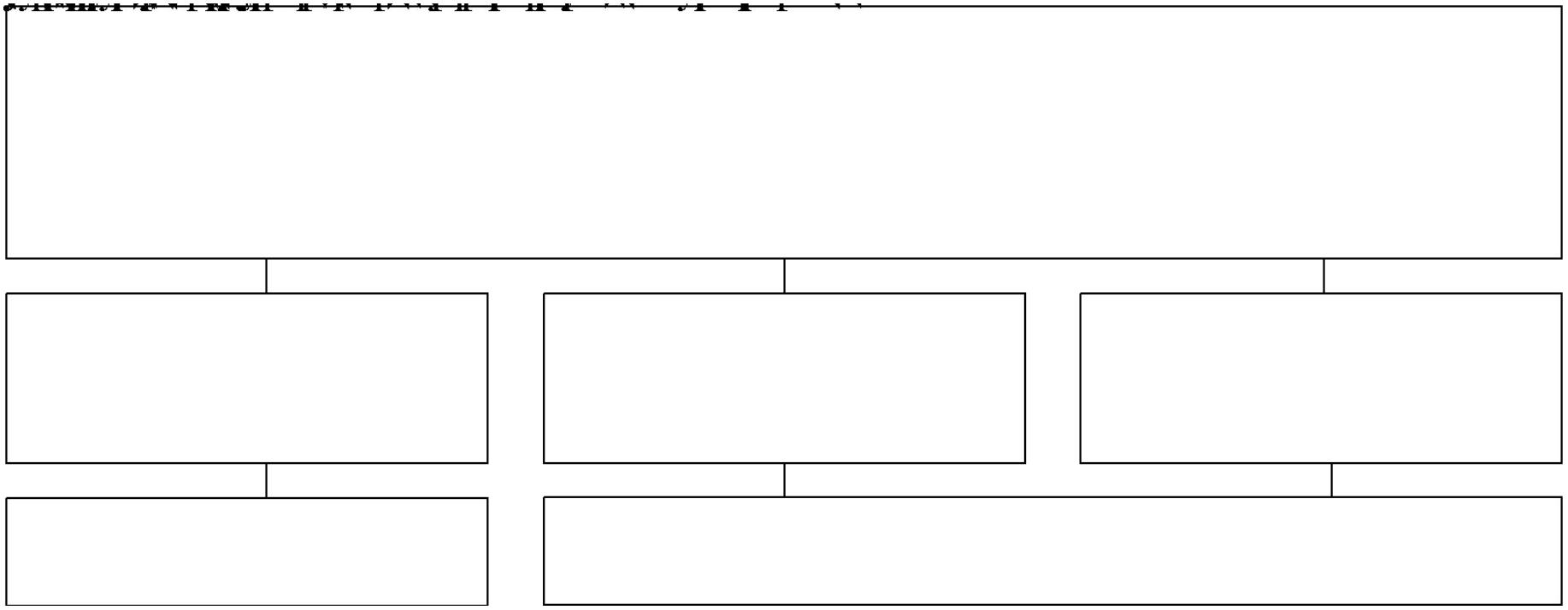
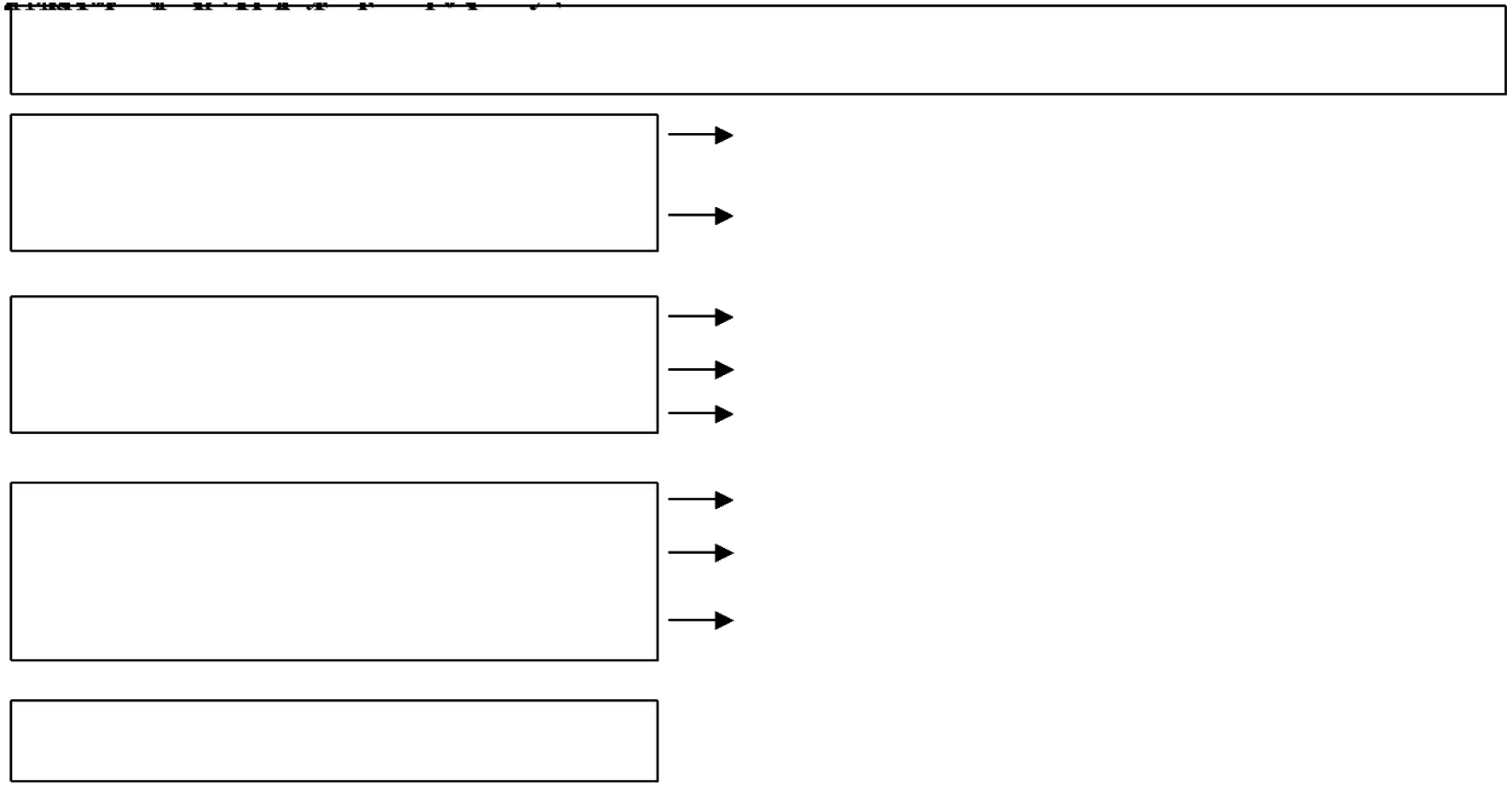
Лекция 2.
Основы проектирования системы защиты объектов информатизации

