|  |
| --- |
|  |
| МИНОБРНАУКИ РОССИИ |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

**ЛЕКЦИОННЫЕ МАТЕРИАЛЫ**

|  |  |
| --- | --- |
| **Защита и обработка персональных данных** | |
| *(наименование дисциплины (модуля) в соответствии с учебным планом)* | |
| Уровень | бакалавриат |
|  | *(бакалавриат, магистратура, специалитет)* |
| Форма обучения | очная |
|  | *(очная, очно-заочная, заочная)* |
| Направление(-я)  подготовки | 46.03.03 «Документоведение и архивоведение» |
|  | *(код(-ы) и наименование(-я))* |
|  |  |
| Институт | комплексной безопасности и специального приборостроения (ИКБСП) |
|  | *(полное и краткое наименование)* |
| Кафедра | Защита информации (КБ-1) |
|  | *(полное и краткое наименование кафедры, реализующей дисциплину (модуль))* |
| Лектор | Вершинин Александр Николаевич |
|  | *(сокращенно – ученая степень, ученое звание; полностью – ФИО)* |

|  |  |  |  |
| --- | --- | --- | --- |
| Используются в данной редакции с учебного года | 2020/21 | | |
|  | *(учебный год цифрами)* | | |
| Проверено и согласовано «\_\_\_\_» \_\_\_\_\_\_\_\_20\_\_\_г. |  |  |  |
|  | *(подпись директора Института/Филиала с расшифровкой)* | | |

Москва 20\_\_ г.

**Конспект лекций**

**Введение.**

Курс дисциплины «Защита и обработка персональных данных» ведет **Вершинин Александр Николаевич**.

Курс построен в соответствии с требованиями федеральных государственных образовательных стандартов по направлениям 46.03.02 «Документоведение и архивоведение» и рабочей программой дисциплины «Защита и обработка персональных данных».

В современном мире информация становится стратегическим ресурсом. Быстрое совершенствование информатизации в России, проникновение ее во все сферы жизненно важных интересов личности, общества и государства вызвали помимо несомненных преимуществ и появление ряда существенных проблем. Одной из них стала необходимость защиты персональных данных и процессов их обработки в информационных системах. Учитывая, что в настоящее время потенциал страны все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная уязвимость от информационных воздействий.

Распространение компьютерных систем, объединение их в коммуникационные усиливает возможности электронного проникновения в них.

Проблема компьютерной преступности в области обработки персональных данных во всех странах мира, независимо от их географического положения, вызывает необходимость привлечения все большего внимания и сил общественности для организации борьбы данным видом преступлений. Особенно широкий размах получили преступления в организации процессов обработки персональных данных в информационных системах.

Хотя уровень внедрения новейших информационных технологий в практику в России не столь значителен, компьютерные преступления с каждым днем дают о себе знать все более и более, а защита персональных данных от них является приоритетной задачей компетентных органов.

Одной из основных причин, связанных с компьютерами, является недостаточная образованность в области безопасности организации процессов защиты и обработки персональных данных. Только наличие некоторых знаний в области безопасности может прекратить инциденты и ошибки, обеспечить эффективное применение мер защиты, предотвратить преступление или своевременно обнаружить подозреваемого.

В связи с этим, основной задачей преподавания дисциплины «Защита и обработка персональных данных» является подготовка кадров, обладающих знаниями, навыками, умениями, в сфере обеспечения информационной безопасности организаций различных форм собственности.

Целью учебного курса является формирование профессиональной компетентности на основе системы теоретических и методологических знаний и специальных умений в области информационной безопасности персональных данных и их использования в профессиональной деятельности будущего специалиста.

Развитие теории информационной безопасности в области персональных данных в настоящее время связано с учетом новых обстоятельств, характерных для современного периода развития информатизации общества.

Контроль знаний обучаемых осуществляется в ходе сдачи зачета.

В случае, если входе обучения будут возникать какие-либо вопросы к лектору, их можно направлять по электронной почте по адресу ve.sa.2009@mail.ru. **Лекция 1. Основы информационной безопасности.**

### 1.1. Основные понятия информационной безопасности

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое информационная безопасность. Термин "информационная безопасность" может иметь различный смысл и трактовку в зависимости от контекста. В данном курсе под **информационной безопасностью** мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры [[1](https://www.intuit.ru/studies/courses/697/553/literature#literature.1)].

ГОСТ "Защита информации. Основные термины и определения" вводит понятие **информационной безопасности** как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

* **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.
* **Целостность** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
* **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

**Угрозы информационной безопасности** – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [[2](https://www.intuit.ru/studies/courses/697/553/literature#literature.2),[3](https://www.intuit.ru/studies/courses/697/553/literature#literature.3)]. **Атакой** называется попытка реализации угрозы, а тот, кто предпринимает такую попытку, - **злоумышленником**. Потенциальные злоумышленники называются источниками угрозы.

Угроза является следствием наличия **уязвимых мест или уязвимостей** в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

* по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
* по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
* по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
* по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход. Выделяют следующие уровни защиты информации:

1. Законодательный – законы, нормативные акты и прочие документы РФ и международного сообщества;
2. Административный – комплекс мер, предпринимаемых локально руководством организации;
3. Процедурный уровень – меры безопасности, реализуемые людьми;
4. Программно-технический уровень – непосредственно средства защиты информации.

Законодательный уровень является основой для построения системы защиты информации, так как дает базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

### 1.2. ФЗ "Об информации, информационных технологиях и о защите информации"

В российском законодательстве базовым законом в области защиты информации является ФЗ "Об информации, информационных технологиях и о защите информации" от 27 июля 2006 года номер 149-ФЗ. Поэтому основные понятия и решения, закрепленные в законе, требуют пристального рассмотрения.

Закон регулирует отношения, возникающие при:

* осуществлении права на поиск, получение, передачу, производство и распространение информации;
* применении информационных технологий;
* обеспечении защиты информации.

Закон дает основные определения в области защиты информации. Приведем некоторые из них:

* **информация** - сведения (сообщения, данные) независимо от формы их представления;
* **информационные технологии** - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
* **информационная система** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;
* **обладатель информации** - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;
* **оператор информационной системы** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.
* **конфиденциальность информации** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [[4](https://www.intuit.ru/studies/courses/697/553/literature#literature.4)].

В статье 4 Закона сформулированы принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации:

1. Свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2. Установление ограничений доступа к информации только федеральными законами;
3. Открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
4. Равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
5. Обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
6. Достоверность информации и своевременность ее предоставления;
7. Неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
8. Недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Вся информация делится на **общедоступную** и ограниченного **доступа**. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. В законе, определяется информация, к которой нельзя ограничить доступ, например, информация об окружающей среде или деятельности государственных органов. Оговаривается также, что ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Закон выделяет 4 категории информации в зависимости от порядка ее предоставления или распространения:

1. Информацию, свободно распространяемую;
2. Информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3. Информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4. Информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Закон устанавливает равнозначность электронного сообщения, подписанного электронной цифровой подписью или иным аналогом собственноручной подписи, и документа, подписанного собственноручно.

Дается следующее определение защите информации - представляет собой принятие правовых, организационных и технических мер, направленных на:

1. Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
2. Соблюдение конфиденциальности информации ограниченного доступа;
3. Реализацию права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1. Предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
2. Своевременное обнаружение фактов несанкционированного доступа к информации;
3. Предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
4. Недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
5. Возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
6. Постоянный контроль за обеспечением уровня защищенности информации.

Таким образом, ФЗ "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет права и обязанности его субъектов.

**Лекция 2: Персональные данные. Законодательство в области защиты персональных данных.**

### 2.1. Персональные данные

Необходимость обеспечения безопасности персональных данных в наше время - объективная реальность. Современный человек не может самостоятельно противодействовать посягательству на его частную жизнь. Возросшие технические возможности по сбору и обработке персональной информации, развитие средств электронной коммерции и социальных сетей делают необходимым принятие мер по защите персональных данных.

Рассмотрим несколько примеров из повседневной жизни, когда нарушаются права человека на конфиденциальность персональных данных. Бывает так, что при оформлении дисконтной карты в магазине покупатель указывает следующие сведения: фамилию, номер телефона, электронный адрес, а затем получает сообщения и письма совершенно из других магазинов, в которых даже никогда не бывал. То есть магазин без согласия покупателя передал его данные третьим лицам. Если газета печатает ФИО и суммы выигрыша победителей лотереи без их ведома, или ТСЖ вывешивает на подъезде списки должников и сумму их долга - это примеры "безобидных " утечек. Кража персональных данных может нанести правообладателю ощутимый материальный ущерб, если речь идет о кредитных картах или информации о сбережениях в банке. Злоумышленники, обладающие достаточными техническими знаниями, похищают реквизиты банковских карт (скиминг) или имитируют сайты финансовых учреждений, чтобы заставить пользователя показать свою личную информацию (фишинг). На самом деле зачастую даже трудно установить источник утечки персональных данных вследствие высокой информатизации современного общества.

Государство на законодательном уровне требует от организаций и физических лиц, обрабатывающих персональные данные, обеспечить их защиту. Законодательство Российской Федерации в области защиты персональных данных основывается на Конституции РФ, международных договорах Российской Федерации, Федеральном законе РФ от 27 июля 2006 г. N 152-ФЗ "О персональных данных", Федеральном законе от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" и других определяющих случаи и особенности обработки персональных данных федеральных законов.

Целью российского законодательства в области защиты персональных данных является обеспечение защиты прав и свобод гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Законодательством регулируются отношения, связанные с обработкой персональных данных, осуществляемой государственными органами власти, органами местного самоуправления, юридическими лицами и физическими лицами.

Основополагающим законом в области защиты персональных данных является Федеральный закон "О персональных данных" №152, который был принят Государственной думой 8 июля 2006 года и вступил в силу с 26 января 2007 года. Закон определяет:

* основные понятия, связанные с обработкой персональных данных;
* принципы и условия обработки персональных данных;
* обязанности оператора персональных данных;
* права субъекта персональных данных;
* виды ответственности за нарушение требований ФЗ-№152;
* государственные органы, осуществляющие контроль за соблюдением требований ФЗ-№152.

В соответствии с Законом **персональные данные** - любая информация, с помощью которой можно однозначно идентифицировать физическое лицо (субъект ПД). К персональным данным в связи с этим могут относиться фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, принадлежащая субъекту ПД.

**Операторами персональных данных** являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Информационная система персональных данных (далее ИСПД)** – 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 [[7](https://www.intuit.ru/studies/courses/697/553/literature#literature.7)].

**Регуляторами** называются органы государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований федерального закона. В ФЗ "О персональных данных" установлены три регулятора:

* Роскомнадзор (защита прав субъектов персональных данных)
* ФСБ (требования в области криптографии)
* ФСТЭК России (требования по защите информации от несанкционированного доступа и утечки по техническим каналам).

Так как ФЗ "О персональных данных" является лишь основой правового обеспечения защиты ПД, его требования в дальнейшем были конкретизированы в актах Правительства РФ и Министерства связи, нормативно-методических документах регуляторов.

### 2.2. Категории персональных данных

ФЗ "О персональных данных" выделяет следующие категории персональных данных.

**Общедоступные ПД -** данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПД или на которые в соответствии с федеральными законами не распространяются требования соблюдения конфиденциальности. Общедоступные источники персональных данных создаются в целях информационного обеспечения (например, справочники и адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

Важно отметить, что сведения о субъекте ПД могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

**Специальные категории ПД -** персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях:

* субъект ПД дал согласие в письменной форме на обработку своих персональных данных;
* персональные данные являются общедоступными;
* персональные данные относятся к состоянию здоровья субъекта ПД и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;
* обработка персональных данных членов (участников) общественного объединения или религиозной организации при условии, что персональные данные не будут распространяться без согласия в письменной форме субъектов ПД;
* обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия [[7](https://www.intuit.ru/studies/courses/697/553/literature#literature.7)].

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных" определяет следующие **категории персональных данных**, которые обрабатываются в ИСПД:

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 ПД и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 – персональные данные, позволяющие идентифицировать субъекта ПД.

Категория 4 – обезличенные и (или) общедоступные персональные данные.

**Биометрические персональные данные** – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПД. Обработка биометрических персональных данных без согласия субъекта ПД может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно - розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством [[7](https://www.intuit.ru/studies/courses/697/553/literature#literature.7)].

Определение биометрических данных в российском законодательстве предоставляет оператору персональных данных возможность принятия самостоятельного решения об отнесении тех или иных данных к биометрическим. Это породило немало споров. Рассмотрим пример с фотографией. С одной стороны, она характеризует физиологические особенности человека. Но человек с течением времени может сильно измениться или злоумышленник может подделать внешние признаки под законного субъекта. Так ли однозначно в данном случае установление личности? В настоящее время представители регуляторов подтверждают, что фотография и видеоизображения относятся к биометрическим данным.

### 2.3. Права субъекта персональных данных

Субъект персональных данных – это физическое лицо, которое может быть однозначно идентифицировано на основе персональных данных, то есть фактически тот, чьи данные необходимо защищать. Рассмотрим основные права субъекта ПД, установленные ФЗ-№152.

1. Право субъекта персональных данных на доступ к своим персональным данным. Это предполагает право субъекта на получение сведений об операторе персональных данных и о том, какие ПД, относящие к этому субъекту, он обрабатывает, а также непосредственный доступ к этим ПД. Субъект вправе требовать от оператора уточнения ПД, их блокирования или уничтожения, если они устаревшие, неполные или не являются необходимыми для заявленной цели обработки. Доступ к своим ПД предоставляется субъекту(или его представителю) при обращении либо на основании запроса. Полученная информация может содержать следующие сведения:

* цель обработки ПД
* способы обработки ПД
* сроки обработки ПД
* перечень допущенных к обработке ПД лиц
* перечень обрабатываемых ПД и источник их получения
* сведения о возможных юридических последствиях обработки ПД для субъекта ПД.

Закон определяет случаи, когда данное право субъекта ПД ограничивается, например, если речь идет о безопасности страны, нарушении конституционных прав и свобод других лиц или оперативно-розыскной деятельности.

1. Права субъектов ПД при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации. В данном случае обработка осуществляется только при условии предварительного согласия субъекта. При этом важно отметить, что обработка признается осуществленной без согласия субъекта, если оператор не доказал обратное. Оператор обязан немедленно прекратить обработку ПД по требованию субъекта.
2. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных. Закон запрещает принятие решений в отношении субъекта ПД исключительно на основании автоматизированной обработки, если не получено его согласия в письменной форме или в случаях, предусмотренных федеральными законами.
3. Право на обжалование действий или бездействия оператора. Если субъект ПД считает, что оператор обрабатывает его ПД ненадлежащим образом, то есть нарушает его права, он может обратиться в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

Необходимо отметить, что субъект ПД имеет право на возмещение убытков и компенсацию материального вреда в судебном порядке.

### 

### 2.4. Обязанности оператора персональных данных

Ранее мы рассмотрели понятие **оператора персональных данных** и действия, являющиеся **обработкой персональных данных** . Исходя из определения, можно сделать вывод о том, что все без исключения организации являются операторами ПД, так как они накапливают, собирают и обрабатывают информацию о своих сотрудниках в рамках Трудового кодекса РФ. Помимо этого многие организации собирают сведения о своих клиентах, подрядчиках, поставщиках и партнерах в рамках своей основной деятельности. Главными обязанностями оператора ПД является уведомление Роскомнадзора об обработке ПД и ,собственно, защита ПД.

Законом предусмотрены случаи, когда оператор не обязан уведомлять Роскомнадзор об обработке ПД:

* если его связывают с субъектом трудовые отношения;
* если между оператором и субъектом существует договор и данные необходимы для исполнения обязательств по нему;
* если данные относятся к членам религиозных объединений и общественных организаций и обрабатываются в соответствии с учредительными документами и с законом.
* если данные являются общедоступными;
* если включают в себя только ФИО;
* данные необходимы для однократного пропуска на территорию оператора или аналогичных целей;
* если данные включены в федеральные автоматизированные информационные системы и государственные информационные системы персональных данных;
* если данные обрабатываются без использования средств автоматизации в соответствии с законами РФ.

Важно отметить, что оговаривается обязанность оператора не передавать персональные данные третьим лицам.

При этом многие организации допускают ошибку в том, что если они не обязаны уведомлять уполномоченный орган об обработке ПД, то можно не выполнять обязанности, возлагаемые законом на операторов ПД. Такие действия являются противозаконными, однозначно трактуются как невыполнение требований законодательства и караются мерами, предусмотренными Законом.

Рассмотрим основные обязанности оператора персональных данных, предусмотренные ФЗ-№152:

1. Обеспечение безопасности обработки персональных данных, что означает обязанность "принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий".
2. Уведомительный характер обработки персональных данных. В соответствии со статьей 2 ФЗ-№152 оператор до начала обработки персональных данных обязан уведомить уполномоченный орган по защите прав субъектов ПД (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. Роскомнадзор вносит сведения об операторе в реестр операторов. Информация, содержащаяся в реестре, за исключением сведений о средствах обеспечения безопасности персональных данных при их обработке, является общедоступной.
3. При получении персональных данных (в том числе от третьих лиц) оператор ПД до начала обработки обязан получить у субъекта этих ПД письменное разрешение на их обработку (за исключением случаев, если персональные данные были предоставлены оператору на основании федерального закона или если они являются общедоступными). Важно отметить, что субъект имеет право отозвать данное разрешение.
4. Оператор обязан предоставить субъекту ПД по требованию все имеющиеся сведения о нем, целях и условиях обработки, способах защиты его персональных данных.

Оператор также должен уничтожить или блокировать соответствующие персональные данные, внести в них необходимые изменения по предоставлении субъектом ПД или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор, являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

Более того, оператор ПД обязан предоставить доказательство получения согласия субъекта ПД на обработку его персональных данных, а в случае обработки общедоступных персональных данных на него возлагается обязанность доказать, что обрабатываемые ПД являются общедоступными.

