Практическое занятие №6

4 часа

Тема: Частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
Профиль защиты персональных данных в ИСПДн.
Инструкция ответственного за обеспечение безопасности ПДн.

Цель практического занятия: Получение практических навыков в разработке:

- частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
- профиля защиты персональных данных в ИСПДн;

- инструкции ответственного за обеспечение безопасности ПДн.

Задание №1.

Разработать частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Задание №2.

Разработать профиль защиты персональных данных в ИСПДн.

Задание №3.

Разработать инструкцию ответственного за обеспечение безопасности ПДн.

Отчет по практическому занятию должен быть выполнен согласно утвержденным на кафедре требованиям и содержать:

1. Тема ПЗ.
2. Цель ПЗ.
3. Частную модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.
4. Профиль защиты персональных данных в ИСПДн.
5. Инструкцию ответственного за обеспечение безопасности ПДн.
6. Выводы по заданию.
7. Заключение.
8. Список использованной литературы.

Методический материал к практическому занятию (Приложение 1).

Приложение 1.

Методический материал

4.8 Типы угроз персональных данных в информационных системах

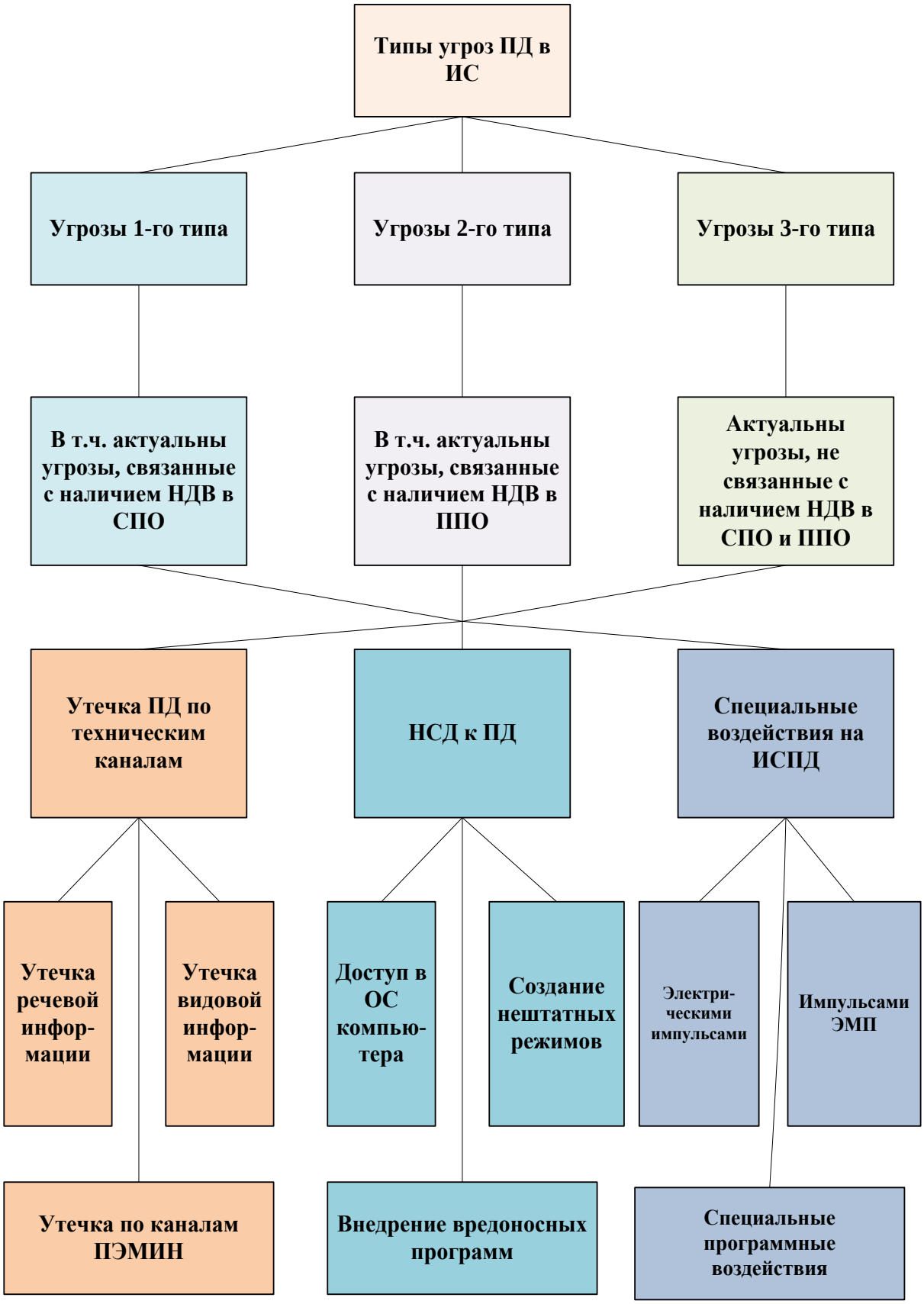

Рисунок 4.8 – Типы угроз персональных данных в ИС

4.9 Виды угроз персональных данных, обрабатываемых в АРМ, в локальных информационных системах персональных данных, в распределенных информационных системах персональных данных, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена

Рисунок 4.9 – Виды угроз персональных данных, обрабатываемых в АРМ, в локальных информационных системах персональных данных, в распределенных информационных системах персональных данных, не имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена

4.10 Виды угроз персональных данных, обрабатываемых в АРМ, в локальных информационных системах персональных данных, в распределенных информационных системах персональных данных, имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена

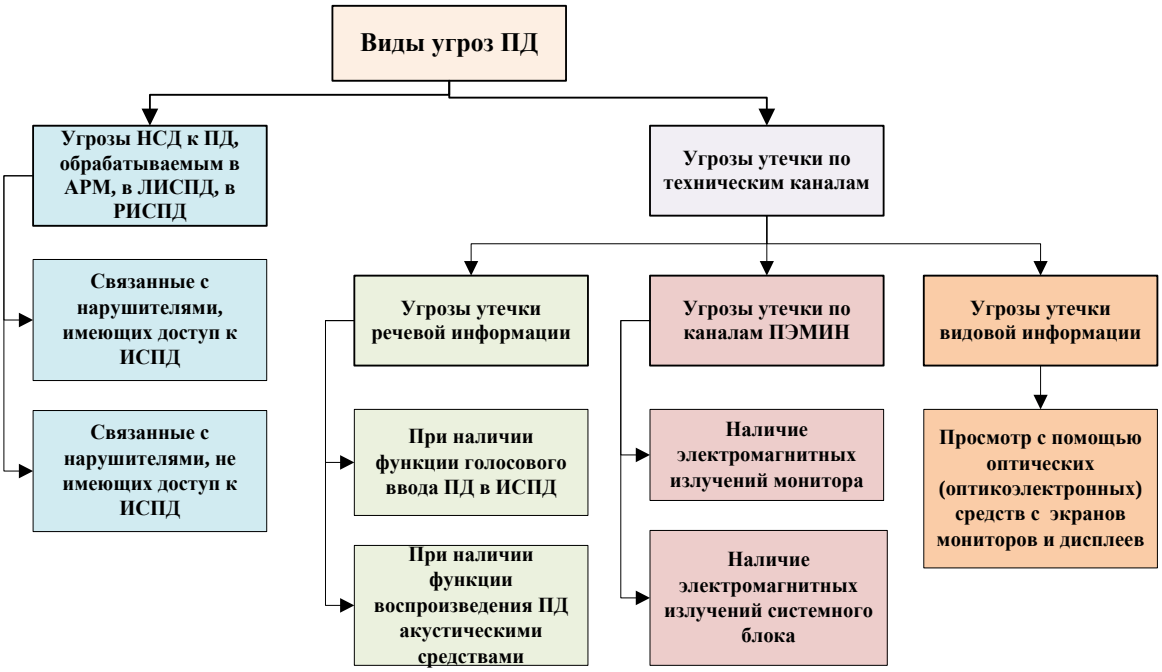

Рисунок 4.10 – Виды угроз персональных данных, обрабатываемых в АРМ, в локальных информационных системах персональных данных, в распределенных информационных системах персональных данных, имеющих подключения к сетям связи общего пользования и (или) сетям международного информационного обмена

