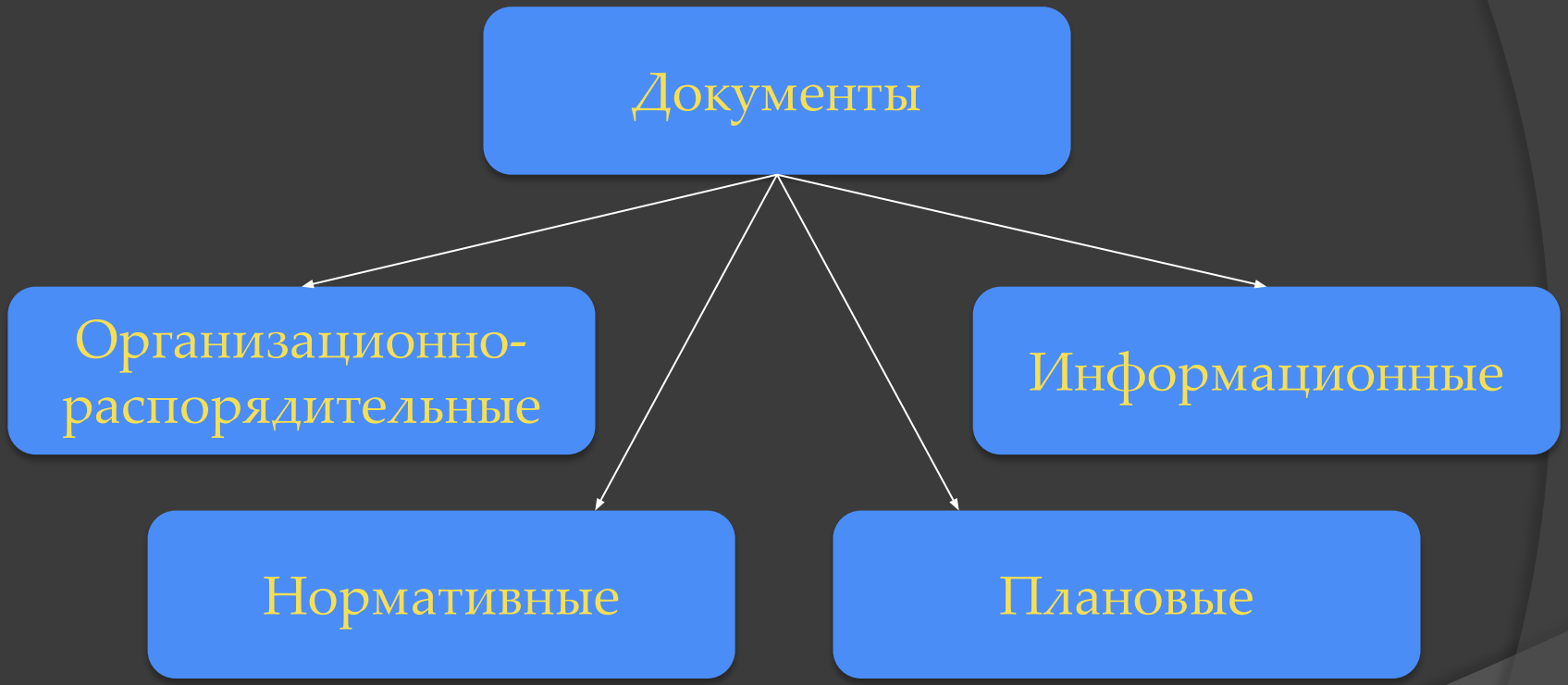
РАЗРАБОТКА НОРМАТИВНОЙ И ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНОЙ ДОКУМЕНТАЦИИ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Докладчик:
Гусев Игорь Михайлович

