**Информационные системы персональных данных.**

**Административная, гражданская, уголовная ответственность**

**УК РФ**

Статья 137. Нарушение неприкосновенности частной жизни

Статья 140. Отказ в предоставлении гражданину информации

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

**КОАП РФ**

Статья 13.11. Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)

Статья 13.12. Нарушение правил защиты информации

Статья 13.13. Незаконная деятельность в области защиты информации

**ТК РФ**

Статья 90. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника

**ФЗ-152**

Ст. 23 Ч.3

…………..

3) требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

В соответствии с Федеральным [законом](http://www.consultant.ru/document/cons_doc_LAW_173429/?dst=100040) от 21.07.2014 N 242-ФЗ с [1 сентября 2015 года](http://www.consultant.ru/document/cons_doc_LAW_173429/?dst=100047) часть 3 статьи 23 будет дополнена пунктом 3.1 следующего содержания:

"3.1) ограничивать доступ к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, в порядке, установленном законодательством Российской Федерации;".

………………….

**ФЗ-152, важные статьи**

<http://www.consultant.ru/document/cons_doc_LAW_166051/?frame=19>

**Статья 3. Основные понятия, используемые в настоящем Федеральном законе**

* персональные данные
* оператор
* обработка персональных данных
* автоматизированная обработка персональных данных

**Статья 5. Принципы обработки персональных данных**

…………………………….

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
……………………………….

7. Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных,……

**Статья 6. Условия обработки персональных данных**

**Статья 9. Согласие субъекта персональных данных на обработку его персональных данных**

**Статья 10. Специальные категории персональных данных**

1. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных [частью 2](http://www.consultant.ru/document/cons_doc_LAW_166051/?frame=9#p165) настоящей статьи.
……………………….

**Статья 11. Биометрические персональные данные**

**Статья 16. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных**

**Статья 19. Меры по обеспечению безопасности персональных данных при их обработке**
………….

3. Правительство Российской Федерации с учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливает:

1) [уровни защищенности](http://www.consultant.ru/document/cons_doc_LAW_137356/?dst=100025) персональных данных при их обработке в информационных системах персональных данных в зависимости от угроз безопасности этих данных;

2) [требования](http://www.consultant.ru/document/cons_doc_LAW_137356/?dst=100009) к защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

3) [требования](http://www.consultant.ru/document/cons_doc_LAW_140009/?dst=100009) к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных.

4. [Состав и содержание](http://www.consultant.ru/document/cons_doc_LAW_166051/?frame=19) необходимых для выполнения установленных Правительством Российской Федерации в соответствии с [частью 3](http://www.consultant.ru/document/cons_doc_LAW_166051/?frame=19#p346) настоящей статьи требований к защите персональных данных для каждого из уровней защищенности, организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются федеральным [органом](http://www.consultant.ru/document/cons_doc_LAW_174373/?dst=100213) исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным [органом](http://www.consultant.ru/document/cons_doc_LAW_174374/?dst=100045) исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

## Постановление правительства от 1 ноября 2012 г. N 1119 Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных

<http://www.consultant.ru/document/cons_doc_LAW_137356/>

П.5

Информационная система является информационной системой, обрабатывающей специальные категории персональных данных, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, 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 персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со [статьей 8](http://www.consultant.ru/document/cons_doc_LAW_166051/?dst=100063) Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в [абзацах первом](http://www.consultant.ru/document/cons_doc_LAW_137356/#p36) - [третьем](http://www.consultant.ru/document/cons_doc_LAW_137356/#p38) настоящего пункта.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

**Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.**

**Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.**

**Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.**

9. Необходимость обеспечения 1-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает либо специальные категории персональных данных, либо биометрические персональные данные, либо иные категории персональных данных;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

10. Необходимость обеспечения 2-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 1-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает биометрические персональные данные;

г) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

д) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

е) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

11. Необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает общедоступные персональные данные сотрудников оператора или общедоступные персональные данные менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

б) для информационной системы актуальны угрозы 2-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

в) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает специальные категории персональных данных сотрудников оператора или специальные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора;

г) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает биометрические персональные данные;

д) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных более чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

12. Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

13. Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

14. Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных [пунктом 13](http://www.consultant.ru/document/cons_doc_LAW_137356/#p66) настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.

15. Для обеспечения 2-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных [пунктом 14](http://www.consultant.ru/document/cons_doc_LAW_137356/#p71) настоящего документа, необходимо, чтобы доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.

16. Для обеспечения 1-го уровня защищенности персональных данных при их обработке в информационных системах помимо требований, предусмотренных [пунктом 15](http://www.consultant.ru/document/cons_doc_LAW_137356/#p72) настоящего документа, необходимо выполнение следующих требований:

а) автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

б) создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

**Приказ ФСТЭК от 18 февраля 2013 г. N 21 Об утверждении состава и содержания Организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**

Еще документы ФСТЭК

[**http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/**](http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/)

<http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty>

**Модель угроз**

Включает в себя:

* Типы возможных нарушителей, включая предположения о возможностях нарушителей, в.т.ч. средств атак имеющихся в наличии.
* Описание каналов возможных атак.
* Показатели исходной защищенности ИСПДн
* Перечень угроз с указанием вероятностью ее реализации, опасности, как следствие актуальности, ее тип, и тип нарушителя, который может ее реализовать.

