Приложение № 1
к приказу
Министерства здравоохранения
Калининградской области
от «25» апреля 2013 г. № 151

КОНЦЕПЦИЯ
информационной безопасности информационных систем персональных данных Министерства здравоохранения Калининградской области и государственных медицинских организаций Калининградской области

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Концепция информационной безопасности информационных систем персональных данных Министерства здравоохранения Калининградской области и государственных медицинских организаций Калининградской области (далее - Концепция) разработана в целях реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иных нормативных правовых актов, руководящих и методических документов по информационной безопасности.

Концепция определяет общую стратегию, основные цели и задачи построения системы защиты персональных данных (далее - СЗПДн), а также основные требования и базовые подходы к их реализации для достижения требуемого уровня информационной безопасности персональных данных (далее - ПДн) в Министерстве здравоохранения Калининградской области (далее - Министерство) и в государственных учреждениях здравоохранения Калининградской области, подведомственных Министерству (далее – медицинские организации).

2. Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности.

Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью ПДн понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может

явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или техническим средствам информационных систем персональных данных.

Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

3. Концепция служит основой для разработки комплекса организационных мер по обеспечению информационной безопасности, мероприятий технической и физической защиты объектов, информационных систем персональных данных (далее - ИСПДн) в Министерстве и медицинских организациях, а также нормативных и методических документов, обеспечивающих ее реализацию. Концепция не подменяет функции государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

4. Концепция является методологической основой:

- формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн в Министерстве и медицинских организациях;
- принятия управленческих решений, разработки практических мер по воплощению Политики информационной безопасности ИСПДн в Министерстве и медицинских организациях и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;
- координации деятельности должностных лиц и структурных подразделений Министерства и медицинских организаций при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн в Министерстве и в медицинских организациях.

5. Область применения Концепции распространяется на все структурные подразделения Министерства и медицинских организаций, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн.

Требования настоящей Концепции не распространяется:

- на обработку ПДн, отнесенных в установленном порядке к сведениям, составляющим государственную тайну;
- на обработку ПДн без использования средств автоматизации в соответствии с постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6. Основные термины и определения:

1) Автоматизированная система – система, включающая государственных гражданских служащих (служащих) Министерства здравоохранения Калининградской области, сотрудников медицинских организаций Калининградской области и комплексы средств автоматизации их деятельности, реализующая информационную технологию предоставления государственных услуг и исполнения установленных государственных функций.

2) Автоматизированная обработка персональных данных - обработка ПДн с помощью средств вычислительной техники.

3) Актуальные угрозы безопасности ПДн - совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия

4) Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

5) База данных - представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины.

6) Безопасность персональных данных – состояние защищенности ПДн, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность ПДн при их обработке в ИСПДн.

7) Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

8) Блокирование персональных данных - временное прекращение обработки ПДн (за исключением случаев, когда обработка необходима для уточнения ПДн).

9) Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

10) Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на ПДн или ресурсы ИСПДн.

11) Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения ПДн, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки ПДн, или в помещениях, в которых установлены ИСПДн.

12) Доступ в операционную среду компьютера (ИСПДн) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

13) Доступ к информации – возможность получения информации и ее использования.

14) Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

15) Защищаемая информация – информация, являющаяся предметом собственности Министерства и (или) медицинских организаций и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

16) Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

17) Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (ПДн), обрабатываемая в ИСПДн.

18) Информационная система персональных данных - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

19) Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

20) Использование персональных данных – действия (операции) с ПДн, совершаемые оператором ПДн в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

21) Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

22) Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

23) Конфиденциальность персональных данных – обязательное для соблюдения оператором ПДн или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

24) Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в ИСПДн и (или) выходящей из информационной системы.

25) Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПДн при их обработке техническими средствами в ИСПДн.

26) Неавтоматизированная обработка персональных данных – обработка ПДн, содержащихся в ИСПДн либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с ПДн как использование, уточнение, распространение, уничтожение ПДн в отношении каждого из субъектов ПДн осуществляются при непосредственном участии человека.

27) Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

28) Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых ИСПДн.

29) Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

30) Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

31) Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

32) Обслуживающий персонал информационной системы персональных данных – физические лица непосредственно не участвующие в эксплуатации ИСПДн, но осуществляющие обслуживание технических средств ИСПДн, вспомогательных технических средств и систем, в результате действий которых

случайно или преднамеренно может быть нарушена безопасность ПДн или несанкционированное ознакомление.

33) Общедоступные персональные данные – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

34) Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

35) Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

36) Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

37) Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

38) Пользователь информационной системы персональных данных – лицо, участвующее в эксплуатации ИСПДн или использующее результаты ее функционирования.

39) Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

40) Предоставление персональных данных - действия, направленные на раскрытие ПДн определенному лицу или определенному кругу лиц.

41) Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

42) Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение ИСПДн и (или) блокировать аппаратные средства.

43) Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

44) Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности ПДн.

45) Распространение персональных данных - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

46) Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

47) Система защиты ПДн – это комплекс организационных и (или) технических мер, определяемых с учетом актуальных угроз безопасности ПДн и информационных технологий, используемых в информационных системах.

48) Специальные информационные системы персональных данных - информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности ПДн требуется обеспечить хотя бы одну из характеристик безопасности ПДн, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

49) Специальные категории персональных данных – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта ПДн.

50) Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

51) Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

52) Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

53) Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

54) Типовые информационные системы персональных данных - информационные системы, в которых требуется обеспечение только конфиденциальности ПДн.

55) Трансграничная передача персональных данных - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

56) Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн.

57) Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

58) Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

59) Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

60) Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

II. КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

7. Все ИСПДн, эксплуатируемые в Министерстве и в медицинских организациях подлежат классификации. Классификация ИСПДн проводится оператором ПДн.

Классификация ИСПДн проводится на этапе создания ИСПДн или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИСПДн) с целью установления методов и способов защиты информации, необходимых для обеспечения безопасности ПДн.

Проведение классификации ИСПДн включает в себя следующие этапы:

- сбор и анализ исходных данных по ИСПДн;
- присвоение ИСПДн соответствующего класса и его документальное оформление.

8. Характеристиками безопасности ПДн при классификации ИСПДн являются:

- конфиденциальность (защита от несанкционированного ознакомления);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- доступность (возможность за приемлемое время получить требуемую информационную услугу).

9. По заданным оператором ПДн характеристикам безопасности ПДн, обрабатываемым в ИСПДн, информационные системы подразделяются на:

- типовые ИСПДн;
- специальные ИСПДн.

Типовые ИСПДн включают одну характеристику безопасности ПДн, которую необходимо обеспечить, - конфиденциальность.

Специальные ИСПДн вне зависимости от необходимости обеспечения конфиденциальности ПДн включают хотя бы одну из характеристик безопасности ПДн, отличной от конфиденциальности.

10. По структуре ИСПДн подразделяются на:

- автономные (не подключенные к иным информационным системам) комплексы технических и программных средств, предназначенные для обработки ПДн (автоматизированные рабочие места);

- комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа (локальные информационные системы);

- комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием технологии удаленного доступа (распределенные информационные системы).

11. По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена ИСПДн подразделяются:

- на системы, имеющие подключения;

- на системы, не имеющие подключений.

12. По режиму обработки ПДн в ИСПДн информационные системы подразделяются на:

- однопользовательские ИСПДн;

- многопользовательские ИСПДн.

13. По разграничению прав доступа пользователей ИСПДн подразделяются на:

- системы без разграничения прав доступа;

- системы с разграничением прав доступа.

14. ИСПДн в зависимости от местонахождения их технических средств подразделяются на:

- системы, все технические средства которых находятся в пределах Российской Федерации;

- системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

15. При проведении классификации типовой ИСПДн учитываются:

- категория ПДн, обрабатываемых в информационной системе;

- объем обрабатываемых ПДн (количество субъектов ПДн, персональные данные которых обрабатываются в ИСПДн);

- исходные данные для классификации, указанные в пунктах 9-14 настоящей Концепции.

Классификация типовых ИСПДн осуществляется на основании совместного приказа Федеральной службы таможенного экспортного контроля, Федеральной службы безопасности Российской Федерации, Министерства информационных технологий и связи Российской Федерации от 13.02.2008 №55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

16. Классификация специальных ИСПДн осуществляется по результатам анализа исходных данных, указанных в пунктах 9-14 настоящей Концепции, на основе модели угроз безопасности ПДн.

Классификация специальных ИСПДн осуществляется в два этапа:

- на первом этапе специальная ИСПДн классифицируется как типовая ИСПДн по характеристике безопасности ПДн «конфиденциальность»;

- на втором этапе специальная ИСПДн классифицируется на основании модели угроз безопасности ПДн – по другим характеристикам безопасности ПДн, после чего специальной ИСПДн присваивается класс информационной системы.

17. В результате классификации ИСПДн присваивается один из следующих классов:

- класс 1 (К1) - информационные системы, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПДн;

- класс 2 (К2) - информационные системы, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к негативным последствиям для субъектов ПДн;

- класс 3 (К3) - информационные системы, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПДн;

- класс 4 (К4) - информационные системы, для которых нарушение заданной характеристики безопасности ПДн, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПДн.

