъектов доступа к объектам доступа внутри виртуальной среды и при доступе к средствам управления этой средой;
- управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;
- регистрация событий безопасности в виртуальной инфраструктуре;
- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;
- контроль целостности виртуальной инфраструктуры и ее конфигураций;
- резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;
- реализация и управление антивирусной защитой в виртуальной инфраструктуре;
- разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

8.8. Регламентация и контроль использования в информационной системе мобильных технических средств

- п.6.16 Инструкции по организации парольной защиты информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-114.

[216] Исполняется в соответствии с:

- п. ЗСВ.1 – п. ЗСВ.4, п. ЗСВ.6- п. ЗСВ.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);
- 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 безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

8.8.1. В ГКУ «КЦСЗН» Забайкальского края допускается использование мобильных технических средств в составе ИС только в порядке, регламентированном нормативно- правовыми, внутренними организационно- распорядительными актами и технической документацией на СЗИИС[217]. При этом данные технические средства должны быть оснащены сертифицированными средствами защиты информации[218], применяемыми в ГКУ «КЦСЗН» Забайкальского края и обеспечивающими необходимый уровень защиты, определенный проектной документацией СЗИИС[219].

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

8.9.1. В связи с тем, что ГИС «АС «АСП» относится к первому уровню защиты персональных данных, то ГКУ «КЦСЗН» Забайкальского края

---

[217] Исполняется с целью обеспечения требований:
- п. 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 Минюсте России 31.05.2013 №28608);
- п. УПД.15 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. УПД.15 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР.

[218] Исполняется в соответствии с:
- п.3) ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных";
- п. в) ст.1 Указа Президента Российской Федерации от 17.03.2008 №351(ред. от 22.05.2015) «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 №17 (Зарегистрировано в Минюсте России 31.05.2013 №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 30.08.2002 № 282;
- п.5.2, п.5.3. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[219] См.:
- Техническое задание «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.

должно выполнять требование Регуляторов по установке (инсталляции) только разрешенного к использованию программного обеспечения и (или) его компонентов[220]. К информационным системам, не относящимся к первому уровню защиты персональных данных такое категоричное требование Регуляторами не выдвигается, но при этом внутренними организационно- распорядительными актами ГКУ «КЦСЗН» Забайкальского края[221] определено, что пользователи не могут самостоятельно устанавливать, удалять или изменять программное обеспечение на компьютере, изменять аппаратную конфигурацию компьютеров.

IX. Телекоммуникационная безопасность ГКУ «КЦСЗН» Забайкальского края

С целью защиты как внутренних, так и внешних сетевых сервисов в ГКУ «КЦСЗН» Забайкальского края должны осуществляться контроль сетевого доступа, для обеспечения которого при необходимости определяются:

- политика в отношении использования сетевых служб[222];
- предопределенный маршрут[223];
- аутентификация пользователей в случае внешних соединений[224];
- принципы разделения в сетях[225];
- контроль сетевых соединений[226];
- управление маршрутизацией сети[227];
- безопасность использования сетевых служб[228];
- политика в отношении электронной почты[229].

---

[220] См.:

- п. ОПС.3Приложения №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.3 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. ОПС.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- п.9.5.3. Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[221] См.: разд.6.3.3 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[222] См.: п.9.1 настоящей Политики.

[223] См.: п.9.2 настоящей Политики.

[224] См.: п.9.3 настоящей Политики.

[225] См.: п.9.4 настоящей Политики.

[226] См.: п.9.5 настоящей Политики.

[227] См.: п.9.6 настоящей Политики.

[228] См.: п.9.7 настоящей Политики.

[229] См.: п.9.8 настоящей Политики.

9.1. Политика в отношении использования сетевых служб[230]

9.1.1. В ГКУ «КЦСЗН» Забайкальского края установлен разрешительный режим доступа к сетевым службам[231].

9.1.2. В связи с тем, что несанкционированные подключения к сетевым службам могут нарушать информационную безопасность ГКУ «КЦСЗН» Забайкальского края, пользователям должен обеспечиваться непосредственный доступ только к тем сервисам, в которых они были авторизованы[232].

