Лекция 1 (продолжение)

Классификация угроз безопасности информации при обработке в автоматизированных системах

Модель угроз

- характеристика КС, объекты защиты и их уязвимости;
- возможные угрозы и отношения между ними;
- объекты и каналы воздействия угроз на уязвимые элементы КС;
- вероятности их реализации и размеры наносимого ущерба;
- условия регионов и мест расположения защищаемых объектов.

Нормативные документы

Нормативными документами Российской Федерации угрозы безопасности информации конкретизированы в:

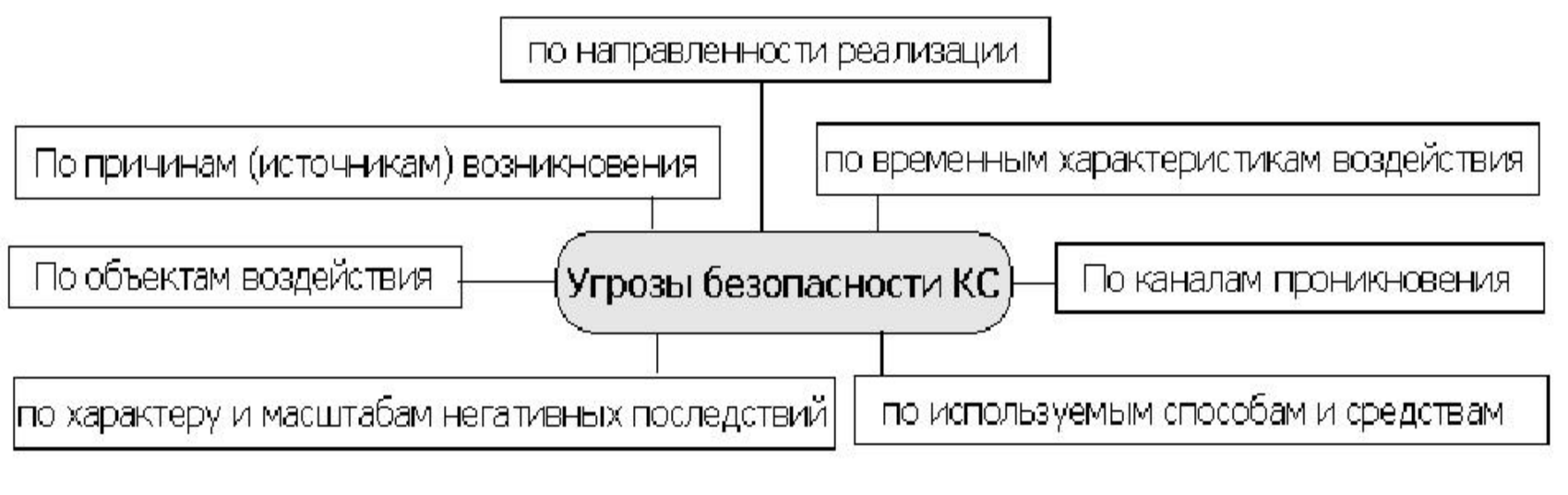
– ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения;

– ГОСТ 21964-78 Внешние воздействующие факторы. Номенклатура и характеристики;

– Модель угроз безопасности информации в ключевой системе информационной инфраструктуры, утверждена 18.05.2007 ФСТЭК России;

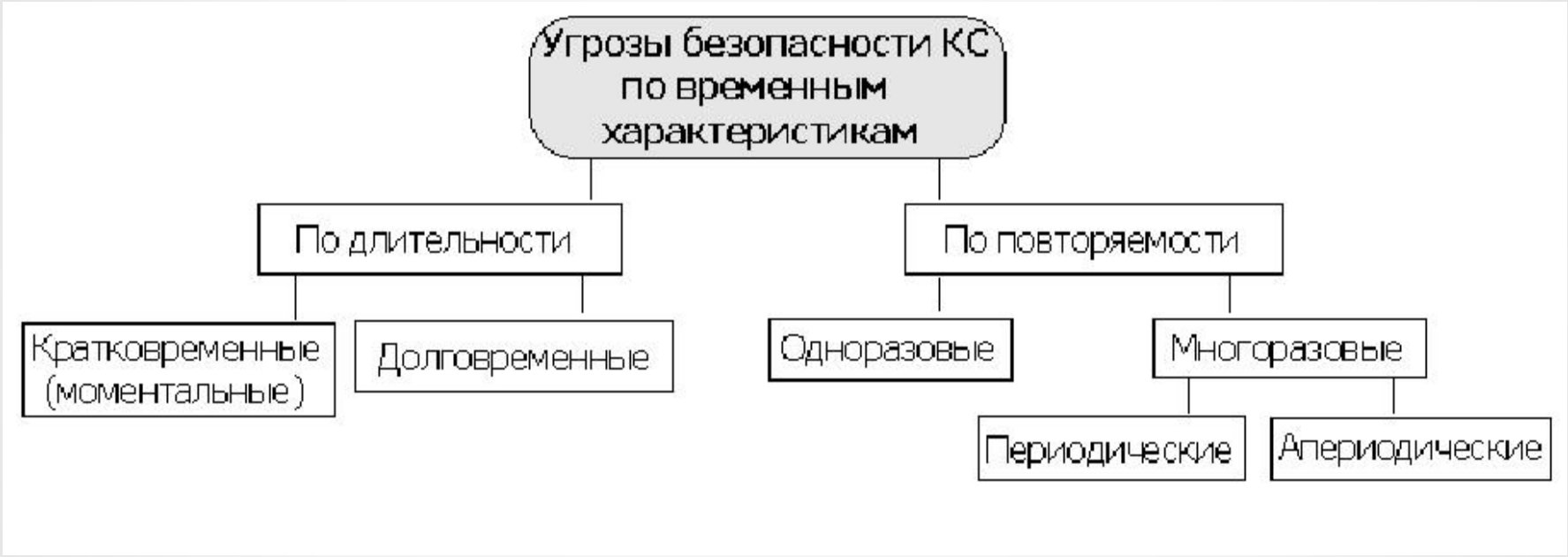
– Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена 15.02.2008 ФСТЭК России.

