Е.В. Дерябин, А.А. Дементеева

Защита персональных данных

Методические рекомендации для руководителей служб здравоохранения Краснодарского края

Департамент здравоохранения Краснодарского края
ГУЗ «Медицинский информационно-аналитический центр»
Краснодар
2010

УДК 65.012.45

Департамент здравоохранения Краснодарского края
ГУЗ МИАЦ

А.А. Дементеева, Е.В. Дерябин

Защита персональных данных: Методические рекомендации для руководителей служб здравоохранения Краснодарского края.

Методические рекомендации написаны с использованием материалов Министерства здравоохранения и социального развития Российской федерации, Федеральной службы по техническому и экспортному контролю, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Материалы могут быть полезны руководителям служб здравоохранения, начальникам отделов АСУ, инженерам по защите информации при организации обеспечения безопасности персональных данных, обрабатываемых в информационных системах медицинских учреждений.

Предисловие

Федеральный закон «О персональных данных» породил волну споров, обсуждений, недоумений и противоречий. Одни схватились за голову, понимая, какие расходы с вязаны с выполнением требований законодательства. Другие беззаботно отмахнулись, не желая вникать в подробности очередной прихоти чиновников. Третьи довольно потерли руки, осознавая, сколько на этом можно заработать. Существует множество примеров судебной практики рассмотрения случаев утечки персональных данных, но наряду с этим бытует мнение, что если один раз сроки приведения информационных систем в соответствие отодвинули, то отодвинут и еще раз.

Кто прав пока не ясно.

Регуляторы пугают нас огромными штрафами за невыполнение требований законодательства, однако давайте посмотрим на эту проблему глазами «потребителя» – субъекта персональных данных. К каким последствиям для субъекта персональных данных может привести их утечка? Если дело касается сведений о состоянии здоровья человека, то последствия могут быть весьма плачевны. У каждого человека свои тайны, порой он не готов делиться ими даже с самыми близкими людьми. Имеем ли мы, работники сферы здравоохранения, право подвергать опасности раскрытия чужие секреты, ставшие нам известными по долгу службы? Нет, не имеем! Потому давайте подойдем к вопросу защиты персональных данных ответственно, отдавая себе отчет о серьезных последствиях, к которым может привести их утечка.

Термины и сокращения

ПЕРСОНАЛЬНЫЕ ДАННЫЕ – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

ОПЕРАТОР – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных;

ОБЩЕДОСТУПНЫЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

УДАЛЕННЫЙ ДОСТУП – форма обращения к ресурсу, при котором подключение к ЛВС удаленной рабочей станции, расположенной в фиксированном месте, происходит с помощью линии связи.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блоки-

рование, уничтожение персональных данных;

ИНФОРМАЦИОННАЯ СИСТЕМА ПЕРСОНАЛЬНЫХ ДАННЫХ – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

ПДн – персональные данные

ИС – информационная система

ИСПДн – информационная система персональных данных

Часть 1

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАЗУМНЫЙ ПОДХОД

- Как организовать защиту персональных данных
- Порядок действий по обеспечению безопасности персональных данных
- Предпроектное обследование информационной системы учреждения

В соответствии с Федеральным законом Российской Федерации от 26.07.2006 № 152-ФЗ «О персональных данных» все информационные системы персональных данных, созданные до 1 января 2010 года должны быть приведены в соответствие с требованиями закона не позднее 1 января 2011 года. Остальные информационные системы должны соответствовать требованиям до начала обработки персональных данных.

Лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность [1].

1.1. Как организовать защиту персональных данных

Существует три подхода к обеспечению безопасности ПДн:

- обеспечить безопасность ПДн самостоятельно;
- передать обеспечение безопасности ПДн сторонней организации;
- выполнить часть работ самостоятельно, а часть доверить сторонней организации.

В методических рекомендациях ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» определены требования к исполнителю работ по проектированию или внедрению системы защиты персональных данных:

> *Операторы ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1, 2 классов и распределенных информационных систем 3 класса должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации в установленном порядке [6].*

Однако в связи со вступлением 15 марта 2010

года в силу Приказа ФСТЭК России № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» действие документов [6] и [8] было отменено.

Следовательно, для проведения работ по защите персональных данных самостоятельно оператору не нужна лицензия на осуществление деятельности по технической защите конфиденциальной информации, но наличие в штате специалиста, обладающего специальными знаниями в области информационной безопасности – необходимо.

Сторонние же организации, берущие на себя работы (или часть работ) по разработке системы защиты персональных данных должны обладать лицензией ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации.

Кроме того, при поставке криптографических средств защиты исполнитель должен обладать лицензией ФСБ России на распространение шифровальных (криптографических) средств, а при осуществлении технического сопровождения систем защиты ПДн, в которых применяются криптографические средства — лицензией ФСБ России на техническое обслуживание шифровальных (криптографических) средств.

Так как медицинские учреждения, как правило, не имеют в штате специалистов по защите информации, то оптимальным решением будет выполнить часть работ своими силами, а часть передать организации-лицензиату.

Данные методические указания содержат подробное описание мероприятий по защите персональных данных, которые могут быть выполнены сотрудниками учреждений здравоохранения самостоятельно без привлечения сторонних организаций. Что позволит сэкономить бюджетные средства, планируемые к выделению в целях обеспечения безопасности и конфиденциальности персональных данных.

1.2. Порядок действий по обеспечению безопасности персональных данных

Итак, с чего же начать? В первую очередь необходимо назначить ответственного за защиту персональных данных. Это может быть заместитель главного врача по информатике или начальник отдела АСУ. Если же таких специалистов в учреждении нет, то ответственность за защиту персональных данных придется взять на себя главному врачу.

Схема 1. Порядок действия по обеспечению безопасности персональных данных

Общий порядок действий по обеспечению безопасности персональных данных, которые могут быть выполнены сотрудниками учреждения без привлечения сторонней организации, приведен на схеме 1.

В приложении 1 представлен сетевой график проведения мероприятий по защите персональных данных, составленный с учетом особенностей обработки персональных данных в учреждениях здравоохранения Краснодарского края.

Далее каждый этап будет рассмотрен более подробно.

1.3. Предпроектное обследование информационной системы учреждения

Предпроектное обследование проводится с целью систематизации сведений об учреждении и обрабатываемых данных. В ходе предпроектного обследования необходимо поговорить со всеми сотрудниками, чтобы выяснить кто имеет доступ к персональным данным. Так же необходимо уточнить схему расположения компьютеров и сетевого оборудования. Результатом проведения предпроектного обследования должны быть ответы на следующие вопросы:

1. Проекты, в рамках которых происходит обработка персональных данных.
2. Для каждого проекта примерное количество субъектов ПДн (физических лиц), обработка ПДн которых производится (0-1000, 1000-100 000, свыше 100 000) и их территориальное расположение (регион, в котором человек работает и проживает).
3. Перечень обрабатываемых категорий ПДн для каждого проекта (фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, др.).
4. Можно ли исключить какую-нибудь категорию ПДн из обработки?
5. Краткое описание процесса работы с ПДн для каждого проекта. Какое программное обеспечение используется.
6. Физическое расположение серверов, рабочих мест пользователей. ФИО и должность сотрудников, работающих с данными. Есть ли доступ в интернет с ПК этих сотрудников?

