Практическая работа 1.

Построение модели угроз ИСПДн

Цель работы: изучить нормативные документы ФСТЭК по построению модели угроз. Построить модель угроз информационной системы персональных данных функционирующей в Вашей организации.

Теоретическая часть

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, определение уровня исходной защищённости производится на основании анализа технических и эксплуатационных характеристик ИСПДн. Характеристики, необходимые для определения уровня защищённости ИСПДн приведены в таблице 1.

Исходный уровень защищенности определяется следующим образом:

ИСПДн имеет *высокий* уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).

ИСПДн имеет *средний* уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.

ИСПДн имеет *низкую* степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности ПДн каждой степени исходной защищенности ставится в соответствие числовой коэффициент Y_1, а именно:

0 - для высокой степени исходной защищенности;

5 - для средней степени исходной защищенности;

10 - для низкой степени исходной защищенности.

Характеристики для определения исходного уровня защищённости ИСПДн приведены в таблице 2.

Определение вероятности реализации угроз безопасности в информационной системе персональных данных

В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, под *частотой (вероятностью) реализации угрозы* понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки.

Вводятся четыре вербальных градации показателя «Вероятность реализации угрозы»:

маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации

средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2, а именно:

0 - для маловероятной угрозы;

2 - для низкой вероятности угрозы;

5 - для средней вероятности угрозы;

10 - для высокой вероятности угрозы

Определение коэффициента реализуемости угрозы

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением (1)

$$Y = (Y_1 + Y_2)/20, \text{ где} \quad (1)$$

Y_1 – коэффициент защищенности ИСПДн

Y_2 – вероятность возникновения угрозы

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

Если $0 \leq Y \leq 0{,}3$ то возможность реализации угрозы признается низкой;

Если $0{,}3 < Y \leq 0{,}6$ то возможность реализации угрозы признается средней;

Если $0{,}6 < Y \leq 0{,}8$ то возможность реализации угрозы признается высокой;

Если $Y > 0{,}8$ то возможность реализации угрозы признается очень высокой;

Далее оценивается опасность каждой угрозы. При оценке опасности на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель опасности для рассматриваемой ИСПДн. Этот показатель имеет три значения:

низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПДн, в соответствии с правилами, приведенными в таблице 1.

Таблица 1 Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	неактуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

На основании экспертных оценок вероятности реализации угроз и показателя опасности, с учетом коэффициента исходной защищенности ИСПДн рассчитывается степень актуальности угроз безопасности ПДн.

Практическое задание

Построить модель угроз ИСПДн Вашего предприятия. Для построения модели угроз необходимо проработать теоретический материал лабораторной работы и заполнить таблицы 2 и 3.

Таблица 2 – Характеристики для определения исходного уровня защищённости ИСПДн

Технические и эксплуатационные характеристики ИСПДн	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению:			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);			
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;			
локальная ИСПДн, развернутая в пределах одного здания			
2. По наличию соединения с сетями общего пользования:			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			
ИСПДн, имеющая одноточечный выход в сеть общего пользования;			
ИСПДн, физически отделенная от сети общего пользования			
3. По встроенным (легальным) операциям с записями баз персональных данных:			
чтение, поиск;			
запись, удаление, сортировка;			
модификация, передача			
4.По разграничению доступа к персональным данным:			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;			

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			
ИСПДн с открытым доступом			
5. *По наличию соединений с другими базами ПДн иных ИСПДн:*			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн			
6. По уровню обобщения (обезличивания) ПДн:			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);			
ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;			
ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн)			
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки:			
ИСПДн, предоставляющая всю базу данных с ПДн;			
ИСПДн, предоставляющая часть ПДн;			
ИСПДн, не предоставляющая никакой информации.			

