Тема N4. Основные критерии защищённости АС. Классы защищённости АС.

Занятие N4. Единые критерии безопасности информационных технологий.

Часть 1. Основные положения «Единых критериев». Функциональные требования. Требования доверия.

Учебные вопросы

1-й учебный вопрос – Концепция и основные понятия ОК.

2-й учебный вопрос - Структура требований безопасности. Функциональные требования. Требования доверия

Литература

1. *Девянин П.Н., Михальский О.О., и др. Теоретические основы компьютеной безопасности: Уч. Пособие для вузов. М.: Радио и связь, 2000.*
2. *Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Уч. Пособие. – М: ИД Форум, 2008.*
3. *Руководящие документы ФСТЭК России.* **http://www.fstec.ru/**

1-й Вопрос

Концепция и основные понятия ОК

Режим ИБ в подобных системах обеспечивается:

-на *процедурном уровне* – путем разработки и выполнения разделов инструкций для персонала по ИБ, а также мерами физической защиты;

-на *программно-техническом уровне* – применением апробированных и сертифицированных решений, стандартного набора контрмер: резервное копирование, антивирусная защита, парольная защита, межсетевые экраны, шифрование данных и т.д.

При обеспечении ИБ важно не упустить каких-либо существенных аспектов. Это будет гарантировать некоторый **МИНИМАЛЬНЫЙ (БАЗОВЫЙ) УРОВЕНЬ ИБ,** обязательный для любой информационной технологии, при котором рассматривается стандартный набор наиболее распространенных угроз безопасности без оценки их вероятностей.

В ряде случаев БАЗОВОГО УРОВНЯ БЕЗОПАСНОСТИ оказывается недостаточно. Примером может служить АСУ технологическим процессом предприятия с непрерывным циклом производства или АСУ войсками, когда даже кратковременный выход из строя автоматизированной системы приводит к очень тяжелым последствиям.

В этом и подобных случаях важно знать параметры, характеризующие уровень безопасности информационной системы (технологии): количественные оценки угроз безопасности, уязвимостей, ценности информационных ресурсов. В случае повышенных требований в области ИБ используется полный вариант анализа рисков.

В отличие от БАЗОВОГО ВАРИАНТА, производится оценка ценности ресурсов, характеристик рисков и уязвимостей, проводится анализ по *критерию стоимость/эффективность* нескольких вариантов защиты.

Предыстория вопроса

В начале 80-х годов в США были разработаны **"Критерии оценки доверенных компьютерных систем" (TCSEC).**

В Европе в 1991г. Европейской Комиссией были опубликованы **"Критерии оценки безопасности информационных технологий" (ITSEC)** версии 1.2, разработанные совместно Францией, Германией, Нидерландами и Великобританией.

В Канаде на основе сочетания подходов TCSEC и ITSEC в начале 1993г. были созданы **"Канадские критерии оценки доверенных компьютерных продуктов" (CTCPEC) версии 3.0.**

В США в это же время был издан проект стандарта **"Федеральные критерии безопасности информационных технологий" (FC) версии 1.0,** использовавший другой подход к объединению североамериканской и европейской концепций критериев оценки.

В 1990г. Международной организацией по стандартизации (ISO) была начата разработка международного стандарта критериев оценки для общего использования.

Новые критерии были призваны удовлетворить потребность взаимного признания результатов стандартизованной оценки безопасности на мировом рынке ИТ. Эта задача была поставлена перед Рабочей группой 3 (WG3) подкомитета 27 (SC27) Совместного технического комитета 1 (JTC1). Вначале работа WG3 шла медленно из-за большого объема и необходимости интенсивных многосторонних переговоров.

В июне 1993г. организации-спонсоры CTCPEC, FC, TCSEC и ITSEC из шести стран (Великобритания, Германия, Канада, Нидерланды, США, Франция) объединили свои усилия и начали действовать совместно, чтобы согласовать различающиеся между собой критерии и создать единую совокупность критериев безопасности ИТ, которые могли бы широко использоваться. Эта деятельность получила название "Проект ОК".

Переработка документа была выполнена преемником CCEB, который в настоящее время называется Советом по реализации ОК (CCIB).

В мае 1998г. была опубликована версия 2.0 ОК, и на ее основе в июне 1999г. был принят международный стандарт ISO/IEC 15408. Официальный текст стандарта издан 1 декабря 1999г.

По историческим причинам и с целью обеспечения преемственности ISO/IEC/JTC1/SC27/WG3 приняла для дальнейшего использования термин "Общие критерии" (ОК) внутри документа, признавая, что его официальным названием, принятым в ISO, является "Критерии оценки безопасности информационных технологий".

ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий".

ГОСТ состоит из 3-х частей:

ГОСТ Р ИСО/МЭК 15408-1-2002 Часть 1. Введение и общая модель.
ГОСТ Р ИСО/МЭК 15408-2-2002 Часть 2. Функциональные требования безопасности.
ГОСТ Р ИСО/МЭК 15408-3-2002 Часть 2. Требования доверия к безопасности.

На основе ГОСТов группы ГОСТ Р ИСО/МЭК 15408 в 2002 и 2003 гг. вышли руководящие документы Гостехкомиссии России:

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий Часть 1,Часть 2, Часть3	**Приказ председателя Гостехкомиссии России от 19 июня 2002 г. № 187**
Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности	Гостехкомиссия России, 2003 год
Руководящий документ. Безопасность информационных технологий. Руководство по регистрации профилей защиты	Гостехкомиссия России, 2003 год
Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты	Гостехкомиссия России, 2003 год
Руководство по разработке профилей защиты и заданий по безопасности	Гостехкомиссия России, 2003 год

Основные группы пользователей ОК:

В оценке характеристик безопасности продуктов и систем ИТ заинтересованы в основном потребители, разработчики и оценщики. Представленные критерии структурированы в интересах этих групп, потому что именно они рассматриваются как основные пользователи ОК.

ПОТРЕБИТЕЛИ:

Результаты оценки помогают потребителям решить, вполне ли оцениваемый продукт или система удовлетворяет их потребности в безопасности. Эти потребности обычно определяются как следствие анализа рисков, а также направленности политики безопасности. Потребители могут также использовать результаты оценки для сравнения различных продуктов и систем. Иерархическое представление требований доверия способствует этому.