7. Существующая технология сбора, хранения, обработки ПДн (данные обрабатываются локально на серверах, локально на рабочих местах пользователей, передача с использованием каналов передачи данных, по ЛВС и т. п.)
8. Где хранятся документы на бумажных носителях? Имеются ли сейфы? Как происходит процедура уничтожения бумажных носителей персональных данных, цель обработки которых достигнута?
9. Где располагается серверное помещение? Как организован туда доступ?
10. Тип здания, где находится главное здание учреждения: собственное или арендованное.
11. Схема локальной сети.
12. Как организован доступ в интернет?
13. Существуют ли какие-то регламенты, инструкции, положения и т. п. по осуществлению информационного обмена, обеспечению информационной безопасности, защите персональных данных?
14. Наличие контролируемой зоны. Как осуществляется охрана периметра контролируемой зоны?

Контролируемая зона – охраняемая территория, в которой исключено пребывание посторонних лиц и не размещаются посторонние организации.

После сбора всех необходимых сведений можно переходить к базовым мерам по обеспечению безопасности персональных данных.

Часть 2

БАЗОВЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Классификация информационных систем персональных данных
- Уведомление об обработке (о намерении осуществлять обработку) персональных данных
- Согласие субъектов на обработку персональных данных
- Список лиц, имеющих доступ к ПДн
- Электронный журнал обращений граждан

Независимо от сроков приведения информационных систем в соответствие существуют требования, которые операторы ПДн должны выполнить незамедлительно.

1. Классифицировать информационные системы персональных данных.
2. Подать уведомление об обработке (о намерении осуществлять обработку) персональных данных.
3. Получить согласие субъектов на обработку персональных данных.
4. Утвердить список лиц, имеющих доступ к ПДн.
5. Разработать электронный журнал обращений.

2.1. Классификация информационных систем персональных данных

Классификация ИСПДн осуществляется согласно Порядку проведения классификации информационных систем персональных данных, утвержденном приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 года N 55/86/20.

Для проведения классификации ИСПДн создается комиссия, состав которой утверждается соответствующим приказом. Комиссией определяются характеристики информационной системы и составляется Акт классификации ИСПДн. Причем, для каждой ИСПДн оформляется вой акт классификации.

При проведении классификации информационной системы учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе персональных данных;
- объем обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);
- заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;
- структура информационной системы;
- наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

- режим обработки персональных данных;
- режим разграничения прав доступа пользователей информационной системы;
- местонахождение технических средств информационной системы.

Для проведения классификации ИСПДн необходимо выполнить следующие действия.

1. Определить категорию персональных данных.

Категории обрабатываемых в информационной системе персональных данных могут принимать следующие значения:

КАТЕГОРИЯ 1 — персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

КАТЕГОРИЯ 2 — персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

КАТЕГОРИЯ 3 — персональные данные, позволяющие идентифицировать субъекта персональных данных;

КАТЕГОРИЯ 4 — обезличенные и (или) общедоступные персональные данные [7].

Так как персональные данные в медицинских учреждениях содержат сведения о состоянии здоровья, то рекомендуется присваивать ПДн категорию 1.

2. Определить объем обрабатываемых персональных данных.

Объем обрабатываемых персональных данных может принимать следующие значения:

1 — в информационной системе одновременно

обрабатываются персональные данные более чем 100000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 — в информационной системе одновременно обрабатываются персональные данные от 1000 до 100000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

3 — в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации [7].

К определению объема обрабатываемых ПДн стоит подходить внимательно. Следует обращать внимание не только на количество субъектов ПДн, но и на территориальные особенности.

Например, если в организации обрабатываются ПДн от 1000 до 100000 субъектов, это вовсе не означает, что объем ПДн равен 2. Возможно, обрабатываются данные субъектов ПДн в пределах конкретной организации. А это уже говорит об объеме ПДн равном 3, так как объем принимает значение 3, если обрабатываются «персональные данные субъектов персональных данных в пределах конкретной организации».

3. Определить тип ИСПДН.

Информационные системы персональных данных подразделяются на типовые и специальные.

ТИПОВЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ — информационные системы, в которых требуется обеспечение только конфиденциальности персональных дан-

ных.

СПЕЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ — информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий) [7].

Кроме того, к специальным информационным системам должны быть отнесены информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных.

Следовательно, все ИСПДн медицинских учреждений, в которых обрабатываются персональные данные пациентов, являются специальными.

4. Определить структуру ИСПДн.

По структуре информационные системы подразделяются на автономные, локальные и распределенные.

АВТОНОМНЫЕ ИС — ИС, не подключенные к иным ИС.

ЛОКАЛЬНЫЕ ИС — комплексы автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа.

РАСПРЕДЕЛЕННЫЕ ИС — комплексы автоматизированных рабочих мест и (или) локальных информационных систем, объединенных в единую информационную систему средствами связи с использованием тех-

нологии удаленного доступа.

5. Охарактеризовать ИСПДН по наличию подключений к сетям связи общего пользования

По наличию подключений к сетям связи общего пользования и (или) сетям международного информационного обмена информационные системы подразделяются на системы, имеющие подключения, и системы, не имеющие подключений [7].

6. Определить режим обработки ПДн и местонахождение технических средств.

По режиму обработки персональных данных информационные системы подразделяются на однопользовательские и многопользовательские.

Многопользовательской информационной системой называется информационная система, допускающая одновременную работу нескольких пользователей.

По разграничению прав доступа пользователей информационные системы подразделяются на системы без разграничения прав доступа и системы с разграничением прав доступа.

В зависимости от местонахождения технических средств ИС подразделяются на системы, все технические средства которых находятся в пределах Российской Федерации, и системы, технические средства которых частично или целиком находятся за пределами Российской Федерации.

7. Определить класс ИСПДн.

По результатам анализа исходных данных информационной системе присваивается один из следующих классов:

КЛАСС 1 (К1) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последст-

виям для субъектов персональных данных;

КЛАСС 2 (К2) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;

КЛАСС 3 (К3) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;

КЛАСС 4 (К4) — информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных [7].

Класс информационной системы определяется в соответствии с таблицей 1.