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. Предопределенный маршрут[233]

9.2.1. Выбор предопределенного маршрута состоит в том, чтобы исключить выбор пользователями иных маршрутов, кроме маршрута между пользовательским терминалом и сервисами, по которому пользователь авторизован осуществлять доступ[234].

9.2.2. Выбор предопределенного маршрута заключается в ограничении вариантов маршрутизации в каждой точке сети посредством[235]:

- распределения выделенных линий или номеров телефона;

---

[230] См.: п. А.11.4.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[231] См.:

- п. 5.4.2 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения;
- п.5.1 Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

[232] Исполняется в соответствии с:

- п.5.1.3 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- п. А.11.4.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- разд.VII Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

[233] См.: п. А.11.4.7 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[234] См.: п. п.9.4.2 ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью».

[235] См.п.2.3 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014)

- автоматического подключения портов к определенным системным приложениям или шлюзам безопасности;
- ограничения опций меню и подменю для индивидуальных пользователей;
- предотвращения неограниченного сетевого роуминга;
- использования определенных прикладных систем и/или шлюзов безопасности для внешних пользователей сети;
- активного контроля разрешенного источника с целью направления соединения через шлюзы безопасности, например, межсетевые экраны;
- ограничения доступа к сети посредством создания отдельных логических доменов, например, виртуальных частных сетей для пользовательских групп в пределах ГКУ «КЦСЗН» Забайкальского края.

9.3. Аутентификация узлов в случае внешних соединений[236]

9.3.1. Аутентификация узлов в случае внешних соединений в ГКУ «КЦСЗН» Забайкальского края должна достигаться средствами криптографии[237].

9.4. Принцип разделения в сетях[238]

---

[236] См.: п.А.11.4.2 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[237] См.:

- п. б) ст.1 Указа Президента РФ от 17.03.2008 №351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";
- п.5.1.1., п.5.1.3, п.5.2.5, п.5.3.5, п.5.8.5 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- приказ ФАПСИ РФ 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 6 августа 2001 г. № 2848) // Бюллетень нормативных актов федеральных органов исполнительной власти, 2001. – № 34;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 2. Паспорт ГИС «АС «АСП» . СЗИИС-КЦСЗН.ПС.01-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 3. Паспорт ИСПДн «Зарплата». СЗИИС-КЦСЗН.ПС.02-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 4. Паспорт ИСПДн «Бухгалтерия». СЗИИС-КЦСЗН.ПС.03-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 5. Паспорт ИСПДн «Кадры». СЗИИС-КЦСЗН.ПС.04-ОР;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 6. Паспорт ИСПДн «Официальный сайт». СЗИИС-КЦСЗН.ПС.05-ОР.

[238] См.: п. А.11.4.5 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

9.4.1. В ГКУ «КЦСЗН» Забайкальского края по управлению информационной безопасностью в пределах сети должны разделяться группы информационных сервисов, пользователей и информационные системы.

9.4.2. Критерии для разделения сетей на домены формируются на основе анализа политики контроля доступа, а также учитывая влияние этого разделения на производительность в результате включения подходящей технологии маршрутизации сетей или шлюзов.

9.5. Контроль сетевых соединений[239]

9.5.1. В ГКУ «КЦСЗН» Забайкальского края для контроля сетевого доступа должны применяться мероприятия по управлению информационной безопасностью, чтобы ограничивать возможности пользователей по подсоединению. Такие мероприятия могут быть реализованы посредством сетевых шлюзов, которые фильтруют трафик с помощью определенных таблиц или правил. Применяемые ограничения должны основываться на политике и требованиях доступа к бизнес-приложениям, а также соответствующим образом поддерживаться и обновляться.

9.5.2. Ограничения должны применяться к следующим бизнес приложениям:

- электронная почта;
- передача файлов в одном направлении;
- передача файла в обоих направлениях;
- интерактивный доступ;
- доступ к сети, ограниченный определенным временем суток или датой.

9.6. Управление маршрутизацией сети[240]

9.6.1. В ГКУ «КЦСЗН» Забайкальского края для обеспечения информационной безопасности при осуществлении маршрутизации должен осуществляться контроль адресов источника и назначения сообщения. Преобразование сетевых адресов осуществляется для изоляции сетей и предотвращения распространения маршрутов от сети одного подразделения ГКУ «КЦСЗН» Забайкальского края в сеть другого.