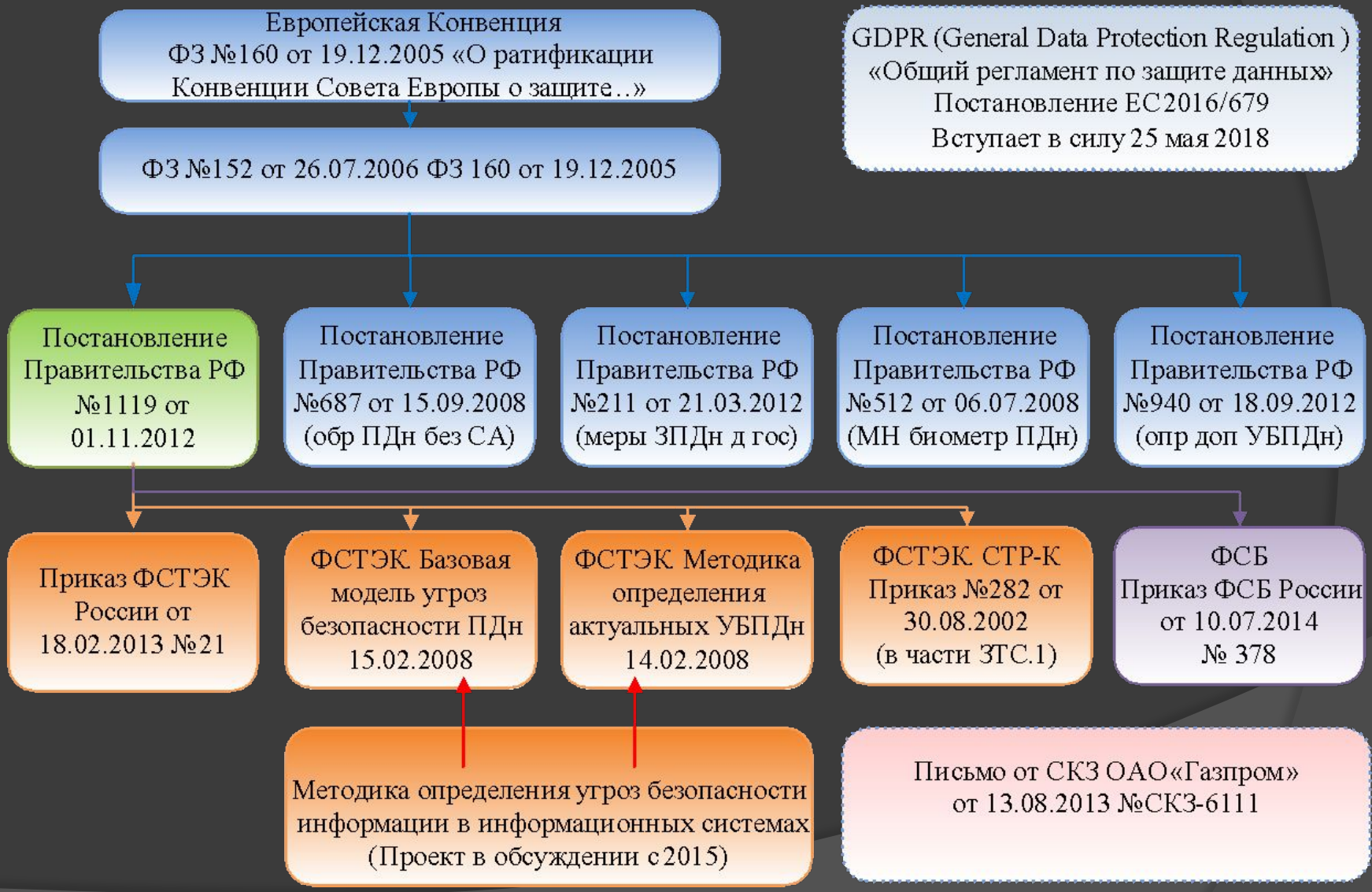
ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ ДОКУМЕНТОВ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

- Организация правового регулирования отношений между предприятием и субъектом ПДн в области обеспечения безопасности ПДн;
- Повышение эффективности и согласованности процесса управления ИБ на Предприятии;
- Информационное обеспечение подготовки и принятия решений по обеспечению защиты ПДн;
- Осуществление эффективного использования (эксплуатации) средств обеспечения ИБ;
- Стандартизация в области обеспечения ИБ;
- Выполнение требований регуляторов: ФСТЭК, ФСБ, РОСКОМНАДЗОР

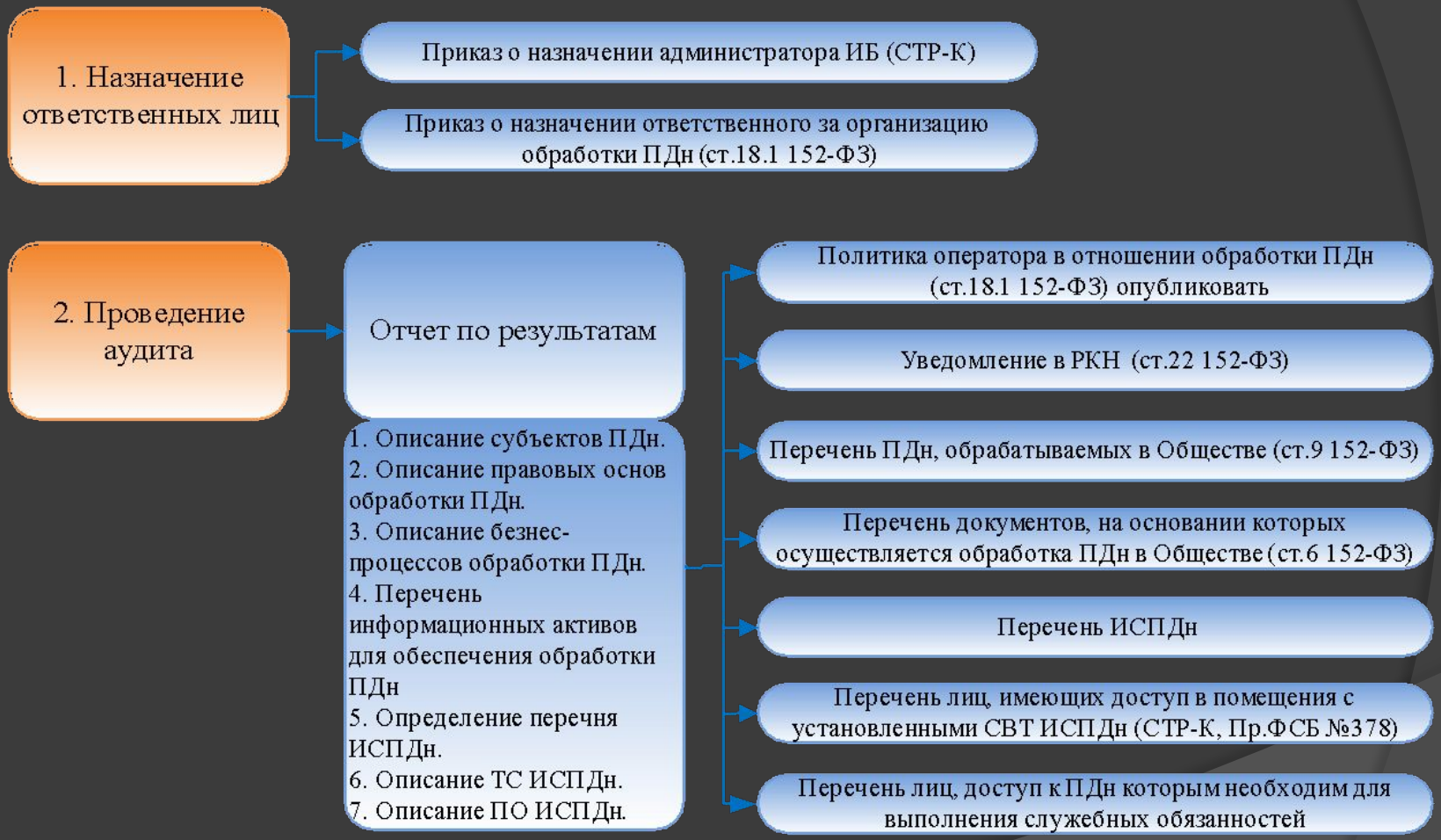
КЛАССИФИКАЦИЯ ДОКУМЕНТОВ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ



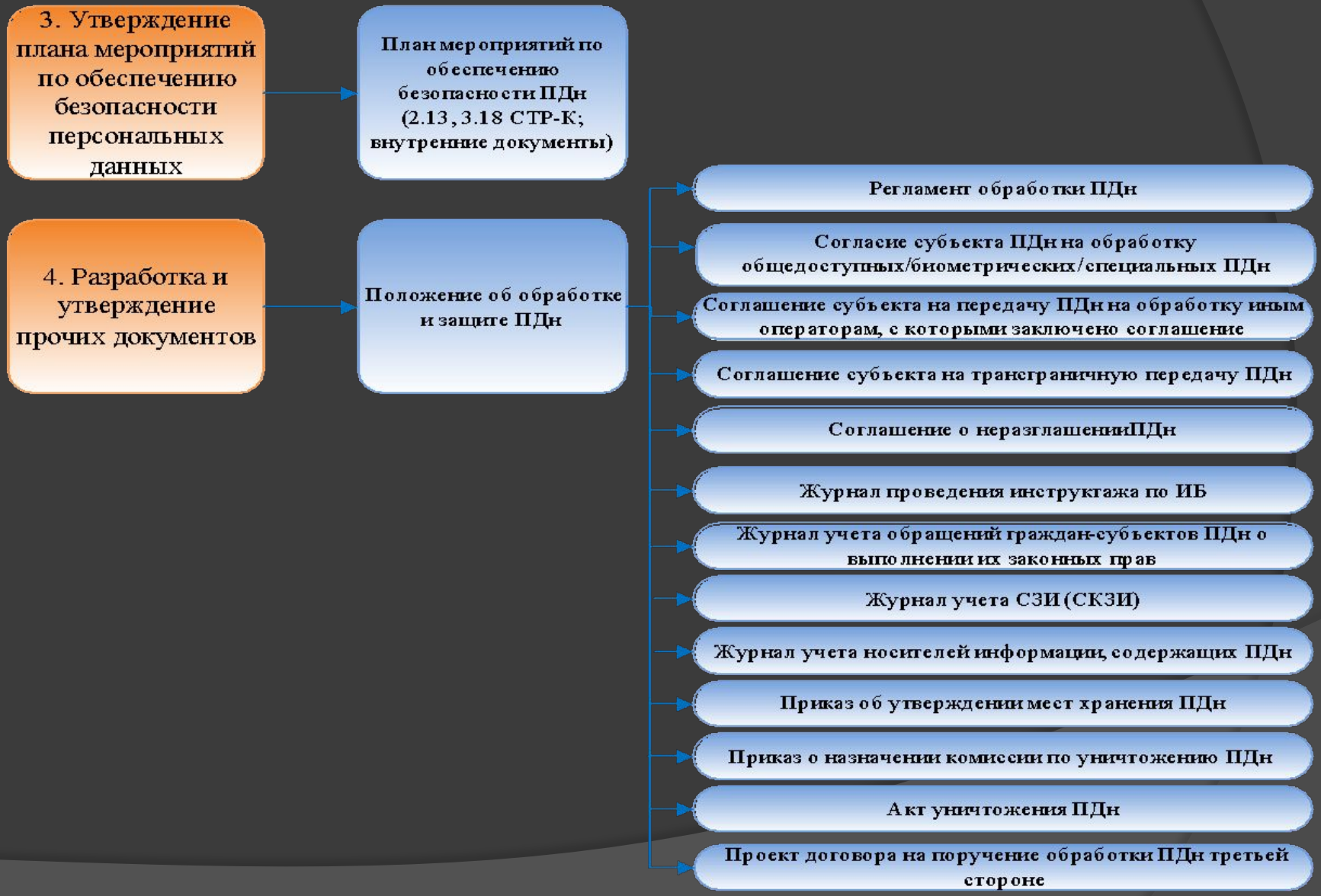
ЗАКОНОДАТЕЛЬСТВО В СФЕРЕ ЗАЩИТЫ ПДн



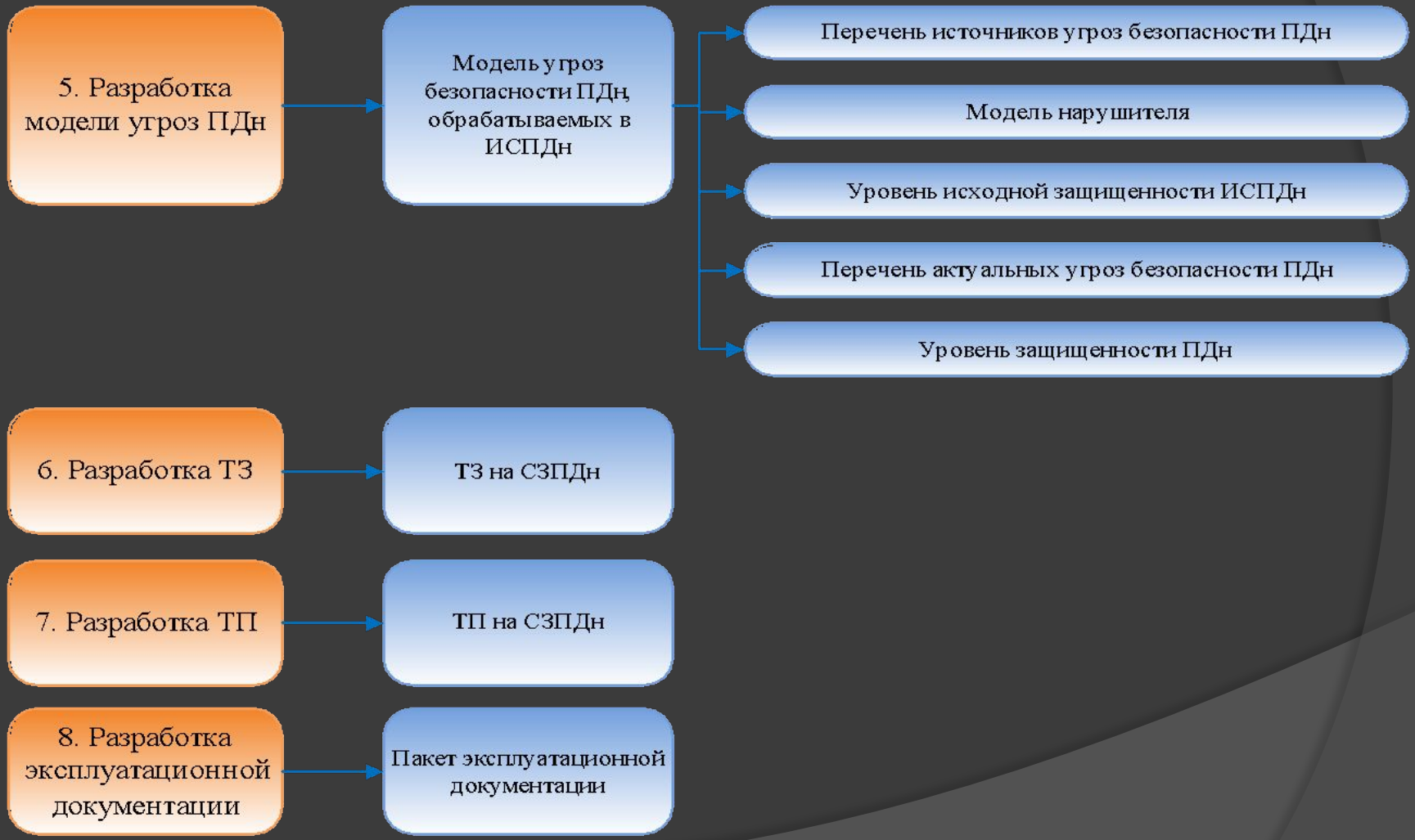
ПРАКТИКА РАЗРАБОТКИ ДОКУМЕНТАЦИИ
(ЧАСТЬ 1)



ПРАКТИКА РАЗРАБОТКИ ДОКУМЕНТАЦИИ
(ЧАСТЬ 2)



ПРАКТИКА РАЗРАБОТКИ ДОКУМЕНТАЦИИ
(ЧАСТЬ 3)



МОДЕЛЬ УГРОЗ (нормативная база)

Требования по разработке модели угроз безопасности ПДн, обрабатываемых в ИСПДн оператора установлены в следующих документах:

1. Федеральный закон РФ «О персональных данных» от 26.07.2006 № 152 (ст.19, ч.2, п.1; ст.19, ч.5; ст.19, ч.6).
2. «Требования к защите ПДн при их обработке в ИСПДн», утвержденные Постановлением Правительства РФ от 01.11.2012 №1119 (п. 7).
3. Приказ от 16.02.2015 № 65 «Положение об обеспечении безопасности ПДн при их обработке в ИСПДн ОАО «Газпром» и ДОО» (п. 2.3)
4. Письмо от СКЗ ОАО «Газпром» от 16.05.2010 №СКЗ-1091.
5. Корпоративный стандарт ПАО Газпром (СТО Газпром 4.2-0-005-2013 «Модель угроз ПДн при их обработке в ИСПДн»)