Таблица 1. Определение класса ИСПДн

Категория ПДн	Объем ПДН		
	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Учитывая особенности ИС учреждений здравоохранения Краснодарского края, рекомендуется классифицировать ИСПДн учреждений здравоохранения согласно таблице 2.

Таблица 2. Классификация ИСПДн учреждений здравоохранения Краснодарского рая

Название программного продукта	Категория Пдн	Объем Пдн	Класс ИСПДн	Тип ИСПДн
Регистр медицинских и фармацевтических работников	2	3	К3	Т
АС Поликлиника	1	*	К1	С
АС Стационар	1	*	К1	С
МедКомТех	1	*	К1	С
ПО Бухгалтерского и кадрового учета	2	3	К3	Т

* — объем персональных данных зависит от специфики конкретного учреждения

Т— типовая ИСПДн

С— специальная ИСПДн

Класс информационной системы может быть пересмотрен:

- по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе [7].

В приложении 2 приведен пример акта классификации информационной системы персональных данных.

2.2. Уведомление об обработке (о намерении осуществлять обработку) персональных данных

Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных.

Существует 8 случаев, когда оператор не обязан подавать уведомление об обработке ПДн. Эти случаи включают обработку персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федера-

ции, для достижения законных целей, предусмотренных их учредительными документами, при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов персональных данных;

- являющихся общедоступными персональными данными;
- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных [1].

Однако так как практически в любом учреждении здравоохранения присутствует автоматизирована обработка персональных данных пациентов – рекомендуется подавать уведомление. В случае, когда существуют сомнения о необходимости подавать уведомление, стоит обратиться за комментариями в территориальный орган Роскомнадзора. Хочется отметить, что подавая уведомление, оператор заявляет о законности своих действий. Не стоит бояться, что подача уведомления приблизит проверку уполномоченным органом выполнения требований законодательства в области защиты персональных данных. График проверок составляется независимо от реестра операторов ПДн. При всем при этом, проверка учреждения, не включенного в реестр, повлечет за собой штрафы. Так что, рекомендуется подавать уведомление независимо от того, попадает учреждение под перечисленные восемь случаев или нет.

Уведомление проще всего подавать в электронной форме на сайте http://pd.rsoc.ru. Справа есть ссылка на «Форму уведомления». Для удобства операторов форма снабжена подсказками и разъяснениями по ее заполнению.

Уведомление должно содержать следующие сведения.

1. Наименование, адрес оператора.
2. Правовое основание обработки персональных данных.

При заполнении данного поля должны быть указаны: ст.85-90 Трудового Кодекса Российской Федерации; Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ; Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781; Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687; Устав (Положение) юри-

дического лица (дата, номер, кем утвержден); номер, дата выдачи и наименование лицензии на осуществляемый вид деятельности, с указанием лицензионных условий, закрепляющих запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных.

Номер лицензии и пункт лицензионных условий, закрепляющий запрет на передачу персональных данных (или информации, касающейся физических лиц), отражается только при наличии лицензии и (или) соответствующего пункта лицензионных условии [3] [4].

3. Цель обработки персональных данных.

Цель обработки указана в учредительных документах. Но не стоит перечислять узкие задачи деятельности. Для медицинских учреждений целью обработки ПДн может быть: оказание медицинских услуг населению, ведение трудовых отношений с сотрудниками, другие цели, зависящие от специфики работы организации.

4. Категории персональных данных.

При заполнении данного поля необходимо выбрать из предложенного списка те категории персональных данных, обработка которых ведется в организации. Это могут быть: фамилия, имя, отчество, год рождения, дата рождения, месяц рождения, место рождения, семейное положение, адрес, социальное положение, образование, имущественное положение, профессия, доходы, состояние здоровья.

Так же если в организации ведется обработка биометрических персональных данных, это необходимо указать. Биометрические персональные данные представляют собой сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность (например, отпечатки пальцев).

5. Категории субъектов, персональные данные которых обрабатываются.

Например, работники, состоящие в трудовых отношениях с оператором, физические лица, которым оказывается медицинская помощь.

6. Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных.

Обработка персональных данных может включать следующие действия: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных [1].

Так же необходимо указать способ обработки ПДн: автоматизированная, неавтоматизированная, смешанная.

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека[5].

Как правило, в каждом медицинском учреждении

присутствует неавтоматизированная обработка ПДн. Это личные карты сотрудников, карты пациентов и т.п.

Но наряду с неавтоматизированной обработкой в большинстве случаев персональные данные обрабатываются с использованием средств автоматизации. Это, например, данные, хранящиеся на серверах баз данных или передаваемые по электронной почте в другие организации.

Поэтому при заполнении данного поля рекомендуется указывать, что обработка ПДн является смешанной.

При автоматизированной или смешанной обработке, необходимо указать, передается ли полученная в ходе обработки персональных данных информация по внутренней сети (информация доступна лишь для строго определенных сотрудников), либо информация передается с использованием сети общего пользования Интернет, либо без передачи полученной информации [3].

7. Осуществление трансграничной передачи персональных данных.

ТРАНСГРАНИЧНАЯ ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ — передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства [1]. Как правило, для медицинских учреждений указывать данный пункт не нужно.

8. Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке.

В качестве мер по обеспечению безопасности ПДн можно указать следующие: управление доступом, регистрация и учет, обеспечение целостности, крипто-

графическая защита, антивирусная защита, обнаружение вторжений.

Поля Средства обеспечения безопасности и Использование шифровальных (криптографических) средств рекомендуется оставить пустыми. Выбор средств обеспечения безопасности будет определяться совместно с организацией-лицензиатом на стадии разработки проекта системы защиты персональных данных.

Далее указывается класс информационной системы. Для медицинских учреждений класс информационной системы обычно равен *К1*, так как обрабатываются персональные данные первой категории — сведения о состоянии здоровья. Порядок проведения классификации информационных систем персональных данных описан в разделе «Классификация информационных систем персональных данных».

9. Дата начала обработки персональных данных.

За дату начала обработки необходимо брать дату, когда были произведены последние изменения по одному из пунктов уведомления (возможно, это реорганизация, смена наименования). Фактически это дата, которая указана в свидетельстве ИНН. Дата должна быть указана полностью.

10. Срок или условие прекращения обработки персональных данных.

В поле указывается конкретная дата или основание (условие), наступление которого повлечет прекращение обработки персональных данных. Данное основание тесным образом связано с целями обработки, при достижении целей обработка должна быть прекращена.

Рекомендуется в качестве условия прекращения обработки персональных данных использовать формулировку: «Прекращение деятельности как юридическо-

го лица».

11. ФИО исполнителя, его контактная информация.