1. Подконтрольность и поднадзорность деятельности операторов персональных данных государственным органам. Это означает обязанность оператора сообщать в уполномоченный орган по защите прав субъектов ПД по его запросу информацию, необходимую для осуществления деятельности указанного органа. Функциями контроля и надзора государство наделило Роскомнадзор, ФСТЭК и ФСБ[[9](https://www.intuit.ru/studies/courses/697/553/literature#literature.9)].

Законом также предусмотрены случаи, когда не требуется согласие субъекта ПД на обработку сведений о нем:

1. Обработка персональных данных осуществляется на основании других федеральных законов, например, некоторыми Федеральными законами предусматриваются случаи обязательного предоставления субъектом ПД своих персональных данных в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;
2. Оператор и субъект ПД связаны договором на выполнение действий, которые требуют обработки персональных данных этого субъекта, например, договор, по которому туристическая фирма (оператор) имеет право использовать персональные данные субъекта для бронирования гостиницы;
3. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПД, если получение его согласия невозможно, например, госпитализация человека при несчастном случае;
4. Обработка персональных данных необходима 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;
5. 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 ПД;
6. Осуществляется обработка персональных данных, подлежащих опубликованию в соответствии с федеральными законами, в том числе ПД лиц, замещающих государственные должности, должности государственной гражданской службы, персональных данных кандидатов на выборные государственные или муниципальные должности[[7](https://www.intuit.ru/studies/courses/697/553/literature#literature.7)].

Во всех других случаях оператор должен соблюдать требования российского законодательства по обработке персональных данных. Законом предусмотрена гражданская, уголовная, административная, дисциплинарная и иная ответственность за нарушение его требований.

Так, Кодекс об административных правонарушениях предусматривает максимальный штраф в 500000 рублей за невыполнение законного предписания Роскомнадзора (ст. 19.5 КоАП). Тот же Кодекс предусматривает приостановку деятельности организации на срок до 90 суток при осуществлении деятельности по защите персональных данных без лицензии (ст. 19.20 КоАП).

В уголовном кодексе говорится о штрафе в 300000 руб., обязательных работах на срок до 1\_го года, аресте до 6\_ти месяцев и лишении права занимать должность на срок до 5\_ти лет в случае осуществления защиты персональных данных без лицензии в случаях, если это деяние причинило крупный ущерб гражданам (ст. 171 УК).

При систематических и грубых нарушениях Роскомнадзор имеет право ходатайствовать об отзыве лицензий на основной вид деятельности.

**Лекция 3: Автоматизированная и неавтоматизированная обработка персональных данных.**

### 3.1. Автоматизированная и неавтоматизированная обработка персональных данных

Существует два вида обработки персональных данных: **автоматизированный** и **неавтоматизированный**.

Неавтоматизированная обработка персональных данных осуществляется в соответствии с Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

Обработка персональных данных является **неавтоматизированной**, если осуществляется при непосредственном участии человека.

Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности, путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (бланков). Не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий ПД для каждой из них должен использоваться отдельный материальный носитель[[10](https://www.intuit.ru/studies/courses/697/553/literature#literature.10)].

Пункты 1 и 2 Постановления РФ помогают решить вопрос о том, какие системы являются автоматизированными, а какие нет. Процитируем их:

1. 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.
2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных либо были извлечены из нее.

При этом оператор также может совершить ошибку, неправильно трактуя данные пункты. Дело в том, что почти во всех операциях по обработке ПД участвует человек, но это не значит, что обработка неавтоматизированная. Достаточно просто сохранить информацию в виде файла на компьютере – и обработка тут же станет автоматизированной. Примером неавтоматизированной обработки может стать выдача бумажного одноразового пропуска на территорию организации или талончика к врачу.

Для более детального определения автоматизированной системы обработки ПД обратимся к Конвенции "О защите физических лиц при автоматизированной обработке ПД" от 28 января 1981 года. Данный документ вводит понятие "автоматизированный файл" – любой комплекс данных, подвергающихся автоматизированной обработке. И, соответственно, "**автоматизированная обработка** " включает следующие операции, осуществляемые полностью или частично с помощью автоматизированных средств: хранение данных, осуществление логических и/или арифметических операций с этими данными, их изменение, уничтожение, поиск или распространение [[11](https://www.intuit.ru/studies/courses/697/553/literature#literature.11)].

### 3.2.Особенности обеспечения безопасности персональных данных в автоматизированных системах

Автоматизированные системы обработки информации (АС) в общем случае классифицируются по следующим признакам:

* наличие в АС информации различного уровня конфиденциальности;
* уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
* режим обработки данных в АС - коллективный или индивидуальный.

Устанавливается 9 классов защищенности АС от несанкционированного доступа. Каждый класс характеризуется установленным набором требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А. [[4](https://www.intuit.ru/studies/courses/697/553/literature#literature.4)]

Деление АС на классы производится в целях выбора оптимальных и достаточных мер защиты для достижения требуемого уровня защищенности.

**АС, обрабатывающие персональные данные, должны быть отнесены по уровню защищенности к классам 3Б, 2Б и не ниже 1Д.**

В зависимости от структуры АС и способа обработки информации руководящими документами предусмотрены требования и рекомендации к нижеследующим случаям обработки информации:

**обеспечение безопасности в автоматизированных рабочих местах (АРМ) на базе автономных ПЭВМ при использовании съемных накопителей большой емкости.** Такие рабочие места обладают всеми признаками автоматизированной системы, соответственно, должны удовлетворять определенным требованиям по защите информации. Основной особенностью является исключение хранения на ПЭВМ информации, подлежащей защите.

Обмен информацией между АРМ должен осуществляться только на учтенных носителях информации с учетом допуска исполнителей. На рабочих местах исполнителей не должно быть неучтенных носителей информации. В случае формирования конфиденциальных документов с использованием, как текстовой, так и графической информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть "закрыты на запись".

При использовании в данном случае Flash-Bios (FB), необходимо обеспечить целостность записанной в FB информации. Для обеспечения целостности, как перед началом работ, с конфиденциальной информацией при загрузке ПЭВМ, так и по их окончании, необходимо выполнить процедуру проверки целостности FB. При несовпадении необходимо восстановить (записать первоначальную версию) FB, поставить об этом в известность руководителя подразделения и службу безопасности, а также выяснить причины изменения FB.

Должна быть согласована и утверждена технология обработки защищаемой информации, предусматривающая такие вопросы, как защита информации, учет носителей, размещения, эксплуатации АРМ и т.п.

**обеспечение безопасности в локальных вычислительных сетях.** Основными особенностями ЛВС являются распределенное хранение информации, удаленная обработка данных, а также сложность контроля за работой пользователей и общей защищенностью сети. В данном случае средства защиты информации должны использоваться во всех узлах сети, независимо от того, обрабатывают они конфиденциальную информацию или нет.

Персональные данные могут обрабатываться только в изолированных ЛВС, расположенных в пределах контролируемой зоны, или с использованием межсетевого экрана соответствующего уровня.

Для управления ЛВС и распределения системных ресурсов могут быть назначены администраторы безопасности, имеющие соответствующие права и квалификацию.

Состав пользователей ЛВС должен утверждаться по письменному разрешению руководства, а все изменения регистрироваться. Каждый пользователь и администратор должен иметь уникальные идентификаторы и пароли, а в случае использования криптографических средств защиты информации - ключи шифрования для криптографических средств.

**Обеспечение безопасности при межсетевом взаимодействии.** Коммуникационное оборудование и все соединения с локальными периферийными устройствами ЛВС должны располагаться в пределах контролируемой зоны. Рекомендуется учитывать разделение трафика по производственной основе и видам деятельности предприятия при построении сети и конфигурировании коммуникационного оборудования.

Подключение ЛВС к другой автоматизированной системе иного класса защищенности должно осуществляться с использованием МЭ, требования к которому определяются РД Гостехкомиссии России "Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации".

Для защиты конфиденциальной информации при ее передаче по каналам связи из одной АС в другую необходимо использовать:

* в АС класса 1Г - МЭ не ниже класса 4;
* в АС класса 1Д и 2Б, 3Б - МЭ класса 5 или выше [[5](https://www.intuit.ru/studies/courses/697/553/literature#literature.5)].

Если каналы связи выходят за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, защищенные волоконно-оптические линии связи либо сертифицированные криптографические средства защиты.

### 3.3 Обеспечение безопасности персональных данных, обрабатываемых в информационных системах персональных данных

Статья 19 Федерального Закона "О персональных данных" гласит, что оператор при обработке ПД обязан принимать необходимые организационные и технические меры для их защиты от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения, а также от иных неправомерных действий.

Обеспечение безопасности в соответствии ФЗ-№152 не требуется лишь для **обезличенных** и **общедоступных** персональных данных.

Персональные данные могут быть **обезличенными**, в случае, если над ними были произведены действия, в результате которых невозможно определить их принадлежность конкретному субъекту ПД.

Персональные данные могут быть **общедоступными** только с письменного согласия субъекта ПД. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом ПД.

Автоматизированная обработка ПД осуществляется в соответствии с Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 г. "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", а также конкретизируются в нормативно-методических документах ФСТЭК и ФСБ.

Во второй лекции мы уже рассматривали определение информационной системы персональных данных.

**Информационная система персональных данных (ИСПД)** – 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.

Безопасность ПД при их обработке в ИСПД обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных – **уполномоченное лицо**. При этом оператор должен заключать договор с уполномоченным лицом. Существенным условием этого договора является обязанность уполномоченного лица обеспечить конфиденциальность и безопасность ПД при их обработке в ИСПД.

Обеспечение безопасности ПД при их обработке в ИСПД достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных. Обязанность по обеспечению безопасности ПД при их обработке в ИСПД полностью возлагается на оператора персональных данных.

В связи с этим оператор обязан:

* проводить мероприятия, направленные на предотвращение несанкционированного доступа (далее НСД) к ПД и (или) передачи их лицам, не имеющим права доступа к такой информации;
* своевременно обнаруживать факты НСД к персональным данным;
* не допускать воздействия на технические средства автоматизированной обработки ПД, в результате которого может быть нарушено их функционирование;
* незамедлительно восстанавливать ПД, модифицированные или уничтоженные вследствие несанкционированного доступа к ним;
* осуществлять постоянный контроль за обеспечением уровня защищенности ПД.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах оператором может назначаться структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности персональных данных [[14](https://www.intuit.ru/studies/courses/697/553/literature#literature.14)].

Информационные системы персональных данных представляют собой совокупность информационных и программно- аппаратных элементов, основными из которых являются:

* ПД, содержащиеся в базах данных, как совокупность информации и ее источников, используемых в информационных системах;
* информационные технологии, применяемые при обработке ПД;
* технические средства, осуществляющие обработку ПД;
* программные средства, применяемые при обработке.
* средства защиты информации.

### 3.4. Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПД

Для обеспечения безопасности персональных данных оператор ПД или уполномоченное лицо обязаны провести следующие мероприятия:

1. Определить угрозы безопасности персональных данных при их обработке и построить модель угроз;
2. Разработать на основе модели угроз системы защиты персональных данных, обеспечивающих нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
3. Проверить готовность средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
4. Установить и ввести в эксплуатацию средства защиты информации в соответствии с эксплуатационной и технической документацией;
5. Обучить персонал работе со средствами защиты информации;
6. Вести учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
7. Вести учет лиц, допущенных к работе с персональными данными в информационной системе;
8. Контролировать соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
9. Разбирать и составлять заключения по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных; осуществить разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
10. Составить описание системы защиты персональных данных.

### 3.5. Основные принципы обеспечения безопасности персональных данных

При построении системы защиты персональных данных оператор ПД должен руководствоваться следующими принципами:

* принцип законности;
* принцип максимальной дружественности и прозрачности;
* принцип превентивности;
* принцип оптимальности и разумной разнородности;
* принцип адекватности и непрерывности;
* принцип адаптивности;
* принцип доказательности и обязательности контроля;
* принцип самозащиты и конфиденциальности самой системы защиты информации;
* принцип многоуровневости и равнопрочности;
* принцип простоты применения и апробированности защиты;
* принцип преемственности и совершенствования;
* принцип персональной ответственности и минимизации привилегий для пользователей всех уровней.

1. **Принцип законности**. Проведение защитных мероприятий должно быть согласовано с действующим законодательством в области информации, информатизации и защиты информации с применением всех дозволенных методов обнаружения и пресечения нарушений при работе с информацией.
2. **Принцип максимальной дружественности и прозрачности**. Противодействие угрозам безопасности информации всегда носит недружественный характер по отношению к пользователям и обслуживающему персоналу ИС, так как меры по защите информации всегда налагают ограничения на работу организационного и технического характера. Поэтому принимаемые меры должны максимально совмещаться с используемыми операционной и программно-аппаратной структурой ИС, а также должны быть понятны и оправданы для пользователей.
3. **Принцип превентивности.** Меры по защите информации и внедряемые СЗИ должны быть нацелены, прежде всего, на недопущение (пресечение) реализации угроз безопасности информации, а не на устранение последствий их проявления.
4. **Принцип оптимальности и разумной разнородности.** Для сокращения расходов на создание систем обеспечения безопасности должен осуществляться оптимальный выбор соотношения между различными методами и способами противодействия угрозам безопасности информации. Дополнительно внедряемые средства защиты должны дублировать основные функции защиты, уже используемые в программно-аппаратной среде ИС, и по возможности иметь другое происхождение, чем сама эта среда, что позволяет существенно затруднить процесс преодоления защиты за счет иной логики построения защиты.
5. **Принцип адекватности и непрерывности.** Решения, реализуемые системами защиты информации, должны быть дифференцированы в зависимости от важности защищаемой информации и вероятности возникновения угроз ее безопасности. Безопасность информации в государственных информационных системах должна обеспечиваться непрерывно в течение всего жизненного цикла систем.
6. **Принцип адаптивности.** Системы обеспечения информационной безопасности должны строиться с учетом возможного изменения конфигурации ИС, роста числа пользователей, изменения степени конфиденциальности и ценности информации.
7. **Принцип доказательности и обязательности контроля**. Должны реализовываться организационные меры внутри сети и применение специальных аппаратно-программных средств идентификации, аутентификации и подтверждения подлинности информации. Должны обеспечиваться обязательность, своевременность и документированность выявления, сигнализации и пресечения попыток нарушения установленных правил защиты.
8. **Принцип самозащиты и конфиденциальности самой системы защиты информации**.
9. **Принцип многоуровневости и равнопрочности.** ИС должна реализовывать защиту информации на всех уровнях своей жизнедеятельности (технологическом, пользовательском, локальном, сетевом). Защита должна строиться эшелонировано, и иметь несколько последовательных рубежей таким образом, чтобы наиболее важная зона безопасности находилась внутри других зон. Все рубежи защиты должны быть равнопрочными к возможности реализации угрозы.
10. **Принцип простоты применения и апробированности защиты**. Должны применяться средства защиты, для которых формально или неформально возможно доказать корректность выполнения защитных функций, проверить согласованность конфигурации различных компонентов, а их применение пользователями и обслуживающим персоналом должно быть максимально простым, чтобы уменьшить риски, связанные с нарушениям правил их использования. По той же причине целесообразно использовать средства защиты информации, допускающие возможность централизованного администрирования.
11. **Принцип преемственности и совершенствования.** Система защиты информации должна постоянно совершенствоваться на основе преемственности принятых ранее решений и анализа функционирования ИС.
12. **Принцип персональной ответственности и минимизации привилегий для пользователей всех уровней**. Принимаемые меры должны определять права и ответственности каждого уполномоченного лица. Распределение прав и ответственности должно в случае любого нарушения позволять определить круг виновных. Система обеспечения информационной безопасности должна обеспечивать разделение прав и ответственности между пользователями[[13](https://www.intuit.ru/studies/courses/697/553/literature#literature.13)].

**Лекция 4: Модель угроз ПД. Организационно-распорядительная документация по защите ПД**

### 4.1. Угрозы информационной безопасности

При построении системы защиты персональных данных (далее СЗПД) ключевым этапом является построение частной модели угроз для конкретной организации. На основании этой модели в дальнейшем подбираются адекватные и достаточные средства защиты, в соответствии с принципами, рассмотренными в ["Автоматизированная и неавтоматизированная обработка персональных данных"](https://www.intuit.ru/studies/courses/697/553/lecture/12445) .

Под **угрозами безопасности ПД** при их обработке в ИСПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Появление угроз безопасности может быть связано как с преднамеренными действиями злоумышленников, так и с непреднамеренными действиями персонала или пользователей ИСПД.

Угрозы безопасности могут быть реализованы двумя путями:

* через технические каналы утечки;
* путем несанкционированного доступа.

Обобщенная схема реализации канала угроз ПД показана на [рисунке 4.1](https://www.intuit.ru/studies/courses/697/553/lecture/12447?page=1#image.4.1)

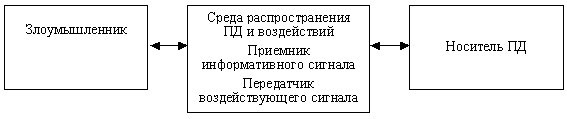


Рис. 4.1 - Обобщенная схема канала реализации угроз безопасности персональных данных

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация. Среда распространения бывает однородной, например, только воздух при распространении электромагнитного излучения, или неоднородной, когда сигнал переходит из одной среды в другую. Носителями ПД могут быть люди, работающие с ИСПД, технические средства, вспомогательные средства и т.д. Главное, что информация при этом отображается в виде полей, сигналов, образов, количественных характеристиках физических величин.