4.11 Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных

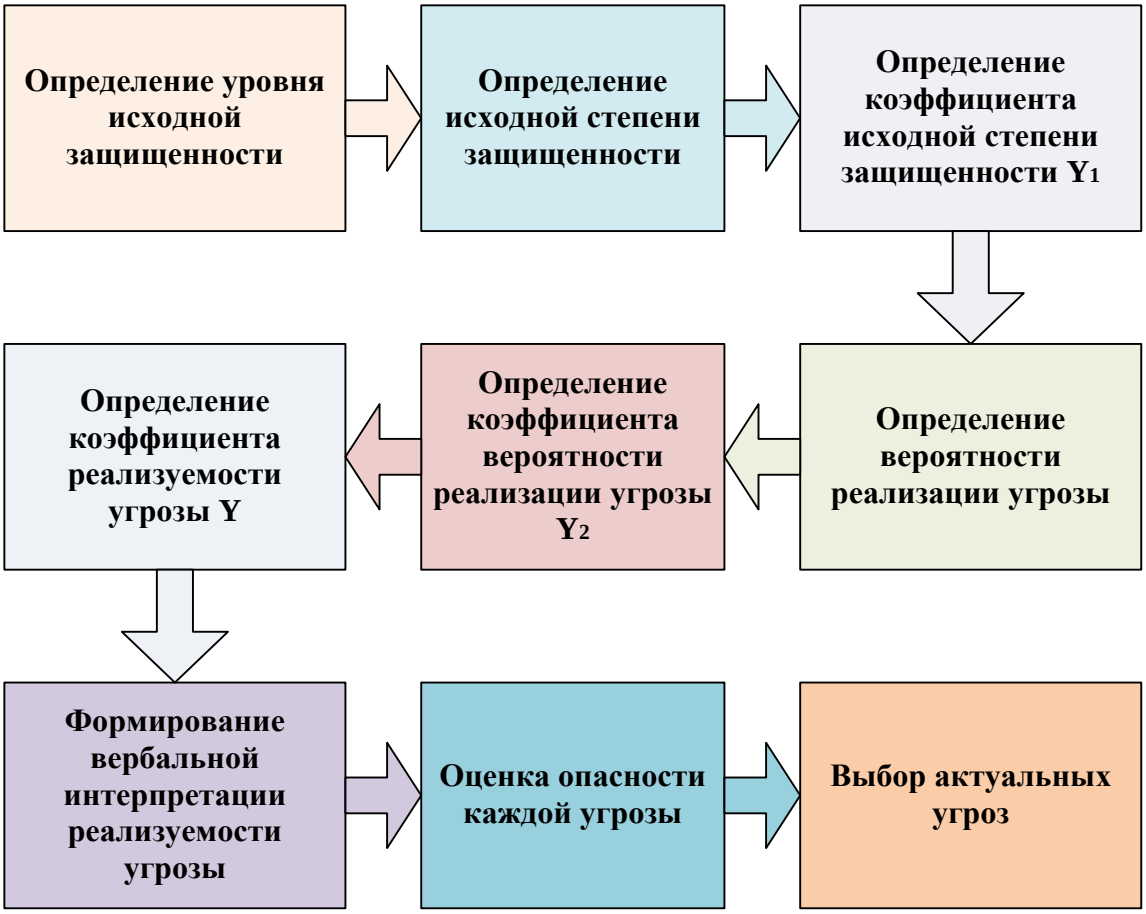

Рисунок 4.11 – Порядок составления перечня актуальных угроз

4.11.1 Определение уровня исходной защищенности

Под **уровнем исходной защищенности ИСПД** понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПД, приведенных в таблице 4.1.