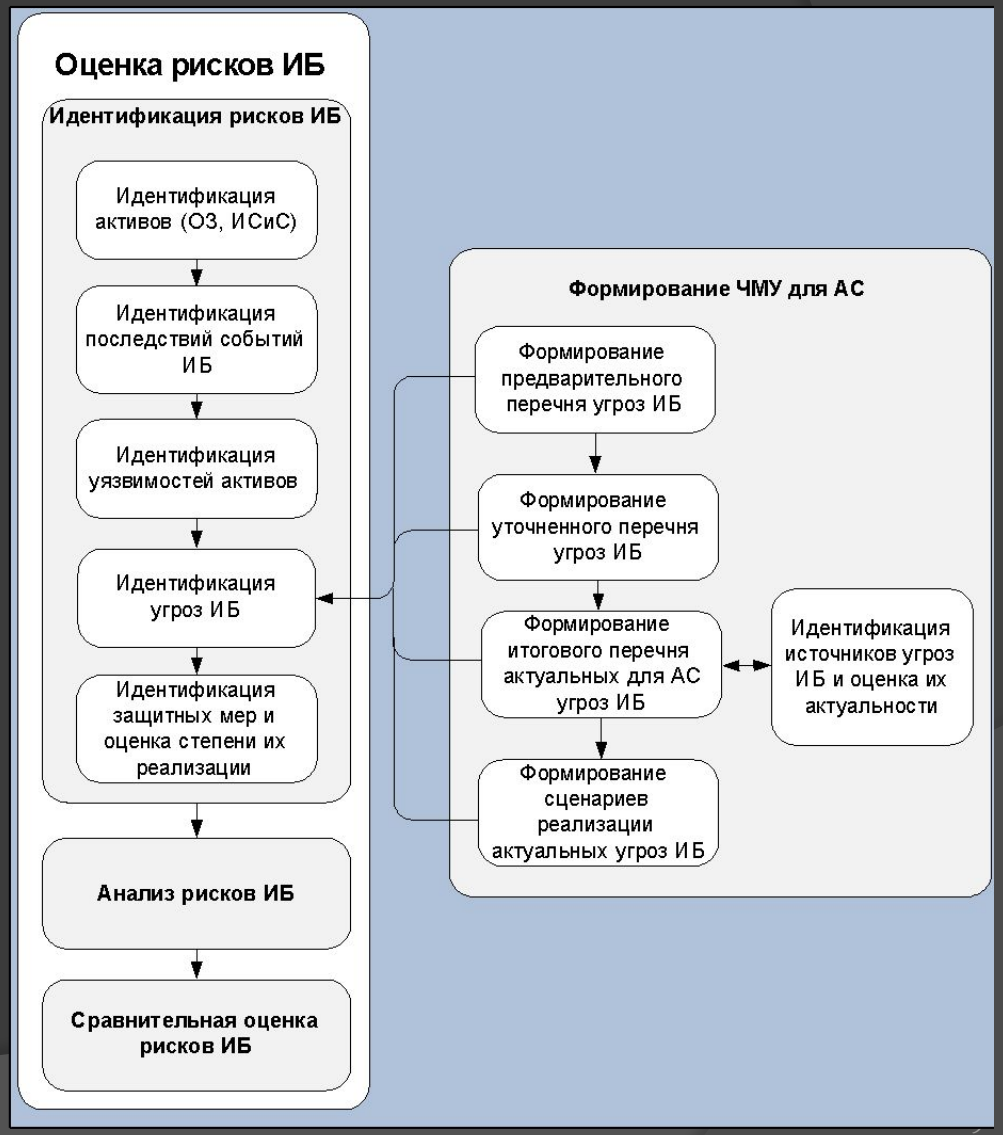
ЗАЧЕМ НУЖНА МОДЕЛЬ УГРОЗ?

Для формирования ЧТЗ (ПОИБ или КСЗИ), оценки рисков

Результаты обследования или ТТ на АС

Частная модель угроз для АС

ЧТЗ ПОИБ, КСЗИ для АС



МОДЕЛЬ УГРОЗ

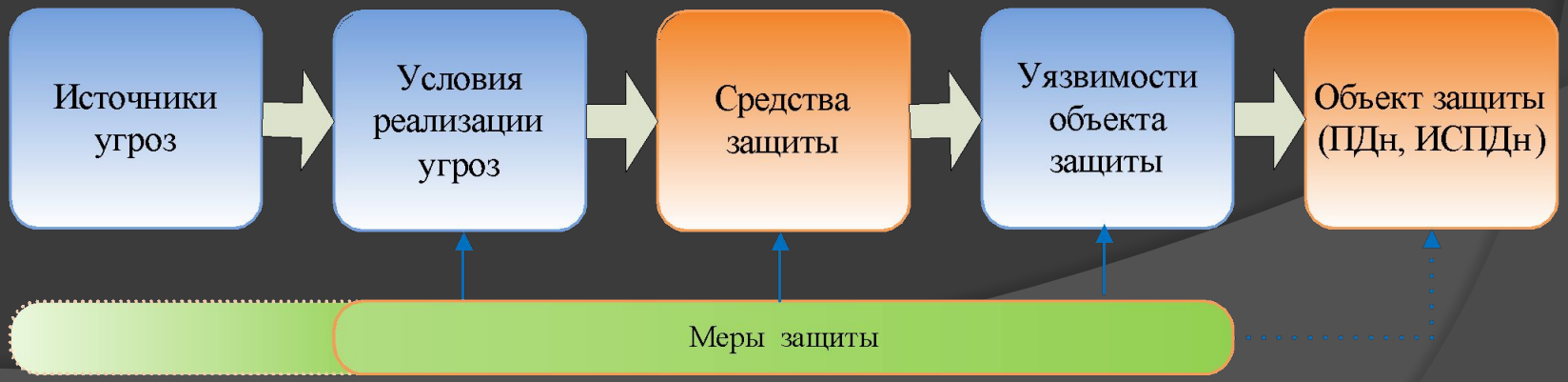
Угроза – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (СТО Газпром 4.2-1-001-2009)

Каждая угроза безопасности информации в ИСПДн описывается следующим образом:

УБИj = [нарушитель (источник угрозы) ;
способы реализации угрозы ;
уязвимости ;
объекты воздействия ;
последствия от реализации угрозы]

Источник угроз выступает в качестве причины возникновения одной или множества угроз