Как правило, выделяют следующие угрозы за счет реализации технических каналов утечки:

* угрозы утечки речевой информации. Фактически злоумышленник перехватывает информацию с помощью специальной аппаратуры в виде акустических, виброакустических волн, а также электромагнитного излучения, модулированного акустическим сигналом. В качестве средств могут использоваться различного рода электронные устройства, подключаемые либо к каналам связи, либо к техническим средствам обработки ПД;
* угрозы утечки видовой информации. В этом случае речь идет о непосредственном просмотре ПД при наличии прямой видимости между средством наблюдения и носителем ПД. В качестве средств наблюдения используются оптические средства и видеозакладки;
* угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН). Речь идет о перехвате побочных (не связанных с прямым функциональным значением элементов ИСПД) информативных электромагнитных полей и электрических сигналов, возникающих при обработке ПД техническими средствами ИСПД. Для регистрации ПЭМИН используется аппаратура в составе радиоприемных устройств и оконечных устройств восстановления информации. Кроме этого, перехват ПЭМИН возможен с использованием электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки ПД. Наводки электромагнитных излучений возникают при излучении элементами технических средств ИСПД информативных сигналов при наличии емкостной, индуктивной или гальванической связей соединительных линий технических средств ИСПД и различных вспомогательных устройств.

Источниками угроз, реализуемых за счет **несанкционированного доступа к базам данных** с использованием штатного или специально разработанного программного обеспечения, являются субъекты, действия которых нарушают регламентируемые в ИСПД правила разграничения доступа к информации. Этими субъектами могут быть:

* нарушитель;
* носитель вредоносной программы;
* аппаратная закладка.

Под **нарушителем** здесь и далее понимается физическое лицо (лица), случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности ПД при их обработке техническими средствами в информационных системах. С точки зрения наличия права легального доступа в помещения, в которых размещены аппаратные средства, обеспечивающие доступ к ресурсам ИСПД, нарушители подразделяются на два типа:

* нарушители, не имеющие доступа к ИСПД, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена, – внешние нарушители;
* нарушители, имеющие доступ к ИСПД, включая пользователей ИСПД, реализующие угрозы непосредственно в ИСПД, – внутренние нарушители.

Для ИСПД, предоставляющих информационные услуги удаленным пользователям, внешними нарушителями могут являться лица, имеющие возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий, алгоритмических или программных закладок через автоматизированные рабочие места, терминальные устройства ИСПД, подключенные к сетям общего пользования.

Обобщим полученные знания с помощью [рисунка 4.2](https://www.intuit.ru/studies/courses/697/553/lecture/12447?page=1#image.4.2).

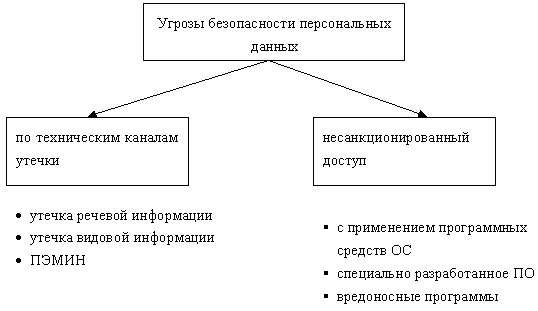


Рис. 4.2 - Классификация угроз безопасности персональных данных по способу реализации

Угрозы можно классифицировать по различным признакам, например, по виду нарушаемого свойства информации (конфиденциальность, целостность, доступность), по типу ИСПД, на которые направлена атака, по типу используемой для атаки уязвимости.

### 4.2. Общая характеристика уязвимостей информационной системы персональных данных

Появление потенциальных угроз безопасности связано с наличием слабых мест в ИСПД - уязвимостей. **Уязвимость информационной системы персональных данных** – недостаток или слабое место в системном или прикладном программном (программно-аппаратном) обеспечении ИСПД, которые могут быть использованы для реализации угрозы безопасности персональных данных.

Причинами возникновения уязвимостей в общем случае являются:

* ошибки при разработке программного обеспечения;
* преднамеренные изменения программного обеспечения с целью внесения уязвимостей;
* неправильные настройки программного обеспечения;
* несанкционированное внедрение вредоносных программ;
* неумышленные действия пользователей;
* сбои в работе программного и аппаратного обеспечения.

Уязвимости, как и угрозы, можно классифицировать по различным признакам:

* по типу ПО – системное или прикладное;
* по этапу жизненного цикла ПО, на котором возникла уязвимость – проектирование, эксплуатация и пр;
* по причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов;
* по характеру последствий от реализации атак – изменение прав доступа, подбор пароля, вывод из строя системы в целом и пр.

Наиболее часто используемые уязвимости относятся к протоколам сетевого взаимодействия и к операционным системам, в том числе к прикладному программному обеспечению.

Уязвимости операционной системы и прикладного ПО в частном случае могут представлять:

* функции, процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений операционной системой;
* фрагменты кода программ ("дыры", "люки"), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
* отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т.п.);
* ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. Так, например, протокол прикладного уровня FTP, широко используемый в Интернете, производит аутентификацию на базе открытого текста, тем самым позволяя перехватывать данные учетной записи.

Прежде чем приступать к построению системы защиты информации необходимо провести анализ уязвимостей ИСПД и попытаться сократить их количество, то есть использовать метод превентивности. Можно закрыть лишние порты, поставить "заплатки" на программное обеспечение (например, service pack для Windows), ввести более сильные методы аутентификации и т.п. Эти меры могут существенно сократить материальные, временные и трудовые затраты на построение системы защиты персональных данных в дальнейшем.

### 4.3. Наиболее часто реализуемые угрозы

В связи с повсеместным развитием Интернета наиболее часто атаки производятся с использованием уязвимостей протоколов сетевого взаимодействия. Рассмотрим 7 наиболее распространенных атак.

**1. Анализ сетевого трафика**

Данный вид атаки направлен в первую очередь на получение пароля и идентификатора пользователя путем "прослушивания сети". Реализуется это с помощью sniffer – специальная программа-анализатор, которая перехватывает все пакеты, идущие по сети. И если протокол, например, FTP или TELNET, передает аутентификационную информацию в открытом виде, то злоумышленник легко получает доступ к учетной записи пользователя.

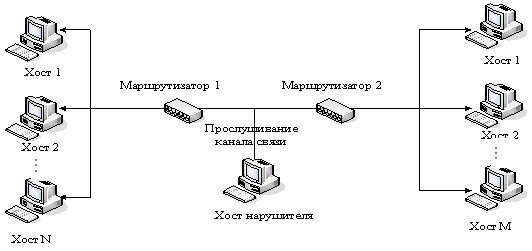


Рис. 4.3 - Схема реализации угрозы “Анализ сетевого трафика”

**2. Сканирование сети**

Суть данной атаки состоит в сборе информации о топологии сети, об открытых портах, используемых протоколах и т.п. Как правило, реализация данной угрозы предшествует дальнейшим действиям злоумышленника с использованием полученных в результате сканирования данных.

**3. Угроза выявления пароля**

Целью атаки является преодоление парольной защиты и получении НСД к чужой информации. Методов для кражи пароля очень много: простой перебор всех возможных значений пароля, перебор с помощью специальных программ (атака словаря), перехват пароля с помощью программы-анализатора сетевого трафика.

**4. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.** Доверенный объект – это элемент сети, легально подключенный к серверу.

Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh-службы UNIX-хоста).

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа, установленные его пользователем для доверенного абонента, к техническому средству ИСПД– цели угроз.

**5. Навязывание ложного маршрута сети**

Данная атака стала возможной из-за недостатков протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP), таких как слабая аутентификация маршрутизаторов. Суть атаки состоит в том, что злоумышленник, используя уязвимости протоколов, вносит несанкционированные изменения в маршрутно-адресные таблицы.

**6. Внедрение ложного объекта сети**

Когда изначально объекты сети не знают информацию друг о друге, то для построения адресных таблиц и последующего взаимодействия, используется механизм запрос (как правило, широковещательный) - ответ с искомой информацией. При этом если нарушитель перехватил такой запрос, то он может выдать ложный ответ, изменить таблицу маршрутизации всей сети, и выдать себя за легального субъекта сети. В дальнейшем все пакеты, направленные к легальному субъекту, будут проходить через злоумышленника.

**7. Отказ в обслуживании**

Этот тип атак является одним из самых распространенных в настоящее время. Целью такой атаки является отказ в обслуживании, то есть нарушение доступности информации для законных субъектов информационного обмена.

Могут быть выделены несколько разновидностей таких угроз:

* скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПД на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований ко времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо-запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP-соединений (SYN-flooding), шторм запросов к FTP-серверу;
* явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов на обслуживание), при котором легальные запросы не могут быть переданы через сеть из-за недоступности среды передачи либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP-эхо-запросов (Smurf), направленный шторм (SYN-flooding), шторм сообщений почтовому серверу (Spam);
* явный отказ в обслуживании, вызванный нарушением логической связности между техническими средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно-адресных данных (например, ICMP Redirect Host, DNS-flooding) или идентификационной и аутентификационной информации;
* явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа "Land", "TearDrop", "Bonk", "Nuke", "UDP-bomb") или имеющих длину, превышающую максимально допустимый размер (угроза типа "Ping Death"), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПД в ИСПД, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПД, какое максимально может "вместить" трафик (направленный "шторм запросов"), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полную остановку компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Мы рассмотрели наиболее часто реализуемые угрозы при сетевом взаимодействии. На практике угроз значительно больше. Частная модель угроз безопасности строится на основе двух документов ФСТЭК – "**Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных"** и "**Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПД"**. Если организация большая, и в ней несколько систем ИСПД, наиболее разумным решением будет привлечение квалифицированных специалистов сторонних фирм для построения частной модели угроз и проектирования СЗПД.

### 4.4. Организационно-распорядительная документация по защите ПД

Помимо технических и процедурных решений создаваемой системы защиты персональных данных, оператор должен обеспечить разработку организационно - распорядительных документов, которые будут регулировать все возникающие вопросы по обеспечению безопасности ПД при их обработке в ИСПД и эксплуатации системы защиты персональных данных (далее СЗПД). Таких документов достаточно много, основные из них:

1. Положение по обеспечению безопасности ПД. Это внутренний (локальный) документ организации. Строгой формы данного документа нет, но он должен удовлетворять требованиям ТК и ФЗ-152, а, следовательно, в нем должно быть указано:

* цель и задачи в области защиты персональных данных;
* понятие и состав персональных данных;
* в каких структурных подразделениях и на каких носителях (бумажных, электронных) накапливаются и хранятся эти данные;
* как происходит сбор и хранение персональных данных;
* как они обрабатываются и используются;
* кто (по должностям) в пределах фирмы имеет к ним доступ;
* принципы защиты ПД, в том числе от несанкционированного доступа;
* права работника в целях обеспечения защиты своих персональных данных;
* ответственность за разглашение конфиденциальной информации, связанной с персональными данными работников.

Положение по обеспечению безопасности персональных данных утверждается руководителем организации или уполномоченным им лицом, вводится в действие приказом руководителя. Работодатель обязан ознакомить работника с Положением… под подпись.

2. Для организации системы допуска и учета лиц, допущенных к работе с ПД в ИСПД, - Список лиц, допущенных к обработке ПД (перечень по должностям тех, кому доступ к ПД необходим для выполнения служебных обязанностей) и Матрица доступа (должна отражать полномочия пользователей по выполнению конкретных действий в отношении конкретных информационных ресурсов ИСПД – чтение, запись, корректировка, удаление).

В первую очередь доступ необходимо оформить сотрудникам кадровой службы, поскольку они собирают и формируют данные о работнике, а также сотрудникам бухгалтерии. Помимо того, доступ к этим сведениям могут получить руководители структурных подразделений (например, начальники отделов) – и это также необходимо отразить в списке. Однако все они вправе запрашивать не любые данные, а только те, которые необходимы для выполнения конкретных трудовых функций (например, чтобы рассчитать льготы по налогам, бухгалтерия получит не все сведения о работнике, а только данные о количестве его иждивенцев). Поэтому целесообразно прописать перечень информационных ресурсов, к которым пользователи допущены.

Список лиц, допущенных к обработке ПД, можно оформить в виде приложения к Положению по обеспечению безопасности персональных данных или отдельным документом, утвержденным руководителем.

3. Частная модель угроз (если ИСПД несколько, то модель угроз разрабатывается на каждую из них) – разрабатывается по результатам предварительного обследования. ФСТЭК России предлагает Базовую модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, согласно которой при создании частной модели должны быть рассмотрены:

* угрозы утечки информации по техническим каналам;
* угрозы несанкционированного доступа, связанные с действиями нарушителей, имеющих доступ к ИСПД, реализующих угрозы непосредственно в ИСПД. При этом необходимо в качестве потенциальных нарушителей рассматривать легальных пользователей ИСПД;
* угрозы несанкционированного доступа, связанные с действиями нарушителей, не имеющих доступа к ИСПД, реализующих угрозы из внешних сетей связи общего пользования и(или) сетей международного информационного обмена.

Разработанная модель угроз утверждается руководителем.

4. На основании утвержденной модели угроз ИСПД необходимо разработать требования по обеспечению безопасности ПД при их обработке в ИСПД. Требования, как и модель угроз, - это самостоятельный документ, который должен быть утвержден руководителем организации.

Для разработки модели угроз и требований оператору целесообразно привлекать специалистов организаций-лицензиатов ФСТЭК.

5. Инструкции в части обеспечения безопасности ПД при их обработке в ИСПД.

6. Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.

Мы рассмотрели только основные организационно-распорядительные документы. Помимо перечисленных документов необходимо составить Акт классификации ИСПД, Технический паспорт ИСПД, Электронный журнал регистрации обращений пользователей ИСПД на получение ПД, Регламент разграничения прав доступа, приказы о назначении лиц, работающих с ИСПД и т.п.

Кроме того, до проведения всех мероприятий по защите ПД оператор должен назначить должностное лицо или (если ИСПД достаточно велика) структурное подразделение, ответственные за обеспечение безопасности ПД. Решение о назначении оформляется приказом руководителя. Задачи, функции и полномочия должностного лица (подразделения), ответственного за обеспечение безопасности ПД, определяются внутренними организационно-распорядительными документами (должностными инструкциями, регламентами).

**Лекция 5: Порядок организации защиты персональных данных. Организационно-распорядительная документация**

### 5.1.Общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных

Основные принципы и правила обеспечения безопасности ПД в информационных системах регулируются **"Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"**, утвержденным Постановлением Правительства Российской Федерации от 17.11.2007 № 781. (Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 настоящее постановление признано утратившим силу.)

При защите персональных данных должно быть обеспечено:

* предотвращение несанкционированного доступа к ПД и передачи их лицам, не имеющим соответствующих прав;
* своевременное обнаружение фактов НСД к ПД;
* предотвращение воздействия на технические средства обработки ПД, которое может нарушить их функционирование;
* возможность немедленного восстановления ПД в случае их модификации или уничтожения в результате НСД.
* постоянный контроль уровня защищенности персональных данных[[18](https://www.intuit.ru/studies/courses/697/553/literature#literature.18)].

Организация безопасности ПД в ИСПД происходит в порядке, который предусматривает следующие этапы:

* оценка обстановки;
* обоснование требований безопасности ПД и постановка задач защиты;
* разработка замысла обеспечения безопасности;
* выбор мер и способов защиты в соответствии с требованиями безопасности и замыслом защиты;
* решения вопросов управления защитой;
* реализация замысла защиты;
* планирование мероприятий по защите;
* создание СЗПД;
* разработка документов для эксплуатации СЗПД и организации обеспечения безопасности ИСПД.

Прежде всего, необходимо ограничить физический доступ к защищаемой информации. В основе защиты от физического доступа лежат организационные мероприятия. Для организации физической защиты помещений и технических средств обработки ПД в первую очередь документально заверяются границы контролируемой зоны, ограничивается доступ в помещения, где обрабатываются ПД, производится их охрана в нерабочее время, определяется порядок и специальное место хранения материальных носителей с ПД, опечатываются корпуса ПЭВМ.

### 5.2. Оценка обстановки и формирование замысла защиты персональных данных

Оценка обстановки является этапом, во многом определяющим эффективность решения задач обеспечения безопасности ПД. В ее основе лежит комплексное обследование организации и ИСПД, использующихся для обработки ПД. Прежде всего, определяется информация, которую необходимо защищать, производится ее категорирование и оценивается необходимость защиты от таких угроз, как уничтожение или хищение аппаратных средств или носителей с ПД, утечки информации по техническим каналам, от НСД и прочих рассмотренных ранее угроз.

При оценке обстановки учитывается степень ущерба в случае успешной реализации одной из угроз. Рассмотрим основные подэтапы оценки обстановки:

1. Анализ информационных ресурсов:

* Определение состава, содержания и местонахождения ПД, подлежащих защите;
* Категорирование ПД;
* Оценка выполнения обязанностей по обеспечению безопасности ПД оператором в текущий момент времени.

2. Анализ уязвимых звеньев и возможных угроз безопасности ПД:

* Оценка возможности физического доступа к ИСПД;
* Выявление технических каналов утечки информации;
* Анализ возможностей программно-математического воздействия на ИСПД;
* Анализ возможностей электромагнитного воздействия на ПД.

3. Оценка ущерба от реализации угроз:

* Оценка непосредственного ущерба от реализации угроз;
* Оценка опосредованного ущерба от реализации угроз;

4. Анализ имеющихся в распоряжении мер и средств защиты ПД:

* от физического доступа;
* от утечки по техническим каналам утечки информации;
* от НСД;
* от программно-математических воздействий;
* от электромагнитных воздействий.

В зависимости от объекта, причинение ущерба которому, в конечном счете, вызывается неправомерными действиями с ПД, рассматриваются два вида ущерба: непосредственный и опосредованный.

**Непосредственный ущерб** связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту ПД. Он возникает за счет незаконного использования (в том числе распространения) ПД или за счет несанкционированной модификации этих данных и может проявляться в виде:

* нанесения вреда здоровью субъекта ПД;
* незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;
* потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием ПД;
* нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь путем осуществления контактов с ним по различным поводам без его на то согласия (например – рассылка персонифицированных рекламных предложений и т.п.).

**Опосредованный ущерб** связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности экономических, политических, военных, медицинских, правоохранительных, социальных, кредитно-финансовых и иных государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с ПД.