Классификация угроз безопасности информации



Формы утечки информации



Угроза (действие) - это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения и потери информации.
Фактор (уязвимость) - это присущие объекту информатизации причины, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации.
Последствия (атака) - это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся факторы (уязвимости).

Модель угроз и модель нарушителя безопасности информации

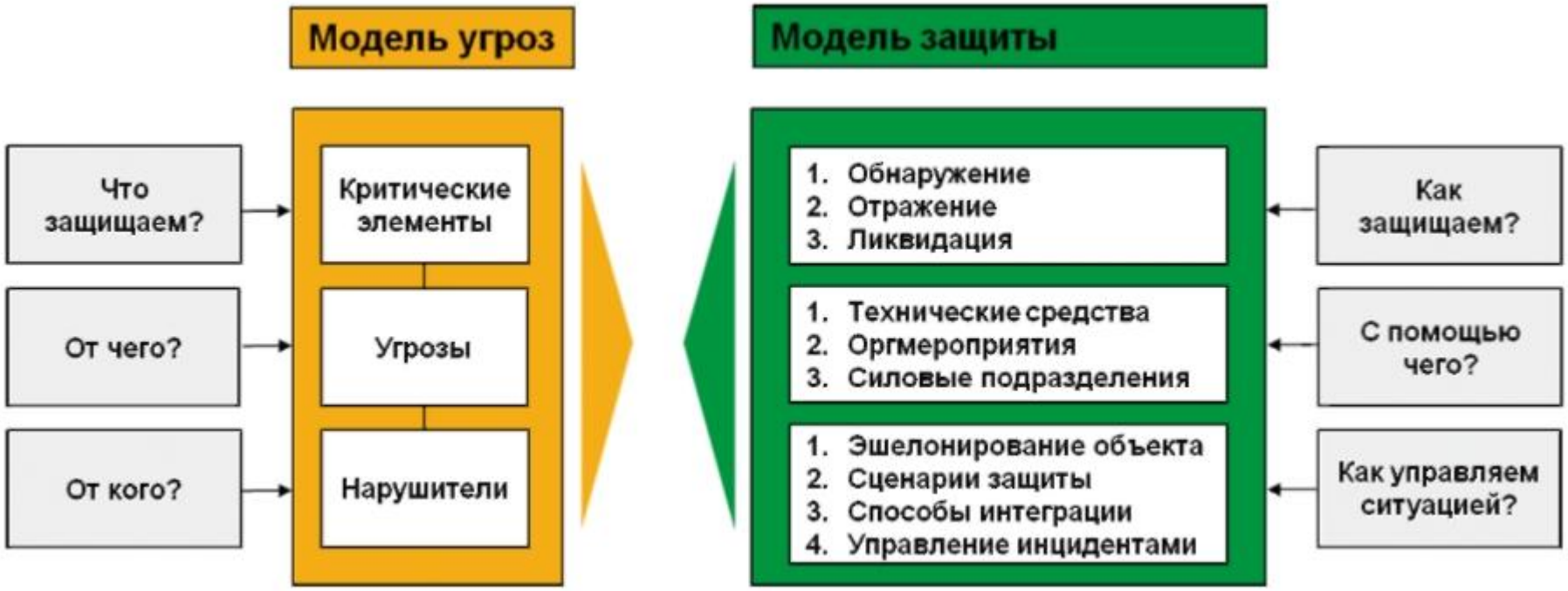
Модель угроз безопасности информации - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации (ГОСТ Р 50922-2006. Защита информации. Основные термины и определения).

Нарушитель – Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации. (ГОСТ Р 53114-2008)

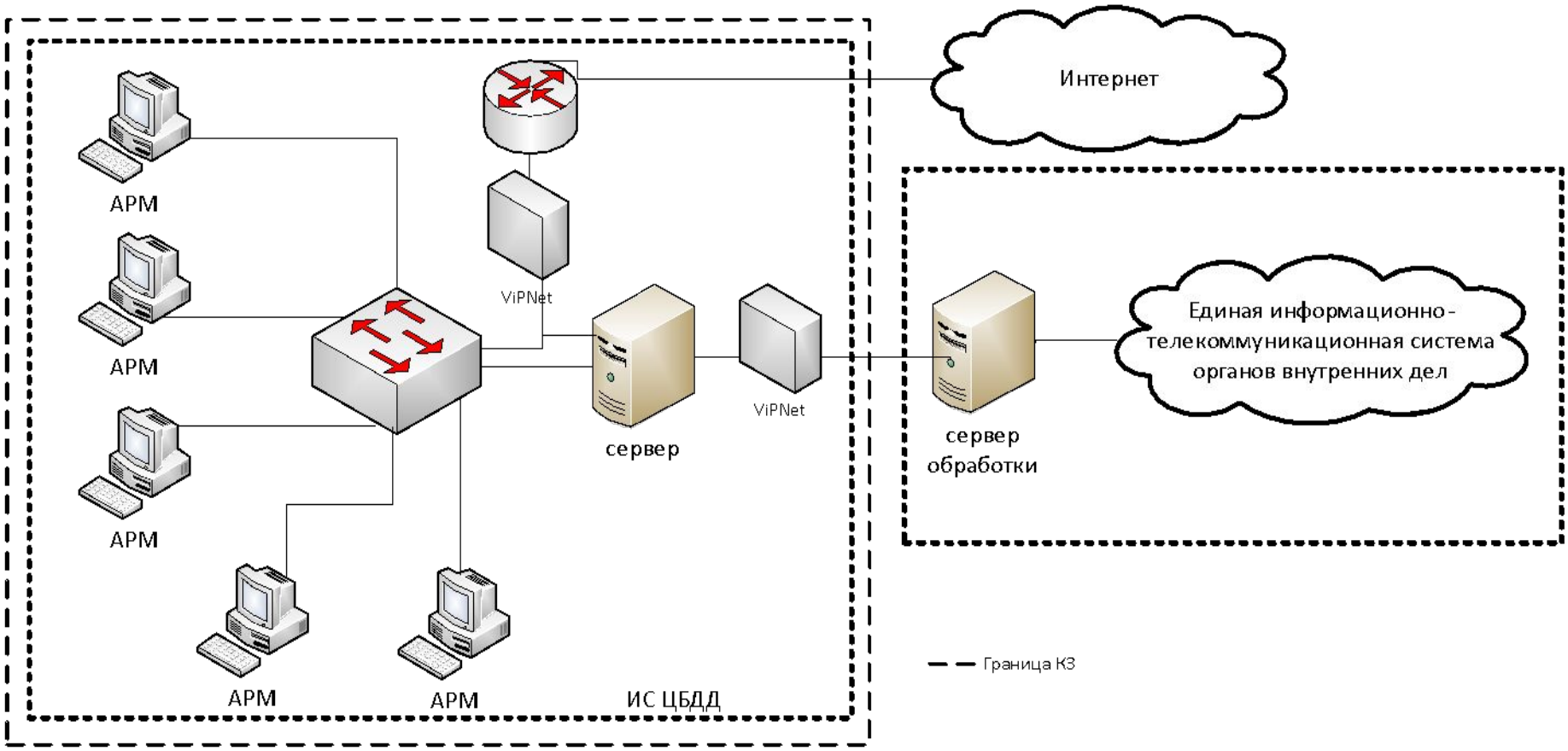
Модель нарушителя – совокупность предположений о возможностях нарушителя, которые он может использовать для разработки и проведения атак, а также об ограничениях на эти возможности.

- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России) 14 февраля 2008 г;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года №149/54-144.

Комплексный анализ угроз



Сведения об информационной системе



Модель потенциального нарушителя по требованиям ФСТЭК России

внешние нарушители - нарушители, не имеющие доступа к ИС, реализующие угрозы из внешних сетей связи общего пользования и (или) сетей международного информационного обмена;

внутренние нарушители - нарушители, имеющие доступ к ИС, включая пользователей ИС, реализующие угрозы непосредственно в ИС.

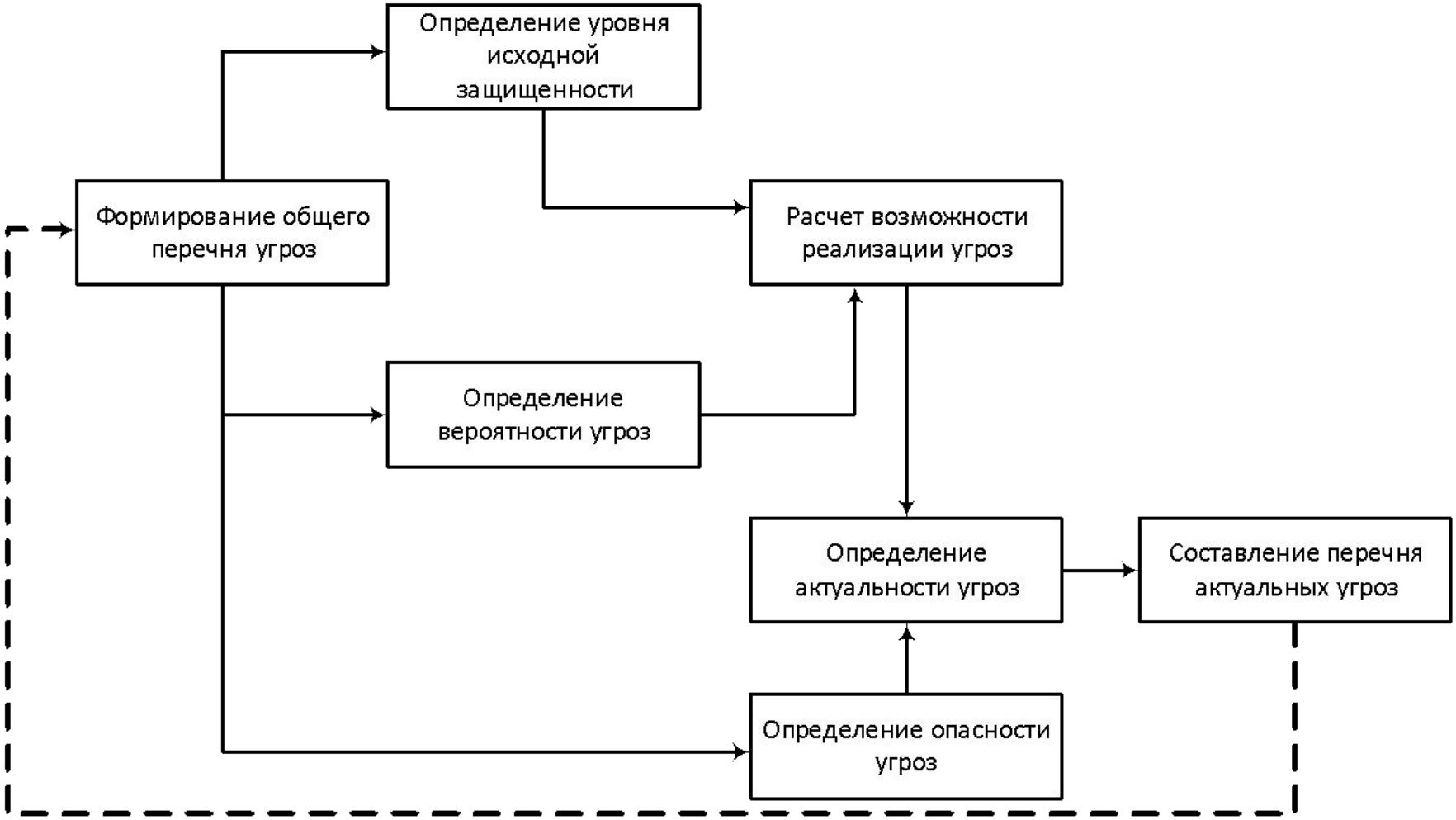
Перечень возможностей потенциальных внешних нарушителей