18. В случае выделения в составе ИСПДн подсистем, каждая из которых является информационной системой, ИСПДн в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем. Результаты классификации ИСПДн оформляются актом оператора ПДн.

III. УСТАНОВЛЕНИЕ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

19. Для всех ПДн, обрабатываемых в Министерстве и в медицинских организациях устанавливается уровень защищенности.

Уровень защищенности ПДн устанавливается оператором ПДн на основании постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и указывается в акте классификации ИСПДн.

Установление уровня защищенности ПДн включает следующие этапы:

- определение типа ИСПДн в соответствии с категорией ПДн;

- учёт актуальных угроз безопасности ПДн;

- установление уровня защищенности ПДн и его документальное оформление.

20. Определение типа ИСПДн.

ИСПДн на основании категории ПДн подразделяются на:

1) ИСПДн, обрабатывающие специальные категории ПДн, если в ней обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн;

2) ИСПДн, обрабатывающие биометрические ПДн, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных;

3) ИСПДн, обрабатывающие общедоступные ПДн, если в ней обрабатываются ПДн субъектов персональных данных, полученные только из общедоступных источников ПДн, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»;

4) ИСПДн, обрабатывающие иные категории персональных данных, если в них не обрабатываются персональные данные, указанные подпунктах 1-3 пункта 20 настоящей Концепции.

Кроме того ИСПДн подразделяются на:

- ИСПДН, обрабатывающие ПДн сотрудников оператора, если в них обрабатываются ПДн только указанных сотрудников;

- ИСПДн, обрабатывающие ПДн субъектов персональных данных, не являющихся сотрудниками оператора.

21. Учет актуальных угроз безопасности ПДн.

Актуальные угрозы делятся на 3 типа:

- угрозы 1-го типа актуальны для ИСПДн, если для них в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИСПДн;

- угрозы 2-го типа актуальны для ИСПДн, если для них в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн;

- угрозы 3-го типа актуальны для ИСПДн, если для них актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

Определение типа угроз безопасности ПДн, актуальных для ИСПДн, производится оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18.1 Федерального закона «О персональных данных», и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона «О персональных данных» на основании частной модели угроз.

22. При обработке ПДн в ИСПДн устанавливается 4 уровня защищенности ПДн в соответствии с пунктами 9-12 постановления Правительства Российской Федерации от 01.11.2012 № 1119.

23. Перечень требований, необходимых для обеспечения заданного уровня защищенности приведен в таблице 1

Таблица 1

Перечень требований	Уровень защищенности персональных данных			
	4 уровень	3 уровень	2 уровень	1 уровень
Организация режима обеспечения безопасности помещений, в которых размещена ИСПДН, препятствующая возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения	+	+	+	+
Обеспечение сохранности носителей ПДн	+	+	+	+
Наличие утвержденного перечня лиц оператора, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей	+	+	+	+
Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства РФ в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации таких угроз	+	+	+	+
Назначение должностного лица, ответственного за обеспечение безопасности ПДн в ИСПДн		+	+	+
Обеспечение доступа к содержанию электронного журнала сообщений только для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей			+	+
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн, содержащимся в ИСПДн				+
Создание структурного подразделения, ответственного за обеспечение безопасности ПДн в ИСПДн, либо возложение на одно из структурных подразделений функции по обеспечению такой безопасности				+

24. Контроль выполнения требований, необходимых для обеспечения заданного уровня защищенности ПДн организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

IV. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

25. Система защиты персональных данных Министерства и медицинских организаций создаётся на основе Перечня ИСПДн и представляет собой совокупность организационных и (или) технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

СЗПДн создаётся индивидуально для каждой ИСПДн 1, 2 и 3 классов, при этом отдельные мероприятия СЗПДн, предусмотренные для одной ИСПДн, могут включаться в состав СЗПДн для другой ИСПДн.

26. Безопасность ПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

27. Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн и уровня защищенности ПДн. СЗПДн включает организационные меры, технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), используемые в информационной системе информационные технологии.

28. Стадии создания СЗПДн включают:

- предпроектную стадию, включающую предпроектное обследование ИСПДн, разработку технического (частного технического) задания на ее создание или отдельного раздела технического задания;
- стадию проектирования (разработки проектов) и реализации ИСПДн, включающую разработку СЗПДн в составе ИСПДн;
- стадию ввода в действие СЗПДн, включающую опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

29. В Министерстве и в медицинских организациях ведутся Перечни ИСПДн. Перечни ИСПДн формируются (уточняются) на основании ежегодных отчётов по результатам проверок условий обработки ПДн, при вводе ИСПДн в эксплуатацию, а также при осуществлении модернизации ИСПДн.