Признаки классификации угроз безопасности

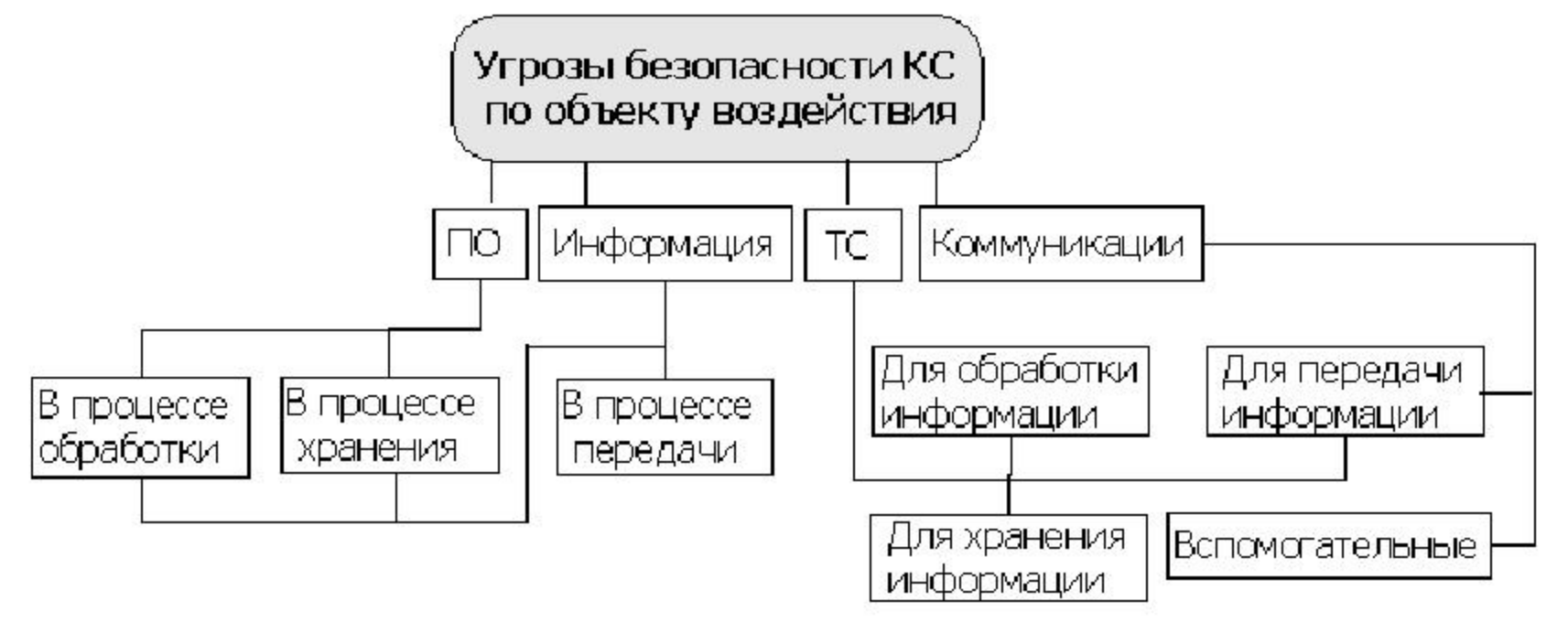


Классификация угроз по направленности реализации

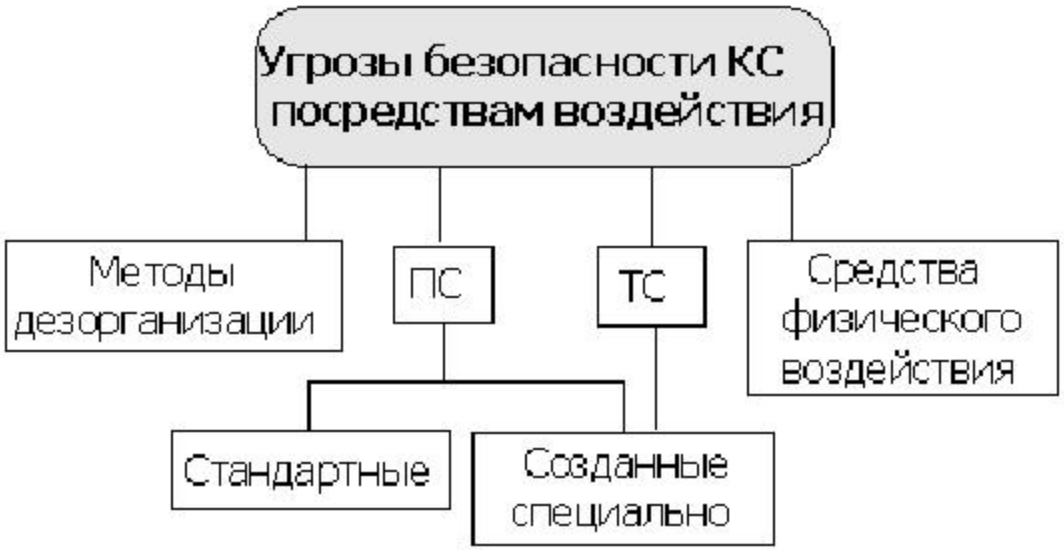
Классификация угроз по временным характеристикам воздействия