Таблица 4.1 – Показатели исходной защищенности ИСПД

Технические и эксплуатационные характеристики ИСПД	Уровень защищенности		
	Высокий	Средний	Низкий
1 По территориальному размещению: распределенная ИСПД, которая охватывает несколько областей, округов или государство в целом	–	–	+
городская ИСПД, охватывающая не более одного населенного пункта (города, поселка)	–	–	+
корпоративная распределенная ИСПД, охватывающая многие подразделения одной организации	–	+	–

Продолжение таблицы 4.1

Технические и эксплуатационные характеристики ИСПД	Уровень защищенности		
	Высокий	Средний	Низкий
локальная (кампусная) ИСПД, развернутая в пределах нескольких близко расположенных зданий	–	+	–
локальная ИСПД, развернутая в пределах одного здания	+	–	–
2 По наличию соединения с сетями общего пользования: ИСПД, имеющая многоточечный выход в сеть общего пользования	–	–	+
ИСПД, имеющая одноточечный выход в сеть общего пользования	–	+	–
ИСПД, физически отделенная от сети общего пользования	+	–	–
3 По встроенным (легальным) операциям с записями баз ПД: чтение, поиск	+	–	–
запись, удаление, сортировка	–	+	–
модификация, передача	–	–	+
4 По разграничению доступа к ПД: ИСПД, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПД, либо субъект ПД	–	+	–
ИСПД, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПД	–	–	+
5 По наличию соединений с другими базами ПД иных ИСПД: интегрированная ИСПД (организация использует несколько баз ПД ИСПД, при этом организация не является владельцем всех используемых баз ПД)	–	–	+
ИСПД, в которой используется одна база ПД, принадлежащая организации – владельцу данной ИСПД	+	–	–
6 По уровню обобщения (обезличивания) ПД: ИСПД, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.)	+	–	–
ИСПД, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	–	+	–

ИСПД, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПД)	–	–	+

Продолжение таблицы 4.1

Технические и эксплуатационные характеристики ИСПД	**Уровень защищенности**		
	Высокий	**Средний**	**Низкий**
7 По объему ПД, которые предоставляются сторонним пользователям ИСПД без предварительной обработки:			
ИСПД, предоставляющая всю базу данных с ПД	–	–	+
ИСПД, предоставляющая часть ПД	–	+	–
ИСПД, не предоставляющая никакой информации	+	–	–

4.11.2 Определение исходной степени защищенности

Исходная степень защищенности определяется следующим образом:

- ИСПД имеет **высокий** уровень исходной защищенности, если не менее 70 % характеристик ИСПД соответствуют уровню «высокий» (берется отношение суммы положительные решений по первому столбцу, соответствующему высокому уровню защищенности, к общему количеству решений), а остальные – среднему уровню защищенности (положительные решения по второму столбцу);
- ИСПД имеет **средний** уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70 % характеристик ИСПД 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;
- ИСПД имеет **низкую** степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.

4.11.3 Определение коэффициента исходной степени защищенности

При составлении перечня актуальных угроз безопасности ПД 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.

4.11.4 Определение вероятности реализации угрозы

Под **частотой (вероятностью) реализации угрозы** понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПД для данной ИСПД в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя (рисунок 4.12):

- **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 ПД недостаточны;
- **высокая вероятность** – объективные предпосылки для реализации угрозы существуют, меры по обеспечению безопасности ПД не приняты.

4.11.5 Определение коэффициента вероятности реализации угрозы

При составлении перечня актуальных угроз безопасности ПД 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.

4.11.6 Определение коэффициента реализуемости угрозы

С учетом изложенного, коэффициент реализуемости угрозы Y будет определяться соотношением **Y =** $\frac{(Y1+Y2)}{20}$.

