Приложение к приказу
АО «ГСМК «Сахамедстрах»
от 26.10.2015 г. №402/14-004

ПОЛИТИКА
информационной безопасности
в АО «ГСМК «Сахамедстрах»

Якутск
2015

1. Термины и определения

1.1. **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники[1].

1.2. **Автоматизированная система (АС)** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[2].

1.3. **Безопасность информации [данных]**-1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность[3]; 2) состояние защищенности и нформации, 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[4].

1.4. **Доступность (санкционированная доступность) информации** - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия[5].

1.5. **Замысел защиты информации**- основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации[6].

1.6. **Информационная система персональных данных (ИСПДн)**- совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств[7].

1.7. **Компьютерный вирус (КВ)** - программа, способная создавать свои

---

[1] См.: ч.4.ст.3 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных».

[2] См.:

- п.1.3 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;
- п.1.1 ГОСТ 34. 003-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения;
- п.3.1.6 ГОСТ Р 51624-2000 «Автоматизированные системы в защищенном исполнении»;
- п.4.1. ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении».

[3] См.: п. 2.4.5 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

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

[5] См.: п.1.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.

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

[7] См.:

- ч.10 .ст.3 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных»;
- абзац первый л.4 Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008.

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[8].

1.8. **Криптографическое средство 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 информации)[9].

1.9. **Межсетевой экран (МЭ) (средство межсетевого экранирования)** - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или

---

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

[9] См.:

- 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.

выходящей из АС[10].

1.10. **Несанкционированный доступ (несанкционированные действия) (НСД)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами[11].

1.11. **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[12].

1.12. **Объект защиты информации-** информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации[13].

1.13. **Организационные меры защиты информации (оргмеры)-** 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[14]. Организационные меры по защите персональных данных включают в себя:
1. разработку организационно – распорядительных документов, которые регламентируют весь процесс получения, обработки, хранения, передачи и защиты персональных данных;
2.перечень мероприятий по защите персональных данных: определение круга лиц, допущенного к обработке персональных данных; организация доступа в помещения, где осуществляется обработка ПДн; разработка должностных инструкций по работе с персональными данными; установление персональной ответственности за нарушения правил обработки ПДн; определение продолжительности хранения ПДн и т.д.

1.14. **Оператор информационной системы** - гражданин или юридическое

---

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

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

[12] См.: ч.3.ст.3 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных».

[13] См.: п. 2.5.1 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

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

лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных[15].

1.15. **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[16].

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

- внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников оператора 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[17];
- контроль организации допуска работников АО «ГСМК «Сахамедстрах» к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности[18].

1.17. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[19].

1.18. **Политика безопасности (информации в организации)**- совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности[20].

---

[15]См.: п.12) ст.2 Федерального закона от 27.07.2006 №149-ФЗ (ред. от 28.07.2012)"Об информации, информационных технологиях и о защите информации".

[16] См.: ч.2.ст.3 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных».

[17]См.: ст.22.1 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных».

[18] См.: п. 12.2 Инструкции по конфиденциальному делопроизводству в АО «ГСМК «Сахамедстрах», утвержденной приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 №403/14-004.

[19] См.: ч.1.ст. Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных».

[20] См.: п. 2.4.4 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

1.19. **Правовые меры защиты информации**[21]- 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[22]. Т.к. АО «ГСМК «Сахамедстрах» не издает ни законов, ни иных нормативно- правовых актов[23] в области защиты информации, то правовые методы защиты информации для АО «ГСМК «Сахамедстрах» заключаются в применении существующих законов и иных нормативных правовых актов, а также в контроле их исполнения.

1.20. **СЗПДн** – система (подсистема) защиты персональных данных.

1.21. **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[24]. В широком смысле слова под техническими средствами защиты информации понимается защита информации как некриптографическими методами, так и методами преобразования при помощи шифрования[25].

1.22. **Целостность информации** - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть

---

[21] См.:
- ч.1 ст.19 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- ч.1 ст.16 Федерального закона «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ.