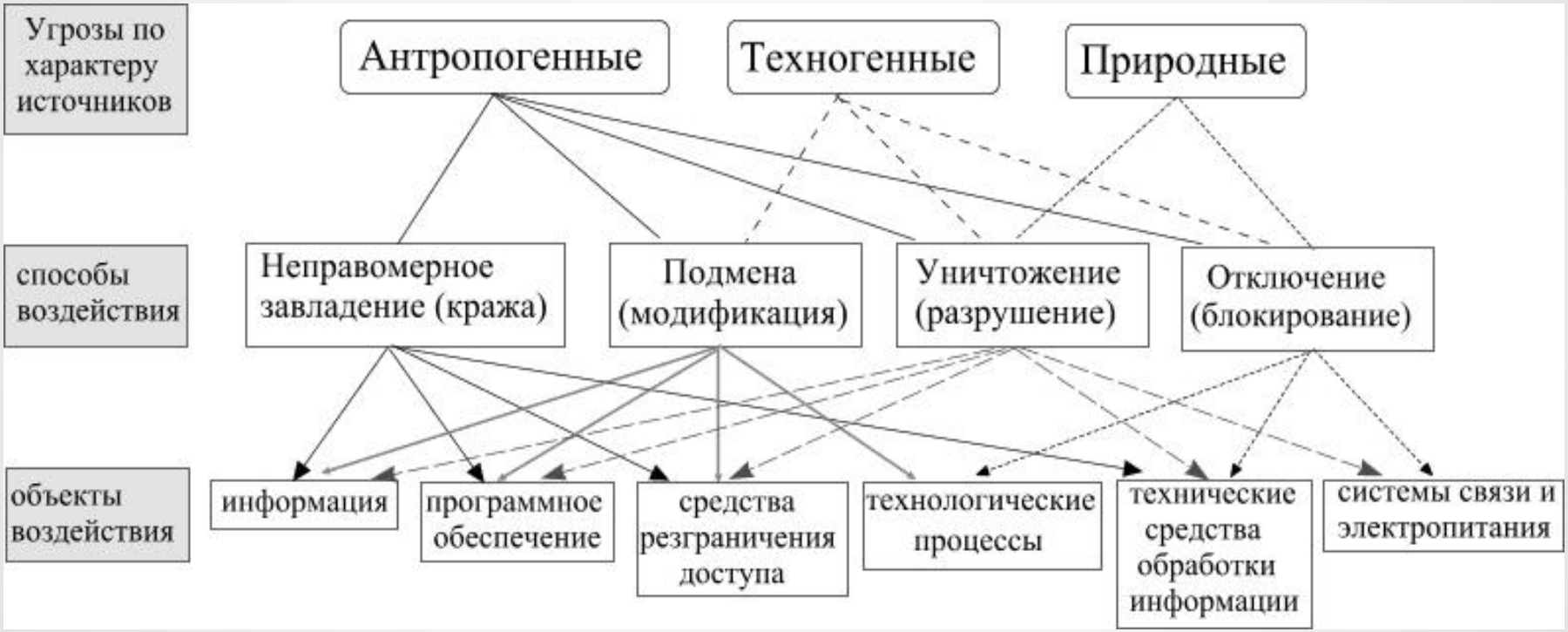
Классификация угроз по объекту воздействия



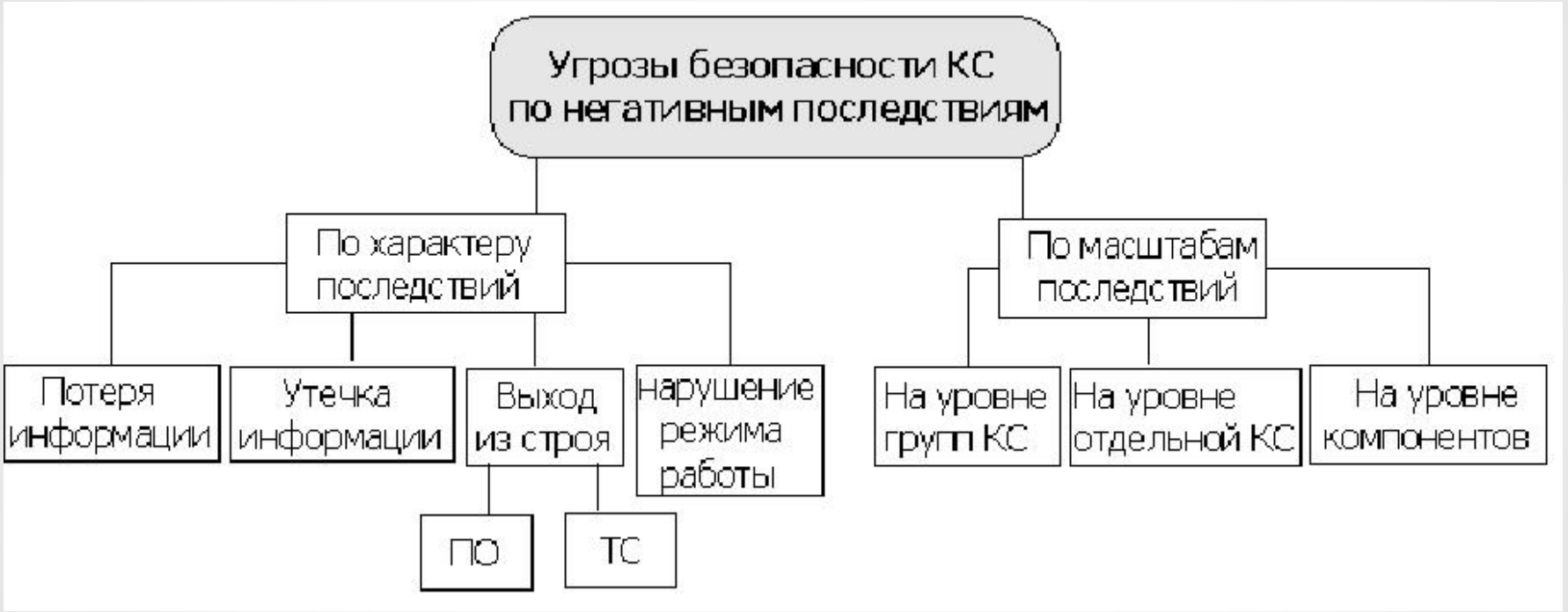
Классификация угроз по используемым средствам воздействия (нападения)