Дополнительные источники информации:

*Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.*

*Банк данных угроз:* [*http://bdu.fstec.ru/ubi/threat*](http://bdu.fstec.ru/ubi/threat)











**Определение вероятности, возможности и опасности реализации угроз и их актуальности**











Результатом должен быть перечень актуальных угроз их тип и как следствие определение уровня защищенности ИСПДн и перечень используемых средств защиты информации.

**Использование СЗИ**

<http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii>

Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014г. №378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

**Выполнение работ по построению системы защиты**

Работы по технической защите информации могут проводиться только организациями, имеющими советующую лицензию ФСТЭК.

**Аттестация ИСПДн**

Понятие «**аттестация ИСПДн**» относится только к государственным информационным системам персональных данных.

«Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные Приказом ФСТЭК России  17 от 11.02.2013 г.

Для информационных систем, не являющихся государственными, аттестация может проводиться в добровольном порядке. Аттестацию ИСПДн проводится в соответствии со cпециальными требованиями и рекомендациями по защите конфиденциальной информации (СТР-К). Процедура аттестации проводится организацией, имеющей лицензию ФСТЭК.



**Декларирование соответствия ИСПДн требованиям по безопасности информации:**

Декларирование соответствия — это документальное подтверждение соответствия свойств и характеристик ИСПДн предъявляемым к ней требованиям, которые установлены законодательством РФ о персональных данных, а также нормативными и методическими документами Роскомнадзора, ФСТЭК и ФСБ России. Декларирование является одной из форм подтверждения соответствия наряду с аттестацией ИСПДн.

При проведении декларирования собственными силами оператору необходимо сформировать комплект документов, состоящий из технической документации, результатов исследований и других документов, которые могут служить основанием для подтверждения соответствия ИСПДн всем предъявляемым требованиям. К примеру, такими документами могут быть протоколы испытаний системы защиты информации, заключения специалистов по защите информации, сертификаты соответствия по требованиям безопасности информации на средства защиты информации, используемые в ИСПДн, и т.п. Такие заключения и протоколы испытаний могут быть получены от сторонних организаций, имеющих лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации.

**Декларация соответствия должна содержать:**

* наименование и местонахождение оператора персональных данных;
* информацию позволяющую идентифицировать информационную систему персональных данных;
* перечень нормативно-правовых актов, нормативных и методических документов, на соответствие требованиям которых производится декларирование; ­
* описание информационной системы, в том числе описание принятых оператором мер по обеспечению безопасности персональных данных в соответствии c необходимыми требованиями;
* сведения и копии документов, служащих основанием для подтверждения соответствия ИСПДн требованиям по безопасности информации;
* срок действия декларации соответствия. Срок действия декларации, как и аттестата, не должен превышать трёх лет.

Задание на РГЗ

|  |  |  |  |
| --- | --- | --- | --- |
| Бригада | Оператор, особенности информационной системы | Объем данных | Используемое ПО |
| №1 | Медицинская организация, филиалов нет, on-line запись на прием | До 100 000 пациентов и сотрудников | СУБД Oracle Enterprise Edition,ОС – Windows Server 2018, Windows 10 |
| №2 | Медицинская организация, сеть филиалов объединенных выделенной ЛВС | Свыше 100 000 пациентов и сотрудников | СУБД Oracle Standard Edition,ОС – RedHat Enterprise Linux 6, Windows 7 |
| №3 | Медицинская организация, сеть филиалов объединенных через Internet | До 100 000 пациентов и сотрудников | СУБД MS SQL Server Standard, ОС – Windows Server 2012, Windows 7 |
| №4 | ВУЗ, есть филиалы, объединены через Internet | Свыше 100 000 студентов, сотрудников, и слушателей | СУБД PostgreSQL,ОС RedHat Linux,Windows 10 |
| №5 | ВУЗ, нет филиалов | До 100 000 студентов, сотрудников, и слушателей | СУБД MS SQL Server Enterprise, ОС – Windows Server 2016, Windows 10 |
| №6 | ВУЗ, есть филиалы, объединены через Internet | До 100 000 студентов, сотрудников, и слушателей | СУБД MS SQL Server Standard, ОС – Windows Server 2008, Windows 10 |
| №7 | Торговая компания, online-продажа | До 100 000 клиентов и сотрудников  | СУБД MS SQL Server Standard, ОС – Windows Server 2016, Windows 8.1,1C-Битрикс |
| №8 | Торговая компания, online-продажа | Свыше 100 000 клиентов и сотрудников | СУБД MS SQL Server Standard, ОС – Windows Server 2012, Windows 8.1 |
| №9 | Торговая компания,  | До 100 000 клиентов и сотрудников | СУБД MS SQL Server Enterprise, ОС – Windows Server 2016, Windows 8 |
| №10 | Производственная компания | До 100 000 клиентов и сотрудников | СУБД Oracle Standard Edition,ОС - Windows Server 2008, Windows 7 |
| №11 | Производственная компания | Свыше 100 000клиентов и сотрудников | СУБД Oracle Standard Edition,ОС – RedHat Enterprise Linux 6, Windows 8.1 |
| №12 | Производственная компания | Свыше 100 000клиентов и сотрудников | СУБД MS SQL Server Standard, ОС – Windows Server 2008, Windows 8.1 |

***Необходимо:***

Составить модель угроз (включая не более чем 10 угроз);

Установить уровень защищенности ИСПДн;

Определить состав средств защиты информации;

Оценить возможные риски для организации и должностного лица, ответственного за защиту ПД в случае не выполнения мероприятий по защите информации;

***Опционально:***

Оценить затраты на построение системы защиты информации.