№	Возможности внешнего нарушителя	ИС ЦБДД
1.	возможность осуществлять несанкционированный доступ к каналам связи, выходящим за пределы служебных помещений	+
2.	возможность осуществлять несанкционированный доступ через автоматизированные рабочие места, подключенные к сетям связи общего пользования и (или) сетям международного информационного обмена	+
3.	возможность осуществлять несанкционированный доступ к информации с использованием специальных программных воздействий посредством программных вирусов, вредоносных программ, алгоритмических или программных закладок	+
4.	возможность осуществлять несанкционированный доступ через элементы информационной инфраструктуры ИС, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны	+
5.	возможность осуществлять несанкционированный доступ через информационные системы взаимодействующих ведомств, организаций и учреждений при их подключении к ИС	+

Перечень возможностей внутреннего нарушителя

№	Возможности (в т.ч. владение информацией) внутреннего нарушителя	ИС ЦБДД
1.	иметь доступ к фрагментам информации, содержащей защищаемую информацию и распространяющейся по внутренним каналам связи ИС	+
2.	располагать фрагментами информации о топологии ИС (коммуникационной части подсети) и об используемых коммуникационных протоколах и их сервисах	+
3.	располагать именами и вести выявление паролей зарегистрированных пользователей	+
4.	изменять конфигурацию технических средств ИС, вносить в нее программно-аппаратные закладки и обеспечивать съем информации, используя непосредственное подключение к техническим средствам ИС	+
5.	знает, по меньшей мере, одно легальное имя доступа	+
6.	обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации	+
7	располагает конфиденциальными данными, к которым имеет доступ	+
8	располагает информацией о топологии ИС на базе локальной и (или) распределенной информационной системы, через которую осуществляется доступ, и о составе технических средств ИС	
9	имеет возможность прямого (физического) доступа к фрагментам технических средств ИС	+
10	обладает полной информацией о системном и прикладном программном обеспечении, используемом в сегменте (фрагменте) ИС	
11	обладает полной информацией о технических средствах и конфигурации сегмента (фрагмента) ИС	+
12.	имеет доступ к средствам защиты информации и протоколирования, а также к отдельным элементам, используемым в сегменте (фрагменте) ИС	
13.	имеет доступ ко всем техническим средствам сегмента (фрагмента) ИС	+
14.	обладает правами конфигурирования и административной настройки некоторого подмножества технических средств сегмента (фрагмента) ИС	
15.	обладает полной информацией о системном и прикладном программном обеспечении ИС	
16.	обладает полной информацией о технических средствах и конфигурации ИС	
17.	имеет доступ ко всем техническим средствам обработки информации и данным ИС	
18.	обладает правами конфигурирования и административной настройки технических средств ИС	

Алгоритм процесса построения модели угроз



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;	–	+	–
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;	–	–	+

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
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.	+	–	–

Определение уровня исходной защищенности Y_1

п/п	Технические и эксплуатационные характеристики ИСПДн	Высокая	Средняя	Низкая
1.По территориальному размещению				
1.1.	распределённая ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом;			
1.2.	городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка);			
1.3.	корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации;			
1.4.	локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;			
1.5.	локальная ИСПДн, развернутая в пределах одного здания.	V		
2.По наличию соединения с сетями общего пользования:				
2.1.	ИСПДн, имеющая многоточечный выход в сеть общего пользования;			
2.2.	ИСПДн, имеющая одноточечный выход в сеть общего пользования;		V	
2.3.	ИСПДн, физически отделенная от сети общего пользования.			
3.По встроенным (легальным) операциям с записями баз персональных данных:				
3.1.	чтение, поиск;			
3.2.	запись, удаление, сортировка;			
3.3.	модификация, передача.			V

4. По разграничению доступа к персональным данным:				
4.1.	ИСПДн, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн;		V	
4.2.	ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			
4.3.	ИСПДн с открытым доступом.			
5.По наличию соединений с другими базами ПДн иных ИСПДн				
5.1.	интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			
5.2.	ИСПДн, в которой используется одна база ПДн, принадлежащая организации-владельцу данной ИСПДн.			V
6. По уровню (обезличивания) ПДн:				
6.1.	ИСПДн в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области, региона и т.д.);			
6.2.	ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации;			
6.3.	ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта ПДн).			V
7.По объему ПДн, которые предоставляются сторонним пользователям без обработки:				
7.1.	ИСПДн, предоставляющая всю БД с ПДн;			
7.2.	ИСПДн, предоставляющая часть ПДн;		V	
7.3.	ИСПДн, не предоставляющие никакой информации.			
7.4.	Количество баллов по уровням	2	3	2
7.5.	Уровень исходной защищенности ИСПДн	средний		
7.6.	Коэффициент защищенности ИСПДн (Y1)	5		

Вероятность реализации угроз Y2

Градация	Описание	Вероятность (Y2)
Маловероятно	маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);	0
Низкая вероятность	низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);	2
Средняя вероятность	средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;	5
Высокая вероятность	высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.	10

Коэффициент реализуемости угрозы

По итогам оценки уровня исходной защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы рассчитывается по формуле:

$$Y=(Y_1+Y_2)/20.$$

По значению коэффициента реализуемости угрозы ***Y*** формируется вербальная интерпретация возможности реализации угрозы 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.