Классификация угроз по причинам (источникам) возникновения

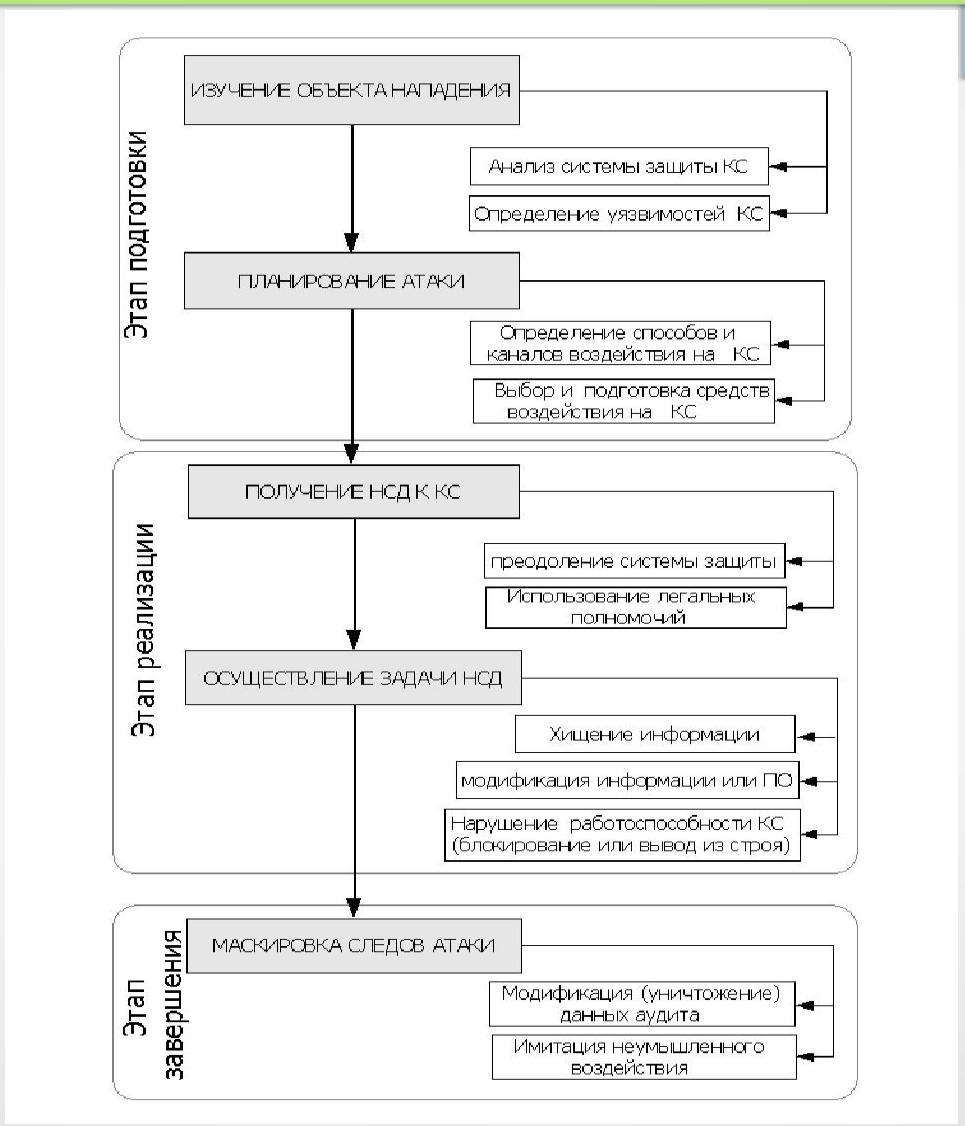


Классификация угроз по характеру и масштабам негативных последствий

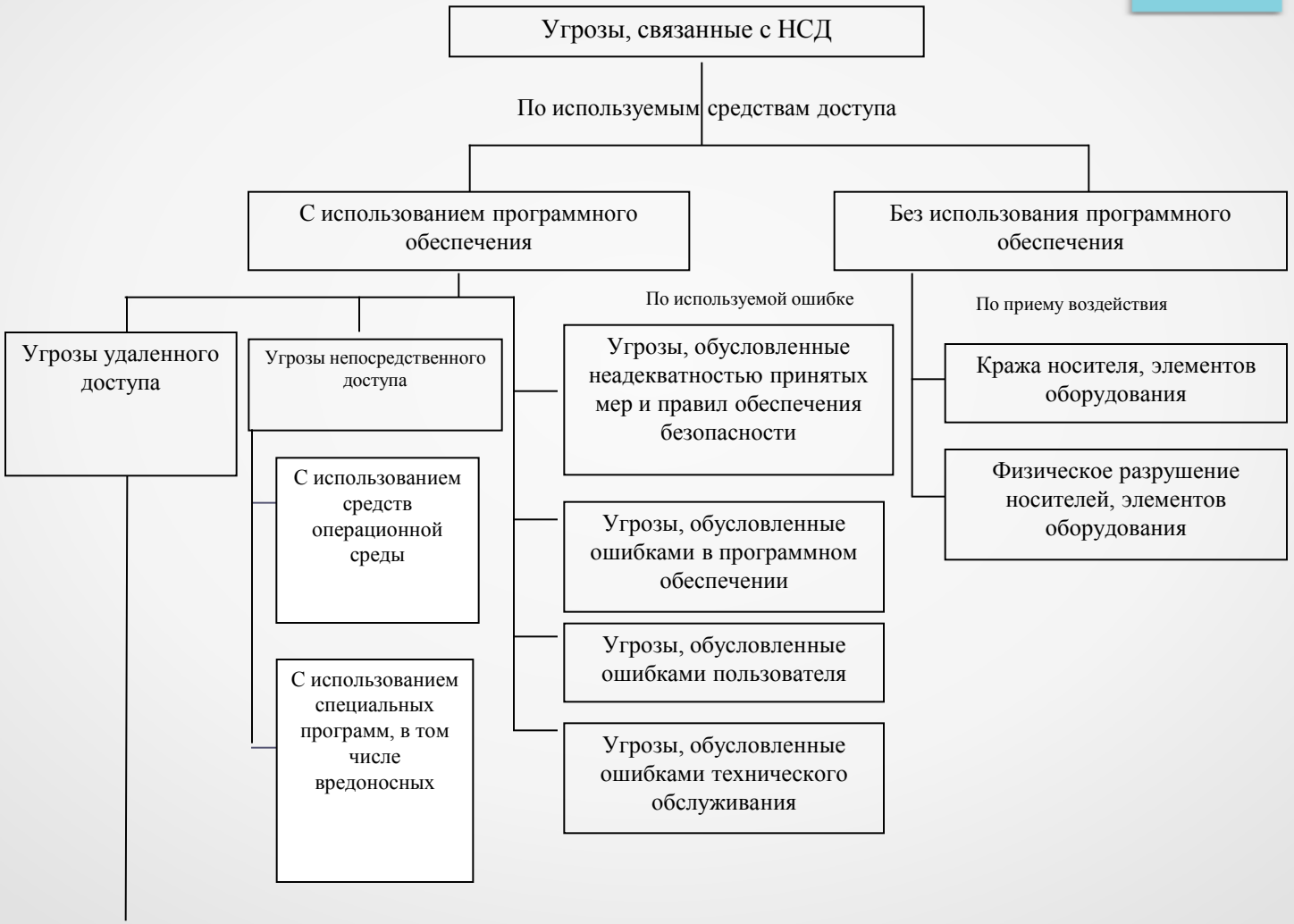


Классификация угроз по каналам доступа

Обобщенный алгоритм воздействия угрозы (атаки)