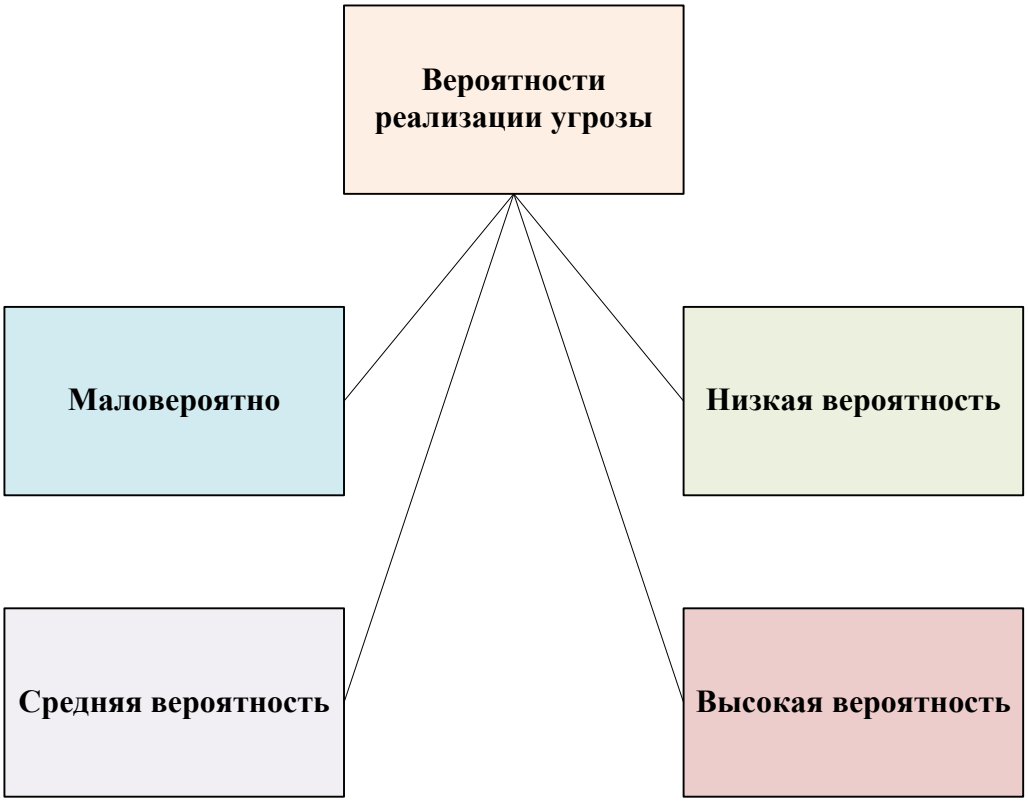

Рисунок 4.12 – Вероятности реализации угрозы

4.11.7 Формирование вербальной интерпретации реализуемости угрозы

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы (рисунок 4.13) следующим образом:

- 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**.