КАНАЛ РЕАЛИЗАЦИИ УГРОЗЫ



ПРАКТИКА РАЗРАБОТКИ МОДЕЛИ УГРОЗ

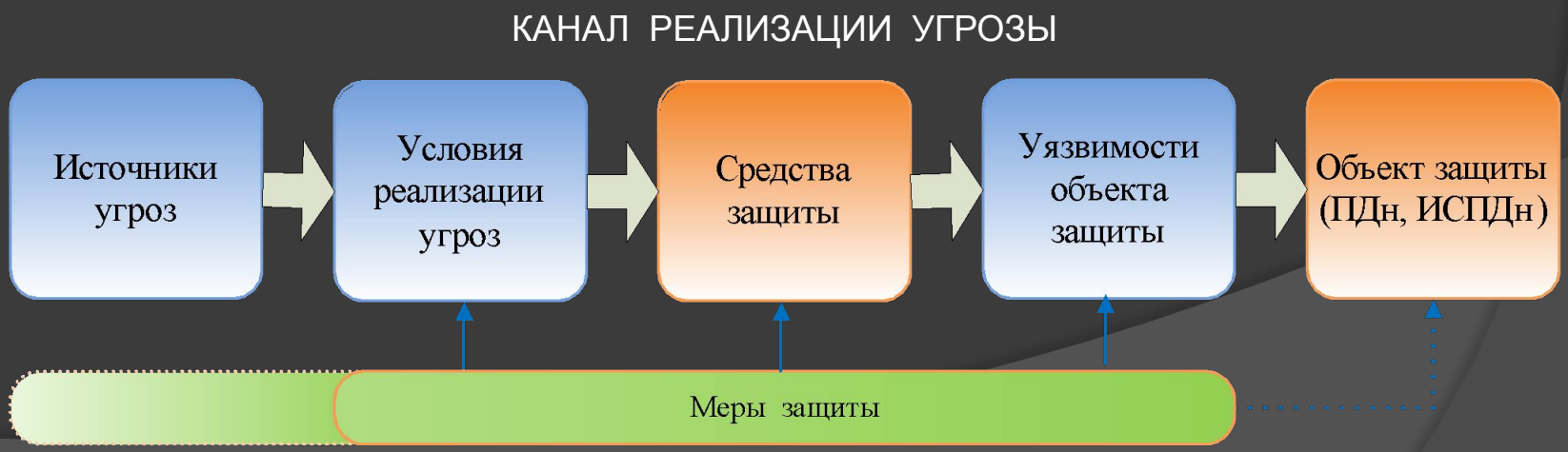
Подход к формированию модели угроз заключается в:

– сокращении типового перечня угроз ПД до минимального набора, актуального для рассматриваемой ИСПД за счет последовательного исключения угроз ИСПД:

а) неактуальных угроз;

б) угроз, для которых не идентифицированы уязвимости;

– анализ реализованных мер защиты в зависимости от необходимого уровня защищенности ИСПД.



ПРАКТИКА РАЗРАБОТКИ МОДЕЛИ УГРОЗ

Р Газпром 4.2-3-004-2015 «Методика формирования частной модели угроз информационной безопасности для автоматизированных систем»

СТО Газпром 4.2-0-005-2013 «Модель угроз персональным данным при их обработке в информационных системах персональных данных ОАО «Газпром», его дочерних обществ и организаций»

Для начала разработки ЧМУ для ИСПД потребуются:

– Акт обследования ИСПД (Отчет об обследовании);
  а) характеристики обрабатываемых ПД;
  б) существующая в организации ОРД в части обработки ПД;
  в) используемые технологии при обработке ПД;
  г) характеристика потенциальных нарушителей ИБ;
  д) реализованные меры защиты ИСПД (в т.ч. компенсирующие);

– Акт классификации ИСПД.

ХАРАКТЕРИСТИКИ ЗАЩИЩАЕМОЙ АС

Характеристика АС	Значения
Структура АС	– автономное АРМ – локальная АС – распределенная АС
Наличие подключения к сетям общего пользования	– подключена – подключена через выделенную инфраструктуру – не подключена
Размещение ТС	– в пределах одной КЗ – в пределах нескольких КЗ – вне КЗ
Режим обработки информации	– однопользовательский – многопользовательский
Сегментирование АС	– без сегментирования – с сегментированием
Взаимодействие с другими АС	– используется – не используется

ТИПОВОЙ ПЕРЕЧЕНЬ ОБЪЕКТОВ ЗАЩИТЫ АС

Тип ОЗ	Подтип ОЗ	Условное обозначение подтипа ОЗ
ТС	Активное сетевое оборудование	АСО
	Каналы связи	КС
	Серверы базовых ИТ-сервисов	СБС
	Системы хранения данных	СХД
	Серверы баз данных системы	СБД
	Серверы резервного копирования	СРК
	Автоматизированные рабочие места пользователей	АРМ
	Системы автоматического управления	САУ
	Контроллеры и исполнительные устройства	КИУ
	Вспомогательные ТС	ВТС
	Периферийные ТС	ТСП
	Съемные носители информации	СНИ
	Мобильные программно-технические устройства	МПТУ
ПО	Операционные системы серверов	ОСС
	Операционные системы АРМ пользователей	ОСК
	Операционные системы АСО	ОС АСО
	Прикладное ПО АС, установленное на сервере	СППО
	Прикладное ПО АС, установленное на АРМ	КППО
ИА	Файлы БД	ФБД
	Файлы резервных копий БД	ФРК
	Файлы с информацией ограниченного доступа	ФсИОД

