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

ПОЛИТИКА

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ГАУЗ «КСП»

Чита
2015

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники[1].
- **Автоматизированная система (АС)** - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[2].
- **Безопасность информации [данных]**-1) состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность[3]; 2) состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами[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].
- **Замысел защиты информации**- основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации[6].
- **Информационная система персональных данных (ИСПДн)**-совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств[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[8].

---

[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).

[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.3Федерального 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.

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

- **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].
- **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[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].
- **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными

---

[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 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.

[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.

данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных[12].

- **Объект защиты информации-**информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации[13].
- **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[14].
- **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[15].
- **Политика безопасности (информации в организации)-** совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности[16].
- **СЗПДн –** система (подсистема) защиты персональных данных[17].
- **Целостность информации** - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации[18].
- **Цель защиты информации-**заранее намеченный результат защиты информации[19].
- **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[20].

---

[12]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).

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

[14]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).

[15] 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).

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

[17]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.

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

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

[20]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.

2 ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящая Политика информационной безопасности ГАУЗ «КСП» (далее – Политика) определяет общуюсовокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется ГАУЗ «КСП»в своей деятельности.

2.2. Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, при их обработке в ГАУЗ «КСП», изложенных в Техническом задании и Техническом проекте на создание СЗПДн[21].

2.3. Политика разработана в соответствии с:

- Конституцией РФ;
- Федеральным законом РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 № 149-ФЗ;
- Федеральным законом РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ);
- Федеральным законом РФ «Об обязательном медицинском страховании в Российской Федерации» от 29.11.2010 № 326-ФЗ;
- Трудовым кодексом Российской Федерации от 30.12.2001 № 197-ФЗ;
- Законом Российской Федерации «О безопасности» от 05.03.1992 № 2446-1.
- Доктриной информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № Пр.-1895;
- Постановлением Правительства РФ от 17.11. 2007 №781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных";
- Постановлением Правительства Российской Федерации от 15.09.2008 №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- Постановлением Правительства РФ от 31 декабря 2010 №1226 «Об издании разъяснений по единому применению Федерального закона «Об обязательном медицинском страховании в Российской Федерации»;
- Постановлением Правительства РФ от 15.02.2011 № 74 "О правилах обязательного медицинского страхования";
- Постановление Правительства Российской Федерации от 26.06.1995 № 608 «О сертификации средств защиты информации»;
- Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 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

[21] См :

- Техническое задание Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»;
- Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»

данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662;

- Правилами обязательного медицинского страхования, утвержденными приказом Министерства здравоохранения и социального развития Российской Федерации от 28.02.2011 № 158н (зарегистрировано в Минюсте РФ 03.03.2011 № 19998);
- 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;
- Порядком ведения персонифицированного учета в сфере обязательного медицинского страхования, утвержденным приказом Министерства здравоохранения и социального развития Российской Федерации от 25.01.2011 № 29н (зарегистрирован в Минюсте РФ 08.02.2011 № 19742);
- Порядком организации и проведения контроля объемов, сроков, качества и условий предоставления медицинской помощи по обязательному медицинскому страхованию, утвержденному приказом ФФОМС от 02.12.2010 № 230 (Зарегистрировано в Минюсте РФ 28.01.2011 № 19614);
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная Заместителем директора ФСТЭК России 14.02.2008;
- Методическими указаниями по представлению информации в сфере обязательного медицинского страхования, утвержденные Председателем Федерального фонда обязательного медицинского страхования 04.04. 2011;
- 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 и др.

2.4. Целью настоящей Политики является определение основных правил обеспечения безопасности объектов защитыГАУЗ «КСП» 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 ГАУЗ «КСП»[22]

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[23].

---

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

[23] 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.

2.7. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей[24]. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных[25].

2.8. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных[26].

2.9. Состав объектов защиты представлен в техническом проекте на создание СЗПДн[27].

2.10. Состав ИСПДн подлежащих защите, представлен в Положении о персональных данных[28].