9.7. Безопасность использования сетевых служб[241]

---

[239] См.: п. А.11.4.6 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[240] См.: п. А.11.4.7 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[241] См.: п. А.11.4.6. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

9.7.1. Безопасность использования сетевых служб в ГКУ «КЦСЗН» Забайкальского края должна достигаться использованием только сертифицированных средств защиты информации, централизованно закупленных у разработчиков (или официальных поставщиков) указанных средств[242].

9.8. Политика в отношении электронной почты[243]

9.8.1. В ГКУ «КЦСЗН» Забайкальского края для обеспечения информационной безопасности должны быть регламентированы

[242] Исполняется в соответствии с:
- п.3) ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "О персональных данных";
- 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 №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 30.08.2002 № 282;
- п.5.2. Инструкции по организации антивирусной защиты в информационных системах ГКУ «КЦСЗН» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-113.

[243] См.:
- Указом Президента РФ от 17.03.2008 №351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена";
- п. ОЦЛ.4Приложения №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.5.7.1,п.6.3.5, п.6.3.9, п.6.3.11.1- п.6.3.11.2, п.6.3.11.5, п.6.3.13, п.6.3.16 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282;
- разд. 3.9 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п. ОЦЛ.4 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. ОЦЛ.4 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
- разд. VI и VII Инструкции по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования, утвержденной приказом Забайкальского края от 17.07.2017 №01-111;
- п.9.11.3 Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

правила использования электронной почты[244], предусматривающие следующие аспекты:

- вероятность атаки на электронную почту (вирусы, перехват);
- защиту вложений в сообщения электронной почты;
- данные, при передаче которых не следует пользоваться электронной почтой;
- исключение возможности компрометации ГКУ «КЦСЗН» Забайкальского края со стороны работников, например, путем рассылки дискредитирующих и оскорбительных сообщений, использование корпоративной электронной почты с целью неавторизованных покупок;
- использование криптографических методов для защиты конфиденциальности и целостности электронных сообщений;
- хранение сообщений, которые, в этом случае, могли бы быть использованы в случае судебных разбирательств;
- дополнительные меры контроля обмена сообщениями, которые не могут быть аутентифицированы.

X. Физическая безопасность в ГКУ «КЦСЗН» Забайкальского края[245]

10.1. Физическая безопасность в ГКУ «КЦСЗН» Забайкальского края должна достигаться проведением мероприятий, касающихся как внешних[246], так и внутренних[247] аспектов.

10.2. Физическая безопасность от внешних угроз должна достигаться:

- установлением контролируемой зоны[248];

---

[244] См.: разделы VI и VII Инструкции по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования, утвержденной приказом Забайкальского края от 17.07.2017 №01-111.

[245] 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.

[246] Например, окружающей обстановки вокруг здания, возможности проникновения через крышки люков.

[247] Например, прочности конструкции здания, замков, системы пожарной сигнализации и защиты, системы сигнализации при затоплении водой/жидкостью, отказов в энергоснабжении и т.д.

[248] См.:

- 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 Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608);
- п.1.16, п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 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;
- А.9.1 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

– контролем доступа посторонних лиц в помещения контролируемой зоны в рабочее и нерабочее время[249].

10.3. Физическая безопасность от внутренних угроз должна достигаться:

– прочностью строительных конструкций здания;
– противопожарной защитой и пожарной сигнализацией;
– регламентацией действий персонала при возгорании, предотвращении и (или) минимизации ущерба при затоплении водой/жидкостью, отключении электроэнергии[250];
– защитой коммуникаций и систем обеспечения энергоносителями в зданиях;
– размещением оборудования, исключающим несанкционированный доступ к нему и несанкционированный доступ к видовой

– п.ЗТС.2, п.ЗИС.3 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п.ЗТС.2, п.ЗИС.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 2. Паспорт ГИС «АС «АСП» . СЗИИС-КЦСЗН.ПС.01-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 3. Паспорт ИСПДн «Зарплата». СЗИИС-КЦСЗН.ПС.02-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 4. Паспорт ИСПДн «Бухгалтерия». СЗИИС-КЦСЗН.ПС.03-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 5. Паспорт ИСПДн «Кадры». СЗИИС-КЦСЗН.ПС.04-ОР;
– Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». Том 6. Паспорт ИСПДн «Официальный сайт». СЗИИС-КЦСЗН.ПС.05-ОР;
– п.4.1.22 настоящей Политики.

