Приложение к приказу
АО «СМК «Сахамедстрах»
от 25.01.2021 г. № 016/14-004

ПОЛИТИКА
информационной безопасности
в АО «СМК «Сахамедстрах»

Якутск
2021 г.

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.

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

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.

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

1.6. **Информационная система персональных данных (ИСПДн)-** совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств[2].

1.7. **Компьютерный вирус (КВ)** - 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.

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

---

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

[2] См.:

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

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).

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 выходящей из АС.

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.

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[3].

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

1.13. **Организационные меры защиты информации (оргмеры)-** под

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

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. 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 лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных[4].

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[5].

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[6];
- контроль организации допуска работников АО «СМК

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

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

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

«Сахамедстрах» к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

1.17. **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[7].

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.

1.19. **Правовые меры защиты информации**[8]- 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. Т.к. АО «СМК «Сахамедстрах» не издает ни законов, ни иных нормативно- правовых актов[9] в области защиты информации, то правовые методы защиты информации для АО «СМК «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. В широком смысле слова под техническими средствами защиты информации понимается защита информации как некриптографическими методами, так и методами преобразования при помощи шифрования.

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

1.23. **Цель защиты информации -** заранее намеченный результат защиты информации.

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

[7] См.: ч.1.ст. Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».
[8] См.:ч.1 ст.19 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ;

системе персональных данных.

2. Общие положения

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

2.2. Политика разработана в соответствии с требованиями:

- Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ;
- п.8) ч.4 ст.13 Федерального закона от 21.11.2011 № 323-ФЗ "Об основах охраны здоровья граждан в 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 "Об обязательном медицинском страховании в Российской Федерации";
- Указа Президента Российской Федерации от 06.03.97 № 188 «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";
- 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);

2.3. Целью настоящей Политики является определение основных правил обеспечения безопасности объектов защиты АО «СМК «Сахамедстрах»

от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизации ущерба от возможной реализации угроз безопасности ПДн.

2.4. 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 «СМК «Сахамедстрах».

2.5. 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.

2.6. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных[10].

2.7. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных[11].

2.8. Состав ИСПДн подлежащих защите, представлен в паспортах ИСПДн и Правилах обработки персональных данных в АО «СМК «Сахамедстрах»[12].

2.9. В Политике определены общий замысел защиты информации АО «СМК «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 «СМК «Сахамедстрах».

2.10. Требования Политики обязательны для всех работников АО «СМК «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[13].

2.11. В соответствии с:

- ч.2. ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О

[10] Исполняется в соответствии с п.6) ч.2. ст.19 Федерального закона » от 27.07.2006 № 152-ФЗ «О персональных данных;

[11] Исполняется в соответствии с п.7) ч.2. ст.19 Федерального закона » от 27.07.2006 № 152-ФЗ «О персональных данных»;

[12] См.: раздел 3.6 Правил обработки персональных данных в АО «СМК «Сахамедстрах.

[13] См.:

- разделы 5.4.2. Правил обработки персональных данных в АО «СМК «Сахамедстрах»
- раздел 3 Положения о разрешительной системе допуска пользователей к информационным системам персональных данных АО «СМК «Сахамедстрах».

персональных данных»;

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

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

3.1. Система защиты персональных данных (СЗПДн), строится на основании применения правовых, организационных и технических мер по обеспечению безопасности персональных данных[14].

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 «СМК «Сахамедстрах»:

- приказом АО «СМК «Сахамедстрах» «Об утверждении Политики информационной безопасности в АО «СМК «Сахамедстрах»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Положения об ответственном за организацию обработки персональных данных в АО «СМК «Сахамедстрах»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Правил обработки персональных данных в АО «СМК «Сахамедстрах»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Положения о порядке организации и проведении работ по защите конфиденциальной информации в информационных системах персональных данных АО «СМК «Сахамедстрах»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Положения о разрешительной системе допуска пользователей к информационным системам персональных данных»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Положения об администраторе безопасности информации»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах персональных данных»;

[14] См.: :

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

- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции по обеспечению информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции по организации антивирусной защиты в информационных системах персональных данных»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции по организации парольной защиты информационных систем персональных данных»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции по обеспечению физической защиты помещений контролируемой зоны»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Плана внутренних проверок состояния защиты персональных данных»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Плана мероприятий по защите персональных данных»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции по внесению изменений в конфигурацию информационных систем персональных данных»;
- приказом АО «СМК «Сахамедстрах» «Об утверждении Инструкции о порядке действий в нештатных ситуациях»;
- приказом АО «СМК «Сахамедстрах» «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 «СМК «Сахамедстрах». На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз, сделано заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

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;
   - регистрацию и учет действий с информацией;
   - обеспечение целостности данных[15];
   - обнаружение вторжений[16].

3.7. 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.

4. Пользователи ИСПДн

4.1. Определены следующие категории пользователей ИСПДн:
   - администратор ИСПДн;
   - администратор безопасности информации;
   - оператор.