РАЗРАБОТЧИКИ:

ОК предназначены для поддержки разработчиков при подготовке к оценке своих продуктов или систем и содействии в ее проведении, а также при установлении требований безопасности, которым должны удовлетворять каждый их продукт или система.

Конструкции из ОК могут тогда использоваться для формирования утверждения о соответствии ОО установленным для него требованиям посредством подлежащих оценке специфицированных функций безопасности и мер доверия.

Требования для каждого ОО содержатся в зависимой от реализации конструкции, называемой заданием по безопасности (ЗБ). Требования широкого круга потребителей могут быть представлены в одном или нескольких ПЗ.

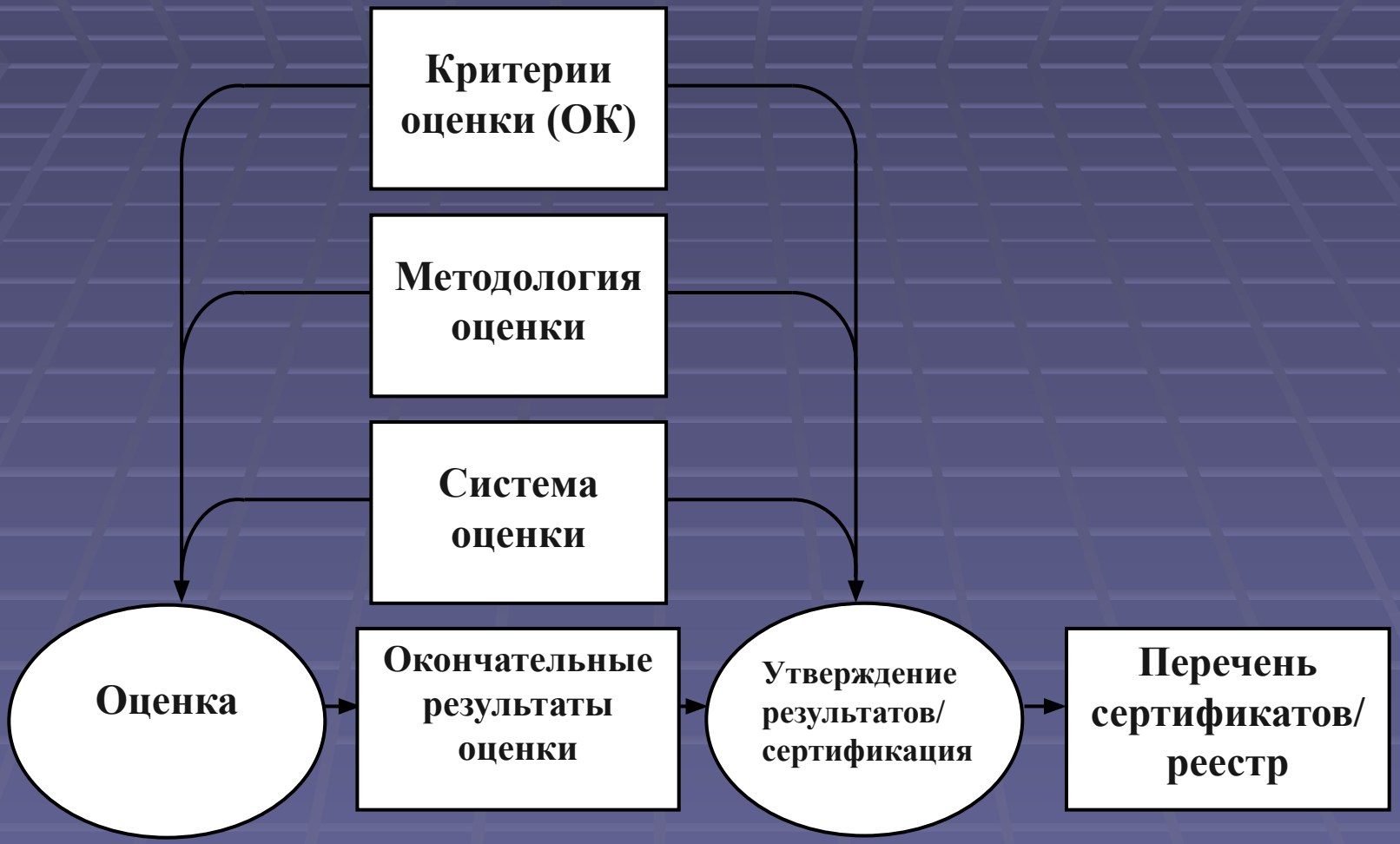
ОЦЕНЩИКИ:

В ОК содержатся критерии, предназначенные для использования оценщиками ОО при формировании заключения о соответствии объектов оценки предъявленным к ним требованиям безопасности. В ОК дается описание совокупности основных действий, выполняемых оценщиком, и функций безопасности, к которым относятся эти действия. В ОК, однако, не определены процедуры, которых следует придерживаться при выполнении этих действий.

ПРОЧИЕ:

а) лица, ответственные за техническое состояние оборудования, и сотрудники служб безопасности, ответственные за определение и выполнение политики и требований безопасности организации в области ИТ;
б) аудиторы, как внутренние, так и внешние, ответственные за оценку адекватности безопасности системы;
в) проектировщики систем безопасности, ответственные за спецификацию основного содержания безопасности систем и продуктов ИТ;
г) аттестующие, ответственные за приемку системы ИТ в эксплуатацию в конкретной среде;
д) заявители, заказывающие оценку и обеспечивающие ее проведение;
е) органы оценки, ответственные за руководство и надзор за программами проведения оценок безопасности ИТ.

Контекст оценки



Безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки.

Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- *проектирование* и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация

В свою очередь, угрозы характеризуются следующими параметрами:

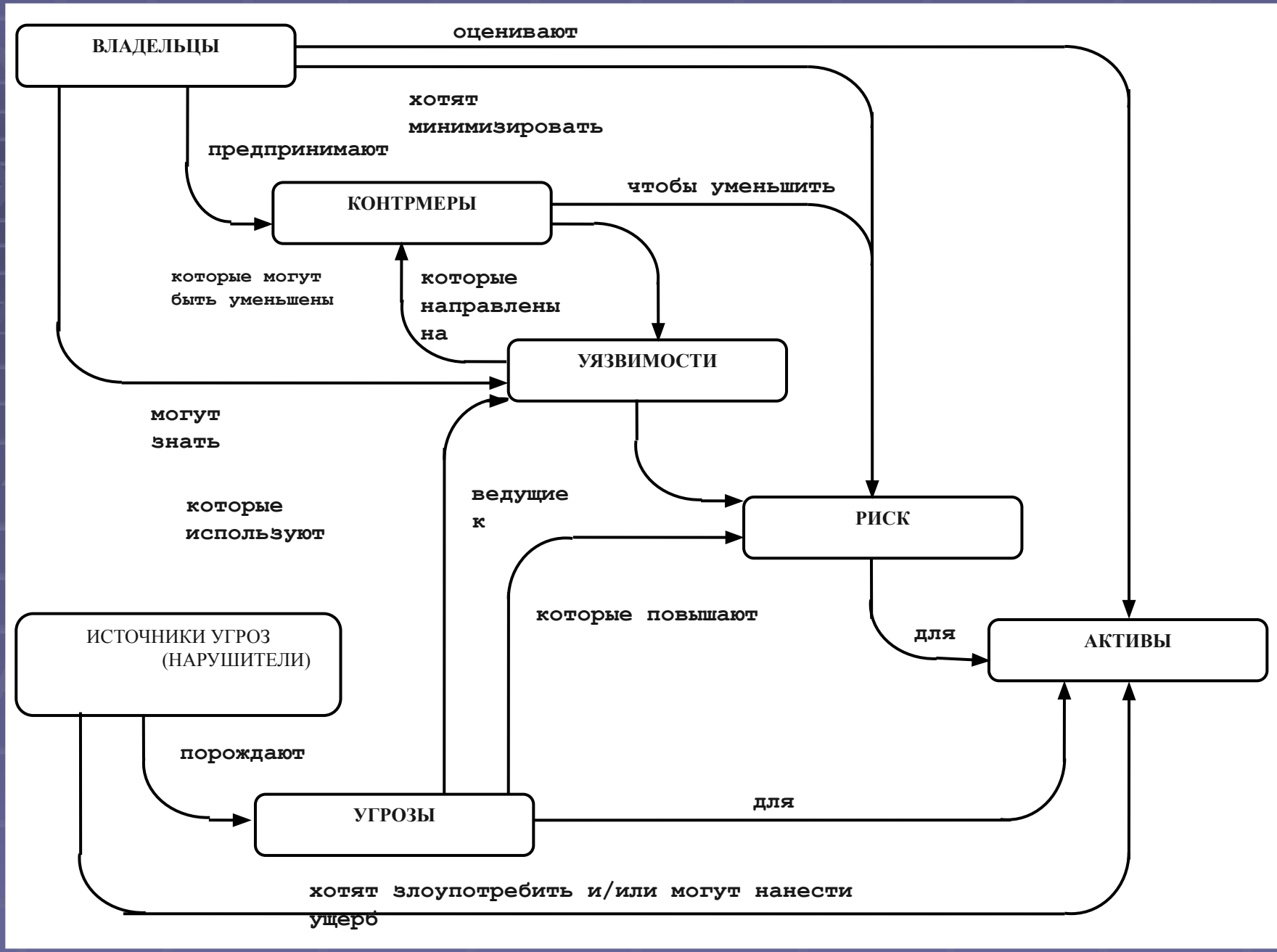
- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка в:

- требованиях безопасности;
- *проектировании*;
- эксплуатации.

Согласно ОК, безопасность связана с защитой активов от угроз, где угрозы классифицированы на основе потенциала злоупотребления защищаемыми активами.

Рисунок иллюстрирует высокоуровневые понятия безопасности и их взаимосвязь.