[249] 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 30.08.2002 № 282;
– п.ЗТС.3 Таблицы 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
– п.ЗТС.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР;
– разделы VI- VII и IX Инструкции по обеспечению физической защиты помещений контролируемой зоны Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-115.

[250] См.: разделы XI и XIII Инструкции по обеспечению физической защиты помещений контролируемой зоны Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-115.

информации[251].

XI. Безопасность персонала ГКУ «КЦСЗН» Забайкальского края[252]

Вопросы безопасности, связанные с персоналом, заключаются в[253]:

- учете вопросов безопасности при найме персонала[254];
- включении вопросов информационной безопасности в должностные регламенты (должностные обязанности)[255];
- соглашении о конфиденциальности[256];
- условиях служебного контракта (трудового договора)[257];
- обучении пользователей[258];
- реагировании на инциденты нарушения информационной безопасности и сбои[259].

11.1. Учет вопросов безопасности при найме персонала[260]

11.1.1. В ГКУ «КЦСЗН» Забайкальского края осуществляются проверки работников[261], принимаемых в постоянный штат по мере подачи заявлений о приеме на 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

---

[251] См.:
- п.5.4.2 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.2002 №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.

[252] 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.

[253] См.:
- раздел 8 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- п. А 8 Таблица А.1 - Цели и меры управления ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования.

[254] См.: п. 11.1 настоящей Политики.

[255] См.: п. 11.2 настоящей Политики.

[256] См.: п. 11.3 настоящей Политики.

[257] См.: п. 11.4 настоящей Политики.

[258] См.: п. 11.5 настоящей Политики.

[259] См.: п. 11.6 настоящей Политики.

[260] См.: разд.8.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[261] См.:
- 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.

квалификаций;

- независимая проверка подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа);
- наличие личных или финансовых проблем у кандидата или уже принятого работника[262].

11.1.2. В случаях, когда новому работнику 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 работников, имеющих значительные полномочия, эта проверка должна проводиться периодически.

11.2. Включение вопросов информационной безопасности в должностные обязанности[263]

11.2.1. Функции (роли) и ответственность в области информационной безопасности следует документировать. В должностные обязанности работников ГКУ «КЦСЗН» 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.

11.3. Соглашение о конфиденциальности[264]

11.3.1. В ГКУ «КЦСЗН» Забайкальского края регламентирован порядок доступа работников ГКУ «КЦСЗН» Забайкальского края и сотрудников иных органов и организаций к конфиденциальной информации[265].

---

[262] См.: п/п е) п.8.1.2 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

[263] См.:

- п. б) ст.1 Постановление Правительства РФ от 21.03.2012 №211 (ред. от 06.09.2014) "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.

[264] 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.

[265] В соответствии с:

- разделом VII Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100;

Соглашение о конфиденциальности заключается в форме Обязательства работника о неразглашении конфиденциальной информации ГКУ «КЦСЗН» Забайкальского края[266] и Соглашения о неразглашении конфиденциальной информации ГКУ «КЦСЗН» Забайкальского края, заключаемого с сотрудниками иных органов и организаций, допускаемых к конфиденциальной информации на основании государственных контрактов, или гражданско- правовых договоров[267], или иных законных основаниях.

11.3.2. В государственные контракты и гражданско- правовые договоры, заключаемые ГКУ «КЦСЗН» 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.

11.4. Условия трудового договора[268]

11.4.1. В ГКУ «КЦСЗН» Забайкальского края в соответствии с действующим законодательством устанавливаются условия трудового договора[269], определяющего ответственность работника в отношении информационной безопасности. Указанная ответственность сохраняться и в течение 36 месяцев после увольнения с работы, если иное не установлено федеральными законами. До работника доводятся меры ответственности, которые будут применимы в случае нарушения требований безопасности.

11.5. Обучение пользователей[270]

– разделом IV Положения о разрешительной системе допуска пользователей к информационным системам Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, в которых обрабатывается конфиденциальная информация, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-105.

[266] См.: Приложение №2 к Положению о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденному приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100.

[267] См.: Приложение №2-1 к Положению о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденному приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100.

[268] 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.