Таблица 3 – Модель угроз ИСПДн «предприятия»

Угрозы безопасности ПДн	Вероятность реализации угрозы	Показатель опасности угрозы для ИСПДн	Возможность реализации угрозы	Актуальность угрозы	Примечание
Угрозы утечки информации по техническим каналам					
Угрозы утечки акустической информации					
Использование направленных (ненаправленных) микрофонов воздушной проводимости для съема акустического излучения информативного речевого сигнала					
использование "контактных микрофонов" для съема виброакустических сигналов					
использование "лазерных микрофонов" для съема виброакустических сигналов					
использование средств ВЧ-навязывания для съема электрических сигналов, возникающих за счет "микрофонного эффекта" в ТС обработки ПДн и ВТСС (распространяются по проводам и линиям, выходящим за пределы служебных помещений)					

применение средств ВЧ-облучения для съема радиоизлучения, модулированного информативным сигналом, возникающего при непосредственном облучении ТС обработки ПДн и ВТСС ВЧ-сигналом					
применение акустооптических модуляторов на базе ВОЛ, находящихся в поле акустического сигнала ("оптических микрофонов")					
Угрозы утечки видовой информации					
визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн					
визуальный просмотр с помощью оптических (оптикоэлектронных) средств с экранов дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн					
использование специальных электронных устройств съема видовой информации (видеозакладки)					
Угрозы утечки информации по каналам ПЭМИН					

применение специальных средств регистрации ПЭМИН, от ТС и линий передачи информации (ПАК, сканерные приемники, цифровые анализаторы спектра, селективные микровольтметры)					
применение токосъемников для регистрации наводок информативного сигналов, обрабатываемых ТС, на цепи электропитания и линии связи, выходящие за пределы служебных помещений					
применение специальных средств регистрации радиоизлучений, модулированных информативным сигналом, возникающих при работе различных генераторов, входящих в состав ТС ИСПДн или при наличии паразитной генерации в узлах ТС					
применение специальных средств регистрации радиоизлучений, формируемых в результате ВЧ-облучения ТС ИСПДн в которых проводится обработка информативных сигналов -параметрических каналов утечки					

Угрозы НСД в ИСПДн					
Угрозы использования уязвимостей ИСПДн					
ошибки либо преднамеренное внесение уязвимостей при проектировании и разработке СПО и ТС, недекларированные возможности СПО					
ошибки либо преднамеренное внесение уязвимостей при проектировании и разработке ППО, недекларированные возможности ППО					
неверные настройки ПО, изменение режимов работы ТС и ПО (случайное либо преднамеренное)					
сбои в работе ТС и ПО (сбои в электропитании, выход из строя аппаратных элементов, внешние воздействия электромагнитных полей)					
Угрозы непосредственного доступа в операционную среду ИСПДн:					
доступ к информации и командам, хранящимся в BIOS с возможностью перехвата управления загрузкой ОС и					

получения прав доверенного пользователя на АРМ					
доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ					
доступ в среду функционирования прикладных программ (локальная СУБД, например)					
доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности					
Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия					
сканирование сети и анализ сетевого трафика для изучения логики работы ИСПДн, выявления протоколов, портов, перехвата служебных данных (в том числе, идентификаторов и паролей), их подмены					

применение специальных программ для выявления пароля (сниффинг, IP-спуффинг, разные виды перебора)					
подмена доверенного объекта сети с присвоением его прав доступа, внедрение ложного объекта сети					
реализация угрозы отказа в обслуживании					
внедрение специализированных троянов, вредоносных программ					
сетевые атаки					
применение утилит администрирования сети					
подключение к ТС и системам					
Угрозы программно-математических воздействий:					
внедрение программных закладок					
внедрение вредоносных программ (случайное или преднамеренное, по каналам связи)					
внедрение вредоносных программ (случайное или преднамеренное, непосредственное)					

Угрозы несанкционированного физического доступа к съемным носителям информации					
повреждение носителя информации					
утрата носителя информации					
хищение носителя информации					
Угрозы доступа к ТС и системам обеспечения					
нарушение функционирования кабельных линий связи, оборудования					
нарушение функционирования ТС обработки информации, НЖМД					
доступ к системам обеспечения, их повреждение					
доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные)					
Угрозы неправомерных действий со стороны лиц, имеющих право доступа к информации					
Несанкционированное изменение информации					
Несанкционированное копирование информации					
Угрозы разглашения информации					

разглашение информации лицам, не имеющим права доступа к ней					
передача защищаемой информации по открытым каналам связи					
копирование информации на незарегистрированный носитель информации, в том числе печать					
передача носителя информации лицу, не имеющему права доступа к имеющейся на нем информации					