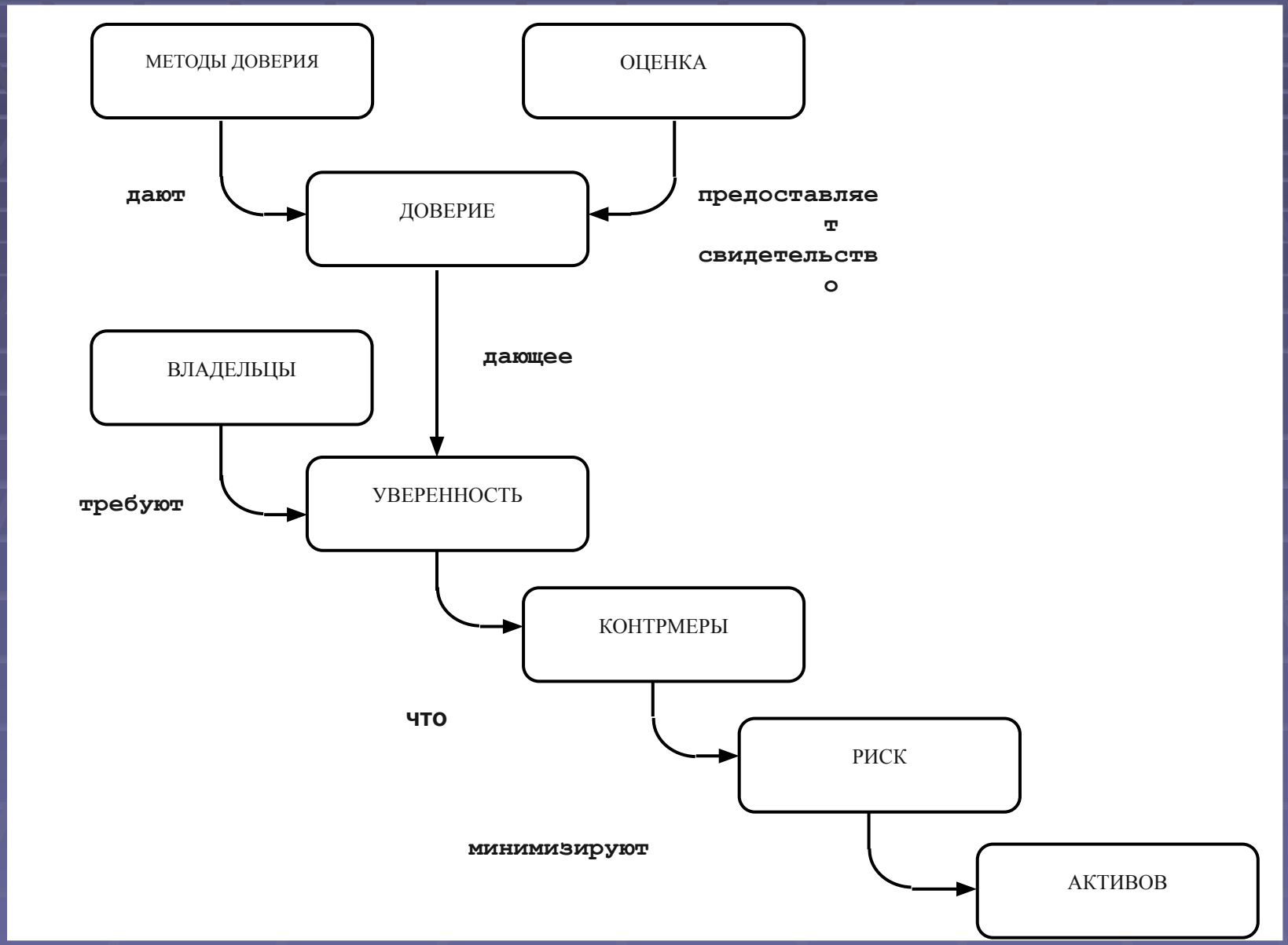


К специфическим нарушениям безопасности обычно относят (но не обязательно ими ограничиваются): наносящее ущерб раскрытие актива несанкционированным получателем (потеря конфиденциальности), ущерб активу вследствие несанкционированной модификации (потеря целостности) или несанкционированное лишение доступа к активу (потеря доступности).

Прежде чем подвергнуть активы опасности воздействия выявленных угроз, их владельцам необходимо убедиться, что предпринятые контрмеры обеспечат адекватное противостояние этим угрозам. Сами владельцы активов не всегда в состоянии судить обо всех аспектах предпринимаемых контрмер и поэтому могут потребовать их оценку.

Результатом такой оценки является заключение о степени доверия контрмерам по уменьшению рисков для защищаемых активов. В этом заключении устанавливается уровень доверия как результат применения контрмер. Доверие является той характеристикой контрмер, которая дает основание для уверенности в их надлежащем действии. Заключение о результатах оценки может быть использовано владельцем активов при принятии решения о приемлемости риска для активов, создаваемого угрозами. Рисунок иллюстрирует эту взаимосвязь.

Понятия, используемые при оценке, и их взаимосвязь



ОСНОВЫ ПОДХОДА ОБЩИХ КРИТЕРИЕВ К БЕЗОПАСНОСТИ ОБЪЕКТОВ ИТ

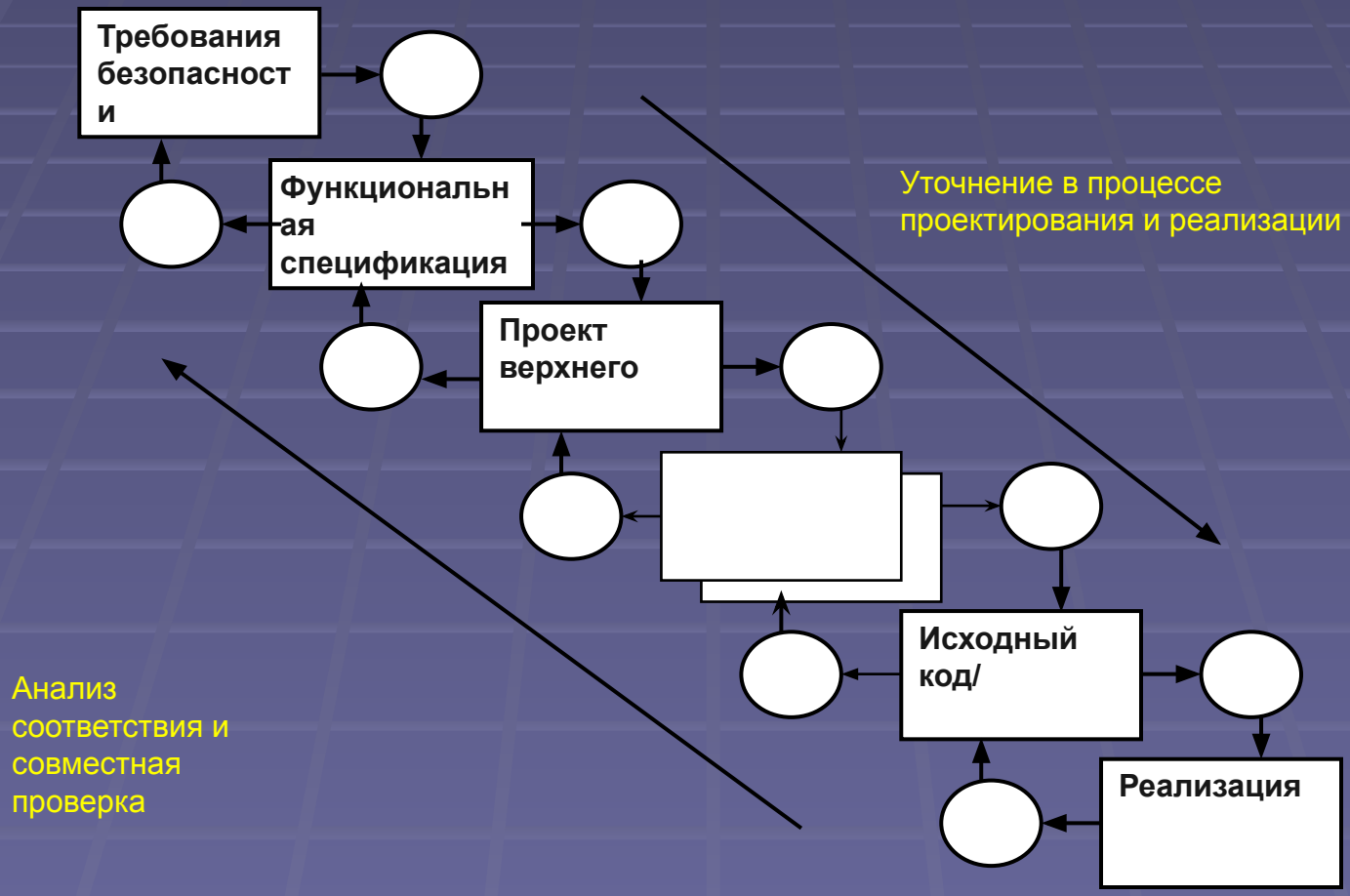
Уверенность в безопасности ИТ может быть достигнута в результате действий, которые могут быть предприняты в процессе

1. разработки,
2. оценки и
3. эксплуатации ОО,

т.е. в процессе всего жизненного цикла изделий ИТ.