Далее необходимо ввести защитный код, отметить поля об ознакомлении с порядком подачи уведомления в электронном виде и подтверждении согласия на передачу информации в электронной форме уведомления (в том числе персональных данных) по открытым каналам связи сети Интернет, нажать кнопку «Отправить электронное уведомление и подготовить форму к распечатке».

Вы можете отслеживать состояние Вашего уведомления на портале персональных данных

После этого уведомление необходимо распечатать в двух экземплярах, подписать у руководителя организации, заверить печатью, зарегистрировать и отправить один экземпляр заказным письмом с уведомлением в соответствующий территориальный орган Роскомнадзора. Адрес назначения можно узнать на странице http://pd.rsoc.ru/authority/authority-contacts.

В случае изменения сведений оператор обязан уведомить уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней от даты возникновения таких изменений [1].

В приложении 3 приведен пример уведомления об обработке (о намерении осуществлять обработку) персональных данных.

2.3. Согласие субъектов на обработку персональных данных

Согласно п.2 статьи 10 Федерального закона «О персональных данных» обработка специальных категорий персональных данных (в том числе сведений о состоянии здоровья) должна осуществляться с письменного согласия субъекта на обработку персональных данных.

При этом согласие субъекта персональных данных не требуется в следующих случаях:

- обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;
- обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;
- обработка персональных данных необ-

ходима для доставки почтовых отправлений организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи;

- обработка персональных данных осуществляется в целях профессиональной деятельности журналиста либо в целях научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и свободы субъекта персональных данных;
- осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе персональных данных лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности.

В случае если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке [1].

Письменное согласие субъекта персональных данных на обработку его персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъек-

та персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

- наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

В случае недееспособности субъекта персональных данных согласие на обработку его персональных данных дает в письменной форме законный представитель субъекта персональных данных.

В случае смерти субъекта персональных данных согласие на обработку его персональных данных дают в письменной форме наследники субъекта персональных данных, если такое согласие не было дано субъектом персональных данных при его жизни [1].

Субъект персональных данных имеет право на отзыв своего согласия на обработку персональных данных. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных оператор обязан прекратить обработку персональных данных и уничтожить персональные данные в

срок, не превышающий трех рабочих дней от даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

Пример письменного согласия субъекта на обработку персональных данных приведен в приложении 4.

2.4. Список лиц, имеющих доступ к ПДн.

Субъект персональных данных имеет право ознакомиться со списком лиц, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ. Поэтому необходимо разработать утвержденные руководством учреждения разрешительные документы, включающие список лиц, допущенных к обработке персональных данных. Работа с персональными данными лиц, не включенных в разрешительные документы, не допускается.

Перечень лиц, допущенных к обработке персональных данных, может быть приложением к Приказу о допуске работников к персональным данным, и оформлен, например, в виде таблицы.

Таблица 3. Перечень лиц, имеющих право доступа к системе АИС 1.

№ п/п	Отдел	Должность	Ф.И.О.
1	Бухгалтерия	Главный бухгалтер	Иванова И.И.
2	Отдел кадров	Начальник отдела кадров	Петрова А.В.
3		Специалист по кадрам	Семенов Л.Д.

2.5. Электронный журнал обращений граждан

В учреждении необходимо разработать электронный журнал обращений, в котором регистрируются запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам.

Журнал ведется в электронном виде. Примером такого журнала служит таблица 4.

Таблица 4. Журнал обращений граждан для получения доступа к персональным данным

№ п/п	Дата обращения	Ф.И.О. гражданина	Сведения о документе, удостоверяющем личность			Роспись гражданина	Отметка о предоставлении доступа к ПДн (отказе в доступе)	Ф.И.О. должность сотрудника, предоставившего доступ к ПДн	Примечание
			Номер, серия	Дата выдачи	Кем выдан				
1	2	3	4	5	6	7	8	9	10

Часть 3

ЗАЩИТА ПДН ПРИ НЕАВТОМАТИЗИРОВАННОЙ ОБРАБОТКЕ

- Общие положения
- Требования к типовым формам документов
- Требования к журналу для однократного пропуска субъекта персональных данных на территорию оператора

Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

3.1. Общие положения

При неавтоматизированной обработке персональных данных должны соблюдаться требования Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденном постановлением Правительства РФ от 15 сентября 2008 г. N 687.

Как правило, в каждом медицинском учреждении часть обработки персональных данных ведется в неавтоматизированном режиме. Обычно это кадровая работа или ведение медицинских карт пациентов.

Итак, при обработке ПДн без использования средств автоматизации необходимо следовать следующим правилам.

1. Персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных. При этом не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы, т.е. для каждой категории персональных данных должен использоваться отдельный материальный носитель.
2. Необходимо обеспечивать раздельное хранение материальных носителей содержащих персональные данные, обработка которых осуществляется в различных целях. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.
3. Лица, осуществляющие обработку персональ-

ных данных, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки. Поэтому рекомендуется разработать должностные регламенты лиц, имеющих доступ и (или) осуществляющих обработку персональных данных. О разработке этих документов говорилось в предыдущем разделе.

3.2. Требования к типовым формам документов

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться перечисленные ниже условия.

1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать:

   - сведения о цели обработки персональных данных;
   - наименование и адрес оператора;
   - фамилию, имя, отчество и адрес субъекта персональных данных;
   - источник получения персональных данных;
   - сроки обработки персональных данных;
   - перечень действий с персональными данными, которые будут совершаться в процессе их обработки;
   - общее описание используемых оператором способов обработки персональных данных.

2. При необходимости получения письменного согласия на обработку персональных данных, типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации. Случаи, в которых не требуется согласие

субъекта на обработку ПДн, были рассмотрены выше.

3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.
4. Типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

3.3. Требования к журналу для однократного пропуска субъекта персональных данных на территорию оператора

Для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, необходимо ведение журнала (реестра, книги), в который будут заноситься персональные данные субъекта. При этом необходимо соблюдать следующие требования.

1. Необходимость ведения такого журнала (реестра, книги) предусматривается актом оператора. Этот акт должен содержать:

   - сведения о цели обработки персональных данных;
   - способы фиксации и состав информации, запрашиваемой у субъектов персональных данных;
   - перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги);
   - сроки обработки персональных данных;
   - сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

2. Копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается.

3. Персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

Часть 4

ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Снижение затрат на создание системы защиты персональных данных
- Разработка внутренних документов по защите ПДн

При обеспечении безопасности ПДн стоит разделять персональные данные, обрабатываемые в неавтоматизированном режиме и с использованием средств автоматизации. В первом случае следует руководствоваться постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687. Особенности обработки ПДн без использования средств автоматизации описаны в предыдущем разделе. Данный раздел посвящен обработке ПДн с использованием средств автоматизации.

