



Утверждаю:
Главный врач ГАУЗ «КСП»
И.Н.Попова

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В
ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ
ГАУЗ «КСП»

Чита
2015

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники¹.
- **Автоматизированная система (АС)** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций².
- **Блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных)³.
- **Безопасность информации [данных]**- 1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность⁴; 2) состояние защищенности информации, характеризующееся 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 средствами⁵.
- **Доступность (санкционированная доступность) информации** - состояние информации, характеризующееся способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия⁶.
- **Информационная система персональных данных (ИСПДн)**- совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств⁷.
- **Несанкционированный доступ (несанкционированные действия) (НСД)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств,

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

²См.:

- 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.: ч.7) ст.3 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ).

⁴ См.: п. 2.4.5 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

⁵ См. п. 1.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282.

⁶ См.: п.1.9. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282.

⁷См.:

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

предоставляемых средствами вычислительной техники или автоматизированными системами⁸.

- **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 данных⁹.
- **Объект защиты информации**- информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации¹⁰.
- **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 данными¹¹.
- **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)¹².
- **СЗПДн** – система (подсистема) защиты персональных данных¹³.
- **Целостность информации** - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации¹⁴.
- **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 данных¹⁵.

⁸ См.: п.1.20. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282.

⁹ См.: ч.3.ст.3 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ).

¹⁰ См.: п. 2.5.1 ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

¹¹ См.: ч.2.ст.3 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ).

¹² См.: ч.1.ст.3 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ).

¹³ См.: раздел Определения 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.

¹⁴ См.: п.1.27. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282.

¹⁵ См.:

– п.2.6.1. ГОСТ Р 50922-2006. ЗАЩИТА ИНФОРМАЦИИ. ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ;

2. ЦЕЛЬ И ПРАВОВЫЕ ОСНОВАНИЯ

2.1. Настоящее Положение по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГАУЗ «КСП» (далее - Положение) разработано в соответствии с:

- Федеральным законом РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ (в ред. Федеральных законов от 27.07.2010 № 227-ФЗ, от 06.04.2011 № 65-ФЗ, с изм., внесенными Федеральным законом от 21.07.2011 № 252-ФЗ);
- Федеральным законом РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федеральных законов от 25.11.2009 № 266-ФЗ, от 27.12.2009 № 363-ФЗ, от 28.06.2010 № 123-ФЗ, от 27.07.2010 № 204-ФЗ, от 27.07.2010 № 227-ФЗ, от 29.11.2010 № 313-ФЗ, от 23.12.2010 № 359-ФЗ, от 04.06.2011 № 123-ФЗ, от 25.07.2011 № 261-ФЗ);
- Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 № 781;
- Положением о методах и способах защиты информации в информационных системах персональных данных, утвержденным приказом ФСТЭК России от 05.02.2010 № 58 (зарегистрирован в Минюсте РФ 19.02.2010 № 16456);
- Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», (зарегистрирован в Минюсте РФ 03.04.2008 г. № 1146);
- Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008;
- Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008;
- Типовой программой аудита организации и состояния работы по защите конфиденциальной информации в исполнительных органах государственной власти Забайкальского края, рекомендованной решением Совета информационной безопасности Забайкальского края от 31.10.2011 № 1 2011 и др.

2.2. В соответствии с ч.2. ст.18.1 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ) ГАУЗ «КСП» обязано опубликовать, разместить на официальном сайте или иным образом обеспечить неограниченный доступ к настоящему Положению.

3. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИСПДН ГАУЗ «КСП»

3.1. Общие положения:

3.1.1. ГАУЗ «КСП» при обработке персональных данных в ИСПДн принимает необходимые правовые, организационные и технические меры для защиты

-
- 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.

персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

3.1.2. Обеспечение безопасности персональных данных при обработке в ИСПДн ГАУЗ «КСП» достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в ИСПДн ГАУЗ «КСП»¹⁶;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн ГАУЗ «КСП», необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных¹⁷;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации¹⁸;

¹⁶ Выполняется в соответствии с:

- п.1) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. а) и п. б) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.2.9, п.2.1.3., п.2.1.4., 3.8., 6.1.2.Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.1.4. и п.1.5. Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15.02.2008;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15.02.2008 и др.

¹⁷ Выполняется в соответствии с:

- п.2) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. б) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.1.16, п.1.23, п.3.16, п.3.18, п.4.2.11, п.4.2.12, п.4.2.14, п.5.1.1., п.5.2.8, п.5.3, п.6.3.10 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- Техническим заданием Система защиты персональных данных информационных систем персональных данных Государственного учреждения здравоохранения «Краевая стоматологическая поликлиника №2»
- Проектом Система защиты персональных данных информационных систем персональных данных Государственного учреждения здравоохранения «Краевая стоматологическая поликлиника №2» и др.