Разработка

Критерии доверия из ОК идентифицируют следующие уровни абстракции проекта: функциональная спецификация, проект верхнего уровня, проект нижнего уровня и реализация. В зависимости от выбранного уровня доверия может потребоваться, чтобы разработчики показали, насколько методология разработки отвечает требованиям доверия из ОК.



Оценка ОО

Процесс оценки ОО может проводиться параллельно с разработкой или следом за ней. Основными исходными материалами для оценки ОО являются:

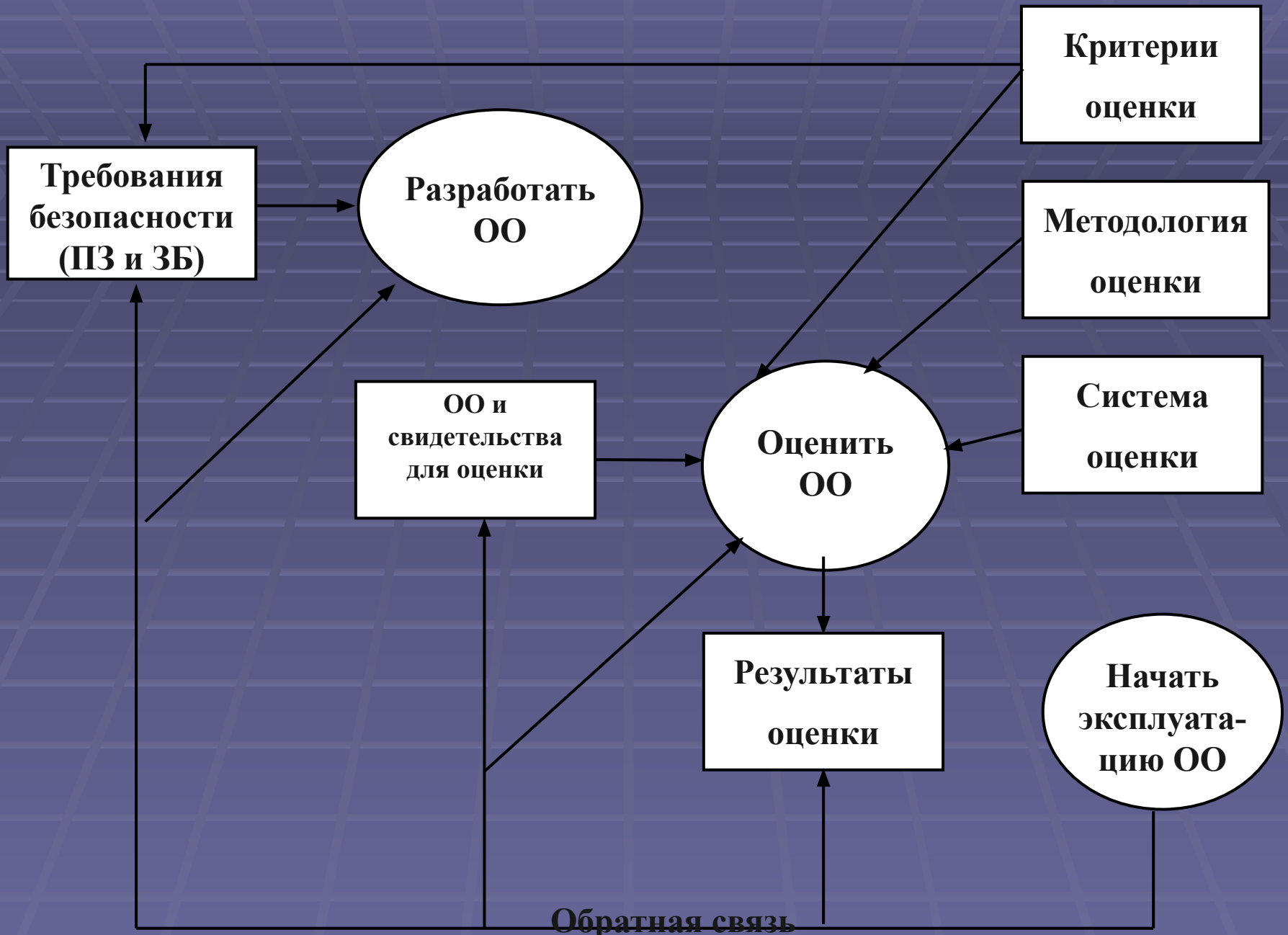
- совокупность свидетельств, характеризующих ОО, включая прошедшее оценку ЗБ в качестве основы оценки ОО;
- ОО, безопасность которого требуется оценить;
- критерии, методология и система оценки.

Ожидаемым результатом оценки является **подтверждение удовлетворения объектом оценки ТРЕБОВАНИЙ БЕЗОПАСНОСТИ, изложенных в его ЗБ,** а также один или несколько отчетов, документирующих выводы оценщика относительно ОО, сделанные в соответствии с критериями оценки. Такие отчеты, помимо разработчика, будут полезны также реальным и потенциальным потребителям продукта или системы, представленным как объект оценки.

Степень уверенности, получаемая в результате оценки, зависит от удовлетворенных при оценке требований доверия (например, от ОЦЕНОЧНОГО УРОВНЯ ДОВЕРИЯ).