Очень часто организационным мерам не уделяется должное внимание при проектировании системы защиты информации. Напрасно. Организационные меры помогают предотвратить 80% утечек информации и при этом не требуют финансовых затрат.

4.1. Снижение затрат на создание системы защиты персональных данных

Очень часто недобросовестные лицензиаты ФСТЭК, предлагающие свои услуги по организации безопасности персональных данных, забывают рассказать операторам ПДн об элементарных способах снижения затрат на создание системы. Поэтому прежде чем заключать договор со сторонней организацией необходимо самостоятельно изучить вопрос защиты персональных данных.

Существует несколько способов сокращения затрат.

1. Обезличивание персональных данных.

> *Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.*

Т.е. если при обработке персональных данных ФИО субъекта заменить некоторым идентификатором, можно добиться понижения класса ИСПДн. Например, на сервере БД останутся данные первой категории, а на рабочих станциях будут обрабатываться данные в обезличенном виде, а значит четвертой категории. Если в среднем при классе ИСПДн К1 защита одной рабочей станции обходится в 11 000 рублей (это только закупка средств защиты), то для защиты рабочих станций в ИСПДн класса К4 закупка дополнительных средств защиты не требуется. Экономия на лицо. Описанная схема снижения затрат за счет обезличивания

персональных данных представлена на схеме 2.

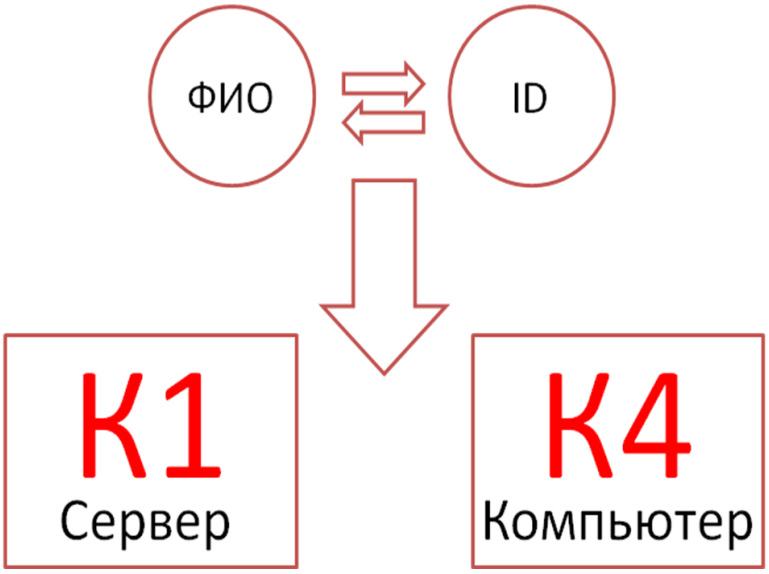

Схема 2. Обезличивание персональных данных.

1. Пересмотр физического размещения рабочих станций

Создание системы защиты персональных данных включает так же защиту от физического проникновения в помещение. А именно установку решеток на окнах, железных верей с надежным замком, оснащение кабинета датчиками пожарной и охранной сигнализации.

Кроме того, для ИСПДн класса К1 и К2 необходимо предусмотреть защиту данных от утечки за счет побочных электромагнитных излучений и наводок. Чаще всего данные средствами защиты оснащается кабинет, а не конкретные рабочие станции.

Из всего вышесказанного можно сделать вывод, что затраты на создание системы защиты персональных данных можно снизить, сократив число кабинетов,

в которых будет происходить обработка персональных данных. При этом не стоит забывать, что совместная обработка ПДн, цели обработки которых различны, не допускается.

4.2. Разработка внутренних документов по защите ПДн

Несомненным плюсом организационных мероприятий является то, что учреждение может их выполнить своими силами без привлечения сторонней организации. Результатом предпроектной стадии будет разработка перечисленных ниже документов:

1. Приказ о создании комиссии по защите персональных данных.

Для проведения мероприятий по обеспечению безопасности персональных данных целесообразно сформировать комиссию с привлечением специалистов в области информационной безопасности. Рекомендуется включить в комиссию руководителей или полномочных представителей всех структурных подразделений учреждения, обрабатывающих персональные данные, председателем комиссии назначить заместителя руководителя учреждения.

Состав комиссии утверждается «Приказом о создании комиссии по защите персональных данных с наделением ее полномочиями по проведению мероприятий, касающихся организации защиты персональных данных».

2. Положение об обработке и защите персональных данных.

Положение об обработке и защите персональных данных должно включать понятие и состав персональных данных, порядок получения и обработки персональных данных, права, обязанности и ответственность субъекта персональных данных и оператора при обработке персональных данных.

2. Приказ о возложении персональной ответственности за защиту персональных данных.

В приказе рекомендуется привести список конкретных лиц, ответственных за защиту персональных данных, обрабатываемых в учреждении.

3. Приказы о создании группы, осуществляющей функции по организации защиты персональных данных и о назначении ответственных лиц по работе с персональными данными.
4. Должностные регламенты лиц, имеющих доступ и (или) осуществляющих обработку персональных данных.

Должностные инструкции сотрудников учреждения рекомендуется дополнить пунктом о необходимости соблюдения утвержденного Положения об обработке и защите персональных данных.

5. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные.

Инструкция должна включать определение персональных данных, порядок обеспечения безопасности при обработке и хранении персональных данных, порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации.

6. Акт классификации ИСПДн

Акт классификации должен содержать сведения о составе обрабатываемых ПДн, категории и объеме ПДн, структуре ИСПДн, режиме обработки ПДн, наличии подключения информационной системы к сетям связи общего пользования и сетям международного информационного обмена, типе ИСПДн, присвоенном ИСПДн классе.

Порядок проведения классификации информационных систем персональных данных описан в разделе «Классификация ИСПДн».

7. Образец акта уничтожения документов

При достижении целей обработки персональных данных необходимо уничтожить материальные носители с персональными данными. Для этого составляется акт уничтожения документов, который заверяется комиссией.

8. План мероприятий по защите персональных данных

Защита информации – процесс не спонтанный. Отнюдь, к вопросу защиты информации нужно подходить серьезно, заранее планируя проведение необходимых мероприятий. Поэтому составление плана мероприятий по защите персональных данных – необходимый этап обеспечении безопасности.

Часть 5

ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Разработка модели угроз безопасности персональных данных
- Разработка технического задание на создание системы защиты персональных данных

После предпроектного обследования, определения класса ИСПДн, осуществления базовых и организационных мероприятий по защите персональных данных можно переходить к проектированию и внедрению системы защиты.

Эти мероприятия можно выполнить самостоятельно при наличии в штате специалиста, имеющего специальные знания в области информационной безопасности.