Разработка замысла защиты является важным этапом построения СЗПД, в ходе которого определяются основные направления защиты персональных данных, и производится выбор способов защиты. К способам защиты относятся как технические средства, так и организационные меры. В качестве технических средств защиты следует использовать сертифицированные средства защиты. Основные этапы формирования замысла защиты показаны на [рисунке 5.1](https://www.intuit.ru/studies/courses/697/553/lecture/12448?page=1#image.5.1).



Рис. 5.1 - Формирование замысла защиты персональных данных

К основным вопросам управления относятся:

* распределение функций управления доступом к данным и их обработкой между должностными лицами;
* определение порядка изменения правил доступа к защищаемой информации;
* определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;
* определение порядка действий должностных лиц в случае возникновения нештатных ситуаций;
* определение порядка проведения контрольных мероприятий и действий по его результатам.

Для поддержания эффективного уровня защиты персональных данных необходимо своевременно решать вопросы по управлению защитой, а также основные вопросы, такие как подготовка кадров, финансирование и закупка необходимого оборудования. Только комплексный подход может гарантировать достаточность принятых мер защиты персональных данных.

**Лекция 6: Классификация ИСПД**

На начальном этапе построения СЗПД определяется класс для каждой ИСПД в конкретной организации. От класса ИСПД зависит, какие требования по обеспечению безопасности должны выполняться для заданной ИСПД, следовательно, выбор мер, способов защиты и их стоимость. Классификация ИСПД проводится в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России № 55/86/20 от 18.02.2009 г. **"Об утверждении порядка проведения классификации информационных систем персональных данных"** (утратил силу 31 декабря 2013 г.).

Классификация ИСПД проводится на этапе ее создания или в ходе эксплуатации, но обязательно до построения СЗПД. В общем случае все информационные системы, обрабатывающие персональные данные, подразделяются на 2 класса в зависимости от характеристик безопасности обрабатываемых данных:

**Типовые информационные системы** – системы, где требуется обеспечить только конфиденциальность обрабатываемых персональных данных.

**Специальные информационные системы** – системы, где требуется обеспечить хотя бы одну из характеристик безопасности, отличную от конфиденциальности (например, целостность или доступность). К специальным информационным системам должны быть отнесены:

1. ИСПД, связанные с обработкой ПД о состоянии здоровья субъектов ПД;
2. ИСПД, принимающие решения на основании исключительно автоматизированной обработки ПД. При этом принятые решения могут повлечь за собой юридические последствия для субъекта ПД или иным способом затронуть его законные права и интересы.

Согласно предлагаемой в Приказе методике ИСПД классифицируется в зависимости от количества субъектов, чьи данные обрабатываются, и типа обрабатываемых персональных данных.

В зависимости от объема обрабатываемых в ИСПД данных XНПД выделяют следующие категории ИСПД:

**1 категория** – в информационной системе одновременно обрабатываются персональные данные **более чем 100 000** субъектов ПД или персональные данные субъектов ПД в пределах субъекта Российской Федерации или Российской Федерации в целом;

**2 категория** – в информационной системе одновременно обрабатываются персональные данные **от 1000 до 100 000** субъектов ПД или персональные данные субъектов ПД, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;

**3 категория** – в информационной системе одновременно обрабатываются персональные данные **менее чем 1000** субъектов ПД или персональные данные субъектов ПД в пределах конкретной организации.

Таким образом, данная категория ИСПД определяется на основании количества субъектов ПД, чьи данные обрабатываются в системе.

Определяются следующие категории обрабатываемых в информационной системе персональных данных (ХПД):

**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.

По результатам анализа вышеперечисленных данных определяется класс ИСПД в соответствии с [таблицей 6.1](https://www.intuit.ru/studies/courses/697/553/lecture/12450?page=1#table.6.1).

Таблица 6.1 - Определение класса информационной системы

|  |  |  |  |
| --- | --- | --- | --- |
| ХНПД | Категория 3 | Категория 2 | Категория 1 |
| ХПД |  | | |
| категория 4 | К4 | К4 | К4 |
| категория 3 | К3 | К3 | К2 |
| категория 2 | К3 | К2 | К1 |
| категория 1 | К1 | К1 | К1 |

Рассмотрим, что значит каждый класс ИСПД в отдельности:

* **класс 1 (К1)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов ПД;
* **класс 2 (К2)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов ПД;
* **класс 3 (К3)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов ПД;
* **класс 4 (К4)** – информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов ПД.

Наивысшим считается класс 1. Если в составе ИСПД выделяют несколько подсистем, то класс ИСПД в целом будет соответствовать наиболее высокому классу входящих компонентов.

Таким образом, чем выше класс ИСПД, тем выше требования по обеспечению безопасности персональных данных.

Порядок определения класса для специальных систем несколько отличается от типовых. Класс специальных ИСПД определяется на основе частной модели угроз организации в соответствии с методическими документами ФСТЭК. Отнесение информационной системы к специальной позволяет существенно снизить затраты на построение СЗПД, так как оператор в данном случае может обоснованно выбрать минимальное количество актуальных угроз, от которых необходима защита ПД. Например, если в системе есть сведения о доходах человека (например, 1С), такая система может быть отнесена к специальной, так как затрагиваются законные интересы человека. То же самое относится к информации об инвалидности, расовой принадлежности и пр. Отнесение ИСПД к специальной на практике является достаточно спорным моментом.

Класс ИСПД может быть пересмотрен:

* по решению оператора после проведения анализа и оценки угроз безопасности с учетом особенностей или (и) изменений информационной системы;
* по результатам испытаний по контролю за выполнением требований по обработке ПД.

ИСПД также классифицируются по структуре, по наличию подключений к сетям общего пользования, по режиму обработки ПД, по разграничению прав доступа. Приведенные классификации отображены схематически на [рисунке 6.1](https://www.intuit.ru/studies/courses/697/553/lecture/12450?page=1#image.6.1).

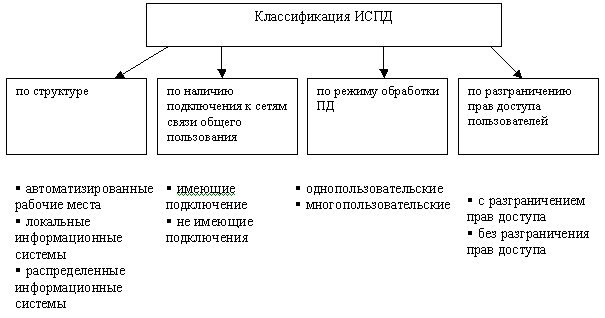


Рис. 6.1 - Классификация ИСПД

Классификация ИСПД - не формальная процедура, так как на основании класса системы будут определяться меры и способы защиты персональных данных, существенно отличающиеся друг от друга. Более того, для 1 и 2 класса систем обязательно лицензирование используемых технических средств защиты, а сами ИСПД должны быть аттестованы. Результат классификации оформляется соответствующим актом оператора.

При классификации информационных систем на практике выявляется множество факторов, впоследствии влияющих на построение СЗПД. Например, если в информационной системе помимо стандартных данных о сотрудниках, таких как ФИО, адрес и телефон, хранятся фотографии, значит, система обрабатывает биометрические ПД. А если наряду со стандартной информацией обрабатывается дата рождения, можно сказать, что ИСПД содержит дополнительную информацию о субъекте и отнести ее не к классу 3, а к классу 2.

При внимательном анализе на предпроектном этапе построения СЗПД, можно оптимизировать некоторые моменты обработки ПД. Так, например, если в системе учета кадров вместо ФИО использовать табельный номер работника, речь будет идти об обработке обезличенных персональных данных, требования к безопасности которых минимальны. Оптимизация представления данных в системе может повлиять на проектирование СЗПД и существенно сократить затраты в конечном итоге.

**Лекция 7: Мероприятия по техническому обеспечению безопасности ПД**

### 7.1. Мероприятия от утечки информации по техническим каналам

При обработке персональных данных в информационной системе они должны быть защищены:

* от несанкционированного доступа (в том числе случайного);
* от утечки информации по техническим каналам.

Если при построении частной модели угроз организации выявлено, что возможна утечка акустической речевой информации, видовой информации и угроза утечки информации через ПЭМИН, необходима защита информации от утечки по техническим каналам.

Для исключения утечки через ПЭМИН в ИСПД 1 класса применяют следующие мероприятия:

* использование технических средств в защищенном исполнении;
* использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
* размещение объектов защиты в соответствии с предписанием на эксплуатацию;
* размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории;
* обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
* обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.

В информационных системах 2 класса для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники[[21](https://www.intuit.ru/studies/courses/697/553/literature#literature.21)].

Если в ИСПД применяется функция голосового ввода, то необходима звукоизоляция помещений ИСПД, систем вентиляции и кондиционирования этих помещений с целью исключения возможности прослушивания. Для исключения просмотра ПД требуется правильно расположить устройства вывода информации, например, расставить мониторы подальше от окон или других мест, откуда потенциальный злоумышленник может получить доступ к ПД.

### 7.2. Обязательные требования по обеспечению безопасности ПД от НСД

В состав мероприятий по защите ПД при их обработке в ИСПД от НСД и неправомерных действий входят следующие мероприятия:

* защита от НСД при однопользовательском режиме обработки ПД;
* защита от НСД при многопользовательском режиме обработки ПД и равных правах доступа к ним субъектов доступа;
* защита от НСД при многопользовательском режиме обработки ПД и разных правах доступа;
* защита информации при межсетевом взаимодействии ИСПД;
* антивирусная защита;
* обнаружение вторжений.

**Несанкционированный доступ (НСД)** - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам [2].

ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" дает следующее определение несанкционированного воздействия на информацию.

Несанкционированное воздействие на информацию - воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

К основным требованиям по защите персональных данных от НСД относится обеспечение следующих мер и способов защиты:

* разрешительная система доступа пользователей ИСПД к системе, информации и документам, связанным с ее работой;
* ограничение доступа в помещения, где обрабатываются ПД и к носителям с ПД;
* разграничение доступа к информационным ресурсам, программным средствам обработки и передачи информации, к средствам защиты информации;
* регистрация и контроль действий пользователей и обслуживающего персонала ИСПД;
* учет, хранение и обращение съемных носителей информации, исключающие их хищение, порчу, подмену и т.п.;
* резервирование технических средств и носителей информации;
* использование технических средств, которые прошли проверку на соответствие;
* использование защищенных каналов связи;
* размещение технических средств для обработки ПД внутри границ охраняемой территории;
* организация физической защиты помещений и технических средств обработки ПД;
* предотвращение внедрения вирусов и программных закладок в ИСПД.
* реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

При подключении ИСПД к сетям общего пользования или к другой ИСПД необходимо применять межсетевые экраны.

Если ИСПД подключена к сетям общего пользования или работает со съемными носителями,

необходимо применение средств антивирусной защиты.

В общем случае обеспечение безопасности ПД от НСД сводится к реализации следующих подсистем в рамках СЗПД:

* управление доступом;
* регистрация и учет;
* обеспечение целостности;

Набор и содержание функций определяется в зависимости от класса ИСПД и исходя из угроз безопасности ПД, структуры ИСПД, наличия межсетевого взаимодействия и режимов обработки персональных данных, рассмотренных нами в лекции 6. Для каждого класса типовых ИСПД требования определены отдельно.

Наименьшие требования по обеспечению безопасности ПД применяются к 4 классу ИСПД – методы и способы защиты ПД, а также целесообразность их применения определяются оператором.

Основные требования к ИСПД в зависимости от класса и режима обработки данных представлены в [таблице 7.1](https://www.intuit.ru/studies/courses/697/553/lecture/12451?page=1#table.7.1).

Таблица 7.1 - Основные требования по обеспечению информационной безопасности в соответствии с классом ИСПД

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Вид мероприятия | Наличие требования для ИСПД конкретного класса | | | | | | | | | |
| Однопользовательский | | | | Многопользовательский | | | | | |
| С равными правами доступа | | | С неравными правами доступа | | |
| 3кл | | 2кл | 1кл | 3кл | 2кл | 1кл | 3кл | 2кл | 1кл |
| Подсистема управления доступом | | | | | | | | | | |
| Идентификация пользователя по условно-постоянному паролю не менее 6 символов | | Да | да | да | - | - | - | да | да | - |
| Идентификация пользователя по идентификатору и условно-постоянному паролю не менее 6 символов | | - | - | - | да | да | да | - | - | да |
| Идентификация технических средств, каналов связи, внешних устройств по их логическим адресам (номерам) | | - | - | - | - | - | да | - | - | да |
| Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам | | - | - | - | - | - | да | - | - | да |
| Контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа | | - | - | - | - |  |  |  |  | да |
| Подсистема регистрации и учета | | | | | | | | | | |
| Регистрация времени и даты входа (выхода) пользователя в систему или загрузки операционной системы и ее программной остановки | | Да | да | да | да | да | да | да | да | да |
| Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета | | Да | да | да | да | да | да | да | да | да |
| Регистрация выдачи печатных документов на бумажный носитель | | - | - | да | - | - | да | - | - | да |
| Дублирующий учет защищаемых носителей | | - | - | да | - | - | да | - | - | - |
| Обнуление освобождаемых областей оперативной памяти и внешних носителей | | - | - | да | - | - | да | - | - | да |
| Регистрация запуска (завершения) программ и процессов, предназначенных для обработки ПД | | - | - | - | - | - | да | - | - | да |
| Регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа | | нет | - | - | - | - | да | - | - | да |
| Подсистема обеспечения целостности программных средств, обрабатываемой информации, неизменность программной среды | | | | | | | | | | |
| Целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных | | да | да | да | да | да | да | - | - | - |
| Целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ | | да | да | да | да | да | да | - | - | - |
| Целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты | | нет | - | - | - | - | - | да | да | да |
| Целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных; | | нет | - | - | - | - | - | да | да | да |
| Физическая охрана информационной системы (технических средств и носителей информации) | | да | да | да | да | да | да | да | да | да |
| Периодическое тестирование функций системы защиты персональных данных | | да | да | да | да | да | да | да | да | да |
| Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности. | | да | да | да | да | да | да | да | да | да |

Из таблицы видно, что требования к ИСПД 2 и 3 классов в однопользовательском режиме совпадают. То же самое совпадение для требований 2 и 3 классов в многопользовательском режиме при равных правах доступа и при разных правах доступа соответственно.

Необходимо отметить, что есть требования, которые необходимо соблюдать во всех режимах работы и для всех классов ИСПД:

* Регистрация времени и даты входа (выхода) пользователя в систему или загрузки операционной системы и ее программной остановки;
* Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал;
* Физическая охрана информационной системы (технических средств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;
* Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
* Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

### 7.3. Требования при подключении ИСПД к сетям общего пользования

Если ИСПД имеет подключение к сетям общего пользования (например, Интернету), то возникает большое количество дополнительных потенциальных угроз, требующих нейтрализации. Помимо ранее рассмотренных требований к СЗПД законодательство определяет ряд дополнительных требований в случае наличия подключения ИСПД к сетям общего пользования. Рассмотрим основные из них:

* использование средств антивирусной защиты;
* межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
* обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
* анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
* защита информации при ее передаче по каналам связи;
* использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
* централизованное управление системой защиты персональных данных информационной системы.

Для обеспечения безопасности персональных данных при подключении информационных систем к информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) с целью получения общедоступной информации

* фильтрация входящих (исходящих) сетевых пакетов по правилам, заданным оператором (уполномоченным лицом);
* периодический анализ безопасности установленных межсетевых экранов на основе имитации внешних атак на информационные системы;
* активный аудит безопасности информационной системы на предмет обнаружения в режиме реального времени несанкционированной сетевой активности;
* анализ принимаемой по информационно-телекоммуникационным сетям международного информационного обмена (сетям связи общего пользования) информации, в том числе на наличие компьютерных вирусов.

Для реализации указанных методов и способов защиты информации могут применяться межсетевые экраны, системы обнаружения вторжений, средства анализа защищенности, специализированные комплексы защиты и анализа защищенности информации [[21](https://www.intuit.ru/studies/courses/697/553/literature#literature.21)].

Требования для разных классов ИСПД при наличии подключения к сетям общего пользования различны.

Межсетевые экраны ИСПД 3 класса должны обеспечивать:

* фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
* идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору и паролю условно-постоянного действия;
* регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программной остановки (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
* контроль целостности своей программной и информационной части;
* фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
* регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Межсетевые экраны ИСПД 2 класса должны обеспечивать:

* фильтрацию на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
* фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
* фильтрацию с учетом любых значимых полей сетевых пакетов;
* регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
* идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
* регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
* регистрацию запуска программ и процессов (заданий, задач);
* контроль целостности своей программной и информационной части;
* восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
* регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Межсетевые экраны ИСПД 1 класса должны обеспечивать:

* фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
* фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
* фильтрацию с учетом любых значимых полей сетевых пакетов;
* фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
* фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
* фильтрацию с учетом даты и времени;
* аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;
* регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
* регистрацию и учет запросов на установление виртуальных соединений;
* локальную сигнализацию попыток нарушения правил фильтрации;
* идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
* предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
* идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
* регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
* регистрацию запуска программ и процессов (заданий, задач);
* регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;
* возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;
* контроль целостности своей программной и информационной части;
* контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;
* восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
* регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления [[22](https://www.intuit.ru/studies/courses/697/553/literature#literature.22)].

Для всех классов ИСПД при наличии подключения к сетям общего пользования необходимо применять системы обнаружения вторжения, анализа защищенности и антивирусные средства. Системы обнаружения вторжений строятся с учетом возможностей реализации атак и используют сигнатурные методы, методы обнаружения аномалий или комбинированные методы. Для обнаружения вторжений в ИСПДн 3 и 4 классов рекомендуется использовать системы обнаружения сетевых атак, применяющие методы сигнатурного анализа, 1 и 2 класса – системы, применяющие сигнатурный метод и метод выявления аномалий, так как последний метод является наиболее прогрессивным и позволяет выявить ранее не встречавшиеся нигде атаки. Средства анализа защищенности позволяют найти уязвимости в операционной системе и используемом программном обеспечении, которые могут быть использованы злоумышленником для реализации атаки.