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

[23] Нормативный правовой акт (НПА) — официальный документ установленной формы, принятый (изданный) в пределах компетенции уполномоченного государственного органа (должностного лица), иных социальных структур (муниципальных органов, профсоюзов, акционерных обществ, товариществ и т.д.) или путём референдума с соблюдением установленной законодательством процедуры, **содержащий общеобязательные правила поведения, рассчитанные на неопределённый круг лиц** и неоднократное применение. К НПА относятся нормативные акты (то есть указы, содержащие нормы права) Президента России, нормативные постановления палат Федерального Собрания (принимаемые по вопросам их ведения), нормативные постановления Правительства России, различные нормативные акты (приказы, инструкции, положения и т. п.) федеральных министерств и ведомств, других федеральных органов исполнительной власти, других федеральных государственных органов. Следует выделить также нормативные правовые акты органов местного самоуправления (именно поэтому подзаконный акт принимается не только государственными органами), издающиеся в соответствии с вышестоящими законами и подзаконными актами и воздействующие на общественные отношения строго на территории данного муниципального образования. (См.: http://ru.wikipedia.org/wiki/Нормативно-правовой_акт). АО «ГСМК «Сахамедстрах» в области защиты информации издает только организационно- распорядительные акты.

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

[25] Именно в широком смысле термин техническая защита употреблен законодателем в:
- Федеральном законе «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- Федеральном законе «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ;
- 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.

уничтожение и искажение информации[26].

1.23. **Цель защиты информации -** заранее намеченный результат защиты информации[27].

1.24. **Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных[28].

2. Общие положения

2.1. Настоящая Политика информационной безопасности в АО «ГСМК «Сахамедстрах» (далее – Политика) определяет общую совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется АО «ГСМК «Сахамедстрах» в своей деятельности.

2.2. Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, при их обработке в АО «ГСМК «Сахамедстрах».

2.3. Политика разработана в соответствии с требованиями:

- Конституции Российской Федерации (принятой 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);
- Федерального закона от 27.07.2006 №149-ФЗ (ред. от 06.04.2011) «Об информации, информационных технологиях и защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных»;
- Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 29.12.2012);
- п.8) ч.4 ст.13 Федерального закона от 21.11.2011 № 323-ФЗ(ред. от 25.06.2012)"Об основах охраны здоровья граждан в

---

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

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

[28] См.:

- п.2.6.1. ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ;
- л.9 Приложения 5 Методических рекомендаций для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, согласованные с начальником 2 управления ФСТЭК России 22.12.2009, утвержденные директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23.12.2009.

Российской Федерации";

- п.7) ч.2 ст.16, п.2) ч.2 ст.20, ст. 43, ч.4 ст.47 Федерального закона от 29.11.2010 № 326-ФЗ (ред. от 01.12.2012) "Об обязательном медицинском страховании в Российской Федерации" (с изм. и доп., вступившими в силу с 01.01.2013);
- Указа Президента Российской Федерации от 06.03.97 № 188 (ред. от 23.09.2005) «Об утверждении Перечня сведений конфиденциального характера»;
- Постановления Правительства Российской Федерации от 01.11.2012 №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- Постановления Правительства Российской Федерации от 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 30.08.02 № 282;
- Положения о методах и способах защиты информации в информационных системах персональных данных", утвержденного приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010, регистрационный № 16456);
- 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;
- Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008;
- Порядком ведения персонифицированного учета в сфере обязательного медицинского страхования, утвержденным приказом Министерства здравоохранения и социального развития Российской Федерации от 25.01.2011 № 29н (ред. от 09.09.2011)

(зарегистрировано в Минюсте РФ 08.02.2011 № 19742);

- ГОСТ Р 50922-2006. Защита информации. Основные термины и определения;
- ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем;
- ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство;
- Уставом Акционерного общества «Государственная страховая медицинская компания «Сахамедстрах», утвержденный Общим собранием акционеров АО «ГСМК «Сахамедстрах» от 23.11.2010, протокол №5 от 26.11.2010 (с изменениями от 29.08.2011),и др.

2.4. Целью настоящей Политики является определение основных правил обеспечения безопасности объектов защиты АО «ГСМК «Сахамедстрах» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизации ущерба от возможной реализации угроз безопасности ПДн.

2.5. 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 персональных данных в АО «ГСМК «Сахамедстрах»[29].