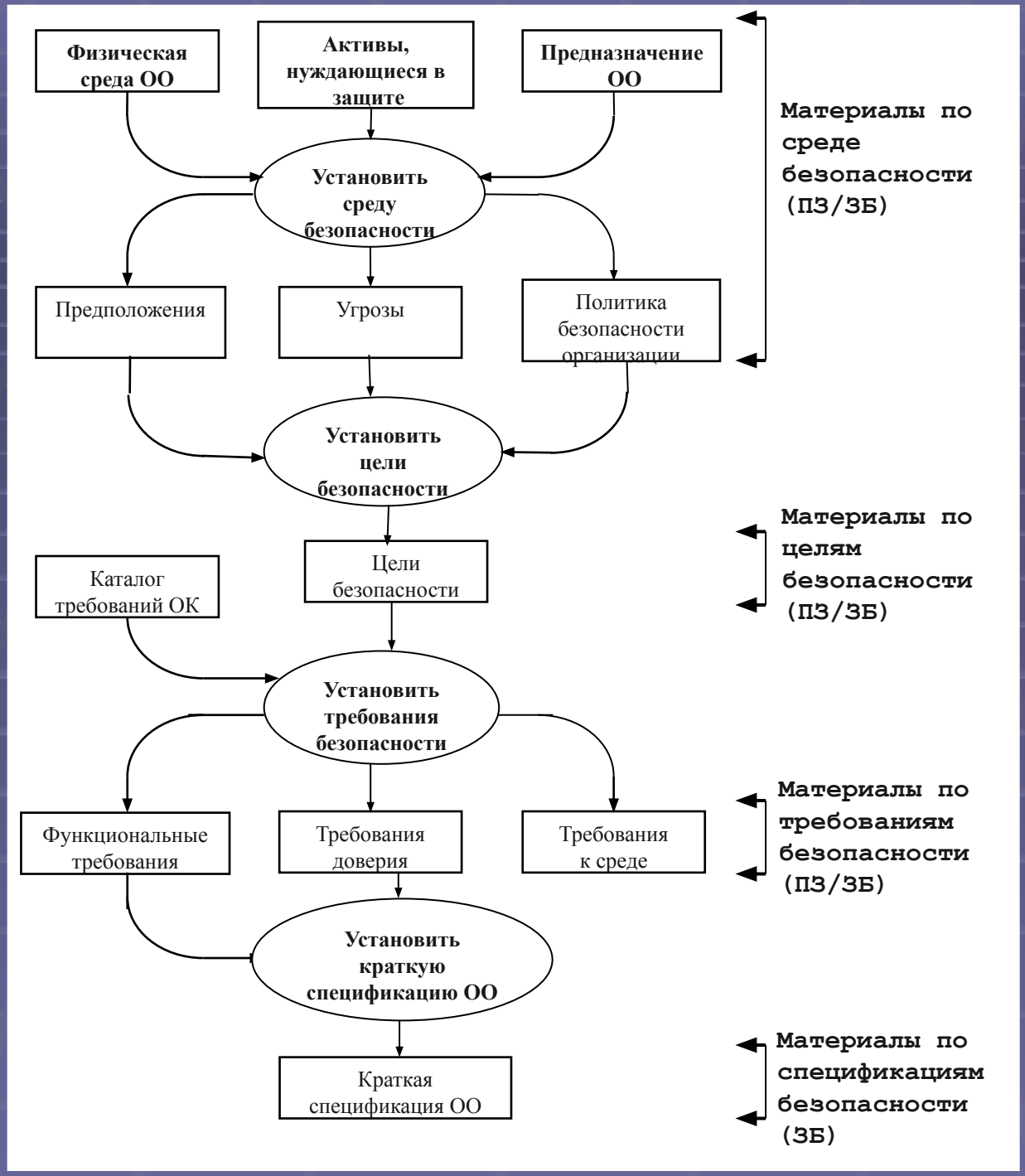
Эксплуатация ОО

Потребители могут выбрать оцененный продукт для использования в своих конкретных условиях. Не исключено, что при эксплуатации ОО могут проявиться не обнаруженные до этого ошибки или уязвимости, а также может возникнуть необходимость пересмотра предположений относительно среды функционирования.
Тогда по результатам эксплуатации потребуется внесение разработчиком исправлений в ОО либо переопределение требований безопасности или предположений относительно среды эксплуатации. Такие изменения, в свою очередь, могут привести к необходимости проведения новой оценки ОО или повышения безопасности среды его эксплуатации.


Критерии оценки
Требования безопасности (ПЗ и ЗБ)
Разработать ОО
Методология оценки
ОО и свидетельства для оценки
Оценить ОО
Система оценки
Результаты оценки
Начать эксплуата-цию ОО
Обратная связь

Понятия безопасности и порядок формирования требований безопасности и спецификаций ОО

Согласно ОК, чтобы показать защищенность активов, вопросы безопасности необходимо рассмотреть на всех уровнях, начиная с самого абстрактного и до конечной реализации ИТ в среде их эксплуатации.
В ОК используются различные формы представления, что показано на рисунке 6, который иллюстрирует возможный способ последовательного формирования требований безопасности и спецификаций при разработке ПЗ или ЗБ.


Физическая среда ОО
Активы, нуждающиеся в защите
Предназначение ОО
Установить среду безопасности
Предположения
Угрозы
Политика безопасности организации
Материалы по среде безопасности (ПЗ/ЗБ)
Установить цели безопасности
Цели безопасности
Каталог требований ОК
Материалы по целям безопасности (ПЗ/ЗБ)
Установить требования безопасности
Функциональные требования
Требования доверия
Требования к среде
Материалы по требованиям безопасности (ПЗ/ЗБ)
Установить краткую спецификацию ОО
Краткая спецификация ОО
Материалы по спецификациям безопасности (ЗБ)

Среда безопасности

ОК рассматривают объект оценки ОО исключительно с учётом внешней среды, в которой функционирует сам объект ИТ.

Среда безопасности включает все законы, политики безопасности организаций, опыт, специальные навыки и знания, для которых решено, что они имеют отношение к безопасности. Таким образом, она определяет контекст предполагаемого применения ОО. Среда безопасности включает также угрозы безопасности, присутствие которых в этой среде установлено или предполагается.

Цели безопасности

Смысл определения целей безопасности заключается в том, чтобы соотнести их со всеми поставленными ранее вопросами безопасности и декларировать, какие аспекты безопасности связаны непосредственно с ОО, а какие – с его средой. Такое разделение основано на совокупном учете инженерного опыта, политики безопасности, экономических факторов и решения о приемлемости рисков.