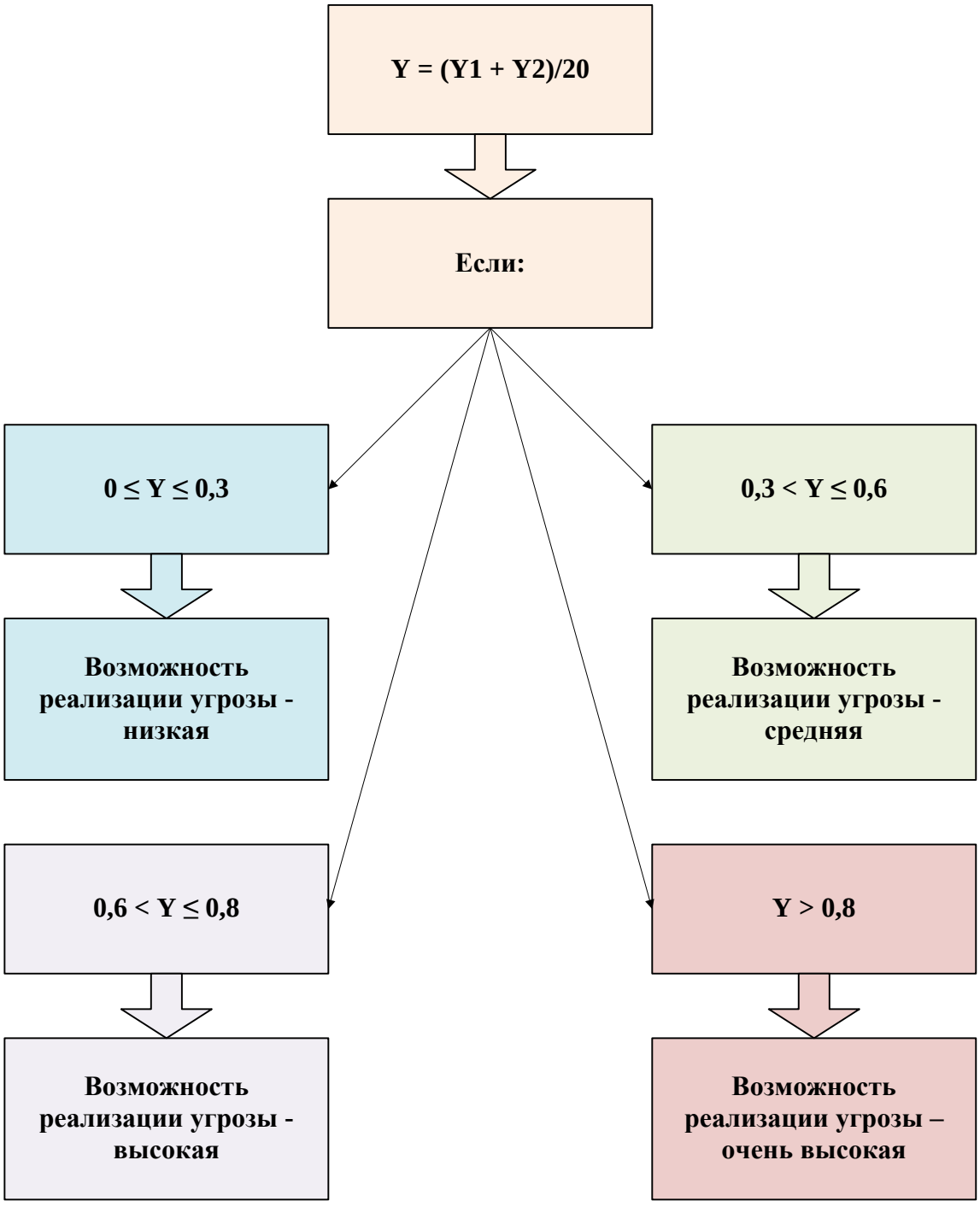

Рисунок 4.13 – Вербальная интерпреация реализуемости угрозы

4.11.8 Оценка опасности каждой угрозы

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

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

4.11.9 Выбор актуальных угроз

Затем осуществляется выбор из общего (предварительного) перечня угроз безопасности тех, которые относятся к актуальным для данной ИСПД, в соответствии с правилами, приведенными в таблице 4.2.

Таблица 4.2 – Правила отнесения угрозы безопасности ПД к актуальной

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

С использованием данных об уровне защищенности ИСПД и составленного перечня актуальных угроз, на основе «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных», формулируются конкретные организационно-технические требования по защите ИСПД от утечки информации по техническим каналам, от НСД, от специальных программных воздействий и осуществляется выбор программных и технических средств защиты информации, которые могут быть использованы при создании и дальнейшей эксплуатации ИСПД.