Угрозы, связанные с НСД



Угрозы, связанные с НСД

Инцидент – сочетание угрозы и уязвимости

Инцидент – сочетание угрозы и уязвимости (примеры)

Безопасность кадровых ресурсов (ISO/IEC 27002:2005, раздел 8)

Уязвимость	Угроза, использующая уязвимость
Недостаточное обучение безопасности	Ошибка персонала технической поддержки
Неосведомленность в вопросах безопасности	Ошибки пользователей
Отсутствие механизмов мониторинга	Несанкционированное использование программного обеспечения
Отсутствие политик в области корректного использования средств телекоммуникаций и передачи сообщений	Несанкционированное использование сетевого оборудования
Не отменяются права доступа при увольнении	Несанкционированный доступ
Не существует процедуры, гарантирующей возврат ресурсов при увольнении	Кража
Немотивированный или недовольный персонал	Злоупотребление средствами обработки информации
Безнадзорная работа внешнего персонала или персонала, работающего в нерабочее время	Кража

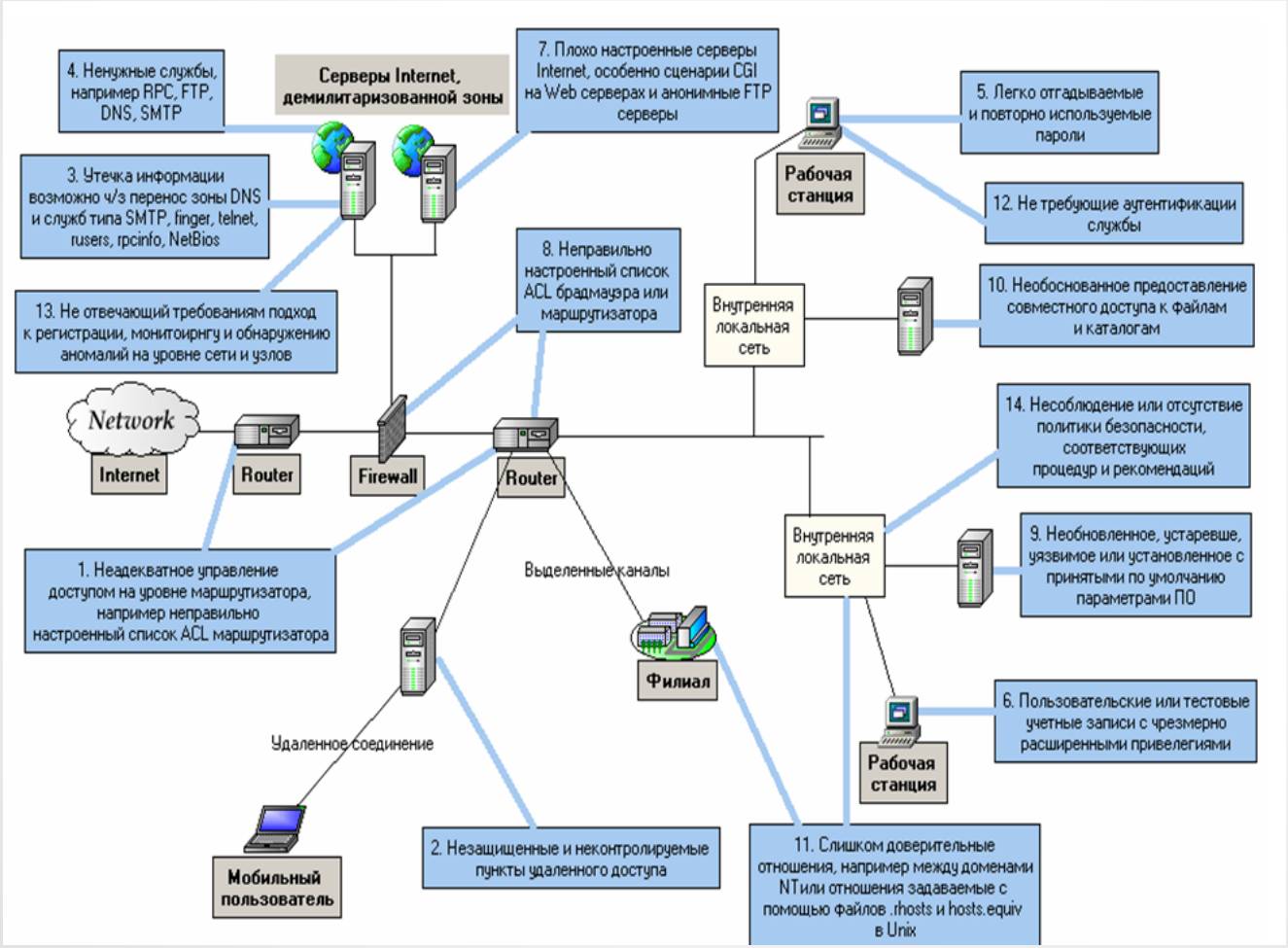
http://анализ-риска.рф/node/231

Инцидент – сочетание угрозы и уязвимости (примеры)