2.6. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий[30].

2.7. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей[31]. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных[32].

---

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

[30] Исполняется в соответствии с:

- п.2.8. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.
- п.1.2. и разделом II «Методы и способы защиты информации от несанкционированного доступа» Положения о методах и способах защиты информации в информационных системах персональных данных", утвержденного приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010, регистрационный № 16456).

[31] Исполняется в соответствии с п. 1.9, п.6.3.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.

[32] Исполняется в соответствии с:

- п.6) ч.2. ст.19 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных;
- п. 3.24. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282;

2.8. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных[33].

2.9. Состав ИСПДн подлежащих защите, представлен в паспортах ИСПДн и в Правилах обработки персональных данных в АО «ГСМК «Сахамедстрах»[34].

2.10. В Политике определены общий замысел защиты информации АО «ГСМК «Сахамедстрах», требования к пользователям ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности лиц, ответственных за обеспечение безопасности персональных данных в ИСПДн АО «ГСМК «Сахамедстрах».

2.11. Требования Политики обязательны для всех работников АО «ГСМК «Сахамедстрах», представителей контрольно-надзорных органов, допущенных к защищаемой информации на законных основаниях, а также индивидуальных лиц и работников иных организаций допущенных к защищаемой информации для проведения работ по гражданско-правовым договорам[35].

2.12. В соответствии с:

- ч.2. ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных»;

АО «ГСМК «Сахамедстрах» обязано опубликовать, разместить на официальном сайте или иным образом обеспечить неограниченный доступ к настоящей Политике.

- п.2.2., п.2.4., п.2.6, п.6 Положения о методах и способах защиты информации в информационных системах персональных данных", утвержденного приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010, регистрационный № 16456).

[33] Исполняется в соответствии с:

- п.7) ч.2. ст.19 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных;
- п.6.1.2., п.6.3.7., п.6.3.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.

[34] См.: раздел 3.6 Правил обработки персональных данных в АО «ГСМК «Сахамедстрах», утвержденных приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №405/14-004.

[35] См.:

- разделы 5.4.2. Правил обработки персональных данных в АО «ГСМК «Сахамедстрах», утвержденных приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 №405/14-004;
- раздел 3 Положения о разрешительной системе допуска пользователей к информационным системам персональных данных, утвержденного приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 №409/14-004.

3. Система защиты персональных данных АО «ГСМК «Сахамедстрах»

3.1. Система защиты персональных данных (СЗПДн), строится на основании применения правовых, организационных и технических мер по обеспечению безопасности персональных данных[36].

3.2. Указанные в п.3.1. настоящей Политики меры по обеспечению безопасности персональных данных регламентированы следующими внутренними организационно- распорядительными и инструктивно-технологическими документами АО «ГСМК «Сахамедстрах»:

- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г.№ 402/14-004 «Об утверждении Политики информационной безопасности в АО «ГСМК «Сахамедстрах»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №403/14-004 «Об утверждении Инструкции по конфиденциальному делопроизводству в АО «ГСМК «Сахамедстрах»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №404/14-004 «Об утверждении Положения об ответственном за организацию обработки персональных данных в АО «ГСМК «Сахамедстрах»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №405/14-004 «Об утверждении Правил обработки персональных данных в АО «ГСМК «Сахамедстрах»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015г. №406/14-004 «Об утверждении Положения об архиве АО «ГСМК «Сахамедстрах» и Положения о Постоянно действующей экспертной комиссии АО «ГСМК «Сахамедстрах»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 №407/14-004 «Об утверждении сроков и мест хранения материальных носителей персональных данных»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №408/14-004 «Об утверждении Положения о порядке организации и проведении работ по защите конфиденциальной информации в информационных системах персональных данных АО «ГСМК «Сахамедстрах»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 №409/14-004 «Об утверждении Положения о разрешительной системе допуска пользователей к информационным системам персональных данных»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №410/14-

[36] См.: :

- п.3) ч.1. ст.18.1 , ст.19 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных»;
- ст.2 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119, и др.