4.2. В Паспортах каждой ИСПДн разработаны матрицы доступа для каждого вида пользователей к ресурсам информационной системы.

4.3. Данные о группах пользователях, уровне их доступа и информированности отражены также в Положении о разрешительной системе допуска пользователей к ИСПДн[17].

4.4. Администратор ИСПДн:

4.4.1. Администратор ИСПДн – работник АО «СМК «Сахамедстрах»[18], ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномоченный осуществлять предоставление и разграничение доступа конечного пользователя (оператора) к

[15] Исполняется в соответствии с п.3.4. 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.

[16] Исполняется в соответствии с п.6) ч.2. ст.19 Федерального закона » от 27.07.2006 № 152-ФЗ «О персональных данных;

[17] См.: Положение о разрешительной системе допуска пользователей к информационным системам персональных данных АО «СМК «Сахамедстрах».

[18] 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 «О персональных данных».

элементам, хранящим персональные данные.

4.4.2. 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.

4.5.Администратор безопасности информации:

4.5.1. Администратор безопасности информации - работник АО «СМК «Сахамедстрах», ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

4.5.2. 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;

4.5.3. 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;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других органов власти и организаций.

4.6.Оператор:

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

4.6.2. 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 «СМК «Сахамедстрах», допущенным в установленном порядке к персональным данным[19], их права и обязанности установлены в:
- Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах персональных данных АО «СМК «Сахамедстрах»
- Положении об администраторе безопасности информации АО «СМК «Сахамедстрах»
- Инструкции по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности АО «СМК «Сахамедстрах»;
- Инструкции по организации антивирусной защиты в информационных системах персональных данных АО «СМК «Сахамедстрах»
- Инструкции по организации парольной защиты информационных систем персональных данных АО «СМК «Сахамедстрах»
- Правилах обработки персональных данных в АО «СМК «Сахамедстрах

5.2. Все работники АО «СМК «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 требования нормативных правовых и внутренних организационно-распорядительных актов в области защиты информации, в части их касающейся[20].

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 «СМК «Сахамедстрах» своим приказом назначает лицо, ответственное за организацию обработки персональных данных.

6.2. Лицо, ответственное за организацию обработки персональных данных,

[19] В соответствии с разделом 4 Положения о разрешительной системе допуска пользователей к информационным системам персональных данных АО «СМК «Сахамедстрах»

[20] Осуществляется в соответствии с :
- п.6) ч.1 ст.18.1 Федерального закона от 27.07.2006 №152-ФЗ "О персональных данных";
- ч.8 ст. 86 Трудового кодекса Российской Федерации от 30.12.2001 №197-ФЗ;

получает указания непосредственно от генерального директора АО «СМК «Сахамедстрах»[21].

6.3. Должностные лица АО «СМК «Сахамедстрах» обязаны предоставлять лицу, ответственному за организацию обработки персональных данных, следующие сведения:[22]

- 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 «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.

6.4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано[23]:

- осуществлять внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных[24];
- доводить до сведения работников оператора положения

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

[22] В соответствии с ч.3 ст.22 и ч.3 ст.22. Федерального закона» от 27.07.2006 № 152-ФЗ «О персональных данных.

[23] В соответствии с ч.4 ст.22.1 Федерального закона » от 27.07.2006 № 152-ФЗ «О персональных данных»;

[24] Осуществляется в соответствии с :п.4) ч.1 ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- Планом внутренних проверок состояния защиты персональных данных АО «СМК «Сахамедстрах».

законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных[25];

- 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[26];
- осуществлять контроль организации допуска работников АО «СМК «Сахамедстрах» к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

7. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства и подзаконных актов[27]

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 «СМК «Сахамедстрах»осуществляют:

- лицо, ответственное за организацию обработки персональных данных, назначаемое приказом АО «СМК «Сахамедстрах»;
- администратор безопасности информации, исполнение обязанностей которого дополнительно возложены на существующего штатного работника[28].

7.2. Внутренний контроль соответствия обработки персональных данных требованиям законодательства и подзаконных актов осуществляется в соответствии с разработаными планами.

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 «СМК «Сахамедстрах»[29] о выявленных нарушениях и принятых мерах.

---

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

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

[27] Устанавливаются во исполнение:

- ч.4 ст.22.1 Федерального закона » от 27.07.2006 № 152-ФЗ «О персональных данных;
- раздела 7 Правил обработки персональных данных в АО «СМК «Сахамедстрах.

[28] п. 3 приказа АО «СМК «Сахамедстрах» «Об утверждении Положения об администраторе безопасности информации».

[29]Исполняется в соответствии с:ч.2 ст.22.1 Федерального закона » от 27.07.2006 № 152-ФЗ «О персональных данных;

- п.5.2.Положения об администраторе безопасности информации АО «СМК «Сахамедстрах»
- п.4.1.3 и п.5.1.5 Положения об ответственном за организацию обработки персональных данных в АО «СМК «Сахамедстрах»