[269] В соответствии с ч.4 ст.57 Трудового кодекса Российской Федерации от 30.12.2001 №197-ФЗ (ред. от 01.05.2017).

[270] 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 (ред. от 22.02.2017) "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

11.5.1. Обучение пользователей должно проводиться с целью обеспечения уверенности в осведомленности пользователей об угрозах и проблемах, связанных с информационной безопасностью, и их оснащенности всем необходимым для соблюдения требований политики информационной безопасности при выполнении должностных обязанностей[271].

11.6. Реагирование на инциденты нарушения информационной безопасности и сбои[272]

Реагирование на инциденты нарушения информационной безопасности и сбои осуществляется с целью сведения к минимуму ущерба от инцидентов нарушения информационной безопасности и сбоев[273] и

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;
- 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;
- п.9.2 Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103;
- п.5.2 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109.

[271] См.: п.13.4.4 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

[272] Осуществляется в соответствии с:

- п.6) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «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 30.08.2002 № 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.

[273] 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.

должно заключаться в:

- информировании об инцидентах нарушения информационной безопасности[274];
- информировании о проблемах безопасности[275];
- информировании о сбоях программного обеспечения[276];
- извлечении уроков из инцидентов нарушения информационной безопасности[277];
- процессе установления дисциплинарной ответственности[278].

11.6.1. Информирование об инцидентах нарушения информационной безопасности[279]

11.6.1.1. В ГКУ «КЦСЗН» 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. Все пользователи должны быть ознакомлены с процедурой информирования об инцидентах нарушения информационной безопасности, а также проинформированы о необходимости незамедлительного сообщения об инцидентах.

11.6.1.2. В ГКУ «КЦСЗН» Забайкальского края предусматриваются процедуры обратной связи по результатам реагирования на инциденты нарушения информационной безопасности.

11.6.1.3. 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.

11.6.2. Информирование о проблемах безопасности[280]

---

[274] См.: п.11.6.1 настоящей Политики.
[275] См.: п.11.6.2 настоящей Политики.
[276] См.: п.11.6.3 настоящей Политики.
[277] См.: п.11.6.4 настоящей Политики.
[278] См.: п.11.6.5 настоящей Политики.
[279] Осуществляется в соответствии с:

- п.6) ч.2. ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "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 30.08.2002 № 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.

[280] См.:

- разд.13.1 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;

11.6.2.1. В обязанностях пользователей информационных сервисов предусматривается[281], что они должны:

- обращать внимание и сообщать о любых замеченных или предполагаемых недостатках и угрозах в области безопасности в системах или сервисах[282];
- немедленно сообщать об этих причинах для принятия решений своему руководству или непосредственно поставщику услуг.

11.6.2.2. 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[283].

11.6.3. Информирование о сбоях программного обеспечения[284]

- разд.А.13.1. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[281] См.: раздел VII Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109.

[282] 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 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.

[283] 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;
- п.8.1.6 Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109;

[284] 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.

11.6.3.1. Для информирования о сбоях программного обеспечения в ГКУ «КЦСЗН» 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.

11.6.3.2. Пользователи не должны пытаться самостоятельно удалить подозрительное программное обеспечение, если они не уполномочены на это. Ликвидировать последствия сбоев должен соответственно обученный персонал[285].

11.6.4. Извлечение уроков из инцидентов нарушения информационной безопасности[286]

11.6.4.1. По закрытию инцидентов информационной безопасности при директоре ГКУ «КЦСЗН» Забайкальского края должно проводиться оперативное совещание, на котором должны анализироваться действия должностных лиц при кризисном управлении и намечаться профилактические мероприятия по предотвращению подобных инцидентов[287].

11.6.4.2. В ГКУ «КЦСЗН» Забайкальского края должен быть установлен порядок мониторинга и регистрации инцидентов и сбоев в отношении их числа, типов, параметров, а также связанных с этим затрат. Данная информация должна использоваться для:

- идентификации повторяющихся или значительных инцидентов, или сбоев;

---

[285] См.:

- п.6.3.3 ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью»;
- п.8.1.8. Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-109.

[286] 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;
- 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.

[287] См.: п.13.4.3 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

- 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;
- возможного пересмотра политики информационной безопасности.

