**Лекция №4: Модель угроз персональным данным.**

**Организационно-распорядительная документация по защите персональных данных в Республике Казахстан**

**Цель: с**формировать у студентов понимание возможных угроз информационной безопасности в отношении персональных данных, научить анализировать и моделировать такие угрозы, а также ознакомить с видами и требованиями организационно-распорядительной документации, регулирующей защиту персональных данных в соответствии с законодательством Республики Казахстан.

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).

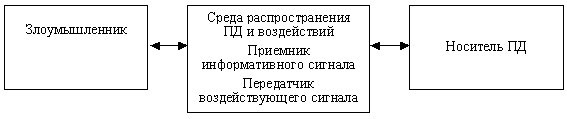
Под **угрозами безопасности ПД** при их обработке в ИСПД понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе *случайного, доступа* к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, *копирование*, распространение 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" \l "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:

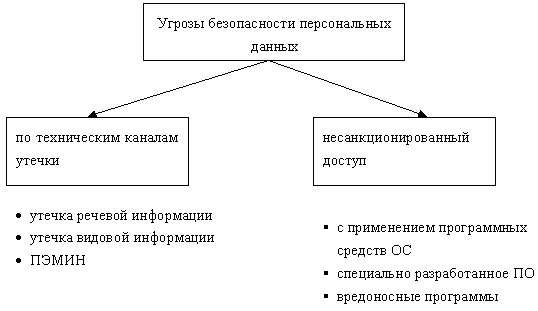
* нарушитель;
* носитель вредоносной программы;
* аппаратная закладка.

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" \l "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:

1. ошибки при разработке программного обеспечения;
2. преднамеренные изменения программного обеспечения с целью внесения уязвимостей;
3. неправильные настройки программного обеспечения;
4. несанкционированное внедрение вредоносных программ;
5. неумышленные действия пользователей;
6. сбои в работе программного и аппаратного обеспечения.

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

1. по типу ПО – системное или прикладное.
2. по этапу жизненного цикла ПО, на котором возникла уязвимость – проектирование, эксплуатация и пр.
3. по причине возникновения уязвимости, например, недостатки механизмов аутентификации сетевых протоколов.
4. 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.

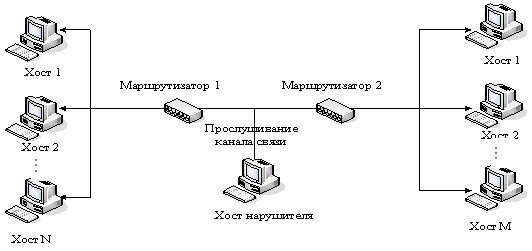
Прежде чем приступать к построению системы защиты информации необходимо провести *анализ уязвимостей* ИСПД и попытаться сократить их количество, то есть использовать метод превентивности. Можно закрыть лишние порты, поставить "заплатки" на *программное обеспечение* (например, *service* pack для *Windows*), 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”

1. **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.

1. **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.

1. **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.

1. **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.

1. **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.

1. **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).

**Вопросов для закрепления:**

1. Что такое угроза безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПД)?
2. Какие два основных пути могут быть использованы для реализации угроз безопасности персональных данных?
3. Объясните, что такое технический канал утечки информации. Приведите примеры угроз, связанных с этим каналом.
4. В чем заключается разница между внешними и внутренними нарушителями в контексте угроз безопасности персональных данных?
5. Какие основные типы угроз можно выделить в зависимости от способа их реализации? Приведите примеры.
6. Что такое уязвимость информационной системы персональных данных и как она может быть использована для реализации угрозы безопасности?
7. Перечислите основные причины возникновения уязвимостей в информационных системах персональных данных.
8. Какие типы атак являются наиболее распространенными в современных информационных системах, использующих Интернет?
9. Что такое "анализ сетевого трафика" и как он может быть использован злоумышленниками для получения доступа к персональным данным?
10. Объясните процесс сканирования сети и его связь с дальнейшими действиями злоумышленников.
11. В чем заключается угроза "подмены доверенного объекта сети" и как она может быть реализована в системе безопасности?
12. Что такое отказ в обслуживании (DoS) и как он может повлиять на доступность информации в ИСПД?
13. Какие документы в рамках организационно-распорядительной документации необходимы для защиты персональных данных в организации?
14. Какие требования должны быть включены в Положение по обеспечению безопасности персональных данных?
15. Что такое "частная модель угроз" и как она разрабатывается для конкретной организации?