Ответственность за ведение Перечней ИСПДн в Министерстве и в медицинских организациях возлагается на ответственных за обеспечение безопасности ПДн в ИСПДн.

Перечень ИСПДн включает:

- наименование ИСПДн (полное и сокращённое);
- наименование оператора ПДн: Министерство, медицинская организация (полное и сокращённое), почтовый адрес;
- ведомственная принадлежность – для медицинских организаций;
- исходные данные для классификации ИСПДн, указанные в пунктах 9-14 настоящей Концепции;
- класс ИСПДн;
- исходные данные для установления уровня защищенности ПДн, указанные в пунктах 20-21 настоящей Концепции;
- уровень защищенности ПДн;
- перечень ПДн, обрабатываемых в ИСПДн.

30. Цели и задачи СЗПДн.

Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

Для достижения основной цели система безопасности ПДн в ИСПДн должна обеспечивать эффективное решение следующих задач:

1) защита от вмешательства в процесс функционирования ИСПДн посторонних лиц (использование автоматизированной системы и доступ к ее ресурсам разрешается только зарегистрированным установленным порядком пользователям);

2) разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защита от несанкционированного доступа:

- к информации, циркулирующей в ИСПДн;
- средствам вычислительной техники ИСПДн;
- аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

3) регистрация действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов, контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

4) защита от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защита системы от внедрения несанкционированных программ;

5) защита ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

6) защита ПДн, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

7) обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

8) своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

9) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

V. МЕРЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

31. При эксплуатации ИСПДн Министерством, медицинской организацией - оператором ПДн планируются и выполняются меры по защите ПДн:

- создание и поддержание правовой базы безопасности ПДн в актуальном состоянии;

- назначение ответственных за организацию обработки ПДн из числа государственных гражданских служащих Министерства, сотрудников медицинских организаций;

- принятие правовых, организационных и технических мер по обеспечению безопасности ПДн при их обработке, предусмотренных соответствующими нормативными правовыми актами, для выполнения установленных Правительством Российской Федерации требований к защите ПДн при их обработке, исполнение которых обеспечивает установленные уровни защищённости ПДн;

- проведение ежегодных проверок условий обработки ПДн с подготовкой отчётов о результатах проведения проверок и указанием мер, необходимых для устранения выявленных нарушений;

- ознакомление государственных гражданских служащих Министерства, сотрудников медицинских организаций, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), правовыми актами по вопросам обработки ПДн, и (или) организация обучения указанных государственных гражданских служащих (служащих) и сотрудников;

- уведомление уполномоченного органа по защите прав субъектов ПДн – Управления Роскомнадзора по Калининградской области об обработке (намерении осуществить обработку) ПДн, за исключением случаев, установленных Федеральным законом от 27.07.2006 № 152-ФЗ;

- обезличивание ПДн, обрабатываемых в ИСПДн, в том числе созданных и функционирующих в рамках реализации целевых программ, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов ПДн.

32. В соответствии с постановлением Правительства Российской Федерации от 21.03.2012 № 211 в целях организации работ по защите ПДн в Министерстве разрабатываются (вводятся в действие) следующие документы:

- Правила обработки ПДн;
- Правила рассмотрения запросов субъектов ПДн или их представителей;
- Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн;
- Правила работы с обезличенными данными;
- Перечень ИСПДн;
- Перечень ПДн, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций;
- Перечень должностей государственных гражданских служащих Министерства, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;
- Перечень должностей государственных гражданских служащих Министерства, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;
- Должностная инструкция ответственного за организацию обработки ПДн в Министерстве;
- Типовое обязательство государственного гражданского служащего Министерства, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными в связи с исполнением должностных обязанностей;
- Типовая форма согласия на обработку ПДн государственных гражданских служащих Министерства, иных субъектов ПДн, а также типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои персональные данные;
- Порядок доступа государственного гражданского служащего Министерства в помещения, в которых ведётся обработка ПДн;

33. В соответствии с Методическими рекомендациями для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, разработанными Министерством здравоохранения и социального развития Российской Федерации и согласованными с Федеральной службой таможенного и экспортного контроля России в целях организации работ по защите ПДн в медицинских организациях выполняются мероприятия и разрабатываются (вводятся в действие) следующие документы:

- приказ об организации внутреннего контроля (внутренней проверки) и классификации ИСПДн;
- отчет о результатах проведения внутреннего контроля (внутренней проверки) обеспечения защиты ПДн в ИСПДн;
- приказ о назначении ответственных за обработку ПДн в ИСПДн;
- приказ о проведении работ по защите ПДн;

- положение о разграничении прав доступа к обрабатываемым ПДн в ИСПДн;

- журнал учета обращений субъектов ПДн о выполнении их законных прав, при обработке ПДн в ИСПДн;

- перечень ПДн, подлежащих защите в ИСПДн;

- план мероприятий по обеспечению защиты ПДн в ИСПДн;

- перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним;

- план внутренних проверок режима защиты ПДн в ИСПДн;

- порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в ИСПДн;

- частная инструкция по обеспечению безопасности информации на объекте вычислительной техники;

- инструкция пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций;

- журнал по учету мероприятий по контролю обеспечения защиты ПДн в ИСПДн;

- инструкция администратора безопасности при использовании ресурсов объекта вычислительной техники;

- инструкция администратора ИСПДн;

- инструкция пользователя ИСПДн;

- положение о защите ПДн в ИСПДн;

- частная модель угроз безопасности ПДн при их обработке в ИСПДн;

- акт классификации ИСПДн;

- Уведомление об обработке (о намерении осуществлять обработку) персональных данных в организацию, уполномоченную по правам субъектов ПДн – Управление Роскомнадзора по Калининградской области.

VI. ОБЪЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

34. Объектами защиты являются информация, обрабатываемая в ИСПДн, технические средства ее обработки и защиты.

Объекты защиты включают:

- обрабатываемую информацию;

- технологическую информацию;

- программно-технические средства обработки;

- средства защиты ПДн;

- каналы информационного обмена и телекоммуникации;

- объекты и помещения, в которых размещены компоненты ИСПДн.

VII. КЛАССИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

35. Пользователем ИСПДн является любой государственный гражданский служащий (служащий) Министерства, любой сотрудник медицинской организации или сотрудник сторонней организации, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком и функциональными обязанностями, или использующий результаты ее функционирования.

36. Пользователи ИСПДн делятся на три основные категории:

1) Администратор ИСПДн – физическое лицо, которое занимается настройкой, внедрением и сопровождением системы.

Администрирование ИСПДн могут осуществлять государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций, осуществляющие эксплуатацию ИСПДн - администрирование собственными силами, государственные гражданские служащие (служащие) других структурных подразделений Правительства Калининградской области или служащие других медицинских организаций - внутренний аутсорсинг, другими организациями - внешний аутсорсинг уполномоченной организацией.

Администратор ИСПДн обладает следующим уровнем доступа:

- 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.

2) Программист-разработчик ИСПДн - служащий медицинской организации или сторонней организации, который занимается разработкой программного обеспечения.

Разработчик ИСПДн обладает следующим уровнем доступа:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

3) Оператор ИСПДн – государственный гражданский служащий (служащий) Министерства, сотрудник медицинской организации, участвующий в процессе эксплуатации ИСПДн.

Оператор ИСПДн обладает следующим уровнем доступа:

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

Категории пользователей, а также группы пользователей, сформированные путём разделения пользователей по функциональным признакам внутри категорий, определяются для каждой ИСПДн.

VIII. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

37. Построение системы защиты информации и ее функционирование осуществляются в соответствии с основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;
- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

38. Законность предполагает осуществление защитных мероприятий и разработку СЗПДн Министерства или медицинской организации в соответствии с действующим законодательством в области защиты ПДн и иными нормативными актами в сфере защиты информации.

Пользователи ПДн и обслуживающий персонал ИСПДн Министерства и медицинских организаций осведомляются о порядке работы с защищаемой информацией и об ответственности за защиту ПДн на основании документов, указанных в пункте 31 настоящей Концепции.

39. Системный подход к построению СЗПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн.

При создании системы защиты учитываются все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты строится с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом

возможности появления принципиально новых путей реализации угроз безопасности.

40. Комплексное использование методов и средств защиты включает согласованное применение разнородных средств защиты при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках её отдельных компонентов.

Защита для ИСПДн 1, 2 и 3 классов строится с учётом эшелонирования. Для каждого канала утечки информации и для каждой угрозы безопасности организуется несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита обеспечивается физическими средствами, организационными и правовыми мерами. Наиболее эффективным рубежом внешней защиты являются средства криптографической защиты, реализованные с использованием технологии VPN (Virtual Private Network) - виртуальных частных сетей. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

41. Непрерывность защиты ПДн предполагает принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должна находиться в защищенном состоянии на протяжении всего времени её функционирования. В соответствии с этим принципом принимаются меры по недопущению перехода ИСПДн в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена, обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и другие). Перерывы в работе средств защиты используются злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

42. Своевременность предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее системы защиты информации в частности.