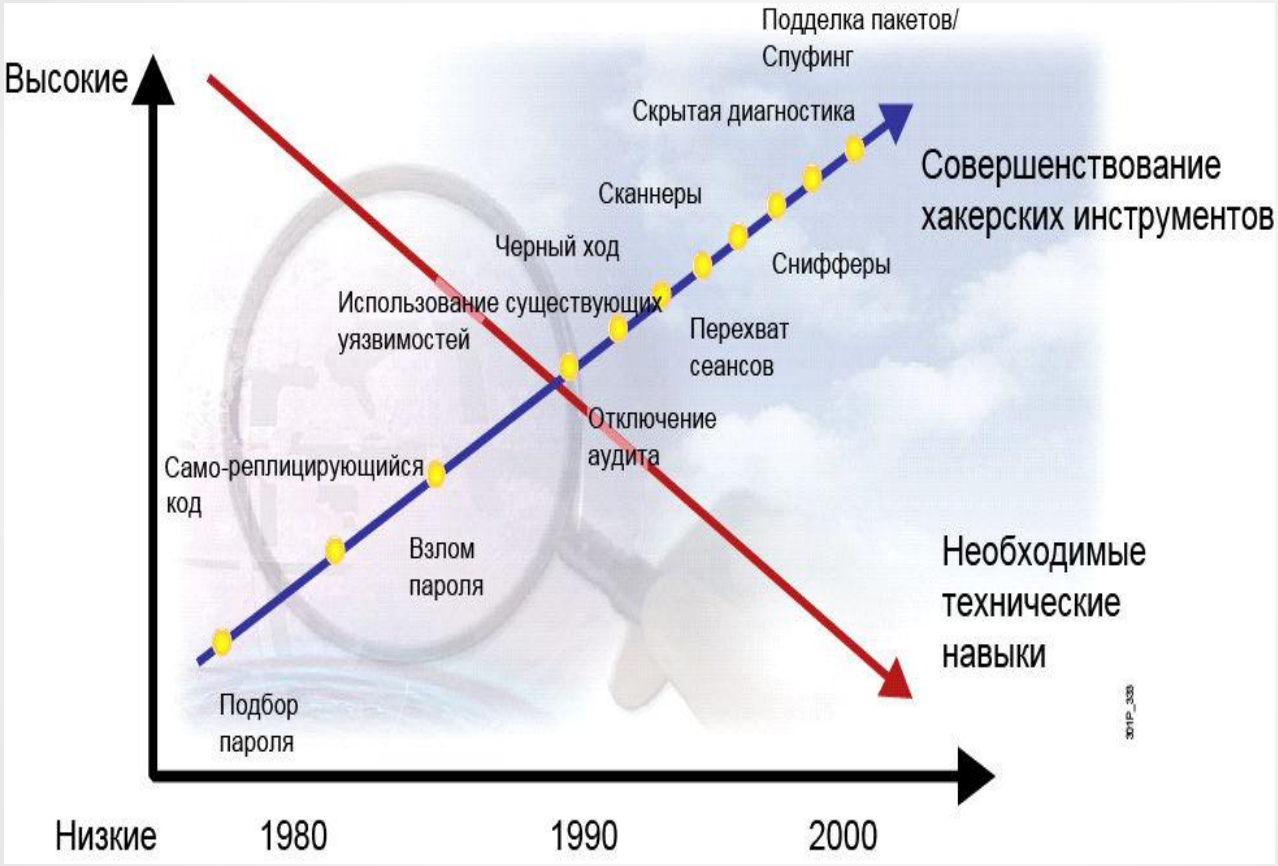
Управление коммуникациями и операциями (ISO/IEC 27002:2005, раздел 10)

Уязвимость	Угроза, использующая уязвимость
Сложный пользовательский интерфейс	Ошибка персонала
Передача или повторное использование средств хранения информации без надлежащей очистки	Несанкционированный доступ к информации
Неадекватный контроль изменений	Сбой системы безопасности
Неадекватное управление сетью	Перегрузка трафика
Отсутствие процедур резервного копирования	Потеря информации
Отсутствие доказательств отправки или получения сообщения	Уход от ответственности
Отсутствие обновления программного обеспечения, используемого для защиты от вредоносного кода	Вирусная инфекция
Нет разделения обязанностей	Злоупотребление системой (случайное или преднамеренное)
Нет разделения тестового и рабочего оборудования	Несанкционированная модификация действующих систем
Неконтролируемое копирование	Кража
Незащищенные соединения с сетями общего пользования	Использование программного обеспечения неавторизованными пользователями

Угрозы и уязвимости сети



Угрозы сети


Высокие
Низкие
1980
1990
2000
Подделка пакетов/
Спуфинг
Скрытая диагностика
Совершенствование
хакерских инструментов
Сканнеры
Черный ход
Снифферы
Использование существующих
уязвимостей
Перехват
сеансов
Отключение
аудита
Само-реплицирующийся
код
Взлом
пароля
Необходимые
технические
навыки
Подбор
пароля
301P_333

Угрозы - источники

Пример анализа угроз - Угрозы ПДн

Управление рисками.

Моделирование угроз безопасности персональных данных (ПДн)*проводится для получения качественной и количественной оценки угроз, актуальных для ПДн, обрабатываемых в информационной системе обработки персональных данных (ИСПДн) на основе методологии, установленной нормативно-методическими документами ФСТЭК России[1] по вопросам обеспечения безопасности ПДн при их обработке в ИСПДн.

*«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г.«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена Заместителем директора ФСТЭК России 15 февраля 2008 г.

Угрозы ПДн

При формировании перечня актуальных угроз безопасности ПДн используются два показателя:

- уровень исходной защищенности ИСПДн
- частота (вероятность) реализации рассматриваемой угрозы.

Построение Модели угроз безопасности ПДн, обрабатываемых в ИСПДн Компании, основывается на классификации, анализе и оценке актуальности совокупности условий и факторов, создающих опасность, связанную с утечкой ПДн и (или) несанкционированными и (или) непреднамеренными воздействиями на них.

В рамках построения Модели угроз безопасности ПДн все вероятные угрозы разделяются на две категории:

- угрозы безопасности ПДн, реализуемые за счет НСД к базам данных (БД) с использованием штатного или специально разработанного ПО;
- угрозы безопасности ПДн, реализуемые за счет утечки ПДн по техническим каналам.