004 «Об утверждении Положения об администраторе безопасности информации»;

- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №411/14-004 «Об утверждении Инструкции по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №412/14-004 «Об утверждении Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах персональных данных»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015г. №413/14-004 «Об утверждении Инструкции по учету, маркировке, очистке и утилизации машинных носителей информации»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015г. №414/14-004 «Об утверждении Инструкции по обеспечению информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015г. №415/14-004 «Об утверждении Регламента безопасного функционирования подсистемы криптографической защиты информации»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №416/14-004 «Об утверждении Инструкции по организации антивирусной защиты в информационных системах персональных данных»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №417/14-004 «Об утверждении Инструкции по организации парольной защиты информационных систем персональных данных»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №418/14-004 «Об утверждении Инструкции по обеспечению физической защиты помещений контролируемой зоны»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №419/14-004 «Об утверждении Плана внутренних проверок состояния защиты персональных данных»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №420/14-004 «Об утверждении Плана мероприятий по защите персональных данных»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №421/14-004 «Об утверждении Инструкции по внесению изменений в конфигурацию информационных систем персональных данных»;

- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №422/14-004 «Об утверждении Инструкции о порядке действий в нештатных ситуациях»;
- приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №423/14-004 «Об утверждении Инструкции по резервному копированию информационных ресурсов информационных систем персональных данных»;

3.3. В нормативных правовых и организационно-распорядительных документах, указанных в п.2.3. п.3.2., определяется необходимый уровень защищенности персональных данных ИСПДн АО «ГСМК «Сахамедстрах». На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз АО «ГСМК «Сахамедстрах», сделано заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые технические мероприятия отражены в Плане мероприятий по обеспечению защиты ПДн[37].

3.4. Для каждой ИСПДн в разработанном Паспорте ИСПДн составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке персональных данных в ИСПДн.

3.5. В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн включает следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранирования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

3.6. СЗПДн включает функции защиты, обеспечиваемые штатными средствами обработки ПДн, операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты:

- управление и разграничение доступа пользователей[38];
- регистрацию и учет действий с информацией[39];
- обеспечение целостности данных;

---

[37] См. План мероприятий по защите персональных данных, утвержденный приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 № 420/14-004.

[38] Исполняется в соответствии с п.5.1.3., п.5.1.9., п.5.9.2., п.6.3.2., п.6.3.11.4 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282.

[39] Исполняется в соответствии с:

- п. 5.1.3., п.5.7.6., п.5.9.1., п.5.9.2. ,п. 6.3.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282:
- п.2.1., п.2.2. Положения о методах и способах защиты информации в информационных системах персональных данных", утвержденного приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010, регистрационный № 16456), и п.2.1.б), п.2.2.б), п.2.3.б), разделами 3 и 4 Приложения к указанному Положению.

- обнаружение вторжений[40].

3.7. Список используемых технических средств должен поддерживаться в актуальном состоянии.

3.8. В соответствии с реализуемыми функциями защиты СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

3.9. Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в акте классификации информационной системы персональных данных[41].

4. Пользователи ИСПДн

4.1. В ИСПДн АО «ГСМК «Сахамедстрах» определены следующие категории пользователей ИСПДн:

- администратор ИСПДн;
- администратор безопасности информации;
- оператор.

4.2. Данные о группах пользователях, уровне их доступа и информированности отражены также в Положении о разрешительной

---

[40] Исполняется в соответствии с:

- п.6) ч.2. ст.19 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных;
- п.2.8., п.2.9., п.2.14, п.3.24, п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282:
- п.2.2., п.2.4, п.2.6 Положения о методах и способах защиты информации в информационных системах персональных данных", утвержденного приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010, регистрационный № 16456), и п.6. Приложения к указанному Положению.

[41] Акты классификации ИСПДн подготовлены в соответствии с требованиями:

- ст.22, ч.2.1. ст.25 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных,
- приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», зарегистрированного в Минюсте РФ 03.04.2008 за №11462;
- приказом Россвязькомнадзора от 17.07.2008 №8 «Об утверждении образца формы уведомления об обработке персональных данных»;
- приказом Роскомнадзора от 18.02.2009 № 42 «О внесении изменений в приказ Россвязькомнадзора от 17.07.2008 №8 «Об утверждении образца формы уведомления об обработке персональных данных».
- приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19.08.2011 № 706 "Об утверждении Рекомендаций по заполнению образца формы уведомления об обработке (о намерении осуществлять обработку) персональных данных".