5.1. Разработка модели угроз безопасности персональных данных

Разработка модели угроз безопасности ПДн осуществляется на основе перечня угроз, содержащихся в документе ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Для разработки модели угроз безопасности в организации должен работать сотрудник, обладающий соответствующими навыками в области информационной безопасности. Если в организации такого сотрудника нет, рекомендуется доверить разработку модели угроз сторонней организации-лицензиату ФСТЭК.

Целью разработки модели угроз является определение перечня актуальных угроз безопасности персональным данным. Этот перечень определяется согласно «Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и включает следующие этапы.

1. Составление перечня всех возможных угроз согласно ФСТЭК «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных»
2. Определение исходной степени защищенности ИСПДн

Исходная степень защищенности определяется для каждой ИСПДн на основании таблицы показателей уровней защищенности.

Таблица 5. Показатели уровней защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;			+
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);			+
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;		+	
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;		+	
локальная ИСПДн, развернутая в пределах одного здания.	+		

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			+
ИСПДн, имеющая одноточечный выход в сеть общего пользования;		+	
ИСПДн, физически отделенная от сети общего пользования.	+		
По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;	+		
запись, удаление, сортировка;		+	
модификация, передача.			+
По разграничению доступа к персональным данным:			
ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;		+	

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			+
ИСПДн с открытым доступом.			+
По наличию соединений с другими базами ПДн иных ИСПДн:			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			+
ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн.	+		
По уровню обобщения (обезличивания) ПДн:			
ИСПДн в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);	+		

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).			+
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю БД с ПДн;			+
ИСПДн, предоставляющая часть ПДн;		+	
ИСПДн, не предоставляющие никакой информации.	+		

Чтобы определить исходную степень защищенности Вашей ИСПДн необходимо:

- исключить из таблицы показателей уровней защищенности лишние строки таким образом, чтобы полученная таблица включала технические и эксплуатационные характеристики Вашей ИСПДн;
- посчитать количество положительных решений по каждому столбцу;
- определить степень исходной защищенности.

Степень исходной защищенности может быть высокой, средней или низкой. Каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1.

ИСПДн имеет высокую степень исходной защищенности, если выполняются оба условия:

- не менее 70% характеристик ИСПДн соответствуют уровню «высокий»;
- остальные характеристики соответствуют «среднему» уровню.

В этом случае $Y_1 = 0$.

ИСПДн имеет среднюю степень исходной защищенности, если выполняются оба условия:

- ИСПДн не имеет высокую степень исходной защищенности – т.е. не выполняется первый пункт;
- не менее 70% характеристик ИСПДн соответствуют уровню не ниже "средний".

$Y_1 = 5$.

ИСПДн имеет низкую степень исходной защищен-

ности, если не выполняются условия по пунктам 1 и 2.

Y_1= 10.

2. Определение вероятности реализации угрозы

Вероятность реализации угрозы определяется экспертным путем и представляет собой показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях.

Для каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y_2.

Показатель вероятности реализации угроз может принимать следующие значения:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y_2 = 0);
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y_2 = 2);
- средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y_2 = 5);
- высокая вероятность – объективные предпосылки для реализации угрозы существуют, и меры по обеспечению безопасности ПДн не приняты (Y_2 = 10).

3. Определение коэффициента реализуемости угрозы

Коэффициент реализуемости угрозы Y определяется соотношением $Y = (Y_1+Y_2)/20$.

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если 0 < Y <0,3, то возможность реализации угрозы признается низкой;
- если 0,3 < Y < 0,6, то возможность реализации угрозы признается средней;
- если 0,6 < Y < 0,8, то возможность реализации угрозы признается высокой;
- если Y > 0,8, то возможность реализации угрозы признается очень высокой.

4. Оценка опасности каждой угрозы

Опасность каждой угрозы оценивается специалистом по защите информации. Так что, если у Вас нет специальных знаний в области защиты информации, придется привлекать эксперта.

Вербальный показатель опасности угрозы может принимать следующие значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;
- средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;
- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

5. Выбор актуальных угроз

Из предварительного перечня угроз безопасности в соответствии с правилами, показанными в табли-

це 6, выбираются угрозы, которые относятся к актуальным для данной ИСПДн.

Таблица 6. Определение актуальности угроз

Реализуемость угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	Н	Н	А
Средняя	Н	А	А
Высокая	А	А	А
Очень высокая	А	А	А

А — актуальная угроза

Н— неактуальная угроза

Таким образом определяется перечень актуальных угроз безопасности персональных данных для каждой ИСПДн.

5.2. Разработка технического задания на создание системы защиты персональных данных

После разработки модели угроз безопасности персональных данных разрабатывается техническое задание на оказание услуг по созданию системы защиты ПДн. Если дальнейшие работы решено доверить сторонней организации, то в техническом задании необходимо указать, что исполнитель должен обладать лицензией ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации, лицензией ФСБ России на распространение шифровальных (криптографических) средств, лицензией ФСБ России на техническое обслуживание шифровальных (криптографических) средств.

В техническом задании описываются требования к каждой из подсистем защиты информации. Для средств защиты информации необходимо указать требование к наличию сертификата соответствия.

На основании технического задания выбираются технические и программные средства защиты информации. Далее производится закупка этих средств, монтаж и настройка оборудования, а так же аттестационные мероприятия.

Оценка соответствия ИСПДн требованиям безопасности ПДн проводится в виде обязательной сертификации (аттестации) по требованиям безопасности информации.

Заключение

Организацию обеспечения безопасности персональных данных в медицинских учреждениях можно разбить на следующие этапы.

1. Предпроектное обследование информационной системы.

На данном этапе уточняется перечень персональных данных, обрабатываемых в учреждении, определяется схема расположения рабочих станций и серверов, строится схема контролируемой зоны.

2. Базовые меры по обеспечению безопасности персональных данных

Данный этап включает действия, выполнение которых нельзя откладывать:

- ♦ классификация ИСПДн;
- ♦ подача уведомления об обработке ПДн;
- ♦ получение согласия субъекта на обработку ПДн;
- ♦ составление списка лиц, имеющих доступ к ПДн;
- ♦ разработка журнала обращений граждан.

3. Защита ПДн при неавтоматизированной обработке

На этом этапе необходимо выполнить требования Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного Постановлением Правительства РФ от 15 сентября 2008 г. N 687

4. Организационные меры по обеспечению безопасности персональных данных

Данный этап включает мероприятия по сниже-

нию затрат на создание системы защиты персональных данных и разработку необходимой документации.

5. Проектирование и внедрение системы защиты персональных данных

На данном этапе разрабатывается модель угроз безопасности, составляется техническое задание на создание системы защиты персональных данных, выбираются технические и программные средства защиты, производится монтаж и настройка оборудования, проводятся аттестационные мероприятия.