4.11.10 Взаимосвязь категорий, моделей нарушителя и типов угроз для ИСПД

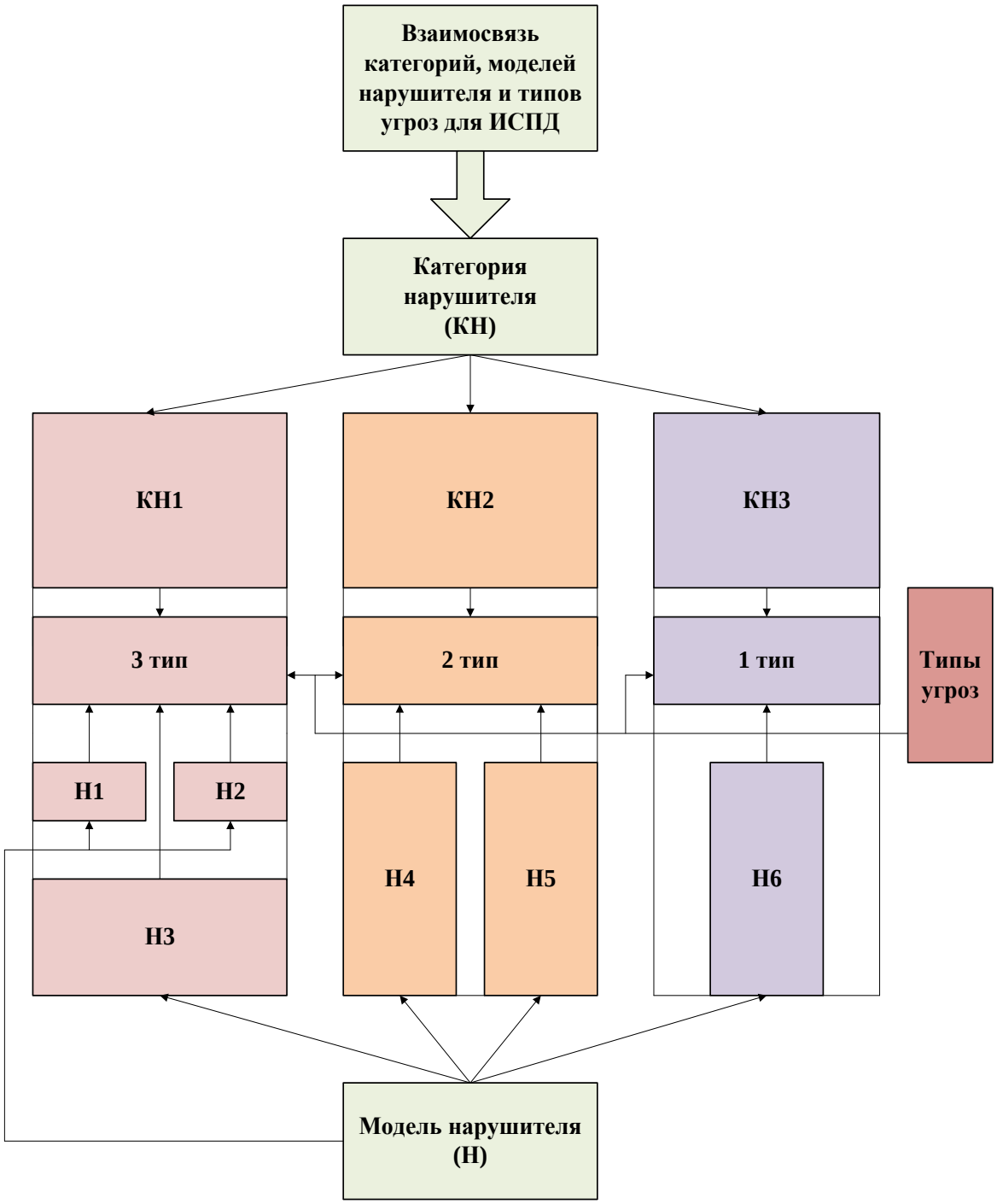

Рисунок 4.14 – Взаимосвязь категорий, моделей нарушителя и типов угроз для ИСПД

Н1 – внешний нарушитель, действующий без помощи изнутри;
Н2 – внутренний нарушитель, не являющийся пользователем СКЗИ;
Н3 – внутренний нарушитель, являющийся пользователем СКЗИ;
Н4 – нарушитель, привлекающий специалистов в области разработки СКЗИ и их анализа;
Н5 – нарушитель, привлекающий НИИ в области разработки СКЗИ и их анализа;
Н6 – спецслужбы иностранных государств.

19. 10 Базовый состав мер по обеспечению безопасности ПД

Базовый состав мер по обеспечению безопасности ПД для соответствующего уровня защищенности ПД, обрабатываемых в ИС, приведен в таблице 19.1.

Таблица 19.2 – Базовый состав мер по обеспечению безопасности ПД

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль	+	+	+	+

	соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами				
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ. 2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных,хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ. 7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.l	Обнаружение вторжений			+	+

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX.Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ. 5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов),методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ОДТ. 5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ. 8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС. 5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ЗИС. 7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС. 8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системы скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ. 5	Принятие мер по устранению последствий инцидентов			+	+

Продолжение таблицы 19.2

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ИНЦ. 6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

«+» - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.
Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.