Источники угроз безопасности ПДн за счёт НСД

Код	Источник угрозы
А 1	Нарушитель
А 1.1	Внешний нарушитель
А 1.2	Внутренний нарушитель
А 1.2.1	Лица, имеющие санкционированный доступ в контролируемую зону, но не имеющие доступа к ИР
А 1.2.2	Зарегистрированные пользователи ИР, имеющие ограниченные права доступа
А 1.2.3	Пользователи ИР, осуществляющие удаленный доступ по локальной вычислительной сети
А 1.2.4	Зарегистрированный пользователь с полномочиями администратора безопасности структурного подразделения
А 1.2.5	Зарегистрированный пользователь с полномочиями системного администратора
А 1.2.6	Зарегистрированный пользователь с полномочиями администратора безопасности ИСПДн
А 1.2.7	Программисты-разработчики прикладного ПО и лица, обеспечивающие его сопровождение
А 1.2.8	Разработчики и лица, обеспечивающие поставку, сопровождение и ремонт ТС
А 1.2.*	Другие категории в соответствии с оргштатной структурой

Источники угроз безопасности ПДн за счёт НСД

Код	Источник угрозы
А 2	Программно-аппаратная закладка
А 2.1	Конструктивно-встроенная программно-аппаратная закладка
А 2.2	Автономная программно-аппаратная закладка
А 3	Вредоносная программа
А 3.1	Программные закладки
А 3.2	Программные вирусы
А 3.3	Сетевые черви
А 3.4	Другие вредоносные программы

Уязвимости безопасности ПДн за счёт НСД

Код	Уязвимость ИСПДн
В 1	Уязвимости ПО (наличие в ИСПДн вредоносной программы)
В 1.1	Уязвимости микропрограмм, прошивок ПЗУ, ППЗУ
В 1.2	Уязвимости драйверов аппаратных средств
В 1.3	Уязвимости ОС
В 1.3.1	В процессе инициализации ОС
В 1.3.2	В незащищенном режим работы процессора
В 1.3.3	В процессе функционирования ОС в привилегированном режиме
В 1.4	Уязвимости прикладного ПО
В 1.5	Уязвимости специального ПО
В 1.6	Уязвимости ПО пользователя
В 2	Уязвимости, вызванные наличием в ИСПДн программно-аппаратной закладки

Уязвимости безопасности ПДн за счёт НСД

Код	Уязвимость ИСПДн
В 3	Уязвимости, связанные с реализацией протоколов сетевого взаимодействия и каналов передачи данных
В 3.1	Уязвимости на канальном уровне
В 3.2	Уязвимости на сетевом уровне
В 3.3	Уязвимости на транспортном уровне
В 3.4	Уязвимости на сеансовом уровне
В 3.5	Уязвимости на презентационном уровне
В 3.6	Уязвимости на прикладном уровне
В 4	Уязвимости, вызванные недостатками организации технической защиты информации от НСД
В 5	Уязвимости СЗИ
В 6	Уязвимости программно-аппаратных средств ИСПДн в результате сбоев в работе, отказов этих средств

Способы реализации угроз безопасности ПДн

Код	Способ реализации угрозы
С 1	Использование существующих уязвимостей программно-аппаратного обеспечения (ПАО) ИСПДн
С 1.1	Обход СЗИ
С 1.2	Деструктивное воздействие на СЗИ
С 1.3	Вскрытие или перехват пароля
С 1.4	Уязвимости протоколов сетевого взаимодействия и каналов передачи данных
С 1.4.1	Перехват информации
С 1.4.2	Модификация передаваемых данных
С 1.4.3	Перегрузка ресурсов (отказ в обслуживании)
С 1.4.4	Внедрение вредоносных программ
С 1.4.5	Удаленный НСД в систему
С 1.4.6	Разглашение и утечка информации на незащищенные автоматизированные рабочие места (АРМ) вычислительной сети
С 1.5	Использование остаточной, неучтенной информации (сбор «мусора»)
С 1.6	Использование нетрадиционных (стеганографических) каналов передачи информации

Способы реализации угроз безопасности ПДн

Код	Способ реализации угрозы
С 2	Внедрение (внесение) новых уязвимостей в ИСПДн
С 2.1	На этапе проектирования и разработки ИСПДн
С 2.2	На этапе эксплуатации
С 2.2.1	Использование нештатного ПАО
С 2.2.2	Внесение уязвимостей с использованием штатных средств
С 2.2.2.1	Обмен программами и данными, содержащими выполняемые модули (скрипты, макросы и т.д.)
С 2.2.2.2	Изменение конфигурации ПАО
С 2.2.2.3	Модификация ПО и данных
С 2.2.2.4	Разработка вредоносных программ
С 2.2.2.5	Публикация, разглашение защищаемых сведений
С 2.3	На этапе сопровождения (модернизации) ИСПДн
С 2.4	На этапе утилизации элементов автоматизированной системы

Объекты воздействия угроз безопасности ПДн

Код	Объект воздействия
D 1	Информация, обрабатываемая на АРМ (узле) вычислительной сети
D 1.1	Информация, хранящаяся на отчуждаемых носителях информации
D 1.1.1	Гибкие магнитные диски
D 1.1.2	Жесткие магнитные диски
D 1.1.3	Накопители ZIP
D 1.1.4	Накопители электронной памяти типа флэш
D 1.1.5	Аудио-, видеокассеты, магнитные ленты
D 1.1.6	Оптические компакт-диски
D 1.1.7	Сотовые телефоны, карманные компьютеры, цифровые фотоаппараты, mp3-проигрыватели
D 1.1.8	Цифровые видеокамеры
D 1.1.*	Другие устройства
D 1.2	На встроенных носителях долговременного хранения информации
D 1.2.1	Жесткие магнитные диски
D 1.2.2	Постоянные запоминающие устройства
D 1.2.3	Перепрограммируемые (перезаписываемые) запоминающие устройства