11.6.5. Процесс установления дисциплинарной ответственности[288]

11.6.5.1. По каждому выявленному факту нарушения информационной безопасности в ГКУ «КЦСЗН» Забайкальского края регламентировано проведение служебной проверки (служебного расследования) и привлечение виновных к ответственности[289].

XII. Безопасность документов и носителей информации в ГКУ «КЦСЗН» Забайкальского края [290]

---

[288] 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.

[289] 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.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;
- п.6.1.5.5.4, п.6.2.5.4, п.6.4.1.5 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[290] См.
- п.2.3 методического документа «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11.02.2014);
- п.10 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. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

12.1. В ГКУ «КЦСЗН» 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)[291].

12.2. Контроль выполнения правил документооборота (в том числе и конфиденциального) в ГКУ «КЦСЗН» Забайкальского края должна осуществлять Постоянно действующая экспертная комиссия[292].

12.3. Контроль за оборотом[293] (учетом, выдачей, использованием, передачей, хранением и уничтожением) машинных носителей конфиденциальной информации[294] должен осуществляться администратором безопасности информации[295].

XIII. Обеспечение непрерывности деятельности ГКУ «КЦСЗН» Забайкальского края, включая планирование действий при

[291] См.:
- раздел VIII Положения о конфиденциальной информации Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-100;
- п.4.1.5, п.4.2, раздел V Положения об архиве Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-119;
- раздел III Положения о Постоянно действующей экспертной комиссии Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-120;
- приказ ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-122 «Об утверждении сроков и мест хранения материальных носителей персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края».

[292] Создается в соответствии с требованиями:
- Примерного положения о Постоянно действующей экспертной комиссии учреждения, организации, предприятия, утвержденного приказом Росархива от 19.01.1995 №2;
- Положения о Постоянно действующей экспертной комиссии Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-120.

[293] Исполняется в соответствии с:
- п.5) ч.2 ст.19 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) "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.

[294] См.: п.4.1.25 настоящей Политики

[295] См.:
раздел VII Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

чрезвычайных ситуациях и восстановлении после аварий[296]

13.1. В ГКУ «КЦСЗН» 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[297].

13.2. В случае чрезвычайных ситуаций, инцидентов информационной безопасности, способных повлиять на непрерывность информационных процессов ГКУ «КЦСЗН» Забайкальского края, создается оперативный штаб и рабочая группа оперативного штаба[298].

---

[296] 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;
- раздел А.14 ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
- разд.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 9. «Определение базового и адаптированного базового набора мер» Технического задания «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- п. ОЦЛ.3 Таблицы 1. «Принятые в техническом проекте решения по защите информации» Пояснительной записки к техническому проекту «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.П2.01-ОР.

[297] См. требования:

- Инструкции о порядке действий в нештатных ситуациях в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-117;
- Инструкции по резервному копированию информационных ресурсов информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-118;
- разделы VIII-XIV Инструкции по обеспечению физической защиты помещений контролируемой зоны Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-115.

[298] См.:

- п.10.4.6 ГОСТ Р 53647.3-2010 Менеджмент непрерывности бизнеса. Часть 3. Руководство по внедрению;
- Приложение №2 к приказу ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125 «Об утверждении Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- План обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденный приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

13.3. Оперативный штаб возглавляет директор ГКУ «КЦСЗН» Забайкальского края. Место сбора оперативного штаба- рабочий кабинет директора ГКУ «КЦСЗН» Забайкальского края.

13.4. В состав оперативного штаба входят руководители подразделений ГКУ «КЦСЗН» Забайкальского края[299].

13.5. Рабочую группу оперативного штаба возглавляет заместитель директора. Место сбора рабочей группы оперативного штаба – кабинет заместителя директора.

13.6. В состав рабочей группы оперативного штаба входят администратор безопасности информации и системный администратор, а также иные должностные лица[300].

13.7. Задача оперативного штаба: активация Плана обеспечения непрерывности и восстановления управления информационных систем ГКУ «КЦСЗН» Забайкальского края[301], организация кризисного управления, проведение разбора недостатков кризисного управления после ликвидации ЧП, закрытия инцидента информационной безопасности.

13.8. Задача рабочей группы оперативного штаба: документирование решений оперативного штаба при кризисном управлении, проведение мероприятий кризисного управления, проведение анализа по результатам кризисного управления[302], подготовка материалов для заседаний оперативного штаба[303], в том числе и по подведению итогов кризисного управления.