¹⁸ Выполняется в соответствии с:

- п.3) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. в) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.2.16, п.3.16 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных¹⁹;
- учетом машинных носителей персональных данных²⁰;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер²¹;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним²²;
- установлением правил доступа к персональным данным, обрабатываемым в ИСПДн ГАУЗ «КСП», а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн ГАУЗ «КСП»²³;

— п.2.1. Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456) и др.

¹⁹ Выполняется в соответствии с:

- п.4) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п.3.2. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и п.9 Памятки Приложения 4 к указанным Специальным требованиям и др.

²⁰ Выполняется в соответствии с:

- п.5) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. е) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.5.1.3., п.5.3.6, п.5.4.4., п.5.6.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.2.1. Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456) и др.

²¹ Выполняется в соответствии с:

- п.6) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п.б) ст.11 и п. и) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п. 2.8- п.2.10, 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, и др.

²² Выполняется в соответствии с:

- п.7) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. г) ст.11 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.5.1.3. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и др.

²³ Выполняется в соответствии с:

- п.8) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- ст.14 и ст.15 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;

- контролем принимаемых мер по обеспечению безопасности персональных данных и уровня защищенности ИСПДн ГАУЗ «КСП»²⁴.

3.1.3. В настоящем Положении под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных²⁵. Под уровнем защищенности персональных данных понимается комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных²⁶.

3.1.4. 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 действий²⁷.

3.1.5. Предпринимаемые правовые, организационные и технические меры направлены на защиту персональных данных при обработке в электронной форме на средствах автоматизации, при передаче по каналам связи или на отчуждаемых машинных носителях информации, а также при обработке персональных данных без средств автоматизации.

3.2. Правовые и организационные меры

-
- п.5.9.1, 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 30.08.02 № 282;
 - п.2.1. Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456);
 - п.5.3. Положения о персональных данных ГАУЗ «КСП», утвержденного приказом ГАУЗ «КСП» от 07.12.2011 № 56;
 - разделом 2 Положения о разрешительной системе допуска исполнителей к ИСПДн, утвержденного приказом ГАУЗ «КСП» от 07.12.2011 №61.

²⁴Выполняется в соответствии с:

- п.8) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. д) ст.11 и п. з) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.3.2, п.3.24, п.4.2.14, п.5.1.3., п.5.7.6., п.5.8.2 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и др.

²⁵ См. ч.11 ст.19. Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);

²⁶ Там же.

²⁷См.:

- ч.11 ст.19. Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- ст.2 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.1.6., п.2.10, п.2.14, п.5.1.3, п.6.1.2 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и др.

3.2.1. ГАУЗ «КСП» осуществляет следующие правовые и организационные меры, направленные на защиту персональных данных в ИСПДн ГАУЗ «КСП»:

- ведет перечень персональных данных, обрабатываемых в ИСПДн ГАУЗ «КСП»²⁸;
- классифицирует ИСПДн ГАУЗ «КСП»²⁹;
- определяет угрозы безопасности персональных данных при их обработке в ИСПДн ГАУЗ «КСП» и формирует на их основе модели угроз³⁰;
- разрабатывает на основе моделей угроз систему защиты персональных данных, обеспечивающую нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем³¹;
- разрабатывает внутренние административно - распорядительные документы, доводит их до сведения работников под роспись, а также контролирует их исполнение³²;

²⁸См.:

- п.5) ч.4. ст.9 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п.3.6, п.3.8, п.3.10, п.6.2.2. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и Приложение 6 к указанным Специальным требованиям.

²⁹ Выполняется в соответствии с:

- ст.6 Постановления Правительства РФ от 17.11. 2007г. №781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных",
- приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных», зарегистрированного в Минюсте РФ 03.04.2008г. №11462;
- п.5.1.6. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и др.

См. также: акты классификации ИСПДн .

³⁰ Выполняется в соответствии с:

- п.1) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. а) и п. б) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.2.9, п.2.1.3., п.2.1.4.,п.3.6.,п. 3.8., 6.1.2.Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.1.4. и п.1.5. Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456);
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15.02.2008;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15.02.2008 и др.;

³¹См.:

- п. а) и п. б) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;

³² Выполняется в соответствии с:

- контролирует правильность функционирования и использования средств защиты информации, применяемых для защиты ПДн³³;
- контролирует неизменность состава программных и технических средств, определенных проектной документацией на систему защиты персональных данных³⁴;
- осуществляет контроль лиц, допущенных к работе с персональными данными³⁵;
- осуществляет контроль применяемых средств защиты информации и ведет их реестр³⁶;
- организует надежную охрану в нерабочее время средств защиты информации и средств вычислительной техники, на которых обрабатываются персональные данные³⁷;

-
- п.2), п. 3) и п.6) ч.1 ст.18¹, п.2) ч.4 ст.22.1 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
 - п.д) и п.з) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781.

³³Выполняется в соответствии с:

- п.9) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. з) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.3.24, п.5.71, п.6.3.13, п.6.3.20 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и п.6. Приложения 2, п.5 Приложения3 и п.9 Приложения 4 к указанным Специальным требованиям.
- п.2.2. Приложения к Положению о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456) и др.