системе допуска пользователей к ИСПДн[42].

4.3. Администратор ИСПДн:

4.3.1. Администратор ИСПДн – работник АО «ГСМК «Сахамедстрах»[43], ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномоченный осуществлять предоставление и разграничение доступа конечного пользователя (оператора) к элементам, хранящим персональные данные.

4.3.2. Администратор ИСПДн обладает следующим уровнем доступа и знаний:

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

4.4. Администратор безопасности информации:

4.4.1. Администратор безопасности информации-работник АО «ГСМК «Сахамедстрах»[44], ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

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

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

4.4.3. Администратор безопасности информации уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор) получает возможность работать с элементами ИСПДн;

---

[42] См.: Положение о разрешительной системе допуска пользователей к информационным системам персональных данных, утвержденное приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 №409/14-004.

[43] Штатный или осуществляющий свои функциональные обязанности по гражданско-правовому договору, заключенному в соответствии с ч.3 ст.6 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных».

[44] Штатный или осуществляющий свои функциональные обязанности по гражданско-правовому договору, заключенному в соответствии с Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 № 1119.

- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других органов власти и организаций.

4.5. Оператор:

4.5.1. Оператор-работник АО «ГСМК «Сахамедстрах», осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

4.5.2. Оператор обладает следующим уровнем доступа и знаний:

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

5. Требования к пользователям по обеспечению защиты персональных данных

5.1. Требования к работникам АО «ГСМК «Сахамедстрах», допущенным в установленном порядке к персональным данным[45], их права и обязанности установлены в:

- Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах персональных данных, утвержденной приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №412/14-004;
- Положении об администраторе безопасности информации, утвержденном приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №410/14-004;
- Инструкции по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности, утвержденной приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №411/14-004;
- Инструкции по организации антивирусной защиты в информационных системах персональных данных, утвержденной приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №416/14-004;
- Инструкции по организации парольной защиты информационных систем персональных данных, утвержденной приказом АО

[45] В соответствии с:
- разделом 12 Инструкции по конфиденциальному делопроизводству в АО «ГСМК «Сахамедстрах», утвержденной приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №403/14-004;
- разделом 4 Положения о разрешительной системе допуска пользователей к информационным системам персональных данных, утвержденного приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №409/14-004.

«ГСМК «Сахамедстрах» от 26.10.2015 г. №417/14-004;

- Правилах обработки персональных данных в АО «ГСМК «Сахамедстрах», утвержденных приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №405/14-004.

5.2. Все работники АО «ГСМК «Сахамедстрах», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

5.3. До пользователей должны доведены под роспись в листе ознакомления требования нормативных правовых и внутренних организационно-распорядительных актов в области защиты информации, в части их касающейся[46].

5.4. Пользователи надлежащим образом должны быть извещены об ответственности за нарушение требований нормативных правовых и внутренних организационно- распорядительных актов в области защиты информации.

6. Лицо, ответственное за организацию обработки персональных данных

6.1. Генеральный директор АО «ГСМК «Сахамедстрах» своим приказом назначает лицо, ответственное за организацию обработки персональных данных.

6.2. Лицо, ответственное за организацию обработки персональных данных, получает указания непосредственно от генерального директора АО «ГСМК «Сахамедстрах»[47].

Должностные лицо АО «ГСМК «Сахамедстрах» ответственный за организацию и обработку персональных данных обязан своевременно предоставить в уполномоченный орган по защите прав субъектов персональных данных следующие сведения:[48]

---

[46] Осуществляется в соответствии с :

- п.6) ч.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ (ред. от 25.07.2011) "О персональных данных";
- ч.8 ст. 86 Трудового кодекса Российской Федерации от 30.12.2001 №197-ФЗ (ред. от 28.07.2012);
- ст.6 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации утвержденного Постановлением Правительства РФ от 15.09.2008 №687;
- п .5.2.2. Специальных требования и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.02 № 282,
- п.2.9. 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, и др.

[47] См. ст.22.1 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных.