13.9. Последствия от бедствий, нарушений безопасности и отказов в обслуживании должны анализироваться должностными лицами, ответственными за обеспечение безопасности информации[304]. На основе

---

[299] См.: Приложение №2 к приказу ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125 «Об утверждении Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края».

[300] См.: Приложение №2 к приказу ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125 «Об утверждении Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края».

[301] См.: План обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденный приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

[302] См.: 13.4.2 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

[303] См.: 13.4.3 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

[304] 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 Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108;

проведенного анализа должно проводиться обучение персонала[305] и разрабатываться планы профилактических и восстановительных мероприятий[306] по управлению информационной безопасностью. Данные планы являются составной частью всех процессов управления. Обучение персонала может проводиться в форме учений с имитацией инцидента информационной безопасности[307].

XIV. Политика аутсорсинга в ГКУ «КЦСЗН» Забайкальского края[308]

14.1. В соответствии с требованиями действующего законодательства ГКУ «КЦСЗН» Забайкальского края вправе поручить на договорной основе уполномоченным лицам исполнять следующие функции обеспечения безопасности:

- физическая защита[309] (охрана помещений, пропускной режим, обслуживание охранно- пожарной сигнализации);

- п.9.7, п. 9.10,. Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.

[305] См.: п.13.4.5 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

[306] См.:

- План обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденный приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125;
- План проведения периодических проверок условий обработки персональных данных в Государственном казенном учреждении «Краевой центр социальной защиты населения» Забайкальского края, утвержденный приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-124;
- План мероприятий по защите конфиденциальной информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденный приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-123.

[307] См.: п.13.4.5 Плана обеспечения непрерывности информационных процессов и восстановления управления информационными системами Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-125.

[308] 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

[309] См.:

- п.15) ч.1 ст12 Федерального закона 04.05.2011 №99-ФЗ (ред. от 30.12.2015) "О лицензировании отдельных видов деятельности" (с изм. и доп., вступ. в силу с 01.01.2017);
- раздел III Закона РФ от 11.03.1992 №2487-1 (ред. от 03.07.2016) "О частной детективной и охранной деятельности в Российской Федерации";
- Постановление Правительства РФ от 14.08.1992 №587 (ред. от 18.03.2017) "Вопросы частной детективной (сыскной) и частной охранной деятельности";
- Постановление Правительства РФ от 30.12.2011 №1225 (ред. от 28.04.2015) "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").

- администрирование информационных систем[310];
- администрирование информационной безопасности[311] и др.

14.2. Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению ГКУ «КЦСЗН» Забайкальского края и (или) предоставляющее ГКУ «КЦСЗН» 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[312]. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии требованиями по защите информации[313] и настоящей Политикой.

XV. Управление изменениями в информационных системах ГКУ «КЦСЗН» Забайкальского края [314]

15.1. 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.

15.2. При внесении изменений конфигурацию информационных систем и конфигурацию системы защиты информации информационных систем ГКУ «КЦСЗН» Забайкальского края должны соблюдаться следующие

---

[310] В соответствии с ч.3 ст.6 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 22.02.2017) «О персональных данных».

[311] 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).

[312] См.: п.3) ч.2 ст.6, ч.1 ст.16 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «Об информации, информационных технологиях и о защите информации».

[313] См.:

- ч.5 ст.16 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 07.06.2017) «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).

[314] См.: 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.

требования[315]:

15.2.1. Изменения в конфигурацию аттестованной ИС и СЗИИС вносятся уполномоченными работниками ГКУ «КЦСЗН» Забайкальского края (или уполномоченным лицом[316]) по согласованию со специализированной организацией - лицензиатом ФСТЭК, аттестовавшей ранее данную информационную систему[317].

15.2.2. При изменении состава технических средств защиты или элементов ИС, соответствующие изменения должны быть внесены в Технический проект по согласованию с разработчиком[318].

15.2.3. Информация об изменениях конфигурации аттестованной ИС и СЗИИС вносится в проектную[319] и эксплуатационную документацию[320] в соответствии с положениями национальных стандартов[321].