Необходимо отметить, что в отношении ИСПД 4 класса оператор сам решает, какие меры и способы защиты применять для обеспечения безопасности персональных данных.

**Лекция 8: Профили защиты, порядок их регистрации и сертификации во ФСТЭК России**

### 8.1. Понятие профиля защиты

Требования к безопасности конкретных средств и информационных систем устанавливаются на основании угроз, которые уже есть или прогнозируются, в соответствии с политикой безопасности и условий применения этих средств(систем). Требования, которые являются общими для некоторого типа продуктов или информационных систем, можно объединить в структуру, называемую профилем защиты. Согласно ГОСТ Р ИСО/МЭК 15408-3-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий" **профиль защиты (ПЗ)** - это независимая от реализации совокупность требований безопасности для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя.

**Продукт ИТ** - совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ.

**Изделие ИТ** - обобщенный термин для продуктов и систем ИТ[[23](https://www.intuit.ru/studies/courses/697/553/literature#literature.23)].

ПЗ не регламентирует, каким образом должны быть выполнены данные требования, тем самым предоставляя возможность разработчику системы защиты самостоятельно выбирать средства защиты. ПЗ может применяться либо к определенному классу продуктов, например, операционным системам или межсетевым экранам, и к совокупности продуктов, образующих систему информационной технологии (например, виртуальные частные сети, PKI). Использование профилей защиты преследует три основные задачи:

* стандартизация наборов требований к информационным продуктам;
* оценка безопасности;
* проведение сравнительного анализа уровней безопасности различных изделий ИТ.

ПЗ подлежат оценке, регистрации и сертификации в соответствии с руководящими документами ФСТЭК России.

Разработчиком ПЗ может быть как юридическое, так и физическое лицо.

ПЗ должен содержать:

* потребности пользователя изделия ИТ в обеспечении информационной безопасности;
* описание среды безопасности изделия ИТ – обоснованность применения данного ИТ с учетом угроз среды, политики безопасности и пр.
* цели безопасности изделия ИТ- то есть что должно быть сделано в результате использования данного ИТ;
* функциональные требования к безопасности и требования доверия к безопасности. Функциональные требования отображают то, что должно выполнять ИТ и его среда, а требования доверия к безопасности отображают степень уверенности в функционале данного ИТ. Совокупность этих требований должна обеспечить достижение целей безопасности;
* обоснование достаточности выдвинутых требований.

Требования безопасности зависят от класса защищенности изделия ИТ, который в свою очередь зависит от ценности информации, потенциальных угроз, развития соответствующих средств безопасности на настоящий момент и стоимости и времени на оценку безопасности данного изделия ИТ. Для определения требований безопасности в зависимости от класса защищенности изделия ИТ необходимо использовать Руководящий документ Гостехкомиссии России "Руководство по разработке семейств профилей защиты".

### 8.2. Содержание профиля защиты

Структура ПЗ в общем виде приведена на [рисунке 8.1](https://www.intuit.ru/studies/courses/697/553/lecture/12453?page=1#image.8.1).

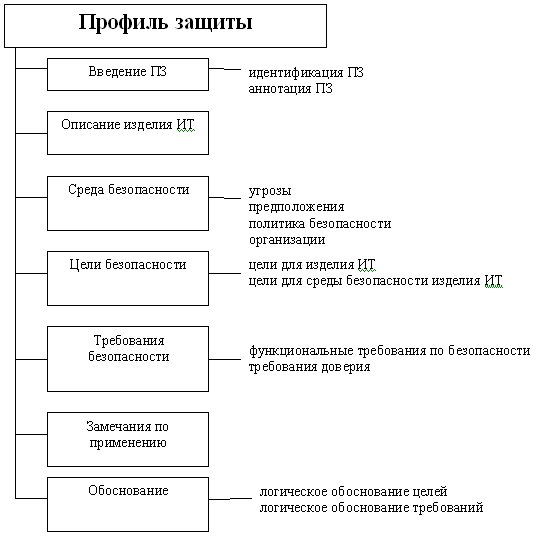


Рис. 8.1 - Структура ПЗ

Идентификация ПЗ должна обеспечить маркировку и описательную информацию, необходимые для однозначной идентификации и регистрации ПЗ.

Аннотация должна давать общую характеристику ПЗ и иметь описательную форму. При этом она должна быть достаточно полной для определения потенциальным пользователем необходимости использования данного ПЗ.

В раздел "Описание изделия ИТ" включается сопроводительная информация об изделии ИТ, предназначенная для пояснения его назначения и требований безопасности.

В раздел ПЗ "Среда безопасности изделия ИТ" включается описание аспектов среды безопасности изделия ИТ: предположения безопасности, потенциальных угроз и политики безопасности организации. Предположения безопасности содержат описание среды, в котором изделие будет использоваться:

* информация относительно предполагаемого использования ИТ - предполагаемая область применения, потенциальная значимость активов и возможные ограничения использования;
* информацию относительно среды применения, включая аспекты физического окружения, персонала и внешних связей.

Цели безопасности должны быть четко изложены, отражать намерение противостоять определенному набору угроз и соответствовать политике безопасности.

В раздел ПЗ "Требования безопасности изделия ИТ" включаются функциональные требования безопасности изделия ИТ, требования доверия к безопасности, а также требования безопасности программного, программно-аппаратного и аппаратного обеспечения ИТ-среды изделия ИТ.

В раздел ПЗ "Замечания по применению ПЗ" может включаться любая дополнительная информация, которую разработчик ПЗ считает полезной. Замечания по применению могут быть распределены по соответствующим разделам ПЗ [[25](https://www.intuit.ru/studies/courses/697/553/literature#literature.25)].

В разделе ПЗ "Обоснование" демонстрируется, что ПЗ специфицирует полную и взаимосвязанную совокупность требований безопасности изделия ИТ, и что соответствующее изделие ИТ учитывает идентифицированные аспекты среды безопасности. Раздел "Обоснование" может быть оформлен в виде отдельного документа.

Сертификат ПЗ - документ, удостоверяющий соответствие ПЗ критериям, приведенным в разделе 4 части 3 Руководящего документа "Критерии оценки безопасности информационных технологий". Цель оценки ПЗ - показать полноту, непротиворечивость и техническую верность конкретного ПЗ. Для повышения согласованности выводов, полученных при оценке, ее результаты могут быть представлены на сертификацию. Сертификация представляет собой независимую инспекцию результатов оценки, которая завершается их утверждением или выдачей сертификата. Сведения о сертификатах обычно публикуются и являются общедоступными.

### 8.3. Регистрация профиля защиты

После составления профиля защиты и его оценки (сертификации) он должен быть зарегистрирован в соответствии с Руководящим документом Гостехкомиссии России "Безопасность информационных технологий. Руководство по регистрации профилей защиты". Данный документ определяет процедуру регистрации не только ПЗ, но и пакетов. **Пакет** - многократно используемая совокупность функциональных компонентов или компонентов доверия, объединенных для достижения определенных целей безопасности [[25](https://www.intuit.ru/studies/courses/697/553/literature#literature.25)]. В результате регистрации ПЗ (или пакет) получает регистрационную метку, которая уникально его идентифицирует в специальном реестре. **Реестр** - совокупность записей (в электронном или электронном и бумажном виде), включающих в себя регистрационные метки, а также связанную с ними дополнительную информацию[[26](https://www.intuit.ru/studies/courses/697/553/literature#literature.26)]. Каждая запись в реестре состоит из трех частей, разделенных дефисом:

* тип элемента реестра;
* год регистрации;
* регистрационный номер.

Тип элемента реестра может иметь три значения:

* "ПЗ" – для профиля защиты;
* "ПД" для пакета требований доверия;
* "ФП" – для функционального пакета.

Год регистрации — год внесения элемента в реестр (четыре цифры).

Регистрационный номер — порядковый номер в текущем году (три цифры).

Пример: ПЗ-2010-005.

Для регистрации ПЗ заявителю необходимо отправить в регистрационный орган (ОР) заявку. Заявка обязательно должна содержать следующую информацию:

* Название организации (если заявитель юридическое лицо) или ФИО (если заявитель физическое лицо) и контактную информацию. Контактная информация должна включать почтовый адрес и/или адрес E-mail, номер телефона и/или факса.
* Тип объекта, который заявитель хочет зарегистрировать.
* Определение представленного объекта как нового или заменяющего уже существующий элемент в реестре. Если объект заменяющий, необходимо указать регистрационные метки элементов, подлежащих удалению или замене.
* Подтверждение от заявителей заменяемых элементов, что при принятии заменяющих элементов они согласны на удаление своих элементов.
* Определение объекта как завершенного или в качестве проекта.
* Описание нового ПЗ или пакета
* Аннотацию ПЗ или пакета.
* Декларацию, что описание ПЗ или пакета, представленного для регистрации, удовлетворяет требованиям руководящего документа по регистрации.

ОР в свою очередь либо отклоняет заявку(если в ней не полный перечень информации), либо присваивает регистрационную метку и вводит в реестр со статусом "проходящий подтверждение соответствия". Затем о результате этой процедуры сообщается заявителю. Начальная обработка занимает не более 14 дней после получения заявки. После этого ОР выполняет проверку описания, представленного в заявке. Если выявляются какие-то недостатки или несоответствия, ОР уведомляет заявителя и тот в свою очередь должен внести коррективы в течение 14 дней. Процедура подтверждения соответствия должна быть завершена в течение 3 месяцев с момента получения заявки на регистрацию.

**Лекция 9: Построение системы защиты персональных данных**

**9.1. Основные этапы при построении системы защиты персональных данных**

Система защиты ПД может быть как отдельной системой, так и подсистемой в составе системы защиты информации организации в целом. Как правило, выполнение работ по построению СЗПД происходит поэтапно и включает в себя следующие стадии:

* предпроектная стадия или оценка обстановки;
* стадия проектирования;
* ввод в действие СЗПД.

Предпроектная стадия или оценка обстановки. В самом начале построения СЗПД производится оценка обстановки. На данном этапе производятся следующие работы:

* разрабатывается перечень информационных систем организации, которые работают с ПД;
* определение состава ПД и необходимость их обработки;
* определение перечня ПД, которые необходимо защищать;
* определение контролируемой зоны и расположения компонентов ИСПД относительно границ этой зоны;
* строится модель корпоративной сети;
* определение топологии и конфигурации ИСПД, программ и технических средств, которые используются или предполагаются к использованию для обработки ПД;
* установление связей ИСПД с другими системами организации;
* определение режимов обработки ПД;
* определение угроз безопасности;
* определение класса ИСПД;
* уточняется степень участия персонала в обработке ПД.

Важным пунктом данного этапа является построение **частной модели угроз** и предварительная **классификация ИСПД** данной организации. Классификация ИСПД производится в соответствии с приказом " **Об утверждении Порядка проведения классификации информационных систем персональных данных"** от 13 февраля 2008 года.Результатом данного этапа является формирование частного технического задания (ТЗ) к СЗПД .

Техническое задание должно содержать:

* обоснование разработки СЗПД;
* исходные данные создаваемой (модернизируемой) ИСПД в техническом, программном, информационном и организационном аспектах;
* класс ИСПД;
* ссылку на нормативные документы, с учетом которых будет разрабатываться СЗПД и приниматься в эксплуатацию ИСПД;
* конкретизацию мероприятий и требований к СЗПД;
* перечень предполагаемых к использованию сертифицированных средств защиты информации;
* обоснование проведения разработок собственных средств защиты информации при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации;
* состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПД.

1. Стадия проектирования. На данном этапе разрабатывается задание и проект проведения работ в соответствии с ТЗ, выполняются все требуемые работы, в том числе закупка технических средств защиты и их сертификация в случае необходимости. Разрабатывается система доступа к ПД должностных лиц и определяются ответственные за эксплуатацию средств защиты информации.

Важным подэтапом является разработка эксплуатационной документации на ИСПД и средства защиты информации, а также организационно-распорядительной документации по защите информации (приказов, инструкций и других документов).

Этап проектирования является наиболее важным и трудоемким, так как при реализации СЗПД необходимо учесть множество факторов, таких как масштабирование, совместимость средств защиты со штатным программным обеспечением, возможность периодического тестирования системы защиты и замены отдельных компонентов системы в случае необходимости.

2. Ввод в действие СЗПД. Данный этап включает в себя:

* генерация пакета прикладных программ в комплексе с программными средствами защиты информации;
* опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами;
* приемо-сдаточные испытания;
* организация охраны и физической защиты помещений ИСПД;
* оценка соответствия ИСПД требованиям безопасности ПД.

В случае если в процессе опытной эксплуатации выявляются недостатки разработанной СЗПД, проводится ее доработка.

Для ИСПД, находящихся в эксплуатации до введения ФЗ №152 "О персональных данных" от 27 июля 2006 года, должны быть проведены работы по их модернизации в соответствии с требованиями Федерального закона и "Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" №781.

**9.2. Комплекс организационных и технических мероприятий в рамках СЗПД**

Для обеспечения безопасности персональных данных организации требуется провести комплекс технических и организационных мероприятий в рамках построения СЗПД и ее эксплуатации.

Организационные меры носят административный и процедурный характер и регламентируют процессы функционирования ИСПД, обработку ПД и действия персонала. Организационные меры включают в себя:

* разработка организационно-распорядительных документов, предназначенных для регламентации процессов хранения, обработки, сбора и накопления персональных данных, а также их защиту;
* уведомление уполномоченного органа (Роскомнадзора) о намерении обрабатывать ПД;
* получение письменного согласия на обработку ПД от субъектов ПД;
* определение должностных лиц, которые будут работать с ПД;
* организация доступа в помещения, где будет вестись обработка ПД;
* разработка должностных инструкций по работе с ПД;
* определение сроков хранения ПД;
* планирование мероприятий по защите ПД;
* обучение персонала.

Организационные меры индивидуальны для каждой организации и в первую очередь определяются классом ИСПД, которые обрабатывают персональные данные. Чем выше класс ИСПД, тем больше мероприятий организационного характера требуется для ее защиты. Организационные меры необходимы для регламентации функционирования системы в целом, но явно не достаточны. Для обеспечения безопасности они должны быть подкреплены использованием технических средств защиты.

Техническое мероприятие – это мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений. Техническая защита по своей структуре и содержанию является более сложным и трудоемким процессом в отличие от организационных мероприятий и предусматривает выполнение следующих условий:

* для выполнения работ по технической защите требуется лицензия;
* для выбора адекватных и достаточных средств защиты необходимо тщательное обследование ИСПД, построение модели угроз и классификация ИСПД;
* на основе данного обследования формируется перечень требований по обеспечению безопасности;
* требуется провести работы по проектированию, созданию и вводу в эксплуатацию СЗПД;
* для проведения аттестации(сертификации) на соответствие ИСПД требованиям законодательства необходимо наличие соответствующих лицензий.

Согласно Указу Президента РФ "Об утверждении перечня сведений конфиденциального характера" персональные данные относятся к категории сведений конфиденциального характера. На основании Федерального закона от 8 августа 2001 г. №128-ФЗ "О лицензировании отдельных видов деятельности" техническая защита конфиденциальной информации (в нашем случае персональных данных) относится к лицензированному виду деятельности. Таким образом, для проведения мероприятий по защите персональных данных необходимо привлекать организации, имеющие соответствующие лицензии ФСТЭК. Деятельность по защите информации без наличия соответствующих лицензий влечет за собой как административную, так и уголовную ответственность.

Помимо вышеперечисленного, средства технической защиты согласно п.6 Положения №781 " "Об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" должны проходить процедуру соответствия. Другими словами, можно применять только те средства защиты, которые имеют сертификат соответствия ФСТЭК или ФСБ в зависимости от назначения средства.

**9.3. Уведомление Роскомнадзора об обработке персональных данных**

До начала обработки персональных данных оператор обязан уведомить Роскомнадзор о своем намерении в соответствии с ФЗ "О персональных данных".Уведомление должно быть в письменной форме с подписью уполномоченного лица или в электронной форме с ЭЦП. Уведомление должно содержать:

* наименование (фамилия, имя, отчество), адрес оператора;
* цель обработки персональных данных;
* категории персональных данных;
* категории субъектов, персональные данные которых обрабатываются;
* правовое основание обработки персональных данных;
* перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
* описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
* дата начала обработки персональных данных;
* срок или условие прекращения обработки персональных данных.

В поле **цель обработки персональных данных** указываются цели обработки персональных данных, указанные в учредительных документах оператора, либо фактические цели обработки.

В поле **категории персональных данных** перечисляются все категории обрабатываемых ПД (основные, специальные, биометрические).

В поле **категории субъектов персональных данных** указываются категории физических лиц и виды отношений с ними, персональные данные которых обрабатываются **(**например: работники, состоящие в трудовых отношениях с Оператором, физические лица (абонент, пассажир, заемщик, вкладчик, страхователь, заказчик и др.), состоящие в договорных и иных гражданско-правовых отношениях Оператором и др.).

В поле **правовое основание обработки персональных данных** необходимо указать не только соответствующие статьи из ФЗ "О персональных данных", но и статьи из других правовых документов, регламентирующих обработку ПД в данном случае. Например, при обработке ПД сотрудников - ст. 85-90 Трудового кодекса Российской Федерации.

В этом поле также указывается номер, дата выдачи и наименование лицензии на осуществляемый вид деятельности, с указанием на пункты, в которых предусмотрено исключение передачи ПД третьим лицам без согласия субъекта ПД.

В поле **перечень действий с персональными данными, общее описание используемых Оператором способов обработки персональных данных**, указываются действия, совершаемые Оператором с персональными данными, а также описание используемых Оператором способов обработки персональных данных:

* неавтоматизированная обработка персональных данных;
* исключительно автоматизированная обработка персональных данных с передачей полученной информации по сети или без таковой;
* смешанная обработка персональных данных.

При этом, если обработка автоматизированная или смешанная, необходимо указать, передается информация только по локальной сети или с использованием Интернета.