Цели безопасности для среды ОО достигаются как в рамках ИТ, так и нетехническими или процедурными способами.

Требования безопасности ИТ проистекают только из целей безопасности ОО и целей безопасности его среды, относящихся к ИТ

Требования безопасности ИТ

В ОК представлены две различные категории требований безопасности

1. Функциональные требования соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;

2. Требования доверия, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Функциональные требования налагаются на те функции ОО, которые предназначены для поддержания безопасности ИТ и определяют желательный безопасный режим функционирования ОО. Функциональные требования определены в части 2 ОК.

Примерами функциональных требований являются требования к идентификации, аутентификации, аудиту безопасности, неотказуемости источника (невозможности отказа от факта отправления сообщения).

Часть 3 ОК определяет требования доверия и шкалу оценочных уровней доверия (ОУД), формируемых с использованием этих компонентов.

Требования доверия налагаются на действия разработчика, представленные свидетельства и действия оценщика. Примерами требований доверия являются требования к строгости процесса разработки, по поиску потенциальных уязвимостей и анализу их влияния на безопасность. Доверие к тому, что цели безопасности достигаются посредством выбранных функций безопасности, зависит от следующих факторов:

- уверенности в корректности реализации функций безопасности, т.е. оценки того, правильно ли они реализованы;
- уверенности в эффективности функций безопасности, т.е. оценки того, действительно ли они отвечают изложенным целям безопасности.

Краткая спецификация ОО

Краткая спецификация ОО, предусмотренная в составе ЗБ, определяет отображение требований безопасности для ОО. В ней обеспечивается высокоуровневое определение функций безопасности, заявляемых для удовлетворения
- функциональных требований, и
- мер доверия, предпринимаемых для удовлетворения требований доверия.

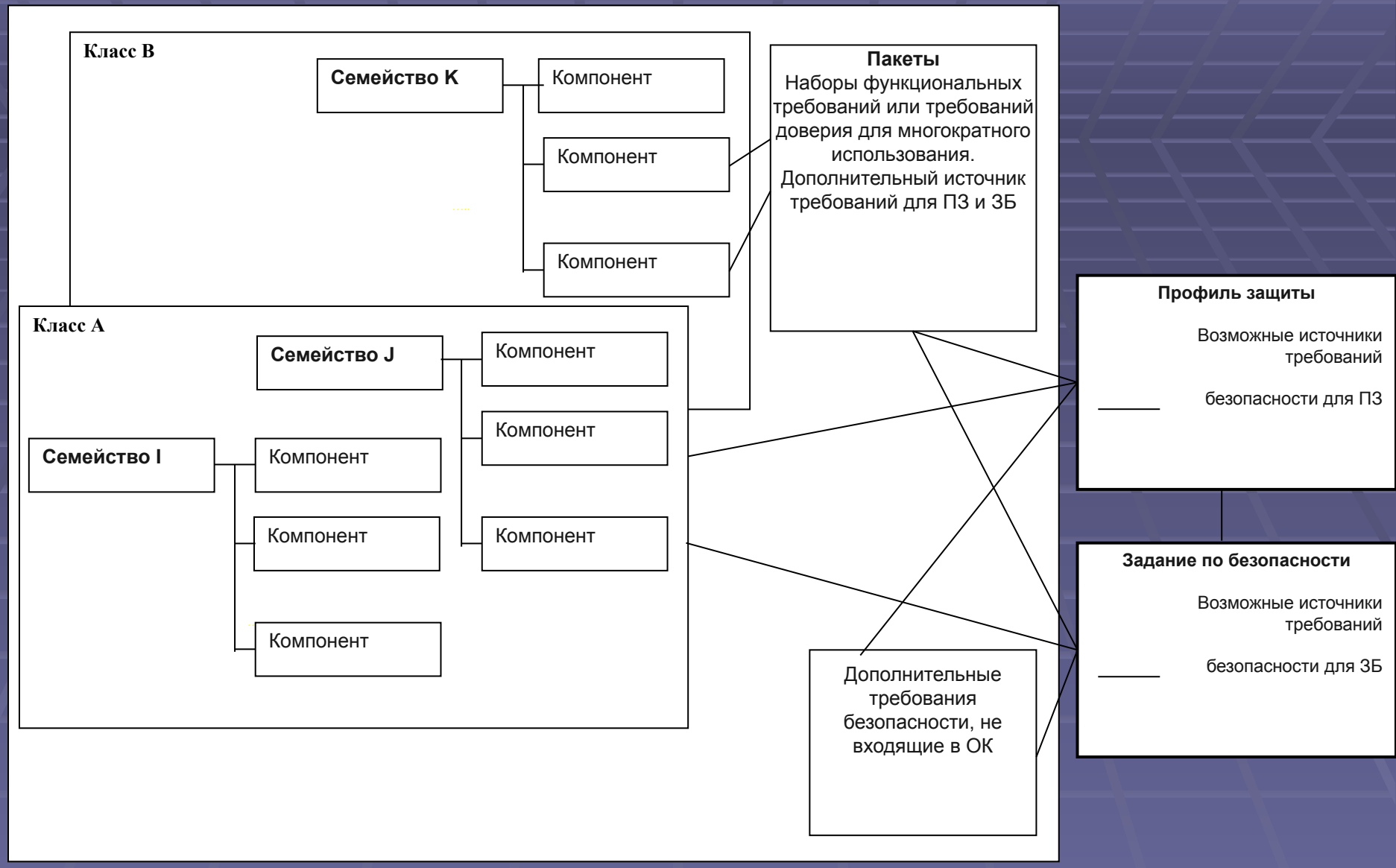
Реализация ОО

Реализацией ОО является его воплощение, основанное на функциональных требованиях безопасности и краткой спецификации ОО, содержащейся в ЗБ. При осуществлении реализации ОО используются инженерные навыки и знания в области ИТ и безопасности. ОО будет отвечать целям безопасности, если он правильно и эффективно реализует все требования безопасности, содержащиеся в ЗБ.

2-й учебный вопрос

Структура, классы требований безопасности. Функциональные требования. Требования доверия.

Организация и структура требований



Классы определяют наиболее общую, "предметную" группировку требований (например, функциональные требования *подотчетности*). Термин "класс" применяется для наиболее общего группирования требований безопасности. Все составляющие класса имеют общую направленность, но различаются по охвату целей безопасности. Составляющие класса называются семействами.

Семейства – это группа наборов требований безопасности, имеющих общие цели безопасности, но различающихся акцентами или строгостью. Составляющие семейства называются компонентами.

Компонент - минимальный набор требований, фигурирующий как целое.

Элемент – это выражение требований безопасности на самом нижнем уровне. Он является тем неделимым требованием безопасности, которое может быть верифицировано при оценке.

Разрешенные операции на компонентах

Компоненты ОК можно использовать точно так, как они сформулированы в ОК, или же можно их конкретизировать, применяя разрешенные операции для выполнения определенной политики безопасности или для противостояния определенной угрозе.

а) **итерация** (iteration), позволяющая неоднократно использовать компонент при различном выполнении в нем операций;
б) **назначение** (assignment), позволяющее специфицировать параметр, устанавливаемый при использовании компонента;
в) **выбор** (selection), позволяющий специфицировать пункты, которые выбираются из перечня, приведенного в компоненте;
г) **уточнение** (refinement), позволяющее осуществлять дополнительную детализацию при использовании компонента.
Некоторые требуемые операции могут быть завершены (полностью или частично) в ПЗ или оставлены для завершения в ЗБ. Однако в ЗБ все операции необходимо завершить.

Функциональные требования

Функциональные требования сгруппированы на основе выполняемой ими роли или обслуживаемой цели безопасности. Всего в "Общих критериях" представлено 11 функциональных классов, 66 семейств, 135 компонентов.

Классы функциональных требований ОК:

1. - *идентификация* и *аутентификация*;
2. - защита данных пользователя;
3. - защита функций безопасности (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
4. - управление безопасностью (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
5. - аудит безопасности (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
6. - доступ к объекту оценки;
7. - приватность (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
8. - использование ресурсов (требования к доступности информации);
9. - криптографическая поддержка (управление ключами);
10. - связь (*аутентификация* сторон, участвующих в обмене данными);
11. - доверенный маршрут/канал (для связи с сервисами безопасности).

Класс "Приватность" содержит 4 семейства функциональных требований.

Анонимность. Позволяет выполнять действия без раскрытия идентификатора пользователя другим пользователям, субъектам и/или объектам. Анонимность может быть полной или выборочной. В последнем случае она может относиться не ко всем операциям и/или не ко всем пользователям (например, у уполномоченного пользователя может оставаться возможность выяснения идентификаторов пользователей).

Псевдонимность. Напоминает анонимность, но при применении псевдонима поддерживается ссылка на идентификатор пользователя для обеспечения *подотчетности* или для других целей.

Невозможность ассоциации. Семейство обеспечивает возможность неоднократного использования информационных сервисов, но не позволяет ассоциировать случаи использования между собой и приписать их одному лицу. Невозможность ассоциации защищает от построения профилей поведения пользователей (и, следовательно, от получения информации на основе подобных профилей).

Скрытность. Требования данного семейства направлены на то, чтобы можно было использовать информационный сервис с сокрытием факта использования. Для *реализации* скрытности может применяться, например, широковещательное распространение информации, без указания конкретного адресата. Годятся для *реализации* скрытности и методы стеганографии, когда скрывается не только содержание сообщения (как в криптографии), но и сам факт его отправки.

Еще один показательный (с нашей точки зрения) класс функциональных требований - "Использование ресурсов", содержащий требования доступности. Он включает три семейства.

Отказоустойчивость. Требования этого семейства направлены на сохранение доступности информационных сервисов даже в случае сбоя или отказа. В ОК различаются активная и пассивная отказоустойчивость. Активный механизм содержит специальные функции, которые активизируются в случае сбоя. Пассивная отказоустойчивость подразумевает наличие избыточности с возможностью нейтрализации ошибок.

Обслуживание по приоритетам. Выполнение этих требований позволяет управлять использованием ресурсов так, что низкоприоритетные операции не могут помешать высокоприоритетным.

Распределение ресурсов. Требования направлены на защиту (путем применения механизма квот) от несанкционированной монополизации ресурсов.

Требования доверия безопасности

Установление доверия безопасности, согласно "Общим критериям", основывается на активном исследовании объекта оценки.

Форма представления требований доверия, в принципе, та же, что и для функциональных требований. Специфика состоит в том, что каждый элемент требований доверия принадлежит одному из трех типов:

- действия разработчиков;
- представление и содержание свидетельств;
- действия оценщиков.

Всего в ОК 10 классов, 44 семейства, 93 компонента требований доверия безопасности. Перечислим классы:

1. - разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до *реализации*);
2. - поддержка жизненного цикла (требования к модели жизненного цикла, включая - порядок устранения недостатков и защиту среды разработки);
3. *- тестирование*;
4. - оценка уязвимостей (включая оценку стойкости функций безопасности);
5. - поставка и эксплуатация;
6. - управление конфигурацией;
7. - руководства (требования к эксплуатационной документации);
8. - поддержка доверия (для поддержки этапов жизненного цикла после сертификации);
9. - оценка профиля защиты;
10. - оценка задания по безопасности.

Оценочные уровни доверия (их семь), содержащие осмысленные комбинации компонентов.

Оценочный **уровень доверия 1** (начальный) предусматривает анализ **функциональной спецификации,** спецификации интерфейсов, эксплуатационной документации, а также независимое *тестирование*. Уровень применим, когда угрозы не рассматриваются как серьезные.

Оценочный **уровень доверия 2**, в дополнение к первому уровню, предусматривает наличие **проекта верхнего уровня** объекта оценки, выборочное независимое *тестирование*, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.

На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

На **уровне 4** добавляются полная спецификация интерфейсов, **проекты нижнего уровня**, анализ подмножества *реализации*, применение неформальной модели *политики безопасности*, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.

Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели *политики безопасности*, полуформальных функциональной спецификации и проекта верхнего уровня с **демонстрацией соответствия** между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.

На **уровне 6** *реализация* должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.

Оценочный **уровень 7** (самый высокий) предусматривает формальную *верификацию* проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.