[48] В соответствии с ч.3 ст.22. Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных.

- наименование, адрес оператора;
- цель обработки персональных данных;
- категории персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- правовое основание обработки персональных данных;
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
- описание мер, предусмотренных статьями 18.1 и 19 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных», в том числе сведения о наличии шифровальных (криптографических) средств и наименования этих средств;
- фамилия, имя, отчество физического лица или наименование юридического лица, ответственных за организацию обработки персональных данных, и номера их контактных телефонов, почтовые адреса и адреса электронной почты;
- дата начала обработки персональных данных;
- срок или условие прекращения обработки персональных данных;
- сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;
- сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

6.3. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано[49]:

- осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных[50];

---

[49] В соответствии с:
- ч.4 ст.22.1 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных;
- абзаца 3 п. б) ст.1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного Постановлением Правительства Российской Федерации от 21.03.2012 №211.

[50] Осуществляется в соответствии с :
- п.4) ч.1 ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. от 25.07.2011) «О персональных данных»;
- п.3.1, п.3.19 Типовой программы аудита организации и состояния работы по защите конфиденциальной информации в исполнительных органах государственной власти Забайкальского края, утвержденной решением Совета информационной безопасности Забайкальского края 31.10.2011 г №1
- разделом 7 настоящих Правил: «Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом "О персональных данных";

- доводить до сведения работников оператора положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных[51];
- организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющее контроль за приемом и обработкой таких обращений и запросов[52];
- осуществлять контроль организации допуска работников АО «ГСМК «Сахамедстрах» к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности[53].

7. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства и подзаконных актов[54]

7.1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами оператора АО «ГСМК «Сахамедстрах» осуществляют:
- лицо, ответственное за организацию обработки персональных данных, назначаемое приказом АО «ГСМК «Сахамедстрах»[55];
- администратор безопасности информации, исполнение обязанностей которого дополнительно возложены на существующего штатного работника[56].

7.2. Внутренний контроль соответствия обработки персональных данных требованиям законодательства и подзаконных актов осуществляется в

- Планом внутренних проверок состояния защиты персональных данных, утвержденным приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №419/14-004.

[51] В соответствии с п.6) ч.1 ст.18.1Федерального закона от 27.07.2006 № 152-ФЗ (в ред. от 25.07.2011) «О персональных данных».

[52] См.: ст.22.1 Федерального закона от 27.07.2006 № 152-ФЗ (в ред. от 25.07.2011) «О персональных данных».

[53] См.: п. 12.Инструкции по конфиденциальному делопроизводству в АО «ГСМК «Сахамедстрах», утвержденной приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №403/14-004.

[54] Устанавливаются во исполнение:
- ч.4 ст.22.1 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных;
- абзаца 3 п. б) ст.1 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного Постановлением Правительства Российской Федерации от 21.03.2012 №211;
- раздела 7 Правил обработки персональных данных в АО «ГСМК «Сахамедстрах», утвержденных приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №405/14-004.

[55] См.п.6.1. настоящей Политики.

[56] п. 3 приказа АО «ГСМК «Сахамедстрах» от 26.10.2015 г.№410/14-004 «Об утверждении Положения об администраторе безопасности информации».

соответствии с планами, разработанными на отчетный период[57].

7.3. По результатам проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства и подзаконных актов оператора лица, указанные в п.7.1 настоящей Политики, докладывают генеральному директору АО «ГСМК «Сахамедстрах»[58] о выявленных нарушениях и принятых мерах.

[57] См.:

- План внутренних проверок состояния защиты персональных данных, утвержденный приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г.№419/14-004;
- План мероприятий по защите персональных данных, утвержденный приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г.№420/14-004.

[58] Исполняется в соответствии с:

- ч.2 ст.22.1 Федерального закона » от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) «О персональных данных;
- п.7 Инструкции, 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.5.2.Положения об администраторе безопасности информации, утвержденного приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г. №410/14-004;
- п.4.1.3 и п.5.1.5 Положения об ответственном за организацию обработки персональных данных в АО «ГСМК «Сахамедстрах», утвержденного приказом АО «ГСМК «Сахамедстрах» от 26.10.2015 г.№404/14-004.