В поле **описание мер** описываются меры, предусмотренные статьями 18 и 19 ФЗ "О персональных данных", в том числе сведения о шифровальных средствах, ФИО и контакты лиц, ответственных за обработку ПД, класс ИСПД, организационные и технические меры, применяемые оператором в целях защиты ПД.

В поле срок или условие прекращения обработки ПД указывается конкретная дата или условие, при выполнении которого обработка будет прекращена.

Роскомнадзор в течение 30 дней после получения уведомления вносит оператора в реестр операторов. Реестр операторов является общедоступным. В случае возникновения изменений, касающихся перечисленных в уведомлении сведений, оператор обязан известить об этом Роскомнадзор в течение 10 рабочих дней.

**Лекция 10: Аттестация, сертификация и лицензирование в области защиты персональных данных**

### 10.1. Сертификация средств защиты ПД

Порядок сертификации средств защиты информации в России устанавливается "Положением о сертификации средств защиты информации" от 26 июня 1995г. Сертификация по требованиям безопасности информации представляет собой процедуру оценки соответствия характеристик продукта, услуги или системы, требованиям стандартов, федеральных законов и других нормативных документов.

Участниками процесса сертификации являются:

* заявители – те, кто хочет получить сертификат соответствия. Заявителями могут быть продавцы продукции, исполнители продукции.
* федеральный орган по сертификации;
* центральный орган сертификации – орган, возглавляющий сертификацию однородной продукции (необязательный участник).
* органы по сертификации средств защиты информации – те, кто проводит сертификацию определенной продукции.
* испытательные лаборатории – лаборатории, проводящие сертификационные испытания определенной продукции.

В России действуют 4 Федеральных органа по сертификации, но в области защиты персональных данных их два – ФСБ России и ФСТЭК России. В основные обязанности Федерального органа по сертификации входит:

* создание системы сертификации;
* выбор способа подтверждения соответствия средств защиты информации;
* определение перечня средств защиты, для которых необходима сертификация;
* установление правил аккредитации центральных органов систем сертификации, органов по сертификации средств защиты информации, испытательных лабораторий и проведение соответствующих аккредитаций;
* выдача сертификатов и лицензий на применение знака соответствия;
* ведение реестра сертифицированных средств и участников сертификации;
* осуществление контроля и надзора за соблюдением участниками сертификации правил сертификации и за сертифицированными средствами защиты информации;
* рассмотрение апелляции по вопросам сертификации;
* периодическая публикация информации о сертификации;
* организация подготовки и аттестации экспертов-аудиторов;
* приостановление, продление или отмена действия выданных сертификатов.

Органы сертификации:

* участвуют в определении схемы проведения сертификации средств защиты информации с учетом предложений заявителя;
* уточняют требования, на соответствие которым проводятся сертификационные испытания;
* рекомендуют заявителю испытательный центр (лабораторию);
* утверждают программы и методики проведения сертификационных испытаний;
* проводят экспертизу технической, эксплуатационной документации на средства защиты информации и материалов сертификационных испытаний;
* оформляют экспертное заключение по сертификации средств защиты информации и представляют их в федеральный орган по сертификации;
* организуют, при необходимости, предварительную проверку (аттестацию) производства сертифицируемых средств защиты информации;
* участвуют в аккредитации испытательных центров (лабораторий) и органов по аттестации объектов информатизации;
* организуют инспекционный контроль за стабильностью характеристик сертифицированных средств защиты информации и участвуют в инспекционном контроле за деятельностью испытательных центров (лабораторий);
* хранят документацию (оригиналы), подтверждающую сертификацию средств защиты информации;
* ходатайствуют перед федеральным органом по сертификации о приостановке или отмене действия выданных сертификатов;
* формируют и актуализируют фонд нормативных и методических документов, необходимых для сертификации, участвуют в их разработке;
* представляют заявителю необходимую информацию по сертификации.

Испытательные центры (лаборатории) в пределах установленной области аккредитации:

* осуществляют отбор образцов средств защиты информации для проведения сертификационных испытаний;
* разрабатывают программы и методики сертификационных испытаний, осуществляют сертификационные испытания средств защиты информации, оформляют протоколы сертификационных испытаний и технические заключения;
* маркируют сертифицированные средства защиты информации знаком соответствия в порядке, установленном правилами системы сертификации;
* участвуют в аттестации производства сертифицируемых средств защиты информации[[29](https://www.intuit.ru/studies/courses/697/553/literature#literature.29)].

Испытательные центры (лаборатории) несут ответственность за полноту испытаний средств защиты информации, достоверность, объективность и требуемую точность измерений, своевременную проверку средств измерений и аттестацию испытательного оборудования.

Органы сертификации средств защиты информации и испытательные лаборатории проходят процедуру аккредитации на право проведения работ по сертификации, в ходе которой федеральный орган по сертификации проверяет их способность на проведение данных работ и выдает разрешение.

Сертификация проводится на материально-технической базе аккредитованных испытательных лабораторий. В отдельных случаях возможно проведение испытаний на базе заявителя при надлежащем контроле со стороны органа сертификации.

Изготовители обязаны извещать орган по сертификации, который выдал сертификат на их продукцию, об изменениях в технологии изготовления или составе сертифицированного средства защиты информации.

Процедура сертификации включает:

1. Подачу и рассмотрение заявки на проведение сертификации (продления срока действия) средства защиты информации в Федеральный орган по сертификации. Заявка оформляется на бланке заявителя и заверяется печатью. Федеральный орган назначает орган по сертификации и испытательную лабораторию, после чего заявитель отправляет туда сертифицируемое средство защиты информации.
2. Сертификационные испытания средств защиты информации и (при необходимости) аттестацию их производства. Сроки проведения испытаний устанавливаются на договорной основе между заявителем и лабораторией. По результатам испытаний оформляется заключение, которое отправляется в орган по сертификации и заявителю.
3. Экспертизу результатов испытаний, оформление, регистрацию и выдачу сертификата и лицензии на право использования знака соответствия. На основании заключения испытательной лаборатории орган сертификации делает заключение и отправляет его в Федеральный орган по сертификации. После присвоения сертификату регистрационного номера, его получает заявитель. Срок действия сертификата – 3 года.
4. Осуществление государственного контроля и надзора, инспекционного контроля за соблюдением правил обязательной сертификации и за сертифицированными средствами защиты информации. По результатам контроля Федеральный орган по сертификации может приостановить или аннулировать сертификат в следующих случаях:

* изменения на законодательном уровне, касающиеся требований к средствам защиты информации, методам испытаний и контроля;
* изменение технологии изготовления, конструкции (состава), комплектности средств защиты информации и системы контроля их качества;
* невыполнение требований технологии изготовления, контроля и испытаний средств защиты информации;
* несоответствие сертифицированных средств защиты информации техническим условиям или формуляру, выявленное в ходе государственного или инспекционного контроля;
* отказ заявителя в допуске (приеме) лиц, уполномоченных осуществлять государственный контроль и надзор, инспекционный контроль за соблюдением правил сертификации и за сертифицированными средствами защиты информации[[29](https://www.intuit.ru/studies/courses/697/553/literature#literature.29)].

1. информирование о результатах сертификации средств защиты информации;
2. рассмотрение апелляций. Апелляция подается в федеральный орган по сертификации и рассматривается в месячный срок с участием независимых экспертов и заинтересованных сторон.

Органы по сертификации и испытательные лаборатории несут ответственность за выполнение своих функций, обеспечение сохранности информации ограниченного доступа, материальных ценностей, предоставленных заявителем, а также за соблюдение авторских прав разработчика при испытаниях его средств защиты информации.

### 10.2.Требования законодательства к средствам защиты ПД

Важным моментом при построении СЗПД является пункт 5 "Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных", утвержденного Постановлением Правительства Российской Федерации от 17.11.2007 № 781, которое гласит, что средства защиты информации, используемые в ИСПД, должны в установленном порядке проходить процедуру соответствия (сертификацию). Порядок сертификации устанавливается уполномоченными органами, которыми в случае защиты ПД являются ФСТЭК и ФСБ России. Сертификации подлежат системы, продукты и услуги защиты информации от НСД. В рамках систем обязательной сертификации организации должны сертифицировать средства и продукты. Например, в руководящих документах Гостехкомиссии России продуктом может выступать средство вычислительной техники (СВТ), средство защиты информации (СЗИ), межсетевой экран (МЭ), программное обеспечение (ПО) и др. Система – это объект информатизации, где обрабатывается реальная информация. По этой причине к системам предъявляются дополнительные требования, касающиеся в том числе организационных мер и физической защиты.

Программное обеспечение СЗПД для защиты от угроз конфиденциальности, целостности и доступности, применяемое в ИСПД 1 класса, подлежит сертификации на отсутствие недекларированных возможностей согласно п.2.12 Приказа ФСТЭК России №58.

В соответствии с Руководящим документом Гостехкомиссии России "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей", утвержденным приказом Председателя Гостехкомиссии от 04.06.1999 № 114, **недекларированные возможности** - функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации. Порядок классификации по уровню контроля отсутствия недекларированных возможностей определен указанным выше руководящим документом Гостехкомиссии. Данное требование обусловлено тем, что большинство современных атак использует уязвимости в программном обеспечении системы. Основной метод нахождения уязвимостей в программе – детальное изучение программного кода. Данное требование может привести к выводу из эксплуатации в ИСПД зарубежных средств защиты информации, так как для сертификации необходимо предоставить код в открытом виде.

При просмотре сертификата к средству защиты информации необходимо обратить внимание, на соответствие каким документам проводились сертификационные испытания.

Что касаемо ФСТЭК России, то это может быть:

* руководящие документы Гостехкомиссии России по защите от несанкционированного доступа к информации (для АС, СВТ или МЭ),
* руководящий документ Гостехкомиссии России по контролю отсутствия недекларированных возможностей,
* техническое условие или формуляр,
* задание по безопасности (по требованиям ГОСТ ИСО/МЭК 15408-2008).

Необходимо отметить, что нормативные документы ФСТЭК на настоящее время не охватывают требования ко всем средствам технической защиты информации в области ПД. Рекомендации и требования предусмотрены для межсетевых экранов (МЭ) и систем обнаружения вторжений(IDS).

* для ИСПД 1 класса – МЭ 3 класса, в IDS должны использоваться аномальные и сигнатурные методы обнаружения вторжений;
* для ИСПД 2 класса – МЭ 4 класса, в IDS должны использоваться аномальные и сигнатурные методы обнаружения вторжений;
* для ИСПД 3 класса – МЭ 5 класса, в IDS должен использоваться сигнатурный метод обнаружения вторжений;
* для ИСПД 4 класса – МЭ 5 класса, в IDS должен использоваться сигнатурный метод обнаружения вторжений.

Требования к средствам защиты ИСПД частично совпадают с требованиями к автоматизированным системам, которые были разработаны ранее в руководящих документах Гостехкомиссии России, в целях преемственности и совместимости.

Корреляция указанных требований отображена в [таблице 10.1](https://www.intuit.ru/studies/courses/697/553/lecture/12456?page=1#table.10.1).

Таблица 10.1. Корреляция требований к средствам защиты в ИСПД с документами по АС

|  |  |  |  |
| --- | --- | --- | --- |
| Класс ИСПД | Класс АС | Класс МЭ | |
| Без подключения к СОД | С подключением к СОД |
| K1, однопользовательская | 3A |  | 2 |
| K1, многопользовательская с одинаковыми правами | 2A | 4 | 2 |
| K1, многопользовательская с разными правами | 1B | 4 | 2 |
| K2, однопользовательская | 3B+ |  | 3 |
| K2, многопользовательская с одинаковыми правами | 2B+ | 4 | 2 |
| K2, многопользовательская с разными правами | 1Г | 4 | 2 |
| K3, однопользовательская | 3Б |  | 4 |
| K3, многопользовательская с одинаковыми правами | 2Б | 4 | 2 |
| K3, многопользовательская с разными правами | 1Д | 4 | 2 |
| K4 | Определяется оператором | | |

В случае если требования нормативных документов ФСТЭК в области защиты ПД и руководящих документов Гостехкомиссии не совпадают, первые должны быть описаны в техническом задании.

### 10.3. Требования законодательства к ИСПД

До февраля 2010 года проведение аттестации ИСПД было обязательным этапом построения системы защиты. После введения Приказа ФСТЭК №58 ситуация изменилась, так как документ отменил обязательность аттестации, предоставив операторам самим решать, проводить ее или нет. Тем не менее, это не отменяет необходимости проведения оценки соответствия принятых мер по обеспечению безопасности требованиям законодательства, о чем говорят в частности – постановление Правительства РФ № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке и ИСПДн" и 184-ФЗ "О техническом регулировании".

Аттестация ИСПД предназначена для официального подтверждения эффективности и достаточности мер по обеспечению безопасности ПД в данной ИСПД. Аттестация должна предшествовать началу обработки данных. Порядок проведения аттестации регламентирован "Положением по аттестации объектов информатизации по требованиям безопасности информации" от 25 ноября 1994 г.

Результатом аттестации является документ, называемый "Аттестат соответствия", который подтверждает, что ИСПД удовлетворяет требованиям стандартов и нормативно-технических документов по безопасности ПД ФСТЭК и Гостехкомиссии России (в настоящее время это другая организация).

Этапы аттестации включают в себя:

* разработка программы и методики аттестационных испытаний;
* подачу и рассмотрение заявки на аттестацию;
* предварительное ознакомление с аттестуемым объектом;
* испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
* заключение договоров на аттестацию;
* проведение аттестационных испытаний объекта информатизации;
* оформление, регистрация и выдача "Аттестата соответствия";
* осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
* рассмотрение апелляций[[33](https://www.intuit.ru/studies/courses/697/553/literature#literature.33)].

Испытания, в процессе которых производится оценка эффективности защищенности информации от несанкционированного доступа (c применением специализированного программного обеспечения). После окончания испытаний подготавливаются отчетные документы, на основании которых принимается решение об аттестации ИСПД.

Органы по аттестации объектов информатизации аккредитуются Гостехкомиссией России и получают от нее лицензию на право проведения аттестации объектов информатизации. Такими органами могут быть отраслевые и региональные учреждения, предприятия и организации по защите информации, специальные центры Гостехкомиссии России.

Аттестационные испытания предполагают проведение следующих проверок:

* проверка состояния технологического процесса автоматизированной обработки персональных данных в ИСПД;
* проверка ИСПД на соответствие организационно-техническим требованиям по защите информации;
* испытания ИСПД на соответствие требованиям по защите информации от несанкционированного доступа.

Результатом аттестации являются:

* Протокол аттестационных испытаний;
* Заключение по результатам аттестационных испытаний;
* Аттестат соответствия на ИСПД (выдается в случае положительного Заключения);
* Акт о переводе СЗПД в промышленную эксплуатацию (в случае наличия положительного заключения по результатам аттестационных испытаний ИСПД).

Следует указать, что если заявитель пожелает только аттестовать ИСПД как объект информатизации, то пока действуют традиционные нормативные требования по аттестации объектов информатизации (СТР-К), в которых обрабатывается конфиденциальная информация.

### 10.4.Лицензирование деятельности по защите персональных данных

Для проведения деятельности по защите ПД операторы должны получить лицензию в соответствии с Постановлением правительства РФ "Об организации лицензирования отдельных видов деятельности" от 26.01.2006 г. Это требование касается обработки ПД в ИСПД 1, 2 класса и распределенных информационных систем 3 класса. Лицензирование деятельности по технической защите информации осуществляет ФСТЭК России. Порядок лицензирования деятельности определяется "Положением о лицензировании деятельности по технической защите конфиденциальной информации".

Лицензионными требованиями и условиями при осуществлении деятельности по технической защите конфиденциальной информации являются:

* наличие в штате соискателя лицензии специалистов, имеющих высшее профессиональное образование в области технической защиты информации либо высшее или среднее профессиональное (техническое) образование и прошедших переподготовку или повышение квалификации по вопросам технической защиты информации;
* наличие у соискателя лицензии помещений для осуществления лицензируемой деятельности, соответствующих техническим нормам и требованиям по технической защите информации, установленным нормативными правовыми актами Российской Федерации, и принадлежащих ему на праве собственности или на ином законном основании;
* наличие на любом законном основании производственного, испытательного и контрольно-измерительного оборудования, прошедшего в соответствии с законодательством Российской Федерации метрологическую поверку (калибровку), маркирование и сертификацию;
* использование автоматизированных систем, обрабатывающих конфиденциальную информацию, а также средств защиты такой информации, прошедших процедуру оценки соответствия (аттестованных и (или) сертифицированных по требованиям безопасности информации) в соответствии с законодательством Российской Федерации;
* использование предназначенных для осуществления лицензируемой деятельности программ для электронно-вычислительных машин и баз данных на основании договора с их правообладателем;
* наличие нормативных правовых актов, нормативно-методических и методических документов по вопросам технической защиты информации в соответствии с перечнем, установленным Федеральной службой по техническому и экспортному контролю[[35](https://www.intuit.ru/studies/courses/697/553/literature#literature.35)].

Для получения лицензии соискатель направляет в ФСТЭК следующие документы:

* заявление на предоставление лицензии;
* копии документов, подтверждающих квалификацию специалистов;
* копии документов, подтверждающих право соискателя на помещения (например, свидетельство о собственности или договор аренды);
* копии аттестатов соответствия защищаемых помещений требованиям безопасности;
* копия технического паспорта АС;
* копии документов, подтверждающих право использования программных средств;
* сведения о наличии производственного и контрольно-измерительного оборудования, средств защиты информации и средств контроля защищенности информации, необходимых для осуществления лицензируемой деятельности, с приложением копий документов о проверке контрольно-измерительного оборудования;
* сведения о том, что соискатель имеет все нормативно- правовые акты, нормативно-методические и методические документы по вопросам технической защиты информации.

Лицензия выдается на 5 лет и по окончании срока действия может быть продлена.