Оценка вероятности и возможности реализации угрозы безопасности

№ п/п	Угрозы безопасности ПДн	Вероятность реализации угрозы Y_2	Возможность реализации угрозы Y
1. Угрозы нарушения процессов идентификации и аутентификации субъектов и объектов доступа			
1	Подмена субъекта доступа	Средняя	Средняя
2	Подмена объекта доступа	Средняя	Средняя
3	Нарушение функционирования средств идентификации и аутентификации	Низкая	Средняя
2. Угрозы нарушения доступа субъектов доступа к объектам доступа			
3.1	Несанкционированное изменение учетных записей пользователей ИСПДн	Низкая	Средняя
3.2	Компрометация учетных записей пользователей ИСПДн	Средняя	Средняя
3.3	Создание неучтенных точек входа (авторизации) в ИСПДн	Низкая	Средняя
3. Угрозы нарушения функциональных возможностей ИСПДн			
4.1	Внедрение недекларированных возможностей в СПО	Маловероятно	Низкая
4.2	Внедрение недекларированных возможностей в ППО	Маловероятно	Низкая
4.3	Умышленное нарушение режимов функционирования ТС и ПО	Маловероятно	Низкая
4.4	Сбои в работе ТС и ПО	Маловероятно	Низкая
	Угрозы непосредственного доступа к среде ИСПДн		
5.1	Доступ к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн	Средняя	Средняя
5.2	Несанкционированный доступ в операционную среду	Низкая	Средняя
5.3	Доступ в среду функционирования прикладных программ	Низкая	Средняя
5.4	Доступ непосредственно к информации, обрабатываемой в ИСПДн	Низкая	Средняя

6. Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия			
6.1	Сканирование сети для изучения логики работы ИСПДн, выявление протоколов, портов	Маловероятно	Низкая
6.2	Перехват идентификационной и аутентификационной информации по каналам связи	Маловероятно	Низкая
6.3	Подмена доверенного объекта сети с присвоением его прав доступа	Маловероятно	Низкая
6.4	Навязывание ложного маршрута сети	Маловероятно	Низкая
6.5	Удаленный запуск приложений	Средняя	Средняя
6.6	Отказ в обслуживании пользователей компонентами ИСПДн	Средняя	Средняя
7. Угрозы несанкционированного физического доступа к компонентам ИСПДн			
7.1	Утрата машинного носителя	Маловероятно	Низкая
7.2	Утрата мобильных технических средств	Маловероятно	Низкая
7.3	Нарушение сетевой коммутации	Маловероятно	Низкая
	Угрозы неправомерных действий со стороны лиц, имеющих право доступа к ИСПДн		
8.1	Сокрытие ошибок и неправомерных действий пользователей и администраторов	Низкая	Средняя
8.2	Передача защищаемой информации по открытым каналам связи	Маловероятно	Низкая
8.3	Передача машинного носителя лицам, не имеющим права доступа к хранимой на нем информации	Низкая	Средняя
8.4	Передача мобильных технических средств лицам, не имеющим права доступа к обрабатываемой на них информации	Маловероятно	Низкая
8.5	Установка ПО, не связанного с использованием служебных обязанностей	Низкая	Средняя
9. Угрозы виртуальной инфраструктуре ИСПДн			
9.1	Доступ к средствам управления виртуальной инфраструктуры	Маловероятно	Низкая
9.2	Нарушение конфигурации компонентов виртуальной инфраструктуры	Маловероятно	Низкая
9.3	Нарушение среды функционирования виртуальной инфраструктуры	Маловероятно	Низкая
9.4	Подмена и/или перехват данных в оперативной памяти виртуальных машин	Маловероятно	Низкая

Показатель опасности угрозы

Показатель опасности угрозы	Показатель опасности (описание)
Низкий	Незначительные негативные последствия для организации или субъектов ПДн при реализации угрозы
Средний	Негативные последствия для организации или субъектов ПДн при реализации угрозы
Высокий	Значительные негативные последствия для организации или субъектов ПДн при реализации угрозы

Матрица определения актуальности угроз безопасности

Возможность реализации угрозы	Показатель опасности		
	Низкий	Средний	Высокий
Низкая	Неактуальна	Неактуальна	Актуальна
Средняя	Неактуальна	Актуальна	Актуальна
Высокая	Актуальна	Актуальна	Актуальна
Очень высокая	Актуальна	Актуальна	Актуальна

Оценка опасности и актуальности угроз предложенной информационной системы

№ п/п	Угрозы безопасности	Показатель опасности угрозы	Актуальность угрозы
1.	**Угрозы нарушения процессов идентификации и аутентификации субъектов и объектов доступа**		
1.1	Подмена субъекта доступа	Средний	Актуальная
1.2	Подмена объекта доступа	Средний	Актуальная
1.3	Нарушение функционирования средств идентификации и аутентификации	Средний	Актуальная
	2Угрозы нарушения доступа субъектов доступа к объектам доступа		
2.1	Несанкционированное изменение учетных записей пользователей ИСПДн	Средний	Актуальная
2.2	Компрометация учетных записей пользователей ИСПДн	Высокий	Актуальная
2.3	Создание неучтенных точек входа (авторизации) в ИСПДн	Средний	Актуальная
	3. Угрозы нарушения функциональных возможностей ИС		
3.1	Внедрение недекларированных возможностей в СПО	Средний	Неактуальная
3.2	Внедрение недекларированных возможностей в ППО	Средний	Неактуальная
3.3	Умышленное нарушение режимов функционирования ТС и ПО	Средний	Неактуальная
3.4	Сбои в работе ТС и ПО	Средний	Неактуальная
	4. Угрозы непосредственного доступа к среде ИС		
4.1	Доступ к информации и командам, хранящимся в базовой системе ввода/вывода (BIOS) ИСПДн	Высокий	Актуальная
4.2	Несанкционированный доступ в операционную среду	Средний	Актуальная
4.3	Доступ в среду функционирования прикладных программ	Средний	Актуальная
4.4	Доступ непосредственно к информации, обрабатываемой в ИСПДн	Высокий	Актуальная

5. Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия			
5.1	Сканирование сети для изучения логики работы ИСПДн, выявление протоколов, портов	Средний	Неактуальная
5.2	Перехват идентификационной и аутентификационной информации по каналам связи	Средний	Неактуальная
5.3	Подмена доверенного объекта сети с присвоением его прав доступа	Средний	Неактуальная
5.4	Навязывание ложного маршрута сети	Средний	Неактуальная
5.5	Удаленный запуск приложений	Средний	Актуальная
5.6	Отказ в обслуживании пользователей компонентами ИСПДн	Средний	Актуальная
6. Угрозы несанкционированного физического доступа к компонентам ИС			
6.1	Утрата машинного носителя	Средний	Неактуальная
6.2	Утрата мобильных технических средств	Средний	Неактуальная
6.3	Нарушение сетевой коммутации	Низкий	Неактуальная
7. Угрозы неправомерных действий со стороны лиц, имеющих право доступа к ИС			
7.1	Сокрытие ошибок и неправомерных действий пользователей и администраторов	Высокий	Актуальная
7.2	Передача защищаемой информации по открытым каналам связи	Средний	Неактуальная
7.3	Передача машинного носителя лицам, не имеющим права доступа к хранимой на нем информации	Высокий	Актуальная
7.4	Передача мобильных технических средств лицам, не имеющим права доступа к обрабатываемой на них информации	Средний	Неактуальная
7.5	Установка ПО, не связанного с использованием служебных обязанностей	Высокий	Актуальная
8. Угрозы виртуальной инфраструктуре ИС			
8.1	Доступ к средствам управления виртуальной инфраструктуры	Средний	Неактуальная
8.2	Нарушение конфигурации компонентов виртуальной инфраструктуры	Средний	Неактуальная
8.3	Нарушение среды функционирования виртуальной инфраструктуры	Средний	Неактуальная
8.4	Подмена и/или перехват данных в оперативной памяти виртуальных машин	Средний	Неактуальная

Домашнее задание № 1
Тема: «Модель угроз и модель нарушителей информационной безопасности". Схемы проектирования.