ТИПОВОЙ ПЕРЕЧЕНЬ ГРУПП УЯЗВИМОСТЕЙ АС

Условное обозначение группы уязвимостей	Наименование группы уязвимостей
У1	Уязвимости кода системного ПО
У2	Уязвимости кода прикладного ПО
У3	Уязвимости кода инструментального ПО
У4	Уязвимости кода СУБД
У5	Уязвимости конфигурации системного ПО
У6	Уязвимости конфигурации прикладного ПО
У7	Уязвимости конфигурации инструментального ПО
У8	Уязвимости конфигурации СУБД
У9	Уязвимости, связанные с техническим обслуживанием ТС
У10	Уязвимости, связанные с сопровождением ПО
У11	Уязвимости физической защиты ТС
У12	Уязвимости, связанные с персоналом организации
У13	Уязвимости организационно-управленческих мер по обеспечению ИБ
У14	Уязвимости, вызванные взаимодействием с третьими лицами (организациями)
У15	Уязвимости нормативно-документационного обеспечения защиты информации
У16	Уязвимости, связанные с местом размещения

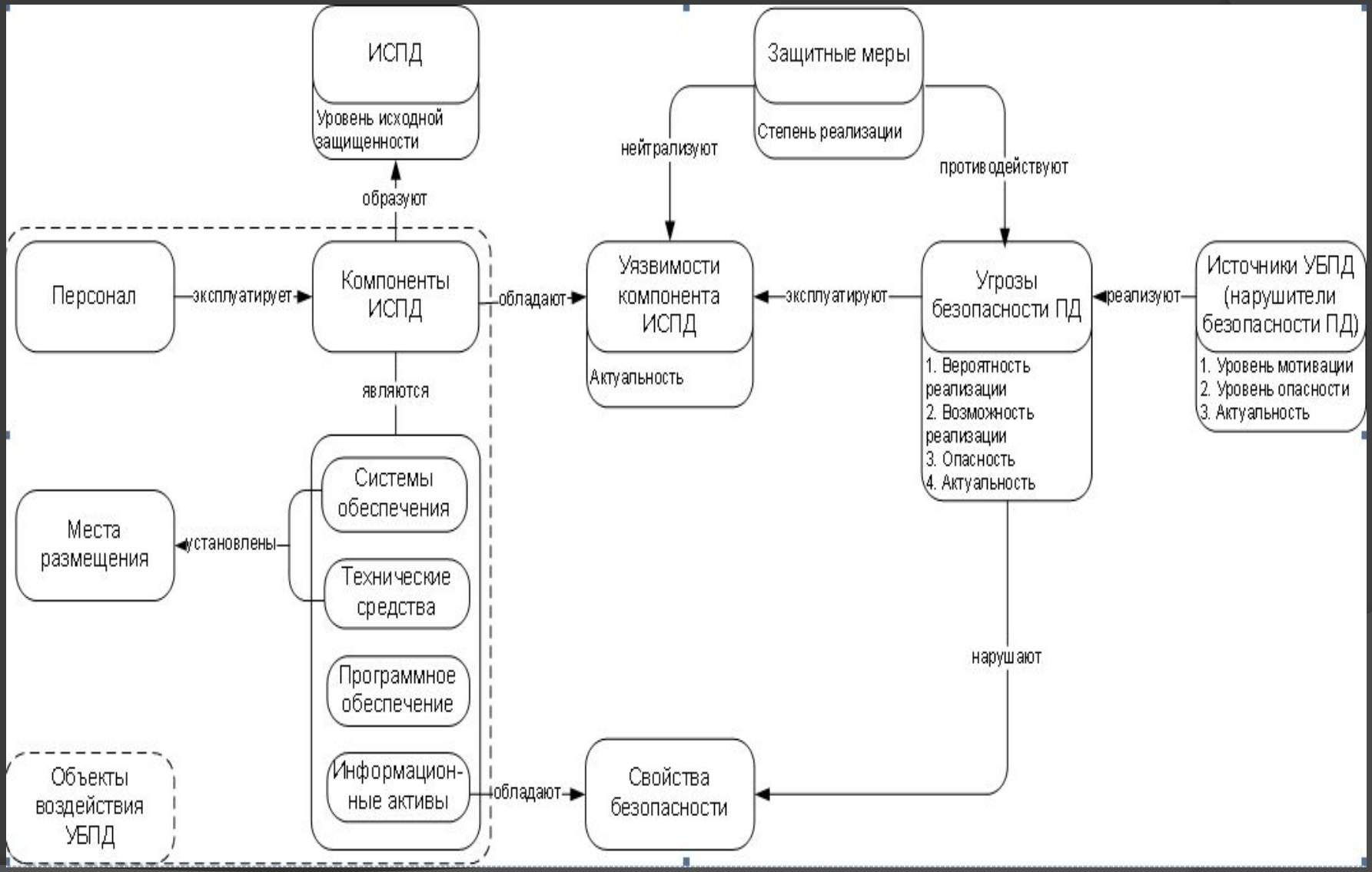
ТИПОВОЙ ПЕРЕЧЕНЬ КАТЕГОРИЙ ЗАЩИТНЫХ МЕР

Условное обозначение категории	Наименование категории защитных мер
ЗМ1	Физическая защита
ЗМ2	Организация безопасной эксплуатации средств обработки, хранения и передачи информации
ЗМ3	Регистрация и учет событий ИБ
ЗМ4	Защита от вредоносного кода и спама
ЗМ5	Резервное копирование
ЗМ6	Защита сетевых сервисов и обеспечение сетевой безопасности
ЗМ7	Обеспечение ИБ при использовании мобильных программно-технических устройств и съемных носителей информации
ЗМ8	Защита программного обеспечения
ЗМ9	Криптографическая защита
ЗМ10	Контроль доступа
ЗМ11	Контроль защищенности