Приведение ИСПДн в соответствие требованиям Федерального закона «О персональных данных» - процесс достаточно сложный и требующий серьезных финансовых затрат. Но стоимость можно снизить, выполнив ряд организационных мер самостоятельно.

Сотрудники Государственного учреждения здравоохранения «Медицинский информационно-аналитический центр» департамента здравоохранения Краснодарского края готовы оказать любую помощь при организации обеспечения безопасности персональных данных в медицинских учреждениях.

Все интересующие Вас вопросы можете присылать на электронный адрес dementeeva@miac.kuban.ru или задать по телефону 8(861)268-99-73 доб. 109.

Список литературы

1. Федеральный закон Российской Федерации от 26.07.2006 № 152-ФЗ «О персональных данных»
2. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 г. N 781
3. Разъяснения по заполнению уведомления об обработке (о намерении осуществлять обработку) персональных данных http://securitypolicy.r
4. Форма уведомления об обработке (о намерении осуществлять обработку) персональных данных http://pd.rsoc.ru/operators-registry/notification/form
5. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденное Постановлением Правительства РФ от 15 сентября 2008 г. N 687
6. Методические материалы ФСТЭК «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 года
7. Порядок проведения классификации информационных систем персональных данных, утвержденный Приказом Федеральной службы по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации, Министерством информационных технологий и связи Российской Федерации от13 февраля 2008 года N 55/86/20
8. Методические материалы ФСТЭК «Рекомендации по проведению работ в подведомственных Рособразо-

ванию учреждениях по обеспечению защиты информационных систем персональных данных» от 15 февраля 2008 года
9. Рекомендации по проведению работ в подведомственных Рособразованию учреждениях по обеспечению защиты информационных систем персональных данных
10. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г
11. Методические материалы ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года (выписки)
12. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, утвержденные Директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 22 декабря 2009 года.
13. Положение о методах и способах защиты информации в информационных системах персональных данных, утвержденное Приказом ФСТЭК России от 5 марта 2010 года №58
14. Методические материалы ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года

Приложение 1 – Сетевой график мероприятий по защите персональных данных в учреждениях здравоохранения Краснодарского края

Наименование этапа	Срок выполнения
1	2
Организационные мероприятия	
Назначение ответственного за защиту персональных данных в учреждении	Немедленно
Подготовка поэтажного плана здания с указанием размещения компьютеров и серверов	до 01.04.2010
Подготовка схемы сети учреждении с указанием сетевого оборудования, IP-адресов, названий серверов	до 01.04.2010
Подготовка перечня персональных данных, обрабатываемых в учреждении с указанием компьютеров, на которых эта обработка ведется	до 01.04.2010
Утверждение документа, регламентирующего допуск сотрудников помещения, в которых ведется обработка персональных данных	до 01.04.2010

Наименование этапа	Срок выполнения
1	2
Дополнить трудовой договор с сотрудниками пунктами о согласии на обработку персональных данных, передаче персональных данных третьим лицам, ознакомлении с положением об обработке персональных данных в учреждении, ознакомлении с согласием о неразглашении персональных данных	до 20.04.2010
Мероприятия по снижению затрат на создание системы защиты персональных данных	
Пересмотр мест размещения компьютеров, на которых ведется обработка персональных данных. По возможности разместить компьютеры в одном кабинете и вести обработку персональных данных на меньшем количестве компьютеров[1]	до 01.05.2010
Обезличивание персональных данных. По возможности часть персональных данных представить в обезличенном виде.	до 01.05.2010
Разработка необходимых документов	
Подача уведомления об обработке (о намерении осуществлять обработку) персональных данных на сайте Роскомнадзора http://pd.rsoc.ru/operators-registry/notification/form/	до 01.04.2010

Наименование этапа	Срок выполнения
1	2
Получение согласия субъектов на обработку персональных данных и передачу персональных данных третьим лицам	до 01.05.2010
Разработка формы отзыва субъектом своих персональных данных	до 01.05.2010
Разработка электронного журнала обращений граждан	до 01.06.2010
Разработка внутренних нормативных документов по защите персональных данных	до 01.05.2010
Разработка образца акта уничтожения персональных данных	до 01.04.2010
Разработка схемы контролируемой зоны учреждения	до 10.04.2010
Создание комиссии для проведения классификации информационных систем персональных данных	до 01.04.2010
Классификация информационных систем персональных данных (ИСПДн)	до 01.04.2010
Выявление угроз безопасности и разработка моделей угроз и нарушителя	до 01.06.2010
Мероприятия по защите персональных данных от физического доступа	

Наименование этапа	Срок выполнения
1	2
Организовать хранение материальных и цифровых носителей с персональными данными в специально оборудованных местах	до 01.07.2010
В помещениях, в которых осуществляется обработка и хранение персональных данных, установить датчики охранной сигнализации с выводом на пульт охранника	до 01.09.2010
В помещениях, в которых осуществляется обработка и хранение персональных данных, установить металлические двери с надежным замком и решетки на окна	до 01.11.2010
Разработать приказ о пропускном режиме на территорию учреждения согласно требованиям ПП №687	до 01.07.2010
Мероприятия по проектированию системы защиты персональных данных	
Разработка технического задания на создание системы защиты персональных данных	до 01.05.2010
Заключение договора на проведение работ в области защиты персональных данных с организацией – лицензиатом ФСТЭК.	до 01.05.2010

Наименование этапа	Срок выполнения
1	2
Мероприятия, выполняемые совместно с организацией – лицензиатом ФСТЭК	
Выбор и закупка средств защиты персональных данных	до 01.09.2010
Установка и настройка средств защиты персональных данных	до 01.10.2010
Создание технического паспорта на рабочие станции	до 01.09.2010
Аттестация информационной системы персональных данных	до 15.11.2010
Эксплуатация информационной системы персональных данных	
Разработка приказа о вводе ИСПДн в эксплуатацию	После получения аттестата
Ежегодный контроль эффективности средств защиты персональных данных	декабрь
Повышение квалификации сотрудников в области защиты ПДн	до 01.04.2010

Приложение 2 – Пример акта классификации ИСПДн

Акт № _____ «____»_____2010 г.
классификации информационной системы персональных данных «АИС 1»

Основание:

Необходимость классификации информационной системы персональных данных в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

Составлен комиссией:

Председатель –	И.И. Иванов.
Члены комиссии –	А.А. Артемов;
	К.М. Михалкова;
	А.Н. Никонов.