- Предложить ИСПДн, обозначить назначение и исходные данные.
- Определить исходный уровень защищенности ПДн по исходным данным.
- Определить актуальность угроз безопасности информации согласно банку угроз ФСТЭК России.

Вариант	Исходные данные
1	УБИ. 088, УБИ. 074, УБИ. 193, УБИ. 140, УБИ. 139
2	УБИ. 088, УБИ. 156, УБИ. 140, УБИ. 038, УБИ. 145
3	УБИ. 086, УБИ. 083, УБИ. 104, УБИ. 128, УБИ. 140
4	УБИ. 156, УБИ. 152, УБИ. 157, УБИ. 205, УБИ. 128
5	УБИ. 168, УБИ. 212, УБИ. 015, УБИ. 086 УБИ. 205
6	УБИ. 145, УБИ. 091, УБИ. 067, УБИ. 128, УБИ. 190
7	УБИ. 158, УБИ. 167, УБИ. 179, УБИ. 156, УБИ. 074
8	УБИ. 190, УБИ. 205, УБИ. 104, УБИ. 179, УБИ. 091
9	УБИ. 139, УБИ. 167, УБИ. 193, УБИ. 038, УБИ. 128
10	УБИ. 145, УБИ. 083, УБИ. 015, УБИ. 167, УБИ. 088
11	УБИ. 074, УБИ. 193, УБИ. 152, УБИ. 145, УБИ. 083
12	УБИ. 212, УБИ. 091, УБИ. 158, УБИ. 156, УБИ. 074

Банк данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru).

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ «УМНЫЙ ДОМ»

Угроза	Влияние на систему	Подверженность	Вероятность
Атака хакеров	Высокое	Высокая	Высокая
Перехват информации	Среднее	Средняя	Средняя
Вирусы	Высокое	Высокая	Высокая
Доступ к сети несанкционированного пользователя (кража)	Среднее	Средняя	Среднее
Утечка через ПЭМИН	Среднее	Средняя	Средняя

Понятия информационной безопасности: что защищать?

ЧТО ТАКОЕ ОБЪЕКТ ИНФОРМАТИЗАЦИИ?

«Объект информатизации - совокупность

- *информационных ресурсов,*
- *средств и систем обработки информации, используемых в соответствии с заданной информационной технологией,*
- *средств обеспечения объекта информатизации,*
- *помещений или объектов (зданий, сооружений, технических средств), в которых они установлены,*

или помещения и объекты, предназначенные для ведения конфиденциальных переговоров»

Понятия информационной безопасности: что защищать?

ЧТО ТАКОЕ АВТОМАТИЗАИРОВАННАЯ СИСТЕМА?

«Автоматизированная система – система, состоящая из

- *персонала*
- *комплекса средств автоматизации его деятельности,*

реализующая информационную технологию выполнения установленных функций»

ГОСТ 34.003-90

Понятия информационной безопасности: что защищать?

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ СИСТЕМА?

«Информационная система – совокупность

- *содержащейся в базах данных информации*
- *обеспечивающих ее обработку информационных технологий и технических средств»*

Федеральный закон от 27 июля 2006 г. № 149-ФЗ
«Об информации, информационных технологиях
и защите информации»

Стандарты ГОСТ Р и ГОСТ РВ по защите информации

- **ГОСТ Р 50739–95** Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования
- **ГОСТ Р 50922-2006** Защита информации. Основные термины и определения
- **ГОСТ Р 51275–2006** Защита информации. Факторы, воздействующие на информацию. Общие положения.
- **ГОСТ Р 53114-2008** Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

2.1 Общие понятия

2.1.1 **защита информации; ЗИ:** Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

2.2 Термины, относящиеся к видам защиты информации

2.2.1 **правовая защита информации:** Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

2.3 Термины, относящиеся к способам защиты информации

2.3.1 **способ защиты информации:** Порядок и правила применения определенных принципов и средств защиты информации.

2.3.2 **защита информации от утечки:** Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами.

П р и м е ч а н и е - Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

2.3 Термины, относящиеся к способам защиты информации

……

2.3.6 **защита информации от несанкционированного доступа; ЗИ от НСД:** Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

П р и м е ч а н и е - Заинтересованными субъектами, осуществляющими несанкционированный доступ к защищаемой информации, могут быть: государство, юридическое лицо, группа физических лиц, в том числе общественная организация, отдельное физическое лицо.

Защита информации *- комплекс целенаправленных мероприятий ее собственников по предотвращению утечки, искажения, уничтожения и модификации защищаемых сведений.*

Система защиты информации *- это совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами по защите информации;*

Мероприятия по защите информации *определяет совокупность действий по разработке и/или практическому применению способов и средств защиты информации, а мероприятие по контролю эффективности защиты информации - совокупность действий по разработке и/или практическому применению методов (способов) и средств контроля эффективности защиты информации.*