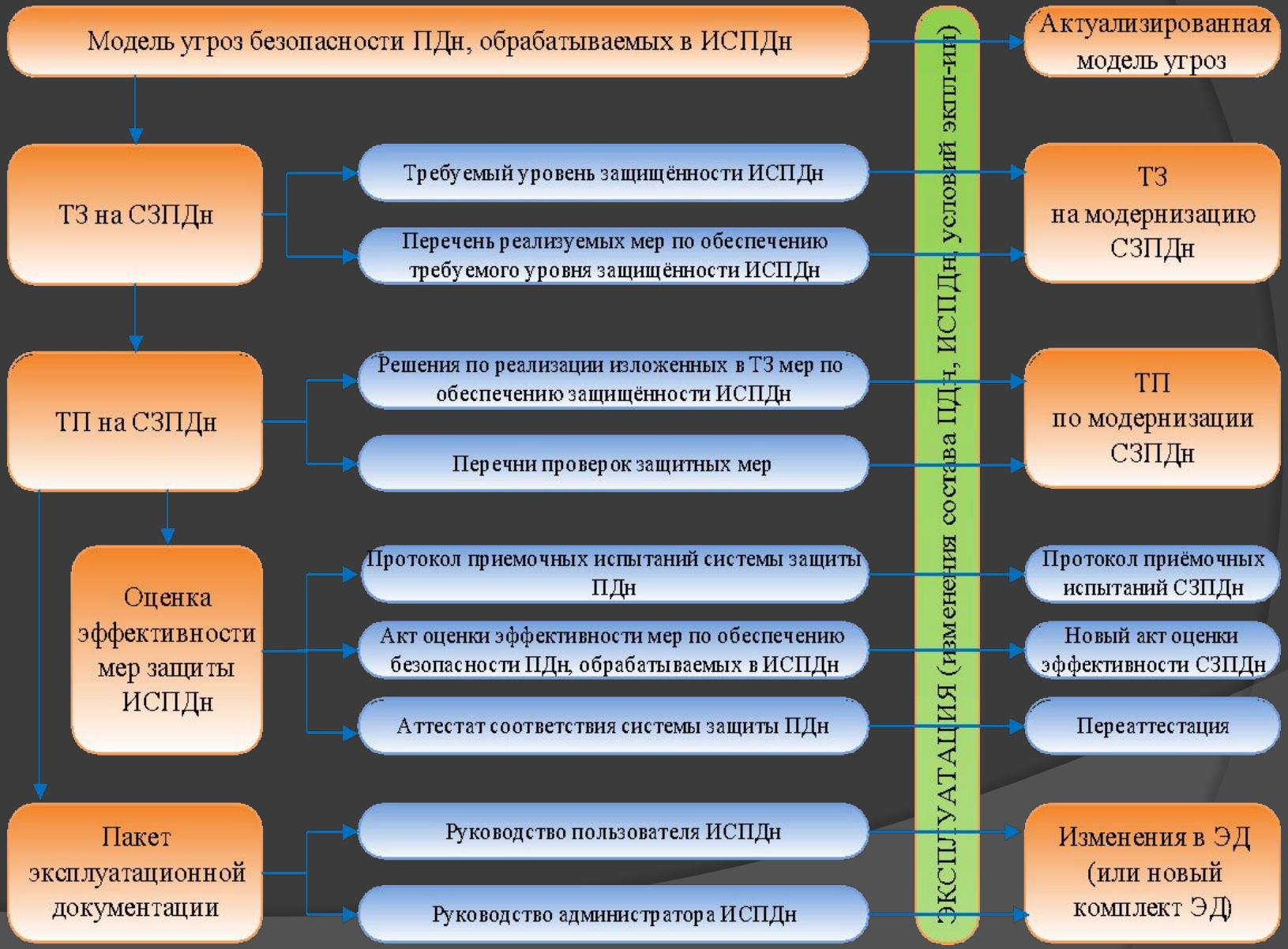
ОПРЕДЕЛЕНИЕ ОПАСНОСТИ НАРУШИТЕЛЯ

Категория угрозы	Нарушаемые свойства безопасности ИА		
	Конфиденциальность	Целостность	Доступность
Взлом	+	+	+
Утечка	+		
Искажение		+	+
Утрата	+	+	+
Блокирование			+
Злоупотребление	+	+	+

МОДЕЛЬ УГРОЗ
(взаимодействие сущностей)



ПРАКТИКА РАЗРАБОТКИ МОДЕЛИ УГРОЗ



ОСНОВНЫЕ ОШИБКИ, ДОПУСКАЕМЫЕ ПРИ РАЗРАБОТКЕ МОДЕЛИ УГРОЗ

1. Неверно определены границы КЗ.
2. Допущены ошибки в построении модели нарушителя.
3. Неверно определен уровень исходной защищенности ИСПДн.
4. Допущены ошибки в процессе определения актуальности угроз.
5. Из рассмотрения исключены угрозы, которые необходимо рассматривать для ИСПДн.
6. Преднамеренно выставлена необходимая актуальность угроз.

КОНТАКТЫ:

Организация: ООО «ГазИнформСервис»

адрес: Г. Санкт-Петербург, ул. Кронштадтская, д. 10а

Телефон: +7 812 677-20-50

Факс: +7 812 677-20-51

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

Докладчик:
Гусев Игорь Михайлович