15.2.4. Внесение изменений в информационной системы осуществляет администратор ИС по согласованию и под контролем начальника отдела автоматизации как руководителя подразделения, ответственного за безопасность информации в информационных системах Учреждения, и администратора безопасности информации (или уполномоченного лица[322]), т.к. неудачно и (или) неправильно

---

[315] См.: разделы 6.3.2 и 6.3.3 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[316] 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).

[317] См.: п.6.3.2.1 Инструкции по администрированию безопасности информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденной приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-108.

[318] Исполняется в соответствии с п.5.4.2. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 №282, а также п.5. Приложения 2 к указанным Специальным требованиям.

[319] См.:

- Техническое задание «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.

[320] См.: п.3.1.1. и п. 5.1.2 ГОСТ 2.601-2006. Единая система конструкторской документации. Эксплуатационные документы.

[321] 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.

[322] 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).

конфигурированные операционные системы по причине неконтролируемых изменений в системе могут являться факторами, приводящими к инцидентам информационной безопасности[323]. Выбор правильной конфигурации и форм администрирования сетей являются эффективными средствами снижения уровня риска информационной безопасности[324].

15.2.5. 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[325].

15.2.6. При внесении изменений в конфигурацию информационных систем и (или) конфигурацию системы защиты информации информационных систем должны быть рассмотрены следующие мероприятия[326]:

- 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.

15.2.7. Данные о конфигурации сети и компоновочном плане должны резервироваться для обеспечения их доступности в аварийных ситуациях[327].

15.2.8. После изменений конфигурации информационной системы

---

[323] См.: п.6.2, п.6.3 ГОСТ Р ИСО/МЭК 18044. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.

[324] 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.

[325] 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.

[326] 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;
- 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.

[327] 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 информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края».

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[328].

15.3. 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.

15.4. При внесении изменений в техническую документацию[329] должны соблюдаться следующие требования:

15.4.1. Изменения в техническую документацию (технический проект) на создание СЗИИС вносятся разработчиком проекта или по предварительному согласованию с разработчиком проекта.

15.4.2. Изменения в техническую документацию (технический проект) на создание СЗИИС вносятся в соответствии с положениями национальных стандартов[330].

15.4.3. При изменении проектных решений, реализованных при создании системы защиты информации информационной системы, проводятся дополнительные аттестационные испытания в рамках действующего аттестата соответствия[331].

---

[328] 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).

[329] См.:

- Техническое задание «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края»;
- Проект «Система защиты информации информационных систем Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края». СЗИИС-КЦСЗН.

[330] 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.

[331] В соответствии с п. 17.4 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от

XVI. Ответственность и полномочия

16.1. Ответственность персонала

16.1.1. За нарушение требований настоящей Политики должностные лица ГКУ «КЦСЗН» Забайкальского края несут ответственность в соответствии с действующим законодательством.

16.1.2. Должностное лицо ГКУ «КЦСЗН» Забайкальского края, разработавшее проект организационно- распорядительного акта ГКУ «КЦСЗН» Забайкальского края в области защиты информации, несет ответственность за соответствие данного акта положениям настоящей Политики.

16.1.3. Должностные лица ГКУ «КЦСЗН» Забайкальского края, вносящие изменения в конфигурацию информационных систем и СЗИИС, несут ответственность за соответствие своих действий процедурам, регламентированным настоящей Политикой.

16.2. Полномочия персонала

16.2.1. Работники ГКУ «КЦСЗН» Забайкальского края имеют право выходить с предложениями к руководству ГКУ «КЦСЗН» Забайкальского края по вопросам защиты конфиденциальной информации.

16.2.2. Изменения в настоящую Политику вносятся приказом ГКУ «КЦСЗН» Забайкальского края после обязательного согласования вносимых изменений с начальником отдела автоматизации как руководителем подразделения, ответственного за безопасность информации в информационных системах Учреждения, отвечающим за соответствие вносимых изменений требованиям законодательства и нормативно- правовых актов Регуляторов[332].

11.02.2013 №17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный №28608).

[332] В соответствии с п.11.2 Положения о подразделении, ответственном за безопасность информации в информационных системах Государственного казенного учреждения «Краевой центр социальной защиты населения» Забайкальского края, утвержденного приказом ГКУ «КЦСЗН» Забайкальского края от 17.07.2017 №01-103.