Комиссия, рассмотрев следующие исходные данные на информационную систему персональных данных:

- категория обрабатываемых персональных данных (Хпд) 2: персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- объем обрабатываемых персональных данных (Хнпд): менее чем 1000 субъектов персональных данных;
- по требуемым оператором характеристикам безопасности персональных

данных информационная система является типовой;

- структура информационной системы – локальная ИСПДн, расположенная в пределах одного здания;
- подключение информационной системы к компьютерным сетям общего пользования – есть подключения информационной системы к сетям связи общего пользования и к сетям международного обмена;
- режим обработки персональных данных и разграничения доступа – многопользовательский с различными правами доступа пользователей;
- местонахождение технических средств информационной системы – все средства находятся в пределах Российской Федерации;

решила установить информационной системе «АИС 1» класс защищенности КЗ. Настоящий акт составлен в единственном экземпляре.

Приложение 3 – Пример Уведомления об обработке (о намерении осуществлять обработку) персональных данных

Руководителю Управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по _____

УВЕДОМЛЕНИЕ
об обработке (о намерении осуществлять обработку) персональных данных

Наименование (фамилия, имя, отчество) оператора: Государственное учреждение здравоохранения "Медицинский информационно-аналитический центр" департамента здравоохранения Краснодарского края (ГУЗ МИАЦ),

Адрес оператора

Адрес местонахождения: 350007, г.Краснодар, ул.Захарова, 63

Почтовый адрес: 350007, г.Краснодар, ул.Захарова, 63

Регионы: Краснодарский край;

ИНН: 2308067989

Коды: ОГРН 1032307165990; ОКВЭД 72.40; ОКПО 51379366; ОКФС 13; ОКОГУ 23340;

Правовое основание обработки персональных данных

руководствуясь ст.85-90 Трудового Кодекса РФ, Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ, Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781, По-

становление Правительства Российской Федерации от 15 сентября 2008 г. № 687, Устав ГУЗ МИАЦ от 10.11.2003 г. №504-ОД утвержден приказом департамента здравоохранения Краснодарского края

Цель обработки персональных данных

с целью Сбор данных о состоянии здоровья граждан Краснодарского края, кадровая работа

Категории персональных данных

осуществляет обработку следующих категорий персональных данных:

фамилия, имя, отчество; образование; семейное положение; адрес; дата рождения; месяц рождения; год рождения;

специальные категории персональных данных:

состояние здоровья;

а также:

Паспортные данные, регистрация, номер телефона, e-mail, ИНН, номер страхового свидетельства

Категории субъектов, персональные данные которых обрабатываются

принадлежащих: Сотрудники ГУЗ МИАЦ, население Краснодарского края

Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных

обработка вышеуказанных персональных данных будет осуществляться путем: смешанная; с передачей по внутренней сети юридического лица; с передачей по сети Интернет; Чтение, запись, поиск, удаление, сортировка, модификация, передача.

осуществление трансграничной передачи персональных данных: не осуществляется

Описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при

их обработке

Контроль доступа к СВТ; регистрация и учет событий безопасности; предотвращение НСД к информации; контроль целостности; антивирусная защита; обеспечение безопасного межсетевого взаимодействия; анализ защищенности; обнаружение вторжений.

средства обеспечения безопасности:

использование шифровальных (криптографических) средств: не используется

класс информационной системы: к1;

Дата начала обработки персональных данных: 25.11.2003

Срок или условие прекращения обработки персональных данных: Прекращение деятельности как юридического лица.

Приложение 4 – Образец письменного согласия субъекта на обработку персональных данных

Согласие на обработку персональных данных

_____

Наименование (Ф.И.О.) оператора

_____

Адрес оператора

_____

Ф.И.О. субъекта персональных данных

_____

Адрес, где зарегистрирован субъект персональных данных

_____

Номер основного документа, удостоверяющего его личность

_____

Дата выдачи указанного документа

_____

Наименование органа, выдавшего документ

заявление.

В соответствии с требованиями статьи 9 федерального закона от 27.07.06 «О персональных данных» № 152-ФЗ даю свое согласие на обработку следующих персональных данных:

1. Дата рождения.
2. Пол.

3. Образование.

4. .....

для (указывается цель).

Предоставляю Оператору право осуществлять следующие действия с моими персональными данными: перечисляются действия.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течении указывается количество дней или условие.

Данное соглашение действует с "__" _____ 20__ г. по "__" _____ 20__ г.

Содержание

Предисловие 3
Термины и сокращения 4

Часть 1

Защита персональных данных. Разумный подход. 6
1.1. Как организовать защиту персональных данных 8
1.2. Порядок действий по обеспечению безопасности персональных данных 11
1.3. Предпроектное обследование информационной системы учреждения 13

Часть 2

Базовые меры по обеспечению безопасности персональных данных 15
2.1. Классификация информационных систем персональных данных 17
2.2. Уведомление об обработке (о намерении осуществлять обработку) персональных данных 25
2.3. Согласие субъектов на обработку персональных данных 33
2.4. Список лиц, имеющих доступ к ПДн. 37
2.5. Электронный журнал обращений граждан 38

Часть 3

Защита ПДн при неавтоматизированной обработке .. 40
3.1. Общие положения 42
3.2. Требования к типовым формам документов 44

3.3. Требования к журналу для однократного пропуска субъекта персональных данных на территорию оператора 46

Часть 4

Организационные меры по обеспечению безопасности персональных данных 48
4.1. Снижение затрат на создание системы защиты персональных данных 50
4.2. Разработка внутренних документов по защите ПДн 53

Часть 5

Проектирование и внедрение системы защиты персональных данных 56
5.1. Разработка модели угроз безопасности персональных данных 58
5.2. Разработка технического задание на создание системы защиты персональных данных 67
Заключение 68
Список литературы 70
Приложение 1 – Сетевой график мероприятий по защите персональных данных в учреждениях здравоохранения Краснодарского края 72
Приложение 2 – Пример акта классификации ИСПДн 77
Приложение 3 – Пример Уведомления об обработке (о намерении осуществлять обработку) персональных данных 79
Приложение 4 – Образец письменного согласия субъекта на обработку персональных данных 82

Защита персональных данных: Методические рекомендации для руководителей служб здравоохранения Краснодарского края / Под ред. Л.Н. Шмыгленко, В.Н. Зиманин. Краснодар. — ГУЗ МИАЦ, 2010. – 85 с.

Исполнители:

Е.В. Дерябин — начальник отдела технического оснащения и телекоммуникаций ГУЗ МИАЦ

А.А. Дементеева — инженер по технической защите информации ГУЗ МИАЦ

Консультант:

В.А. Кучер — проф., заместитель заведующего кафедры Компьютерных технологий и информационной безопасности Кубанского Государственного Технологического Университета

Рецензент:

О.Н. Мызников — к.т.н., доцент, заместитель директора Института информационных технологий и безопасности

Свои замечания и предложения можете направлять по адресу: 350007, г. Краснодар, ул. Захаров, 63, а также сообщать по телефону: 268-99-73 доб. 109.

e-mail: dementeeva@miac.kuban.ru