Разработка системы защиты ведётся параллельно с разработкой и развитием самой защищаемой системы. Это позволяет учитывать требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

43. Преемственность и совершенствование предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

44. Персональная ответственность предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого пользователя ИСПДн в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей пользователей ИСПДн строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

45. Принцип минимизации полномочий означает предоставление пользователям минимальных прав доступа в соответствии с необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо пользователю ИСПДн для выполнения его должностных обязанностей.

46. Взаимодействие и сотрудничество предполагает создание благоприятной атмосферы в коллективах Министерства и медицинских организациий, обеспечивающих эксплуатацию ИСПДн, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственных за организацию безопасности информации.

47. Гибкость системы защиты ПДн предполагает возможность изменения уровня защищенности ИСПДн в зависимости от принятых мер и используемых средств защиты. Это особенно важно в начальный период эксплуатации ИСПДн, когда может обеспечиваться как чрезмерный, так и недостаточный уровень защиты, а также в случае установки средств защиты на работающую ИСПДн без нарушения процесса ее нормального функционирования.

48. Открытость алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет конфиденциальности структуры и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже разработчикам). Однако, это не означает, что информация о конкретной системе защиты должна быть общедоступна.

49. Простота применения средств защиты. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств

защиты не должно быть связано со знанием специальных языков программирования или с выполнением действий, требующих значительных дополнительных трудозатрат пользователей, зарегистрированных установленным порядком, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

50. Научная обоснованность и техническая реализуемость достигается использованием информационных технологий, технических и программных средств, средств и мер защиты информации, реализованных на современном уровне развития науки и техники, научно обоснованных с точки зрения достижения заданного уровня безопасности информации и соответствующих установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на такие решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

51. Специализация и профессионализм предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области.

52. Обязательность контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль деятельности любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

IX. МЕРЫ, МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЁННОСТИ

53. Обеспечение требуемого уровня защищенности ИСПДн достигается с использованием мер, методов и средств безопасности.

Все меры обеспечения безопасности ИСПДн подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в Частной модели угроз безопасности ПДн при их обработке в ИСПДн, а также в Плане мероприятий по обеспечению защиты ПДн.

54. К законодательным (правовым) мерам защиты относятся действующие в Российской Федерации законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн, и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

55. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере внедрения информационных технологий в стране или обществе. Эти нормы большей частью не являются обязательными как законодательно утвержденные нормативные акты, однако их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

56. Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы эксплуатации ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер - обеспечить выполнение мероприятий, указанных в Политике информационной безопасности ИСПДн, контролируя состояние дел и выделяя необходимые ресурсы на их реализацию.

Организационные меры включают разработку распорядительных документов, указанных в пунктах 32, 33 настоящей Концепции.

57. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации осуществляется путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

58. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

С учетом всех требований и принципов обеспечения безопасности ПДн в ИСПДн по всем направлениям защиты в состав системы защиты включаются:

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей информационной системы к ресурсам ИСПДн;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты ПДн.

Успешное применение технических средств защиты на основании принципов, указанных в настоящей Концепции, предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонент ИСПДн;
- каждый государственный гражданский служащий (служащий) Министерства, сотрудник медицинской организации - пользователь ИСПДн или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения ими своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- в ИСПДн разработка и отладка программ осуществляется за пределами ИСПДн, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИСПДн производятся строго установленным порядком (регистрируются и контролируются);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);
- государственными гражданскими служащими (служащими) Министерства, сотрудниками медицинских организаций осуществляется

непрерывное управление и административная поддержка функционирования средств защиты.

X. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ

59. Контроль эффективности СЗПДн должен осуществляется на плановой и внеплановой основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль может проводиться:

- руководителями структурных подразделений Министерства и медицинских организаций по вопросам организации и исполнения законодательных, организационных и физических мер защиты;
- ответственными за организацию обработки ПДн по вопросам исполнения законодательных, организационных и физических мер защиты;
- администраторами ИСПДн по вопросам эксплуатации ИСПДн, а также выполнения технических мер защиты в процессе эксплуатации ИСПДн;
- привлекаемыми компетентными организациями, имеющими лицензию на этот вид деятельности, по вопросам внедрения, настройки и функционирования средств защиты информации;
- Роскомнадзором России, ФСТЭК России и ФСБ России в пределах их компетенции.