2.11. В Политике определены общий замысел защиты информации ГАУЗ «КСП»,требования к пользователям ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн ГАУЗ «КСП».

2.12. Требования Политики обязательны для всех работников ГАУЗ «КСП», представителей контрольно- надзорных органов, допущенных к защищаемой информации на законных основаниях, а также работников иных организаций допущенных к защищаемой информации для проведения работ по гражданско-правовым договорам[29].

2.13. 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 настоящей Политике.

3 СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХГАУЗ «КСП»

3.1. Система защиты персональных данных (СЗПДн), строится на основаниипримененияправовых, организационных и технических мер по обеспечению безопасности персональных данных[30].

– 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).

[24] 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.

[25] Исполняется 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. 3.24. 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, 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).

[26] Исполняется 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.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.

[27] См.:Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждения здравоохранения «КСП №2»

[28] См. раздел 3.3. Положения о персональных данных ГАУЗ «КСП №2».

[29] См. разделы 6.1- 6.2.2. Положения о персональных данных ГАУЗ «КСП №2».

[30] См.: п.3) ч.1. ст.18.1, ст.19 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. Федерального закона от 25.07.2011 № 261-ФЗ).

3.2. Указанные в п.3.1. настоящей Политики меры по обеспечению безопасности персональных данных регламентированы следующими внутренними административно- распорядительными и инструктивно- технологическими документамиГАУЗ «КСП»:

- Техническое задание Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»[31];
- Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»[32];
- Акты классификации информационных систем персональных данных;
- Инструкция по конфиденциальному делопроизводству в ГАУЗ «КСП»;
- Положение о персональных данных ГАУЗ «КСП»[33];
- 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»;
- Инструкция 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;
- Инструкция по учету, маркировке, очистке и утилизации машинных носителей информации;
- Инструкция по обеспечению информационной безопасности при подключении и использовании информационно- вычислительной сети общего пользования;
- Регламент безопасного функционирования подсистемы криптографической защиты информации;
- Инструкция пользователям по обеспечению правил информационной безопасности при работе в информационных системах персональных данных;
- Инструкция по организации антивирусной защиты в информационных системах персональных данных;
- Инструкция по организации парольной защиты информационных систем персональных данных;
- Правила обработки персональных данных без средств автоматизации;
- План внутренних проверок состояния защиты персональных данных;
- План мероприятий по защите персональных данных;
- приказ «Об утверждении сроков и мест хранения материальных носителей персональных данных»;
- приказ «Об утверждении типовых форм журналов регистрации обращений граждан»;
- Инструкция по обеспечению физической охраны помещений контролируемой зоны ГАУЗ «КСП».

3.3. На основании указанных в п.2.3. п.3.2.нормативно- правовых и административно-распорядительных документов определяется необходимый уровень защищенности

[31] Модели угроз безопасности персональных данных рассматриваются в указанном Техническом задании.

[32] Разграничение прав доступа к обрабатываемым персональным данным описано в указанном Техническом проекте.

[33] Перечень персональных данных, подлежащих защите указан в разделе 3.3. названного Положения о персональных данных.

ПДн каждой ИСПДн ГАУЗ «КСП». На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз[34], сделано заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые технические мероприятия отражены в Техническом проекте[35] в Плане мероприятий по обеспечению защиты ПДн[36].

3.4. Для каждой ИСПДн в разработанном соответствующем Паспорте ИСПДн[37]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. Разработанная в Техническом проекте 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[40];
- обнаружение вторжений[41].

---

[34] См. Техническое задание Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2».

[35] См.: Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»

[36] См. План мероприятий по защите персональных данных

[37] См.Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»

[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.

[40] Исполняется в соответствии с:

- п.1.27, п.2.8, п.2.9., п.3.4. , п.3.24, 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.2.2., п.2.7, п.2.8, п.2.9 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, п.2.1.в), п.2.2.в), п.2.3.в), п.2.4.в), п.3, п.3.4., п.4, п.4.1.в), п.4.2.в), п.4.3.в), п.4.4. Приложения к указанному Положению;
- 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.