**Лекция 11: Подсистемы в составе СЗПД**

**11.1. Подсистемы в составе СЗПД**

В соответствии с руководящими документами регуляторов, рассмотренных в предыдущих лекциях, СЗПД может содержать до 10 подсистем, среди которых подсистема антивирусной защиты, защиты от утечки по техническим каналам, подсистема обеспечения безопасности межсетевого взаимодействия, анализа защищенности и выявления уязвимостей, криптографической защиты информации, подсистема обнаружения вторжений. В таблице 11.1 приведена информация о подсистемах, которые должны быть внедрены в зависимости от класса ИСПД в соответствии с руководящими документами ФСТЭК.

Таблица 11.1. Перечень подсистем СЗПД в зависимости от класса и типа ИСПД

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Класс и тип ИСПД | Антивирус-ная защита | Подсистема управления доступом, регистрации и учета | Подсистема обеспечения целостности | Анализ защищенности | Подсистема обнаружения вторжений | Подсистема безопасности межсетевого взаимодействия | Подсистема криптогра-фической защиты информации |
| ИСПД 1кл. | распред. | + | + | + | + | + | + |
| ИСПД 1 кл. | локальная | + | + | + | - | - | + |
| ИСПД 2 кл. | распред. | + | + | + | + | + | - |
| ИСПД 2 кл. | локальная | + | + | + | - | - | - |
| ИСПД 3 кл. | распред. | + | + | + | + | + | - |
| ИСПД 3 кл. | локальная | + | + | + | - | - | - |

Рассмотрим функции, которые должна выполнять каждая из перечисленных в таблице подсистем.

1. Подсистема управления доступом, регистрации и учета. Данная подсистема предназначена для защиты от несанкционированного доступа и реализуется с помощью средств блокирования НСД, регистрации попыток доступа и сигнализации. Средства данной группы могут быть программными или программно-аппаратными. Функция регистрации реализуется журналированием действий и операций в ИСПД, сигнализации - извещение в случае выявления нарушения нормального режима функционирования ИСПД или попыток НСД к ИСПД.
2. Подсистема обеспечения целостности. Данная подсистема может быть реализована с помощью средств операционной системы, СУБД или с помощью специальных программных средств. Функция контроля целостности основывается, как правило, на вычислении контрольных сумм, хэш-функциях или ЭЦП. В современных системах контроль целостности должен распространяться не только на отдельные компоненты системы, но и на распределенные конфигурации и потоки данных.
3. Подсистема антивирусной защиты предназначена для обеспечения безопасности обрабатываемых данных и программно-аппаратных средств системы. Реализуется с помощью антивирусных программ, основной функцией которых является выявление вредоносного программного кода (вируса) и удаление (по возможности) его из системы. Для современных антивирусных средств очень важным и необходимым качеством является способность обнаружения неизвестных ранее вирусов. В составе СЗПД антивирусные средства должны иметь систему централизованного управления и средства оповещения администратора или другого ответственного лица обо всех "нестандартных" событиях в ИСПД.
4. Подсистема обеспечения безопасности межсетевого взаимодействия ИСПД предназначена для разграничения доступа к компонентам ИСПД и обрабатываемым ПД при межсетевом взаимодействии. Функционал подсистемы реализуется с помощью программных и программно-аппаратных межсетевых экранов (МЭ). МЭ устанавливается на границе внутренней и внешней сети и предназначен для ограничения доступа пользователей во внешнюю сеть и фильтрации "подозрительных пакетов", поступающих из внешней сети во внутреннюю.
5. Подсистема анализа защищенности предназначена для контроля настроек операционных систем на рабочих станциях и серверах, средств защиты и сетевого оборудования. Функционал данной подсистемы реализуется с помощью специальных программ – сканеров. Сканеры обследуют сеть и ведут поиск "слабых" мест, таких как:

* слабые пароли и механизмы аутентификации в целом;
* "люки" в программах;
* неправильная настройка межсетевых экранов, операционных систем, баз данных и пр.;
* использование сетевых протоколов, имеющих уязвимости.
* открытые порты.

Сканеры находят только известные уязвимости, детальным образом описанные в их базе данных. В этом они похожи на антивирусы, работающие по сигнатурному методу обнаружения вирусов. Функционировать они могут на сетевом уровне, уровне операционной системы и уровне приложения. Помимо выявления уязвимостей средства анализа защищенности могут помочь построить топологию сети: выявить узлы корпоративной сети, протоколы и сервисы, приложения и пр. Как правило, эти средства также дают рекомендации и пошаговые инструкции для устранения выявленных уязвимостей.

1. Подсистема обнаружения вторжений предназначена для выявления попыток НСД к ИСПД. Реализуется с помощью систем обнаружения вторжений – IDS, строящихся на основе информации об этапах проведения атак, поведении злоумышленника и пр. Выделяют два класса систем – узловые (HIDS) и сетевые (NIDS). HIDS располагается на узле и отслеживает атаки только на этот узел, NIDS контролирует весь сетевой трафик на наличие признаков атак.
2. Подсистема криптографической защиты информации. Как правило, предназначена для защиты ПД при передаче по открытым каналам связи или в несегментированной сети. Криптографические средства также могут применяться при хранении, обработке ПД, при аутентификации пользователей. Данное требование выдвигается только к ИСПД 1 класса.

В ряде случаев необходима также **подсистема защиты от утечки по техническим каналам**. Данная подсистема предназначена для защиты акустической, видовой информации, а также от утечек информации через ПЭМИН. При этом выделяются **пассивные** и **активные меры защиты**. Пассивные меры защиты направлены на ослабление побочных информационных сигналов и наводок до уровня, когда их невозможно выделить средством съема на фоне естественных шумов. Пассивные меры защиты чаще всего реализуются на этапе строительства или реконструкции зданий и могут включать в себя: звукоизоляцию помещений, экранирование отдельных элементов ИСПД и заземление. К пассивным мерам защиты можно также отнести установку на объекте технических средств и систем ограничения и контроля доступа. Активные меры заключаются в создании маскирующих акустических и вибрационных помех. Для создания таких помех используются, как правило, генераторы шума или прицельных помех. Для уничтожения закладных устройств в телефонной линии могут использоваться специальные генераторы импульсов, которые фактически выжигают "жучков". Подсистема защиты от утечки по техническим каналам обязательна для ИСПД 1 класса или если в частной модели угроз имеются соответствующие угрозы утечки.

В качестве серверной и клиентской операционной системы можно использовать операционную систему Windows.

Далее в ходе лекции мы рассмотрим подробнее антивирусные программы, средства обнаружения вторжений и межсетевые экраны, так как именно эти средства нашли широкое применение в современных информационных системах и обязательны для всех классов ИСПД.

**11.2. Подсистема антивирусной защиты**

Подсистема антивирусной защиты предназначена для защиты информационной системы от вирусов (вредоносных программ) и реализуется с помощью антивирусных программ.

Для обнаружения вирусов антивирус использует 2 метода:

* сигнатурный
* аномальный.

**Сигнатурный метод** основан на сравнении подозрительного файла с образцами известных вирусов. Сигнатурой вируса называется совокупность характеристик, позволяющих идентифицировать данный вирус или присутствие вируса в файле. Сигнатуры известных вирусов хранятся в антивирусной базе. При этом одна сигнатура может соответствовать группе похожих вирусов. Преимуществом данного метода является гарантированность обнаружения вируса, сигнатура которого имеется в базе. Антивирусные базы регулярно обновляются производителем антивируса. При использовании антивирусов, которые используют сигнатурный метод, необходимо регулярно обновлять антивирусную базу. В противном случае антивирус не сможет находить новые вирусы, которые появляются в Интернете каждый день. Изначально все антивирусные программы работали с сигнатурным методом, но присутствие такого недостатка как невозможность обнаружения ранее неизвестных вирусов привело к появлению второго метода – эвристического анализа.

**Эвристический метод** представляет собой совокупность приблизительных методов обнаружения вирусов, основанных на тех или иных предположениях. Как правило, выделяют следующие эвристические методы:

поиск вирусов, похожих на известные. Данный эвристический метод основан на предположении о том, что новый вирус может иметь сходные черты с уже известными вирусами. В данном методе в системе ищутся файлы или части файлов, которые соответствуют сигнатуре не полностью (как в сигнатурном методе), а частично.

Поиск аномального поведения (аномальный метод)

Данный метод основан на предположении о том, что при заражении системы в ней начинают происходить события, не свойственные работе системы в нормальном режиме. Примером таких действий может быть удаление файла, запись в определенные области реестра, перехват данных с клавиатуры, рассылка писем и т.п.

Достоинством эвристического метода является способность находить новые вирусы, сигнатуры которых неизвестны. Недостатком же является большое количество ложных срабатываний, то есть отнесение нормальных файлов к вирусам.

В составе антивируса обязательно должны присутствовать следующие модули:

* модуль обновления – доставляет обновленные базы сигнатур пользователю антивируса. Модуль обновления обращается к серверам производителя и скачивает обновленные антивирусные базы.
* модуль планирования – предназначен для планирования действий, которые регулярно должен выполнять антивирус. Например, проверять компьютер на наличие вирусов и обновлять антивирусные базы. Пользователь может выбрать расписание выполнения данных действий.
* модуль управления – предназначен для администраторов крупных сетей. Данные модули содержат интерфейс, позволяющий удаленно настраивать антивирусы на узлах сети, а также способы ограничения доступа локальных пользователей к настройкам антивируса.
* модуль карантина – предназначен для изолирования подозрительных файлов в специальное место – карантин. Лечение или удаление подозрительного файла не всегда является возможным, особенно если учесть ложные срабатывания эвристического метода. В этих случаях файл помещается в карантин и не может выполнять какие-либо действия оттуда.

Для обеспечения антивирусной защиты персональных данных можно воспользоваться продуктами компании "Лаборатория Касперского", которые имеют сертификаты ФСТЭК. В частности, на рабочие станции можно установить Антивирус Касперского 6.0 для Windows Workstation, на рабочее место администратора – Kaspersky Administration Kit 6.0, на сервера - Антивирус Касперского 6.0 для Windows Servers. Если ИСПД подключена к Интернету, антивирусы должны быть установлены на всех узлах корпоративной сети.

**11.3. Подсистема обнаружения вторжений**

Подсистема обнаружения вторжений предназначена для обнаружения несанкционированных попыток доступа к системе. Системы обнаружения вторжений (IDS) работают наподобие сигнализации здания. Существует два типа IDS- узловые (HIDS) и сетевые (NIDS).

HIDS располагается на отдельном узле и отслеживает признаки атак на этот узел.Узловые IDS представляют собой систему датчиков, которые отслеживают различные события в системе на предмет аномальной активности. Существуют следующие типы датчиков:

* Анализаторы журналов – чаще всего контролируются записи системного журнала и журнала безопасности.
* Датчики признаков – сопоставляют между собой признаки определенных событий, связанных либо со входящим трафиком, либо с журналами.
* Анализаторы системных вызовов – анализируют вызовы между приложениями и операционной системой на предмет соответствия атаке. Данные датчики носят превентивный характер, то есть могут предотвратить атаку в отличие от предыдущих двух типов.
* Анализаторы поведения приложений- анализируют вызовы между приложениями и операционной системой на предмет того, разрешено ли приложению то или иное действие.
* Контролеры целостности файлов – отслеживают изменения в файлах с помощью контрольных сумм или ЭЦП.

NIDS располагается на отдельной системе и анализирует весь трафик сети на признаки атак. В данные системы встроена база данных признаков атак, на которые система анализирует сетевой трафик.

В случае обнаружения атаки IDs принимает пассивные действия. Пассивные действия заключаются в уведомлении соответствующего должностного лица, например, администратора безопасности, о факте атаки. Активная обработка событий заключается в попытке остановить атаку – завершить подозрительный процесс, прервать соединение или сеанс. Системы обнаружения вторжений также, как и антивирусы, используют сигнатурный и аномальный метод обнаружения атак. В контексте обеспечения безопасности персональных данных, ФСТЭК рекомендует использовать для ИСПД 3 и 4 класса – IDS с сигнатурным методом, для 1 и 2 класса – с сигнатурным и аномальным методом обнаружения вторжений. К таким продуктам можно отнести Cisco Intrusion Detection System/Intrusion Preventing System (IPS/IDS), который является основным компонентом решений Cisco Systems по обнаружению и отражению атак. Наряду с сигнатурым методом обнаружения в Cisco IDS/IPS используются и уникальные алгоритмы, отслеживающие аномалии в сетевом трафике и в поведении сетевых приложений. Это позволяет обнаруживать как известные, так и многие неизвестные атаки.

**11.4. Межсетевые экраны**

Межсетевой экран (МЭ) в СЗПД – это устройство обеспечения безопасного межсетевого взаимодействия, в частности, при подключении локальной сети организации к Интернету. МЭ контролирует доступ к сети, блокируя весь трафик, кроме разрешенного. Фильтрация производится на основе критериев, заданных администратором.

Существует два метода настройки МЭ:

* изначально "запретить всё", а затем определить то, что следует разрешить.
* изначально "разрешить всё", а затем определить то, что следует запретить.

Очевидно, что первый вариант является более безопасным, так как запрещает всё и, в отличие от второго, не может пропустить нежелательный трафик.

Процедура фильтрации представляет собой анализ заголовка каждого пакета, проходящего через МЭ, и передача его дальше по маршруту в том случае, если он удовлетворяет заданным правилам фильтрации. Таким образом удаляются пакеты, потенциально опасные для ИСПД.

Помимо функции фильтрации МЭ позволяет скрыть реальные адреса узлов в защищаемой сети с помощью трансляции сетевых адресов - NAT ( Network Address Translation ). При поступлении пакета в МЭ, он заменяет реальный адрес отправителя на виртуальный. При получении ответа МЭ выполняет обратную процедуру.

МЭ могут реализовываться как с помощью программного обеспечения, так и программно-аппаратного. МЭ устанавливается на границе защищаемой внутренней сети и внешней. Для обеспечения безопасности персональных данных ФСТЭК рекомендует использовать для ИСПД 3 и 4 классов - МЭ не ниже пятого уровня защищенности, в ИСПД 2 класса – МЭ не ниже четвертого уровня защищенности, в ИСПД

1 класса – МЭ не ниже третьего уровня защищенности.

В качестве МЭ можно использовать Microsoft ISA Server 2006 SE или Cisco PIX Firewall PIX-515E ver. 6.3, которые обладают соответствующими лицензиями ФСТЭК России.

При выборе конкретных средств для реализации обеспечения безопасности ПД необходимо использовать только сертифицированные средства защиты информации. Реестры сертифицированных средств публикуются на сайтах ФСТЭК и ФСБ России.

**Лекция 12: Контроль в области защиты персональных данных**

### 12.1. Регуляторы в области защиты персональных данных

В соответствии с ФЗ "О персональных данных" выделяют три регулятора в области защиты персональных данных:

* Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее Роскомнадзор) в части, касающейся соблюдения норм и требований по обработке персональных данных и защиты прав субъектов персональных данных;
* Федеральная служба безопасности РФ (далее ФСБ) в части, касающейся соблюдения требований по организации и обеспечению функционирования шифровальных (криптографических) средств в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПД;
* Федеральная служба по техническому и экспортному контролю (далее ФСТЭК) в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПД (не криптографическими методами) при их обработке в ИСПД.

В целях контроля соблюдения операторами требований безопасности в области защиты ПД регуляторы проводят плановые и внеплановые проверки.

Роскомнадзор проводит плановые проверки с целью контроля сведений, указанных в уведомлении уполномоченного органа по защите ПД, а также внеплановые – на основании заявления физических лиц с целью проверки информации, указанной в данном заявлении.

ФСБ России имеет право проводить плановые проверки:

* представление по запросу отчета по лицензируемым видам деятельности;
* представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы, в составе которых эксплуатируются системы криптографической защиты информации (СКЗИ);
* явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности.

ФСТЭК РФ уполномочен осуществлять плановые проверки:

* представление по запросу отчета по лицензируемым видам деятельности;
* представление копий аттестатов соответствия по требованиям информационной безопасности на автоматизированные системы;
* представление копий аттестатов соответствия на защищаемые помещения по требованиям безопасности;
* явочная проверка выполнения организационных мер на объектах лицензируемых видов деятельности[[9](https://www.intuit.ru/studies/courses/697/553/literature#literature.9)].

Плановые и внеплановые проверки осуществляются в соответствии с Федеральным законом от 26 декабря 2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

В рамках межведомственного сотрудничества между Роскомнадзором, ФСТЭК России и ФСБ РФ достигнута договоренность о проведении совместных мероприятий по контролю и надзору в области персональных данных.

### 12.2. Проверки Роскомнадзора

Роскомнадзор осуществляет проверку выполнения требований законодательства в области обеспечения безопасности персональных данных с целью защиты прав субъектов.

В соответствии с ФЗ "О персональных данных" Роскомнадзор имеет право:

1. Запрашивать у физических или юридических лиц информацию, необходимую для реализации своих полномочий, и безвозмездно получать такую информацию;
2. Осуществлять проверку сведений, содержащихся в уведомлении об обработке персональных данных, или привлекать для осуществления такой проверки иные государственные органы в пределах их полномочий;
3. Требовать от оператора уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
4. Принимать решение по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований ФЗ "О персональных данных";
5. Обращаться в суд с исковыми заявлениями в защиту прав субъектов персональных данных и представлять интересы субъектов персональных данных в суде;
6. Направлять заявление в орган, осуществляющий лицензирование деятельности оператора, для рассмотрения вопроса о принятии мер по приостановлению действия или аннулированию соответствующей лицензии в установленном законодательством Российской Федерации порядке, если условием лицензии на осуществление такой деятельности является запрет на передачу персональных данных третьим лицам без согласия в письменной форме субъекта персональных данных;
7. Направлять в органы прокуратуры, другие правоохранительные органы материалы для решения вопроса о возбуждении уголовных дел по признакам преступлений, связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью;
8. Вносить в Правительство Российской Федерации предложения о совершенствовании нормативного правового регулирования защиты прав субъектов персональных данных;
9. Привлекать к административной ответственности лиц, виновных в нарушении настоящего Федерального закона.