60. Контроль может осуществляться как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

61. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

XI. СФЕРЫ ОТВЕТСТВЕННОСТИ ЗА БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ

62. Ответственным за разработку мер и контроль обеспечения безопасности ПДн является:

- в Министерстве – заместитель министра;
- в медицинской организации – главный врач медицинской организации (директор).

Заместитель министра, главный врач медицинской организации (директор) может частично делегировать полномочия по обеспечению безопасности ПДн ответственному за организацию обработки ПДн.

63. Сфера ответственности заместителя министра включает следующие направления обеспечения безопасности ПДн:

- назначение ответственного за организацию обработки ПДн из числа государственных гражданских служащих (служащих) Министерства;

- создание и поддержание правовой базы безопасности ПДн в актуальном состоянии;

- организация проведение ежегодных проверок условий обработки ПДн (внутренних проверок) с подготовкой отчётов о результатах проведения проверок и указанием мер, необходимых для устранения выявленных нарушений;

- организация классификации ИСПДн и установления уровня защищенности ПДн;

- разработка должностной инструкции ответственного за организацию обработки ПДн;

- ввод в действие политики «чистого стола»;

- организация исполнение требований законодательства Российской Федерации, иных правовых актов в области безопасности информации, настоящей Концепции, Политики информационной безопасности ИСПДн, процедур, инструкций, организационных документов по обеспечению безопасности в Министерстве, указанных в пункте 32 настоящей Концепции.

64. Сфера ответственности главного врача медицинской организации (директора) включает следующие направления обеспечения безопасности ПДн:

- назначение ответственного за организацию обработки ПДн из числа сотрудников медицинской организации;

- создание и поддержание правовой базы безопасности ПДн в актуальном состоянии;

- организация проведение ежегодных проверок условий обработки ПДн (внутренних проверок) с подготовкой отчётов о результатах проведения проверок и указанием мер, необходимых для устранения выявленных нарушений;

- организация классификации ИСПДн и установления уровня защищенности ПДн;

- разработка должностной инструкции ответственного за организацию обработки ПДн;

- организация выполнения мероприятий по защите ПДн, предусмотренных Планом мероприятий по обеспечению защиты ПДн в ИСПДн;

- ввод в действие политики «чистого стола»;

- организация исполнения требований законодательства Российской Федерации, иных правовых актов в области безопасности информации, настоящей Концепции, Политики информационной безопасности ИСПДн, процедур, инструкций, организационных документов по обеспечению безопасности в Министерстве и медицинской организации, указанных в пункте 33 настоящей Концепции.

65. Сфера ответственности должностного лица, отдела правовой и кадровой работы Министерства включает следующие направления обеспечения безопасности ПДн:

- ознакомление государственных гражданских служащих (служащих) Министерства, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), иными правовыми актами по вопросам обработки ПДн и (или) организация обучения указанных лиц;

- разработка Перечня ПДн, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций;

- разработка Перечня должностей государственной гражданской службы Министерства, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн;

- разработка Перечня должностей государственной гражданской службы Министерства, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн;

- разработка Типового обязательства государственного гражданского служащего, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными в связи с исполнением должностных обязанностей;

- разработка Типовой формы согласия на обработку ПДн государственными гражданскими служащими Министерства, иных субъектов ПДн, а также типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои персональные данные.

66. Сфера ответственности должностного лица, ответственного за организацию обработки ПДн в Министерстве включает следующие направления обеспечения безопасности ПДн:

- уведомление уполномоченного органа по защите прав субъектов ПДн – Управления Роскомнадзора по Калининградской области, об обработке (намерении осуществить обработку) ПДн в Министерстве;

- организация обезличивания ПДн, обрабатываемых в ИСПДн Министерства, в том числе созданных и функционирующих в рамках реализации целевых программ, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов ПДн;

- разработка Правил обработки ПДн;

- разработка Правил рассмотрения запросов субъектов ПДн или их представителей;

- разработка Правил осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн;

- разработка Правил работы с обезличенными данными;

- реализация политики «чистого стола»;

- формирование и поддержание в актуальном состоянии Перечня ИСПДн;

- организация проведения аттестации ИСПДн Министерства (для ИСПДн 1 и 2 классов);

- разработка Типового порядка доступа государственного гражданского служащего (служащего), сотрудника медицинской организации в помещения, в которых ведётся обработка ПДн;

- предотвращение, выявление, реагирование, участие в расследовании нарушений безопасности ПДн;

- разработка, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности информации в Министерстве;

- проведение анализа угроз безопасности ПДн в ИСПДн Министерства;

- организация обучения и информирования пользователей ИСПДн Министерства о порядке работы с ПДн и средствами защиты;

- организация резервирования и копирования ПДн в ИСПДн;

- организация учёта носителей информации;

- организация эксплуатации технических средств защиты ИСПДн.