Обеспечение защиты информации от

хищения
утраты
искажения
уничтожения
утечки

← за счет НСД и специальных воздействий

Обеспечение защиты информации от

утечки ← по техническим каналам

↘ *при* ↘

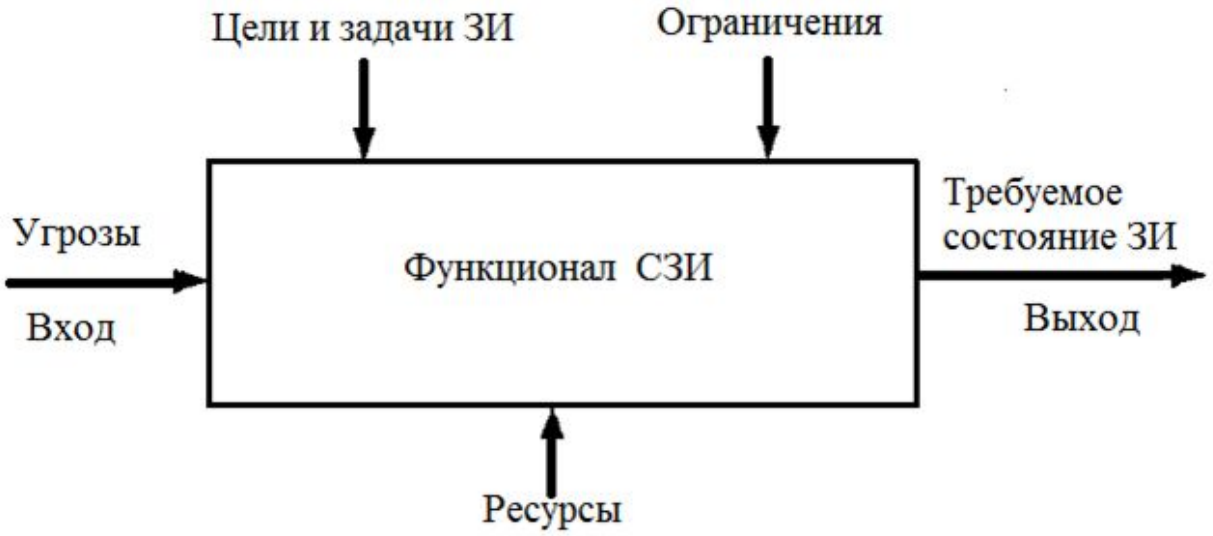
обработке
хранении
передаче по каналам связи

Защита информации является **слабоформализуемой задачей**, то есть не имеет формальных методов решения, и характеризуется следующим:

- большое количество факторов, влияющих на построение эффективной защиты;
- отсутствие точных исходных входных данных;
- отсутствие математических методов получения оптимальных результатов по совокупности исходных данных.

Параметры системы защиты информации:

- цели и задачи;
- входы и выходы системы;
- процессы внутри системы, которые преобразуют входы в выходы.



Обеспечение информационной безопасности

ГОСТ РВ 15.002-2003	ГОСТ РВ 0015-002-2012
4.3.2 В организации должны быть разработаны и согласованы с ПЗ процедуры по обеспечению: порядка разработки, обращения и хранения секретных и несекретных документов, допуска и ознакомления с ними, определена степень секретности документов; организации пропускного, объектового и внутриобъектового режимов, охраны организации в целом и рабочих помещений.	**4.3.2** В организации должно быть определено подразделение (ответственный), осуществляющее **менеджмент информационной безопасности** на всех этапах жизненного цикла военной продукции. **4.3.3** При наличии соответствующих требований в контрактах (договорах) в организации должен быть определен и документально оформлен порядок выполнения работ по обеспечению информационной безопасности **в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001.**

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

3.2 Термины, относящиеся к объекту защиты информации

3.2.1 информационная безопасность организации; ИБ организации: Состояние защищенности интересов организации в условиях угроз в информационной сфере.

П р и м е ч а н и е - Защищенность достигается обеспечением совокупности свойств информационной безопасности - ***конфиденциальностью, целостностью, доступностью*** информационных активов и инфраструктуры организации. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации.

3.2.2 объект защиты информации: Информация или носитель информации, или информационный процесс, которую(ый) необходимо защищать в соответствии с целью защиты информации.

Информационные ресурсы по категориям доступа

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

3.2.7 инцидент информационной безопасности: Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

П р и м е ч а н и е - Инцидентами информационной безопасности являются:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

3.2.17 ……

3.2.18 политика информационной безопасности (организации); политика ИБ (организации): Формальное изложение правил поведения, процедур, практических приемов или руководящих принципов в области информационной безопасности, которыми руководствуется организация в своей деятельности.

П р и м е ч а н и е - Политики должны содержать:

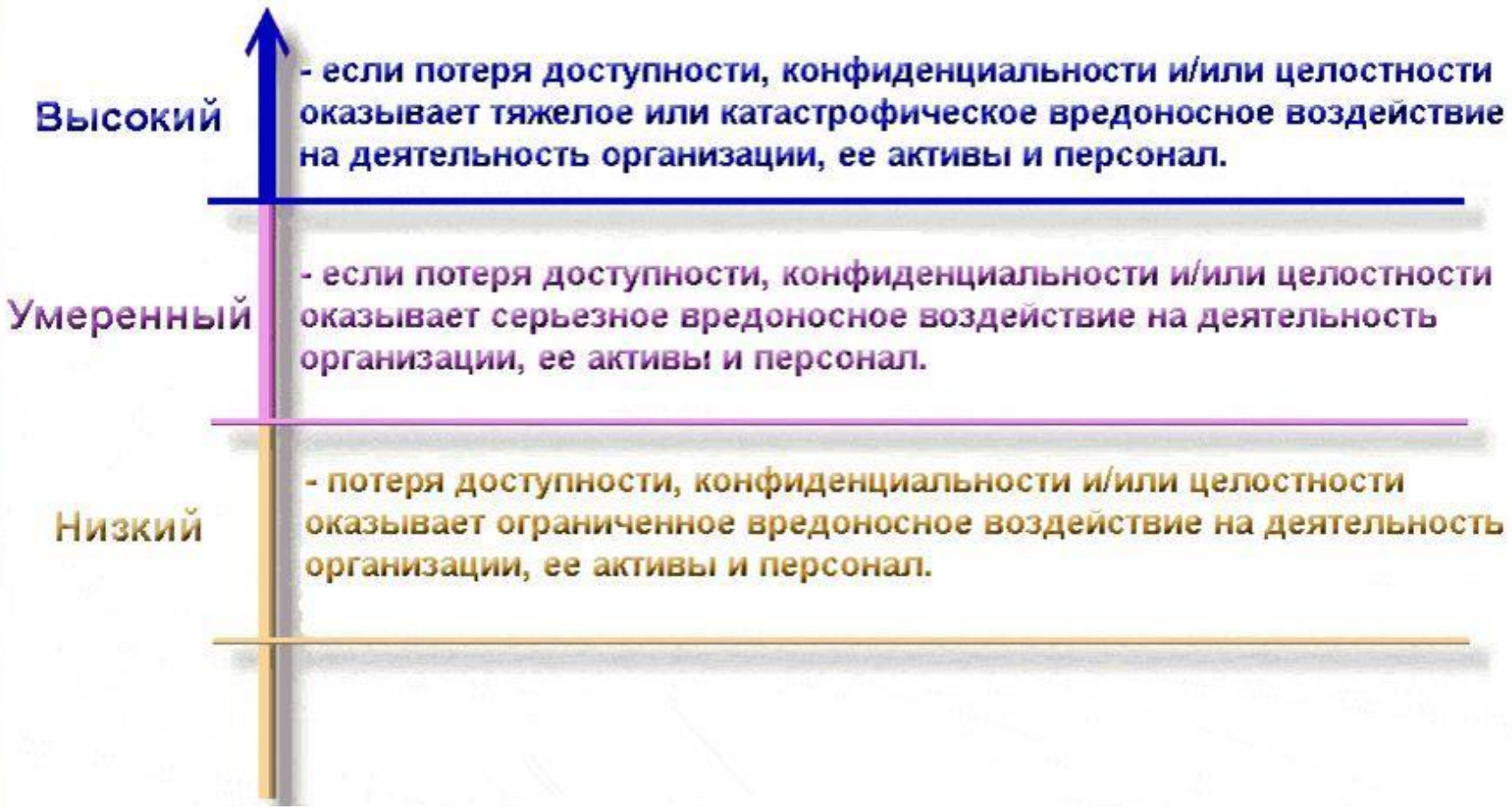
- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства организации в отношении выполнения политики безопасности и организации режима информационной безопасности организации в целом;
- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности организации:
- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