[41] Исполняется 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 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного Постановлением Правительства РФ от 17.11. 2007 №781;

3.7. Список используемых технических средств отражается в Техническом проекте на создание СЗПДн[42]. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Технический проект по согласованию с разработчиком[43].

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

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты[44].

3.9. Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных[45].

3.10. Подсистемы СЗПДн, указанные в п.3.8. настоящей Политики подробно разработаны для каждой ИСПДн в Техническом проекте[46].

4 ПОЛЬЗОВАТЕЛИ ИСПДН

4.1. В Техническом проекте определены следующие категории пользователей ИСПДн[47]:

- администратор ИСПДн;

- 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.

[42] См.:Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2».

[43] Исполняется в соответствии с п.5.4.2. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282, а также п.5. Приложения 2 к указанным Специальным требованиям.

[44] См.: Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2».

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

- ст.22, ч.2.1. ст.25 Федерального закона РФ «О персональных данных» от 27.07.2006 № 152-ФЗ,
- ст.6, п. б) ст.12 Постановления Правительства РФ от 17.11.2007 №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 13.02.2008 №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".

[46] См.: Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»

[47] См.: Проект Система защиты персональных данных информационных систем персональных данных Государственного учреждение здравоохранения «Краевая стоматологическая поликлиника №2»

- администратор безопасности информации;
- оператор.

4.2. В Паспортах каждой ИСПДн указанного Технического проекта разработаны матрицы доступа[48] 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 исполнителей к ИСПДн[49].

4.4. Администратор ИСПДн:

4.4.1. Администратор ИСПДн – работник ГАУЗ «КСП», ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора) к 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 ГАУЗ «КСП», ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

4.5.2. Администратор безопасности 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).

4.5.3. Администратор безопасности 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 субъектов и участников ОМС[50].

---

[48] Разрабатывается во исполнение:

- п.1.24, п.5.1.3., п.5.9.1., п.5.9.2., п.6.3.2., п.6.3.11.4. Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных, приказом Гостехкомиссии России от 30.08.02 № 282;
- п.2.1. и п.4.3. 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).

[49] См.:Положения о разрешительной системе допуска исполнителей к ИСПДн,

[50] Устанавливается в соответствии сс требованиями ст.9, п.7 и п.9 ст.38, п.1 ч.4 ст.39, главы 10 Федерального закон РФ «Об обязательном медицинском страховании в Российской Федерации» от 29.11.2010 № 326-ФЗ.

4.6. Оператор:

4.6.1. Оператор- работник ГАУЗ «КСП», 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 ПОЛЬЗОВАТЕЛЯМПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Требования к работникам ГАУЗ «КСП» , допущенным в установленном порядке к персональным данным[51], их права и обязанности установлены в:

- Инструкции пользователям по обеспечению правил информационной безопасности при работе в информационных системах персональных данных;
- Положенииоб администраторе безопасности информации ГАУЗ «КСП»;
- Инструкции администратору безопасности информации по администрированию средств защиты информации от несанкционированного доступа, криптографических средств защиты информации, средств анализа защищенности;
- Инструкции по организации антивирусной защиты в информационных системах персональных данных;
- Инструкции по организации парольной защиты информационных систем персональных данных;
- Правилах обработки персональных данных без средств автоматизации.

5.2. Все работники ГАУЗ «КСП», 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 нормативно- правовых и внутренние административно- распорядительных актов в области защиты информации, в части их касающейся[52].

---

[51] В соответствии с разделом 12 Инструкции по конфиденциальному делопроизводству в ГАУЗ «КСП №2», утвержденной приказом ГАУЗ «КСП №2» от 07.12.2011 № 38

[52] Осуществляется в соответствии с :

- п.6) ч.1 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);
- п. д) ст.12 Постановления Правительства РФ от 17.11.2007 №781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных";
- ст.6 Постановления Правительства Российской Федерации от 15.09.2008 №687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- п.5.2.2., п.5.3.1., п.6.3.14. Специальных требований 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.

5.4. Пользователи надлежащим образом должны быть извещены об ответственности за нарушениетребований нормативно- правовых и внутренние административно-распорядительных актов в области защиты информации.