67. Сфера ответственности должностных лиц медицинских организаций включает следующие направления обеспечения безопасности ПДн:

- ознакомление служащих медицинских организаций, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн (в том числе с требованиями к защите ПДн), иными правовыми актами по вопросам обработки ПДн и (или) организация обучения указанных служащих;

- назначение ответственного за организацию обработки ПДн из числа служащих медицинских организаций;

- разработка должностной инструкции ответственного за организацию обработки ПДн в медицинской организации;

- проведение ежегодных проверок условий обработки ПДн с подготовкой отчётов о результатах проведения проверок и указанием мер, необходимых для устранения выявленных нарушений;

- ввод в действие политики «чистого стола»;

- уведомление уполномоченного органа по защите прав субъектов ПДн – Управления Роскомнадзора по Калининградской области, об обработке (намерении осуществить обработку) ПДн в медицинской организации;

- формирование и поддержание в актуальном состоянии Перечня ИСПДн;

- классификация ИСПДн и установление уровня защищенности ПДн;

- проведение контроля обеспечения защиты ПДн в ИСПДн в медицинской организации, ведение Журнала по учету мероприятий по контролю обеспечения защиты ПДн в ИСПДн;

- формирование и поддержание в актуальном состоянии Частной модели угроз безопасности ПДн при их обработке в ИСПДн;

- планирование и реализация мер по обеспечению безопасности ПДн в ИСПДн, ведение Плана мероприятий по обеспечению защиты ПДн в ИСПДн медицинской организации;

- администрирование ИСПДн медицинской организации по вопросам безопасности информации;

- организация резервирования и копирования ПДн в ИСПДн;
- организация учёта носителей информации;
- разработка и утверждение Порядка доступа сотрудников медицинской организации в помещения, в которых ведётся обработка ПДн;
- эксплуатация технических средств защиты ИСПДн медицинской организации;
- проведение анализа угроз безопасности ПДн в ИСПДн медицинской организации;
- исполнение требований законодательства Российской Федерации, иных правовых актов в области безопасности информации, настоящей Концепции, Политики информационной безопасности ИСПДн в Министерства и государственных медицинских организаций Калининградской области, процедур, инструкций, организационных документов по обеспечению безопасности в медицинских организациях, указанных в пункте 33 настоящей Концепции;
- предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

68. При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, указанным в разделе V настоящей Концепции, с этими организациями должно быть заключено Соглашение о конфиденциальности либо Соглашение о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн.

XII. МОДЕЛЬ НАРУШИТЕЛЯ БЕЗОПАСНОСТИ

69. Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты, указанным в разделе VI настоящей Концепции.

Нарушители подразделяются по признаку принадлежности к ИСПДн на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

Классификация нарушителей указывается в Частной модели угроз безопасности ПДн при их обработке в ИСПДн для каждой ИСПДн отдельно.

XIII. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

70. Для ИСПДн Министерства и медицинских организаций выделяются следующие основные категории угроз безопасности персональных данных:

1) Угрозы от утечки по техническим каналам.

2) Угрозы несанкционированного доступа к информации:

- угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн;

- угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

- угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, от угроз неантропогенного характера (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания), а также от угроз стихийного характера (ударов молний, пожаров, наводнений и т.п.);

- угрозы преднамеренных действий внутренних нарушителей;

- угрозы несанкционированного доступа по каналам связи.

Описание угроз, вероятность их реализации, опасность и актуальность указываются в Частной модели угроз безопасности ПДн при их обработке в ИСПДн для каждой ИСПДн отдельно.

XIV. МЕХАНИЗМ РЕАЛИЗАЦИИ КОНЦЕПЦИИ И ОЖИДАЕМЫЙ ЭФФЕКТ

71. Реализация Концепции должна осуществляется во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;

- постановлений Правительства Российской Федерации;

- руководящих, организационно-распорядительных и методических документов ФСТЭК России;

- потребностей ИСПДн в средствах обеспечения безопасности информации.

72. Реализация Концепции позволяет:

- оценить состояние безопасности информации ИСПДн, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;

- провести классификацию и аттестацию ИСПДн;

- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

- обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности регионального сегмента единой государственной информационной системы в сфере здравоохранения и отдельных ИСПДн в Министерстве и в медицинских организациях и создаст условия для ее дальнейшего совершенствования.