Объекты воздействия угроз безопасности ПДн

Код	Объект воздействия
D 1.3	В средствах обработки и хранения оперативной информации
D 1.3.1	Оперативная память
D 1.3.2	Кэш-память, буферы ввода-вывода
D 1.3.3	Видео-память
D 1.3.4	Оперативная память подключаемых устройств
D 1.4	В средствах (портах) ввода/вывода информации
D 1.4.1	Клавиатура
D 1.4.2	Манипулятор «мышь»
D 1.4.3	Сканер
D 1.4.4	Дисплей, монитор
D 1.4.5	Принтер
D 1.4.6	Плоттер
D 1.4.7	Приводы магнитных и оптических дисков
D 1.4.8	Порты ввода/вывода для подключения периферийных устройств
D 1.4.9	Информация о средствах (аппаратуре) передачи данных
D 1.4.*	Другие устройства ввода/вывода информации

Объекты воздействия угроз безопасности ПДн

Код	Объект воздействия
D 2	Информация в средствах, реализующих сетевое взаимодействие, и каналах передачи данных в сети
D 2.1	Информация на канальном уровне
D 2.2	Информация на сетевом уровне
D 2.3	Информация на транспортном уровне
D 2.4	Информация на сеансовом уровне
D 2.5	Информация на презентационном уровне
D 2.6	Информация на прикладном уровне

Деструктивные воздействия угроз безопасности ПДн

Код	Деструктивное воздействие
E 1	Нарушение конфиденциальности
E 1.1	Утечка информации
E 1.2	Несанкционированное копирование
E 1.3	Перехват информации в каналах передачи данных
E 1.4	Разглашение защищаемой информации
E 1.*.1	Информация, обрабатываемая на объекте
E 1.*.2	Состав и конфигурация ПАО
E 1.*.3	Состав и конфигурации СЗИ
E 2	Нарушение целостности
E 2.1	Воздействие на ПО и данные пользователя
E 2.2	Воздействие на микропрограммы, данные и драйвера устройств системы
E 2.3	Воздействие на программы, данные и драйвера устройств, обеспечивающих загрузку ОС и СЗИ
E 2.4	Воздействие на программы и данные ОС
E 2.5	Воздействие на программы и данные прикладного ПО
E 2.6	Воздействие на программы и данные специального ПО

Деструктивные воздействия угроз безопасности ПДн

Код	Деструктивное воздействие
E 2.7	Воздействие на промежуточные значения программ и данных в процессе их обработки
E 2.8	Внедрение вредоносной программы
E 2.9	Внедрение программно-аппаратной закладки
E 2.10	Воздействие на технологическую сетевую информацию
E 2.10.1	Средства управления конфигурацией сетей
E 2.10.2	Средства управления адресами и маршрутизацией передачи данных в сети
E 2.10.3	Средства управления функциональным контролем сети
E 2.10.4	Средства управления безопасностью информации в сети
E 2.11	Воздействие на СЗИ
E 3	Нарушение доступности
E 3.1	Нарушение функционирования и отказы средств обработки информации
E 3.2	Нарушение и отказы функционирования средств ввода/вывода информации
E 3.3	Нарушение и отказы функционирования средств хранения информации
E 3.4	Нарушение и отказы функционирования аппаратуры и каналов связи
E 3.5	Нарушение и отказы функционирования СЗИ

Показатели исходной защищенности

1.	По территориальному размещению:			
	распределенная ИСПДн, которая охватывает несколько областей или государство			+
	городская ИСПДн, охватывающая не более одного населенного пункта			+
	корпоративная распределенная ИСПДн		+	
	локальная (кампусная) ИСПДн, развернутая в близко расположенных зданиях		+	
	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 операциям с записями:			
	чтение, поиск;	+		
	запись, удаление, сортировка;		+	
	модификация, передача.			+

Показатели исходной защищенности

4.	По разграничению доступа к ПДн:			
	ИСПДн, к которой имеют доступ определенные перечнем сотрудники		+	
	ИСПДн, к которой имеют доступ все сотрудники организации			+
	ИСПДн с открытым доступом.			+
5.	По наличию соединений с другими базами ПДн иных ИСПДн:			
	интегрированная ИСПДн (организация использует несколько баз)			+
	ИСПДн, в которой используется одна база ПДн	+		
6.	По уровню обобщения (обезличивания) ПДн:			
	ИСПДн, в которой данные являются обезличенными	+		
	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;		+	
	ИСПДн, в которой данные не являются обезличенными			+
7.	По объему ПДн, предоставляемых сторонним пользователям			
	ИСПДн, предоставляющая всю БД с ПДн;			+
	ИСПДн, предоставляющая часть ПДн;		+	
	ИСПДн, не предоставляющая никакой информации.	+		

Исходная степень защищенности

- 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 Y1, а именно:

0 – для высокой степени исходной защищенности;

5 – для средней степени исходной защищенности;

10 – для низкой степени исходной защищенности.

Оценка вероятности угроз безопасности ПДн

- 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 СЗИ);
- 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.

Реализумость угроз безопасности ПДн

Вычисление коэффициентов реализуемости выявленных угроз (Y) в соответствии с формулой:

$$Y=(Y1+Y2)/20$$

с последующей вербальной интерпретацией полученных коэффициентов для всех выявленных угроз:

если $0<Y<0,3$, то возможность реализации угрозы признается низкой;

Если $0,3<Y<0,6$, то возможность реализации угрозы признается средней;

Если $0,6<Y<0,8$, то возможность реализации угрозы признается высокой;

если $Y>0,8$, то возможность реализации угрозы признается очень высокой.

Оценка опасности угроз безопасности ПДн

Оценки (исходя из Хк и Хо)

- низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов ПДн;
- средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов ПДн;
- высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов Пдн.

Категории (Хк)

- категория 1 – ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2 – ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1;
- категория 3 – ПДн, позволяющие идентифицировать субъекта ПДн;
- категория 4 – обезличенные и (или) общедоступные Пдн.

Объемы (Хо)

- 1 – ПДн более чем 100 000 субъектов ПДн;
- 2 – ПДн от 1000 до 100 000 субъектов ПДн;
- 3 – ПДн менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации.

Опасность и актуальность угроз безопасности ПДн

Уровень опасности

Хо Хк	3	2	1
Категория 4	низкая	низкая	низкая
Категория 3	низкая	низкая	средняя
Категория 2	низкая	средняя	высокая
Категория 1	высокая	высокая	высокая

Актуальность угроз

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