Объективные факторы ИБ:

- угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;
- уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;
- риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает *вероятные финансовые потери* – прямые или косвенные).

Модель построения корпоративной системы защиты информации

Шкала оценки ущерба при нарушении информационной безопасности



Защита информации - комплекс целенаправленных мероприятий ее собственников по предотвращению утечки, искажения, уничтожения и модификации защищаемых сведений.
Под системой защиты информации можно понимать государственную систему защиты информации и систему защиты информации на конкретных объектах.

Система защиты информации - это совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно - распорядительными и нормативными документами по защите информации;

Мероприятия по защите информации определяет совокупность действий по разработке и/или практическому применению способов и средств защиты информации, а мероприятие по контролю эффективности защиты информации - совокупность действий по разработке и/или практическому применению методов (способов) и средств контроля эффективности защиты информации.

Цикл создания КСЗИ

Государственная система защиты информации включает в себя:

• систему государственных нормативных актов, стандартов, руководящих документов и требований;

• разработку концепций, требований, нормативно-технических документов и научно-методических рекомендаций по защите информации;

• порядок организации, функционирования и контроля за выполнением мер, направленных на защиту информации, являющейся собственностью государства, а также рекомендаций по защите информации, находящейся в собственности физических и юридических лиц;

• организацию испытаний и сертификации средств защиты информации;

• создание ведомственных и отраслевых координационных структур для защиты информации;

• осуществление контроля за выполнением работ по организации защиты информации;

• определение порядка доступа юридических и физических лиц иностранных государств к информации, являющейся собственностью государства, или к информации физических и юридических лиц, относительно распространения и использования которой государством установлены ограничения.

Государственная система защиты информации:

- Система лицензирования деятельности предприятий в области ЗИ;
- Система сертификации средств ЗИ;
- Система аттестации.

Цели защиты информации от технических средств разведки

• предотвращение утечки, хищения, утраты, искажения, подделки информации;

• предотвращение угроз безопасности личности, общества, государства;

• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

• предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

• защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

• сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

• обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Эффективность защиты информации определяется ее своевременностью, активностью, непрерывностью и комплексностью. Очень важно проводить защитные мероприятия комплексно, то есть обеспечивать нейтрализацию всех опасных каналов утечки информации (та как даже один-единственный не закрытый канал утечки может свести на нет эффективность всей системы защиты).

Модель комплексной защиты информации


Организация защиты информации
Система защиты информации
Мероприятия по защите информации
Мероприятия по контролю эффективности защиты информации
Органы и/или исполнители
Техника ЗИ
Объект ЗИ
Способы ЗИ
Лицензирование
Категорирование
Аттестация
Сертификация
Методы контроля эффективности ЗИ
Контроль состояния ЗИ
Контроль организации ЗИ
Контроль эффективности ЗИ
Организационный контроль
Технический контроль


МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ
ОРГАНИЗАЦИОННО-ПРАВОВЫЕ
ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ
Физические
Аппаратные
Программные
Криптографические

Организация и проведение работ по защите информации

Порядок организации работ по созданию и эксплуатации объектов информатизации определяется в разрабатываемом на предприятии «Руководстве по защите информации» или в специальном «Положении о порядке организации и проведении работ по ЗИ».

Эти документы должны предусматривать:

- порядок определения защищаемой информации;
- порядок привлечения подразделений предприятия, специалистов сторонних организаций к разработке и эксплуатации СЗИ объекта информатизации;
- порядок взаимодействия всех занятых сил;
- порядок разработки, ввода в действие и эксплуатации объекта информатизации;
- ответственность должностных лиц.


Защита информациинот НСД
Подсистема управления доступом
Подсистема регистрации и учета
Подсистема обеспечения целостности
Подсистема анализа защищенности (сканер безопасности)
Подсистема межсетевого экранирования и криптографической защиты информации
Подсистема антивирусной защиты и обнаружения вторжений
СЗИ от НСД Secret Net
Аппаратно-программный модуль доверенной загрузки «Соболь»
СЗИ от НСД Dallas Lock
СЗИ от НСД Страж NT
СЗИ от НСД «Аккорд»
Программно-аппаратные средства аутентификации:
Электронный ключ eToken
Идентификатор iButton
Идентификатор ruToken
средство анализа защищенности XSpider
Программно-аппаратный комплекс ViPNet CUSTOM
ПАК ФПСУ-IP
Cisco Virtual Security Gateway
Kaspersky Endpoint Security
Dr. Web
АПКШ «Континент»