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

**Цель лекции**: изучить требования законодательства и соответствующие им мероприятия по отношению к ИСПД разных классов в области технической защиты информации

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

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

1. от несанкционированного доступа (в том числе случайного);
2. 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:

1. использование технических средств в защищенном исполнении;
2. использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия;
3. размещение объектов защиты в соответствии с предписанием на эксплуатацию;
4. размещение понижающих трансформаторных *подстанций* электропитания и контуров заземления технических средств в пределах охраняемой территории;
5. обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал;
6. 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" \l "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 РК 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:

1. разрешительная система доступа пользователей ИСПД к системе, информации и документам, связанным с ее работой;
2. ограничение доступа в помещения, где обрабатываются ПД и к носителям с ПД;
3. разграничение доступа к информационным ресурсам, программным средствам обработки и передачи информации, к средствам защиты информации;
4. регистрация и контроль действий пользователей и обслуживающего персонала ИСПД;
5. учет, хранение и обращение съемных носителей информации, исключающие их хищение, порчу, подмену и т.п.;
6. резервирование технических средств и носителей информации;
7. использование технических средств, которые прошли проверку на соответствие;
8. использование защищенных каналов связи;
9. размещение технических средств для обработки ПД внутри границ охраняемой территории;
10. организация физической защиты помещений и технических средств обработки ПД;
11. предотвращение внедрения вирусов и программных закладок в ИСПД.
12. 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:

1. управление доступом;
2. регистрация и учет;
3. 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.

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:

1. использование средств антивирусной защиты;
2. межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
3. обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
4. анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
5. защита информации при ее передаче по каналам связи;
6. использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
7. 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" \l "literature.21)].

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

Межсетевые экраны ИСПД 3 класса должны обеспечивать:

1. 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);
2. идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору и паролю условно-постоянного действия;
3. 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);
4. контроль целостности своей программной и информационной части;
5. фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
6. восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
7. 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:

1. 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);
2. фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
3. фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
4. фильтрацию с учетом любых значимых полей сетевых пакетов;
5. регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
6. идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
7. 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);
8. регистрацию запуска программ и процессов (заданий, задач);
9. контроль целостности своей программной и информационной части;
10. восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
11. 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:

1. 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);
2. фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
3. фильтрацию с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
4. фильтрацию с учетом любых значимых полей сетевых пакетов;
5. фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя;
6. фильтрацию на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя;
7. фильтрацию с учетом даты и времени;
8. аутентификацию входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети;
9. регистрацию и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
10. регистрацию и учет запросов на установление виртуальных соединений;
11. локальную сигнализацию попыток нарушения правил фильтрации;
12. идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
13. предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась;
14. идентификацию и аутентификацию администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
15. 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);
16. регистрацию запуска программ и процессов (заданий, задач);
17. регистрацию действия администратора межсетевого экрана по изменению правил фильтрации;
18. возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации;
19. контроль целостности своей программной и информационной части;
20. контроль целостности программной и информационной части межсетевого экрана по контрольным суммам;
21. восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
22. 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" \l "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.

**Вопросов для закрепления материала:**

1. Какие виды утечек информации учитываются при защите ПД в ИСПД?
2. Какие мероприятия применяются в ИСПД 1 класса для защиты от ПЭМИН?
3. В чем заключается электромагнитная развязка в рамках защиты от технических каналов утечки?
4. Какие требования предъявляются к средствам вычислительной техники в ИСПД 2 класса?
5. Как обеспечивается защита речевой информации в ИСПД с голосовым вводом?
6. Что такое несанкционированный доступ (НСД) и несанкционированное воздействие на информацию?
7. Перечислите основные мероприятия по защите от НСД при обработке ПД.
8. Какие меры защиты обязательны вне зависимости от класса ИСПД?
9. Какие подсистемы включает система защиты ПД (СЗПД)?
10. Чем отличаются требования к 2 и 3 классам ИСПД в однопользовательском и многопользовательском режимах?
11. Какие дополнительные угрозы возникают при подключении ИСПД к сетям общего пользования?
12. Назовите основные требования к безопасности при таком подключении.
13. Какие функции должен обеспечивать межсетевой экран в ИСПД 3 класса?
14. В чем заключается отличие требований к межсетевым экранам ИСПД 1, 2 и 3 классов?
15. Какие методы используются системами обнаружения вторжений в ИСПД разных классов?
16. Для чего используются средства анализа защищенности?
17. Какие средства идентификации и аутентификации рекомендуются при подключении ИСПД к Интернету?
18. Что включает в себя централизованное управление системой защиты ПД?
19. Какие действия необходимо регистрировать в межсетевом экране ИСПД 1 класса?
20. Кто определяет меры защиты персональных данных в ИСПД 4 класса?