Контроль осуществляется с помощью плановых и внеплановых проверок и в строгом соответствии с установленным порядком проведения данных проверок. Проверки осуществляет Роскомнадзор или его территориальные органы.

Плановые проверки проводятся на основании ежегодного плана проведения проверок:

* в отношении Операторов, включенных в Реестр операторов, осуществляющих обработку персональных данных;
* в отношении Операторов, не включенных в Реестр, но осуществляющих обработку персональных данных.

Внеплановые проверки проводятся по следующим основаниям:

* истечение срока исполнения оператором ранее выданного предписания об устранении выявленного нарушения установленных требований законодательства Российской Федерации в области персональных данных.
* поступление в Роскомнадзор или его территориальные органы обращений и заявлений граждан, юридических лиц, индивидуальных предпринимателей, информации от органов государственной власти, органов местного самоуправления, из средств массовой информации о следующих фактах:

1. возникновение угрозы причинения вреда жизни, здоровью граждан;
2. причинение вреда жизни, здоровью граждан;
3. нарушение прав и законных интересов граждан действиями (бездействием) Операторов при обработке их персональных данных;
4. нарушение Операторами требований законодательства в области персональных данных, а также о несоответствии сведений, содержащихся в уведомлении об обработке персональных данных, фактической деятельности.

Обращение гражданина РФ, не позволяющее установить его лицо, либо не содержащее сведения о фактах, указанных выше, не может являться основанием для внеплановой проверки.

О проведении внеплановой выездной проверки оператор уведомляется не менее чем за двадцать четыре часа до начала ее проведения любым доступным способом.

Если в результате деятельности оператора причинен или причиняется вред жизни, здоровью граждан, предварительное уведомление оператора о начале проведения внеплановой выездной проверки не требуется.

**Срок проведения, как плановой, так и внеплановой проверки не может превышать двадцать рабочих дней.**

В исключительных случаях срок проведения проверки может быть продлен, но не более чем на 20 рабочих дней, в отношении малых предприятий и микропредприятий – на 15 часов.

В ходе проверки осуществляется следующее:

* рассмотрение документов оператора, таких как уведомление об обработке, письменное согласие субъекта, локальных документов, регламентирующих порядок хранения и обработки ПД;
* исследование ИСПД в части, касающейся субъектов ПД.

Основанием для приостановления проверки является:

* необходимость получения заключений экспертов по вопросам обработки персональных данных, связанным с необходимостью проведения сложных и (или) длительных исследований, испытаний, специальных экспертиз и расследований;
* мотивированное решение руководителя контролирующего органа, принятое по причине изъятия документов, являющихся объектами контроля, проведенного ранее сотрудниками прокуратуры, правоохранительных органов, болезни должностных лиц, проводящих проверку. Оператору представляется копия приказа, в котором указываются причины приостановления проверки и период, на который данная проверка приостановлена.

Основанием для принятия решения об исключении Оператора из плана проведения плановых проверок является:

* ликвидация или реорганизация Оператора;
* прекращение Оператором деятельности по обработке персональных данных.

Проверка соответствия обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных завершается:

* составлением и вручением Оператору акта проверки;
* выдачей Оператору предписания об устранении выявленных нарушений требований законодательства Российской Федерации в области персональных данных;
* составлением протокола об административном правонарушении в отношении Оператора;
* подготовкой и направлением материалов проверки в органы прокуратуры, другие правоохранительные органы для решения вопроса о возбуждении дела об административном правонарушении, о возбуждении уголовного дела по признакам правонарушений (преступлений), связанных с нарушением прав субъектов персональных данных, в соответствии с подведомственностью.

### 12.3. Проверки ФСБ

Проверка ФСБ проводится на основании распоряжения или приказа начальника 8 Центра ФСБ России либо лица его замещающего. Проверка осуществляется должностными лицами, указанными в данном приказе. В приказе указывается следующее:

* наименование органа государственного контроля (надзора);
* фамилии, имена, отчества, должности должностного лица или должностных лиц, уполномоченных на проведение проверки, а также привлекаемых к проведению проверки экспертов, представителей экспертных организаций;
* наименование юридического лица или фамилия, имя, отчество индивидуального предпринимателя, проверка которых проводится;
* цели, задачи и предмет проверки;
* правовые основания проведения проверки;
* перечень мероприятий по контролю (надзору), необходимых для достижения целей и задач проведения проверки;
* даты начала и окончания проведения проверки[[43](https://www.intuit.ru/studies/courses/697/553/literature#literature.43)].

**Общий срок проверки** не может превышать 20 рабочих дней, для малого предпринимательства – не более 50 часов, для микропредприятия – 15 часов.

При проведении проверки ФСБ не вправе:

* проверять выполнение требований, не относящихся к компетенции ФСБ России;
* Осуществлять плановую или внеплановую проверку в случае отсутствия при ее проведении руководителя или уполномоченного представителя юридического лица, индивидуального предпринимателя, его уполномоченного представителя;
* требовать представления документов, информации, если они не являются объектами проверки и не относятся к предмету проверки, а также изымать оригиналы документов, относящихся к предмету проверки;
* распространять информацию, составляющую охраняемую законом тайну и полученную в результате проведения проверок, за исключением случаев, предусмотренных законодательством Российской Федерации;
* превышать установленные сроки проведения проверки;
* осуществлять выдачу юридическим лицам, индивидуальным предпринимателям предписаний или предложений о проведении за их счет мероприятий по контролю.

Ниже приведен перечень проверяемых в рамках проверки требований:

1. Организация системы организационных мер защиты персональных данных:

* область применения средств криптографической защиты информации (далее - СКЗИ) в информационных системах персональных данных;
* наличие ведомственных документов и приказов по организации криптографической защиты информации;
* Выполнение рекомендаций и указаний ФСБ России (при их наличии) по вопросам организации связи с использованием криптосредств.

2. Организация системы криптографических мер защиты информации:

* наличие модели угроз нарушителя;
* соответствие модели угроз исходным данным;
* соответствие требуемого уровня криптографической защиты полученной модели нарушителя;
* соответствие используемых СКЗИ полученному уровню криптографической защиты;
* наличие документов по поставке СКЗИ оператору.

3. Разрешительная и эксплуатационная документация:

* наличие необходимых лицензий для использования СКЗИ в информационных системах персональных данных;
* наличие сертификатов соответствия на используемые СКЗИ;
* наличие эксплуатационной документации на СКЗИ (формуляров, правил работы, руководств оператора и т.п.);
* порядок учета СКЗИ, эксплуатационной и технической документации к ним;
* выявление несертифицированных ФСБ России (ФАПСИ) СКЗИ.

4. Требования к обслуживающему персоналу:

* порядок учета лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности персональных данных в информационной системе;
* наличие функциональных обязанностей ответственных пользователей СКЗИ;
* укомплектованность штатных должностей личным составом, а также достаточность имеющегося личного состава для решения задач по организации криптографической защиты информации;
* организация процесса обучения лиц, использующих СКЗИ, применяемых в информационных системах, правилам работы с ними и другим нормативным документам по организации работ (связи) с использованием СКЗИ.

5. Эксплуатация СКЗИ:

* проверка правильности ввода СКЗИ в эксплуатацию и соответствие условий эксплуатации технических средств удостоверяющего центра (при наличии) требованиям эксплуатационной документации и сертификатов соответствия;
* оценка технического состояния СКЗИ, соблюдения сроков и полноты проведения технического обслуживания, а также проверка соблюдения правил пользования СКЗИ и порядка обращения с ключевыми документами к ним.

6. Оценка соответствия применяемых СКЗИ:

* соответствие программного обеспечения, реализующего криптографические алгоритмы используемых СКЗИ, эталонным версиям, проходившим сертификацию в ФСБ России;
* проведение (при необходимости) на местах осуществления проверки оперативных тематических исследований используемых СКЗИ.

7. Организационные меры:

* выполнения требований по размещению, специальному оборудованию, охране и организации режима в помещениях, где установлены СКЗИ или хранятся ключевые документы к ним, а также соответствия режима хранения СКЗИ и ключевой документации предъявляемым требованиям;
* оценка степени обеспечения оператора криптоключами и организации их доставки.
* проверка наличия инструкции по восстановлению связи в случае компрометации действующих ключей к СКЗИ.
* порядок проведения разбирательств и составления заключений по фактам нарушения условий хранения носителей персональных данных или использования СКЗИ.

По результатам проверки составляется акт проверки в двух экземплярах. В акте указываются результаты проверки, в том числе нарушения, если они есть.

### 12.4. Проверка ФСТЭК

ФСТЭК осуществляет плановые и внеплановые проверки лицензиатов (тех, кто имеет лицензии ФСТЭК). Плановая проверка в отношении одной организации может проводиться не чаще 1 раза в год. Предметом плановой проверки является соблюдение лицензиатом лицензионных требований и условий в процессе осуществления деятельности по технической защите конфиденциальной информации. Плановые проверки осуществляются согласно ежегодному плану.

Основанием для включения лицензиата в план является истечение трех лет со дня:

* государственной регистрации;
* последней плановой проверки.

Плановая проверка проводится в документарной или выездной форме. Порядок проведения проверок регламентируется Федеральным законом "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля".

О проведении проверки лицензиата уведомляют не позднее, чем за 3 дня до проведения.

Основанием для проведения внеплановой проверки является:

1. истечение срока действия предписания об устранении нарушений;
2. поступление обращений и заявлений в ФСТЭК о фактах:

* возникновения угрозы причинения вреда безопасности государства;
* причинение вреда безопасности государства.

Если обращение или заявление не позволяет идентифицировать заявителя, а также не содержат фактов, перечисленных выше, оно не может быть основанием для внеплановой проверки.

В ходе документарной проверки проверяются сведения, содержащиеся в документах лицензиата, устанавливающих его организационно-правовую форму, права и обязанности, документы, используемые при осуществлении его деятельности и связанные с исполнением им лицензионных требований и условий, исполнением предписаний ФСТЭК России.

Документарная проверка (как плановая, так и внеплановая) проводится по месту нахождения ФСТЭК России (управления ФСТЭК России по федеральному округу).

Предметом выездной проверки являются содержащиеся в документах лицензиата сведения, а также соответствие лицензиата лицензионным требованиям и условиям.

Выездная проверка (как плановая, так и внеплановая) проводится по месту нахождения лицензиата -юридического лица, месту осуществления деятельности лицензиата - индивидуального предпринимателя и (или) месту фактического осуществления их деятельности[[44](https://www.intuit.ru/studies/courses/697/553/literature#literature.44)].

Выездная проверка проводится в случае, если при документарной проверке не представляется возможным:

* удостовериться в полноте и достоверности сведений, содержащихся в имеющихся в распоряжении ФСТЭК России (управления ФСТЭК России по федеральному округу) документах лицензиата;
* оценить соответствие деятельности лицензиата лицензионным требованиям и условиям без проведения соответствующего мероприятия по контролю.

**Срок проведения каждой из проверок** не может превышать двадцать рабочих дней.

Проверка проводится на основании приказа ФСТЭК России.

При проведении проверки проверяющие не вправе:

* требовать представления документов, информации, если они не являются объектами проверки или не относятся к предмету проверки, а также изымать оригиналы таких документов;
* распространять информацию, полученную в результате проведения проверки и составляющую государственную, коммерческую, служебную, иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации;
* превышать установленные сроки проведения проверки;
* осуществлять выдачу юридическим лицам, индивидуальным предпринимателям предписаний или предложений о проведении за их счет мероприятий по контролю[[44](https://www.intuit.ru/studies/courses/697/553/literature#literature.44)].

В результате проверки составляется акт в двух экземплярах. В случае выявления нарушений, проверяющие должны выдать предписание об их устранении и проконтролировать его выполнение.

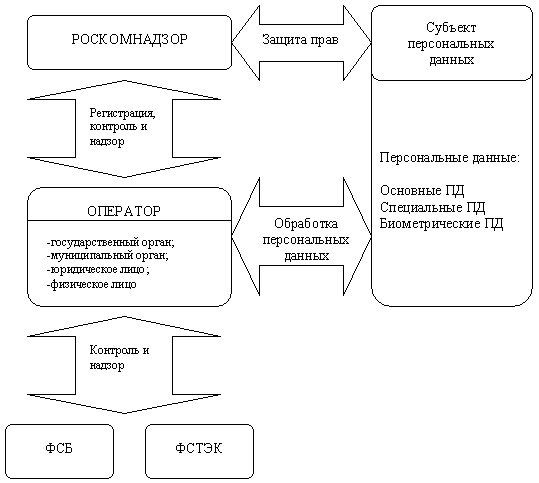
Общая схема взаимодействия регуляторов и операторов персональных данных представлена на рисунке 12.1.

Рис. 12.1 - Взаимодействие регуляторов и операторов персональных данных

В случае выявления в ходе плановых и внеплановых проверок нарушений в области обеспечения безопасности персональных данных, предусмотрена гражданская, уголовная, административная, дисциплинарная ответственность, которая может применяться в отношении руководителя организации, подразделения или виновного в разглашении работника. Наказанием за нарушение требований Федерального закона "О персональных данных" могут стать исправительные работы до 1 года или лишение свободы на срок до 2-х лет.

**Список используемых источников**

1. Галатенко В.А Основы информационной безопасности M: Интернет-университет информационных технологий - ИНТУИТ.ру, 2018

2. ГОСТ Р 50922-2006 “Защита информации. Основные термины и определения”

3. Рекомендации по стандартизации Р 50.1.056 – 2005 “Техническая защита информации. Основные термины и определения”

4. Федеральный закон РФ от 27.07.2006 №149-ФЗ “Об информации, информационных технологиях и о защите информации"

5. [Законодательный, административный, процедурный, программно-технический уровни](http://citforum.ru/seminars/cis99/galat2_5.shtml)

6. [1-й Российский портал о персональных данных](https://www.intuit.ru/www.persondata.ru)

7. Федеральный закон от 27.07.2006 №152 “О персональных данных”

8. [Защита персональных данных](http://www.jetinfo.ru/Sites/info/Uploads/2009_5.BBD027D438044A32AA55B9D1CA6988EB.pdf) Информационный бюллетень Jet Info - №5/2019

9. Постановление Правительства Российской Федерации от 15 сентября 2008 г. N 687 г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

10. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации Утвержден решением председателя Гостехкомиссии России от 30.03.1992

11. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) Утверждены приказом Гостехкомиссии России от 30.08.2002 № 282

12. Постановление Правительства Российской Федерации от 17 ноября 2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"

13. Системный проект формирования в Российской Федерации инфраструктуры электронного правительства 2010г

14. “Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» от 17.11.2007 № 781

15. Приказ ФСТЭК №58 “Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных” от 5 февраля 2010 года

16. Приложение к положению о методах и способах защиты информации в информационных системах персональных данных от 5 февраля 2010 года

17. ГОСТ Р ИСО/МЭК 15408-3-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий». Часть 3. Требования доверия к безопасности (на основе прямого применения еждународного стандарта

18. Руководящий документ “Безопасность информационных технологий. Критерии оценки безопасности информационных технологий” Гостехкомиссия России, 2002 г

19. Руководящий документ “Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности” Гостехкомиссия России, 2003 г

20. Руководящий документ “Безопасность информационных технологий. Руководство по регистрации профилей защиты” Гостехкомиссия России, 2003 г

21. Рекомендации по заполнению уведомления об обработке (о намерении осуществлять обработку) персональных данных Утверждены приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 16 августа 2011г. № 706 24. Положение о сертификации средств защиты информации по требованиям безопасности информации Утверждено приказом Гостехкомиссии России от 27.10.1995 № 199

22. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных Утвержденно Постановлением Правительства Российской Федерации от 17.11.2007 № 781

23. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

24. Руководящий документ. Защита от несанкцкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей Утвержден приказом председателя Гостехкомиссии России от 04.06.1999 №114

25. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) Утверждены приказом Гостехкомиссии России от 30.08.2002 № 282

26. Положение об аттестации объектов информатизации по требованиям безопасности информации Утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г

27. Постановление Правительства Российской Федерации от 26.01.2006 № 45 «Об организации лицензирования отдельных видов деятельности»

28. Положение о лицензировании деятельности по технической защите конфиденциальной информации Утверждено постановлением Правительства Российской Федерации от 15 августа 2006 г. № 504

29. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищенности от несанкионированного доступа к информации Утвержден решением председателя Гостехкомиссиии России от 25.07.1997 г

30. [Антивирусная защита компьютерных систем(Лаборатория Касперского)](http://www.intuit.ru/department/security/antiviruskasp/) М: Интернет университет информационных технологий “Интуит”, 2017г

31. Фаронов А.Е [Введение в защиту персональных данных](http://www.intuit.ru/department/security/secpdata/) М: Интернет университет информационных технологий “Интуит”, 2018г

32. Мэйволд Э [Безопасность сетей](http://www.intuit.ru/department/security/netsec/) М.: Интернет университет информационных технологий «Интуит», 2016, электронный курс

33. [Официальный сайт Федеральной службы по техническому и экспортному контролю](http://www.fstec.ru/) Утвержден решением председателя Гостехкомиссиии России от 25.07.1997 г

34. [Официальный сайт Федеральной службы безопасности РФ](http://www.fsb.ru/) М: Интернет университет информационных технологий “Интуит”, 2007г

35. [Административный регламент проведения проверок Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного контроля (надзора) за соответствием обработки персональных данн](http://www.intuit.ru/department/security/secpdata/) М: Интернет университет информационных технологий “Интуит”, 2011г

36. [Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных](http://www.intuit.ru/department/security/netsec/) Утвержден Руководством 8 Центра ФСБ России 08 августа 2009 года № 149/7/2/6-1173

37. [Административный регламент Федеральной службы по техническому и экспортному контролю по исполнению государственной функции по лицензированию деятельности по технической защите конфиденциальной информации](http://www.fstec.ru/) Утвержден приказом ФСТЭК России от 28 августа 2007 г. № 181

38. [Федеральный закон от 26 декабря 2008 г. N 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"](http://www.fsb.ru/).

# 39. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"

40. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»