³⁴Выполняется в соответствии с:

- п.5.4.1, п.6.3.9, п.6.3.19 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и п.5. Приложения 2, п.4 Приложения3 к указанным Специальным требованиям.
- п. в) ст.2.2 и п. в) ст.2.3. Положения о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456) и др.

³⁵Выполняется в соответствии с:

- п.8) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п.ж) ст.12, ст.14 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.2.1.а) и п. 2.1.б) Приложения к Положению о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456);
- раздел 5.3. Положения о персональных данных ГАУЗ «КСП»;
- раздел 12 Инструкции по конфиденциальному делопроизводству в ГАУЗ «КСП».

³⁶Выполняется в соответствии с:

- п. е) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.3.24, п.6.3.13, Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, и п.6. Приложения 2 к указанным Специальным требованиям.

³⁷Выполняется в соответствии с:

- проводит контроль состояния системы защиты персональных данных с установленными в проектной документации интервалами³⁸.

3.2.2. Комплекс внутренней административно - распорядительной и технической документации в области защиты персональных данных включает в себя:

- Техническое задание Система защиты персональных данных информационных систем персональных данных Государственного учреждения здравоохранения «Краевая стоматологическая поликлиника №2»;
- Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждения здравоохранения «Краевая стоматологическая поликлиника №2»;
- Политику информационной безопасности ГАУЗ «КСП»;
- Инструкцию по конфиденциальному делопроизводству в ГАУЗ «КСП»;
- Приказ ГАУЗ «КСП» « Об утверждении Положения об архиве ГАУЗ «КСП» и Положения о Постоянно действующей экспертной комиссии ГАУЗ «КСП»;
- Положение о персональных данных ГАУЗ «КСП»;
- Положение о порядке организации и проведении работ по защите информации, в отношении которой установлено требование о соблюдении ее конфиденциальности;
- Положение об администраторе безопасности информации ГАУЗ «КСП»;
- Инструкцию администратору безопасности информации по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности;
- Положение о разрешительной системе допуска исполнителей к ИСПДн;

-
- п.2) ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
 - ст.8 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
 - п.3.16, п.5.1.3., п.5.1.6 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
 - п.2.1.в), п. 2.2.в) и п. 2.3.в) Приложения к Положению о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456
 - Инструкцией по обеспечению физической охраны помещений контролируемой зоны ГАУЗ «КСП» и др.

³⁸Выполняется в соответствии с:

- п.4)ч.1 ст.18.1, п.9 ч.2 ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п. в) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
- п.3.2.4 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.2.1.в), п. 2.2.в) и п. 2.3.в) Приложения к Положению о методах и способах защиты информации в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 05.02.2010 №58 (зарегистрирован в Минюсте РФ 19.02.2010 №16456 и др.

- Инструкцию по учету, маркировке, очистке и утилизации машинных носителей информации;
- Инструкцию по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования, утвержденную приказом ГАУЗ «КСП»;
- Регламент безопасного функционирования подсистемы криптографической защиты информации;
- Инструкцию пользователям по обеспечению правил информационной безопасности при работе в информационных системах персональных данных;
- Инструкцию по организации антивирусной защиты в информационных системах персональных данных;
- Инструкцию по организации парольной защиты информационных систем персональных данных;
- Инструкцию по обеспечению физической охраны помещений контролируемой зоны ГАУЗ «КСП»;
- Правила обработки персональных данных без средств автоматизации;
- План внутренних проверок состояния защиты персональных данных;
- План мероприятий по защите персональных данных;
- «Об утверждении сроков и мест хранения материальных носителей персональных данных»;
- «Об утверждении типовых форм журналов регистрации обращений граждан».

3.2.3. Контроль исполнения требований административно- распорядительных и технических документов осуществляет администратор безопасности информации, ответственный за защиту информации³⁹.

3.3. Технические меры

3.3.1. Для обеспечения безопасности персональных данных в ИСПДн ГАУЗ «КСП» применяет следующие средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия и определенные проектной документацией⁴⁰:

- средства защиты информации от несанкционированного доступа;
- средства межсетевого экранирования;
- средства обнаружения вторжений и анализа защищенности
- средства антивирусной защиты;
- криптографические средства.

3.3.2. Обслуживание средств защиты информации в ходе их эксплуатации возлагается на администратора безопасности информации⁴¹.

³⁹ Выполняется в соответствии с:

- п.2), п. 3) и п.6) ч.1 ст.18.1, , п.2) ч.4 ст.22.1 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ; (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- п.д) и п.з) ст.12 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781.

⁴⁰ См.: Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждения здравоохранения «Краевая стоматологическая поликлиника №1».

⁴¹ См.:

-
- п.3) ст.12.Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11.2007 №781;
 - п.1.5, п.5.7.2, п.5.7.5, п.6.3.7, п.6.3.9, п.6.3.20 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
 - Положение об администраторе безопасности информации ГАУЗ «КСП
 - Инструкцию администратору безопасности информации по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности.