Обеспечение информационной безопасности, разделы

- Определения, цели, основные положения
- Угрозы
- Построение систем защиты информации
- Стандартизация в области ИБ
- Управление ИБ

Здесь и далее используется терминология документов Государственной Технической Комиссии при Президенте Российской Федерации, которая является основным государственным органом в России, курирующем вопросы защиты информации. Руководящие документы, Положения и Постановления Гостехкомиссии России формируют большую часть отечественной нормативной базы в области защиты информации. С 08.2004 название ГТК изменено на Федеральная служба по техническому и экспортному контролю (ФСТЭК), подчинена МО РФ. http://www.fstec.ru/

Определения

- ***Информация*** в теории компьютерной безопасности определяется как сведения в некоторой предметной области, необходимые для оптимизации принимаемых решений. *(в отличии от вероятностного подхода к определению информации Шеннона, здесь учитывается полезность сведений, и .т.п. свойства)*

- ***Автоматизированная система*** обработки информации (АС) – организационно-техническая система, совокупность взаимосвязанных компонентов: технических средств, программного обеспечения, информации и персонала.

- ***Угроза*** – это потенциальная возможность ущерба ресурсу, как со стороны злоумышленника, так и со стороны различных катастроф: пожаров, наводнений, землетрясений.

- ***Информационная безопасность АС*** – совокупность условий работоспособного состояния АС, при котором АС способна противостоять внутренним и внешним угрозам, а ее функционирование не создает угроз для АС и внешней среды.

Свойства информации и АС

- Из *конфиденциальности* (англ. confidential: доверительный, «по секрету») информации следует необходимость введения ограничений на доступ
- *Целостность* – существование информации в неискаженном виде
- *Доступность* – своевременный и беспрепятственный доступ
- Безопасность обеспечена, если поддерживаются необходимые уровни К, Ц и Д.

Цель создания системы защиты информации

- Организации создают системы защиты информации, чтобы защитить свои ресурсы от угроз.
- Ресурсы включают: производственные секреты, служебную переписку, базы данных клиентов, информацию о транзакциях и т.д.
- Угроза – это ***потенциальная возможность ущерба*** ресурсу, как со стороны злоумышленника, так и со стороны различных катастроф: пожаров, наводнений, землетрясений.

Классификация атак STRIDE

- Spoofing identity (направлена на нарушение конфиденциальности данных)
- Tampering with data (модификация данных, атаки MITM – нарушение целостности)
- Repudiation (любая недоказуемая впоследствии атака)
- Information disclosure (раскрытие – угроза конфиденциальности)
- Denial of service (DoS и DDoS атаки, отказ в обслуживании)
- Elevation of privilege (непривилегированный пользователь получает права более высокого уровня, обычно через уязвимость/ошибки системы. Может быть направлена на любую часть триады CIA)

Анализ угроз, классификация ГТК/ФСТЭК

- По природе возникновения
  - Естественные
  - Искусственные (вызванные деятельностью человека)
- По степени преднамеренности
  - Ошибки, халатности, неумышленная порча носителей и т.п.
  - Преднамеренные действия, хищение информации

Анализ угроз, классификация ГТК/ФСТЭК

- По непосредственному источнику
  - Стихия
  - Человек
    - внедрение агентов
    - разглашение паролей
    - несанкционированное копирование пользователем
  - Санкционированные программно-аппаратные средства (некомпетентное использование)
  - Несанкционированные программно-аппаратные средства (игры, программы не необходимые для выполнения нарушителем служебных обязанностей)

Анализ угроз, классификация ГТК/ФСТЭК

- По положению источника угроз
  - Вне контролируемой зоны (перехват, дистанционная съемка)
  - В пределах контролируемой зоны (подслушивающие устройства, отключение или вывод из строя подсистемы обеспечения работы ВТ)
  - Источник имеет доступ к периферийным устройствам
  - Источник расположен в АС (некорректное использование)

Анализ угроз, классификация ГТК/ФСТЭК

- По степени воздействия на АС
  - Пассивные (структура и содержание АС неизменны)
  - Активные (изменяют АС)
- По этапам доступа к ресурсам АС
- По способу доступа к ресурсам АС
- По текущему месту расположения информации

Основные виды угроз для АС

1. Нарушение конфиденциальности
2. Нарушение целостности
3. Угроза отказа служб

Прим. В англоязычных источниках – т.н. триада CIA (Confidentiality, Integrity, Availability)

4. Угроза раскрытия параметров АС

Методы реализации угроз и принципы обеспечения информационной безопасности

- Угрозы и методы обеспечения защиты реализуются на разных уровнях:
  - Уровень носителей информации
  - Уровень средств взаимодействия с носителем
  - Уровень представления информации
  - Уровень содержания информации

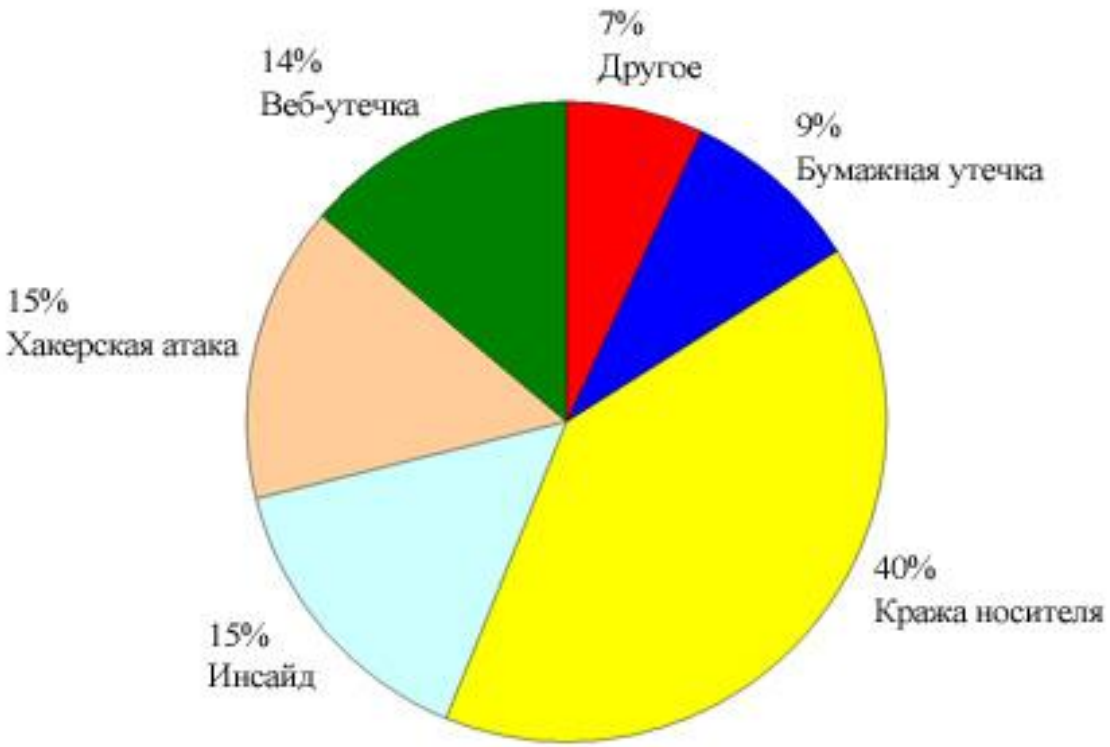
Методы реализации угроз безопасности

Уровень доступа к информации в АС	Основные методы реализации угроз информационной безопасности			
	Угроза раскрытия параметров системы	**Угроза нарушения конфиденциальности**	**Угроза нарушения целостности**	**Угроза отказа служб (отказа доступа к информации)**
Носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации. Перехват ПЭМИН	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Средств взаимодействия с носителем	Получение информации о программно-аппаратной среде. Получение детальной информации о функциях, выполняемых АС. Получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам АС. Совершение пользователем несанкционированных действий. Несанкционированное копирование программного обеспечения. Перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные. Установка и использование нештатного программного обеспечения. Заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонент АС. Обход механизмов защиты АС
Представления информации	Определение способа представления информации	Визуальное наблюдение. Раскрытие представления информации (дешифрование)	Внесение искажения в представление данных; уничтожение данных	Искажение соответствия синтаксических и семантических конструкций языка
Содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации

Виды, каналы утечки информации

- Виды утечки И по ГОСТ 50922-96
  - разглашение
  - несанкционированный доступ
  - получение информации разведками
- Каналы утечки:
  - электромагнитный канал;
  - акустический (виброакустический)канал;
  - визуальный канал;
  - информационный канал.

Распределение утечек по типам



Источник: Perimetrix, 2008

Основные каналы утечек, 1 полугодие 2008 года

Источник: InfoWatch, 2008

Топ-10 утечек, связанных с кражей различных носителей

	Организация	**Сфера деятельности**	**Украденный (потерянный) носитель**	**Количество пострадавших**	**Экспертная оценка ущерба (млн. $)**
1	Bank of New York Mellon	Финансы	Лента	4 500 000	100
2	University of Utah	Образование	Лента	2 200 000	80
3	University of Miami	Образование	Лента	2 100 000	70
4	Central Collection Bureau	Госструктура	Сервер	700 000	50
5	Horizon	Финансы	Ноутбук	300 000	40
6	Lifeblood	Медицина	Ноутбук	320 000	40
7	HSBC	Финансы	Жесткий диск	370 000	40
8	CollegeInvest	Финансы	Жесткий диск	200 000	15
9	Saks Inc.	Розничная сеть	Ноутбук	100 000	15
10	HSBC	Финансы	Сервер	159 000	14

Источник: Perimetrix, 2008

Уровни квалификации атакующих и характерные причины атак

- Низкий уровень
  - Привлечение внимания к себе
  - Опасны тем, что не представляют всех последствий
- Средний уровень
  - Желание заявить о себе в своем сообществе
  - Мщение уволенных/отстраненных сотрудников
  - Часто атакуют известные ресурсы для получения наибольшей огласки, обсуждают свои атаки в форумах
- Высокий уровень
  - Шпионаж, терроризм, получение вознаграждения
  - Методы часто включают введение в заблуждение пользователей и администраторов (social engineering), составление тактических планов атаки
  - Открыто не обсуждают свои атаки

Принципы обеспечения ИБ в АС

- Системности
  - использование системного подхода
- Комплексности
  - комплексное использование разнородных средств
- Непрерывности защиты
  - отсутствие перерывов в обеспечении
- Разумной достаточности
  - затраты, риск и размер возможного ущерба согласованы
- Гибкости управления и применения
  - возможность варьировать уровень защиты
- Открытости алгоритмов и механизмов защиты
  - знание алгоритмов не должно давать преимущества
- Простоты применения
  - минимальные затраты при внедрении и использовании

Методология построения систем защиты информации в АС

- Идентификация угроз
- Анализ рисков (создание плана УР)
- Разработка подсистем безопасности для различных угроз
- Разработка ответных мер для возможных нарушений ИБ

Разработка систем безопасности

- Разработка систем безопасности использует концепцию **управления рисками**, чтобы определить соответствующее риску противодействие.
- Данные, собранные в ходе определения адекватных противодействий, с точки зрения управления рисками, также полезны для аргументации важности информационной защиты и затрат на обеспечение безопасности.

Концепции систем безопасности

- «Глубокая» (многоуровневая) защита – определяет использование совместных технологических и организационных мер на нескольких уровнях противодействия угрозам
- «Минимальных привилегий»
- «Минимальной поверхности атаки»

Фазы решения проблем ИБ системы

- Планирование:
  - команда, угрозы (STRIDE sections/life-cycle), план УР
- Создание:
  - политики и процедуры (создание и внедрение), тренинг администраторов и пользователей, внедрение мер противодействия угрозам
- Управление:
  - мониторинг и управление безопасностью (обнаружение вторжений и реагирование), каждодневное управление, оптимизация политик и процедур.

План управления рисками, стадии

- Идентификация
  - Для каждой угрозы – RS (возможно несколько для каждого ресурса).
- Анализ
  - RS: условия возникновения, последствия, оценка урона: количественно (100-бальная шкала PxI, годовые потери, и т.п.), качественно.
- Планирование УР
  - 4 стратегии: принять, уменьшить, передать, избежать.
  - Должен быть назначен ответственный за каждый риск.
- Разработка методов отслеживания изменений рисков
  - Измерение частоты появления, успеха противодействия.
- Меры по управлению
  - Когда и как изменять план УР, актуализировать его.

Политики безопасности

- Политика безопасности – документ (заверенный руководством организации) в котором сформулированы **основные принципы** обеспечения ИБ организации
- Типы политик безопасности (по основному средству обеспечения):
  - Административная (например, «соглашение о неразглашении»)
  - Техническая (правила сетевых экранов, шаблоны безопасности)
  - Физическая (камеры видеонаблюдения, замки)

- Процедуры безопасности определяют как именно выполнять те или иные действия, касающиеся политики безопасности.
- В организации должны быть не только разработаны политики безопасности, но и также разработаны и опубликованы простые и ясные процедуры соответствующие политике.

- В узком смысле, термин «политика безопасности» часто используется по отношению к системам управления доступом:
- Политика безопасности включает:
  - множество возможных операций над объектами
  - для каждой пары субъект-объект множество разрешенных операций, являющееся подмножеством всего множества возможных операций
- Типы политик безопасности (в части управления доступом):
    - Дискреционная (дискретная, Discretionary Access Control -DAC)
      - все объекты и субъекты идентифицированы
      - права доступа субъекта к объекту определяются внешним правилом
    - Мандатная (полномочная, Mandatory Access Control MAC)
      - все объекты и субъекты идентифицированы
      - задан упорядоченный набор меток секретности
      - каждому объекту присвоена метка секретности – уровень секретности
      - каждому субъекту присвоена метка секретности – уровень доступа

Объекты и субъекты моделей администрирования

- Понятия *объектов* и *субъектов* моделей администрирования и реальных систем эквиваленты соответствующим понятиям теории информационной безопасности (ИБ).
- Под *объектами* моделей понимают данные и функции информационной системы.
- *Субъекты* – это активные компоненты модели – процессы системы часто ассоциированные с пользователями информационной системы.
- *Задачами администрирования в области обеспечения ИБ*, относительно субъектов (С) и объектов (О), являются ранжирование С и О по уровням и контроль за обеспечением соответствия уровня объекта уровню субъекта.

Пример политики безопасности

Политика информационной безопасности

Информация является ценным ресурсом для деятельности Компании и обеспечение информационной безопасности является обязанностью каждого сотрудника.
Настоящая политика определяет основные принципы защиты информационных ресурсов Компании от угроз нарушения конфиденциальности, целостности и доступности.

Доступ к информационным ресурсам предоставляется только в объеме, необходимом для выполнения сотрудниками своих должностных обязанностей.
При построении эффективной системы управления информационной безопасностью Компания руководствуется международными стандартами ISO 17799 и ISO 27001.
Для обеспечения эффективной защиты информации ежегодно проводится комплексный аудит информационной безопасности, включающий в себя аудит системы управления информационной безопасностью и тестирование на возможность несанкционированного проникновения.
Политики информационной безопасности утверждаются президентом Компании.
Все руководители отвечают за выполнение политик информационной безопасности в подчиненных им подразделениях.
Все сотрудники Компании, текущие и бывшие, выполняют требования политик информационной безопасности.
Департамент информационной безопасности осуществляет разработку и внедрение технических и организационных мер для минимизации рисков информационной безопасности.
Департамент внутреннего аудита проводит регулярный аудит эффективности исполнения политик, стандартов и процедур информационной безопасности.
Для обеспечения непрерывности бизнеса Компании должен быть разработан и поддерживаться в актуальном состоянии план непрерывности бизнеса.
Сотрудники Компании проходят ежегодное обучение в области обеспечения информационной безопасности.

Стандартизация в области ИБ

Руководящие документы ГТК,1992

- Концепция защиты средств вычислительной техники от НСДкИ.
- Защита от несанкционированного доступа к информации (НСДкИ). Термины и определения.
- Средства вычислительной техники. Защита от НСДкИ. Показатели защищенности от НСДкИ.
- Автоматизированные системы (АС). Защита от НСДкИ. Классификация АС и требования по защите информации.
- Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в АС и средствах вычислительной техники.

Развитие нормативной базы, 1997-1999 гг.

- СВТ. Межсетевые экраны. Защита от НСД. Показатели защищенности от НСД к информации. 1997

Новые нормативные документы по ГОСТ Р ИСО/МЭК 15408-2002 (т.н. «Общие критерии»)

для продуктов и систем информационных технологий, предназначенных для обработки информации, отнесенной к информации ограниченного доступа

- Безопасность информационных технологий. Критерии оценки безопасности информационных технологий
- Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности
- Безопасность информационных технологий. Руководство по регистрации профилей защиты
- Безопасность информационных технологий. Руководство по формированию семейств профилей защиты
- Руководство по разработке профилей защиты и заданий по безопасности

Структура Системы сертификации средств защиты информации по требованиям безопасности информации

- **Гостехкомиссия России** (федеральный орган исполнительной власти, уполномоченный проводить работу по обязательной сертификации). С 08.2004 ФСТЕК http://www.fstec.ru/ ;
- **органы по сертификации средств защиты информации** - органы, проводящие сертификацию определенной продукции;
- **испытательные лаборатории** - лаборатории, проводящие сертификационные испытания (отдельные виды этих испытаний) определенной продукции;
- **заявители** - изготовители, продавцы или потребители продукции

Перечень объектов информатизации, подлежащих аттестации в Системе сертификации средств защиты информации по требованиям безопасности информации

- Автоматизированные системы различного уровня и назначения.
- Системы связи, приема, обработки и передачи данных.
- Системы отображения и размножения.
- Помещения, предназначенные для ведения конфиденциальных переговоров.

Способы НСД и принципы защиты от информации (по документам ГТК)

- НСД – доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств СВТ и АС
- Способы НСД (по ГТК):
  - непосредственное обращения к объектам;
  - создание ПО для обхода защиты;
  - модификация средств защиты;
  - внедрение программных или технических средств НСД.
- Принципы защиты информации (по ГТК):
  - защита основывается на положениях и требованиях существующих законах и стандартах РФ
  - защита СВТ обеспечивается комплексом программно-технических средств (КПТС)
  - защита АС обеспечивается КПТС и организационными мерами
  - защита обеспечивается во всех режимах и на всех этапах
  - КПТС защиты не должен существенно ухудшать основные характеристики производительности АС
  - неотъемлемая часть работ по защите СВТ – оценка ее эффективности
  - тоже для АС

Классы защищенности СВТ (ГТК)

Показатель защищенности	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	=	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчужденный физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Текстовая документация .	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Примечания: "-"- нет требований к данному классу;"+"- новые или дополнительные требования; "="- требования совпадают с требованиями к СВТ предыдущего класса.

Классы защищенности АС (ГТК)

- Три группы классов защищенности:
  - 3 группа – один пользователь и один уровень конфиденциальности (УК);
  - 2 группа – многопользовательские, с носителями различного УК;
  - 1 группа – многопользовательские, с разными правами доступа, одновременная обработка информации с различными УК
- Всего – 9 классов защищенности АС:
  - 3Б, 3А, 2Б, 2В, 2А, 1Д, 1Г, 1Б, 1В, 1А

Классы защищенности АС (ГТК)

Подсистемы защиты и требования к ним	Классы защищенности								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. ***Подсистема управления доступом***									
1.1. Идентификация. Проверка подлинности и контроль доступа субъектов:									
в систему	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ				+		+	+	+	+
к программам				+		+	+	+	+
к томам, каталогам, файлам, записям, полям записей				+		+	+	+	+
1.2. Управление потоками информации				+			+	+	+
Примечание: "+"- требование к данному классу присутствует, в остальных случаях данное требование необязательно.									

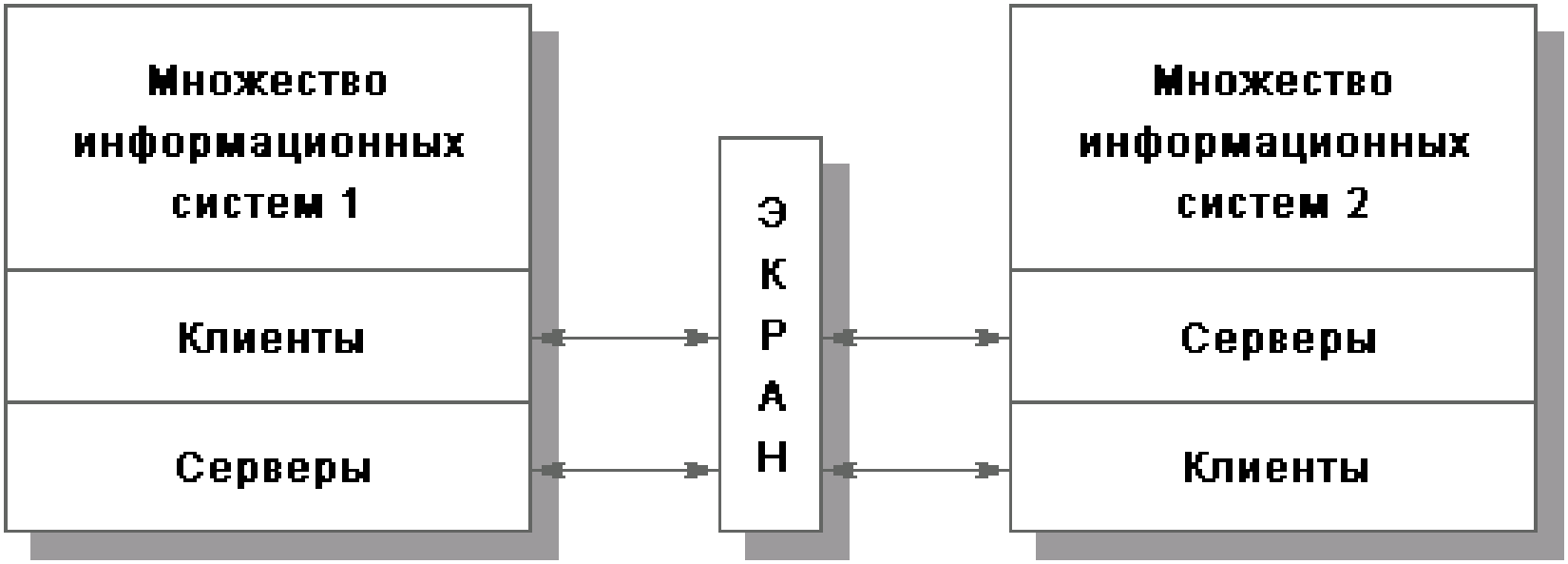
Классы защищенности АС (ГТК)

Подсистемы защиты и требования к ним	Классы защищенности								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
2. Подсистема регистрации и учета									
2.1. Регистрация и учет:									
входа/выхода субъектов доступа в/из системы (узла сети)	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов		+		+		+	+	+	+
запуска/завершения программ и процессов (заданий, задач)				+		+	+	+	+
доступа программ субъектов к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи				+		+	+	+	+
доступа программ субъектов,			+		+	+	+	+	
доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, каталогам, файлам, записям, полям записей изменения полномочий субъектов доступа						+	+	+	
создаваемых защищаемых объектов доступа			+			+	+	+	
2.2. Учет носителей информации	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей		+		+		+	+	+	+
2.4. Сигнализация попыток нарушения защиты							+	+	+
Примечание: "+"- требование к данному классу присутствует, в остальных случаях данное требование необязательно.									

Классы защищенности АС (ГТК)

Подсистемы защиты и требования к ним	Классы защищенности								
	3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**
3. Криптографическая подсистема									
3.1. Шифрование конфиденциальной информации				+				+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах									+
3.3. Использование аттестованных (сертифицированных) криптографических средств				+				+	+
4. Подсистема обеспечения целостности									
4.1. Обеспечение целостности программных средств и обрабатываемой информации	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы) защиты информации в АС				+			+	+	+
4.4. Периодическое тестирование СЗИ НСД	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты		+		+			+	+	+
Примечание: "+"- требование к данному классу присутствует, в остальных случаях данное требование необязательно.									

МЭ


Множество информационных систем 1
Клиенты
Серверы
Э К Р А Н
Множество информационных систем 2
Серверы
Клиенты

МЭ – набор фильтров

Классы защищенности МЭ (ГТК)

Выделяется пять показателей защищенности:

1. Управление доступом
2. Идентификация и аутентификация
3. Регистрация событий и оповещение
4. Контроль целостности
5. Восстановление работоспособности

Определяется следующие пять классов защищенности МЭ:

- Простейшие фильтрующие маршрутизаторы - 5 класс
- Пакетные фильтры сетевого уровня - 4 класс
- Простейшие МЭ прикладного уровня - 3 класс
- МЭ базового уровня - 2 класс
- Продвинутые МЭ - 1 класс

Trusted Computer System Evaluation Criteria - TCSEC,DoD-83

- Trusted Computer System Evaluation Criteria. US Department of Defense, CSC-STD-001-83, Aug. 1983
  - Trusted network Interpretation. National Computer Security Center, July 1987
  - Trusted DBMS Interpretation. National Computer Security Center, April 1991
  - The Interpreted TCSEC Requirements, Jan 1995

Критерии TCSEC

- Три категории требований
  - Политика безопасности:
    - Поддержка политики безопасности
    - Метки безопасности (грифы)
  - Подотчетность
    - Идентификация и аутентификация
    - Регистрация событий
  - Гарантии (корректность)
    - Контроль функционирования средств защиты
    - Непрерывность защиты

Классы защищенности TSEC

Базовые требования "Оранжевой книги"	Классы защищенности					
	C1	C2	B1	B2	B3	A1
Политика безопасности						
1 . Дискреционная политика безопасности	+	+	+	=	=	=
2. Мандатная политика безопасности	-	-	+	+	=	=
3. Метки секретности	-	-	+	+	=	=
4. Целостность меток	-	-	+	=	=	=
5. Рабочие метки	-	-	-	+	=	=
6. Повторение меток	-	-	+	=	=	=
7. Освобождение ресурсов при повторном использовании объектов	-	+	=	+	=	=
8. Изолирование модулей	-	+	=	=	=	=
9. Пометка устройств ввода/вывода	-	-	+	=	=	=
10. Пометка читаемого вывода	-	-	+	=	=	=
Подотчетность						
11. Идентификация и аутентификация	+	+	=	=	=	=
12. Аудит	-	+	+	+	+	=
13. Защищенный канал (доверенный путь)	-	-	-	+	=	=
Гарантии						
14. Проектная спецификация и верификация	-	-	+	+	+	+
15. Системная архитектура	+	=	=	+	+	=
16. Целостность системы	+	=	=	=	=	=
17. Тестирование системы безопасности	+	+	+	+	+	=
18. Доверенное восстановление после сбоев	-	-	-	-	+	=
19. Управление конфигурацией системы	-	-	-	+	+	+
20. Доверенное дооснащение системы	-	-	-	+	+	=
21. Доверенное распространение	-	-	-	-	+	=
22. Анализ скрытых каналов	-	-	-	+	+	+
Документация						
23. Руководство пользователя	+	=	=	=	=	=
24. Руководство по конфигурированию системы защиты	+	+	+	+	+	=
25. Документация по тестированию	+	=	=	=	=	+
26. Проектная документация	+	=	+	+	=	+
Примечания. "-"- нет требований к данному классу; "+"- новые или дополнительные требования; "="-требования совпадают с требованиями к СВТ предыдущего класса						

Европейские критерии безопасности. ITSEC, 1991

- Information Technology Security Evaluation Criteria. Harmonized Criteria of France-Germany-Netherlands-United Kingdom. – Department of Trade and Industry, London, 1991
  - Target of Evaluation (аналог Trusted Computer Base)
    - «система»
    - «продукт»

Применение критериев ранжирования к F требованиям

Функциональное требование	Широта сферы применения	Степень детализации	Функциональный состав средств защиты	Обеспечиваемый уровень безопасности
Политика безопасности	*	*	*	*
Политика аудита	*	*	*	*
Идентификация и аутентификация			*	*
Регистрация в системе			*	
Обеспечение прямого взаимодействия с компьютерной системой	*			
Регистрация и учет событий			*	*
Политика управления доступом			*	
Контроль скрытых каналов	*			
Политика обеспечения работоспособности	*	*		*
Контроль над распределением ресурсов				
Отказоустойчивость	*	*	*	*
Управление безопасностью			*	*
Мониторинг взаимодействий	*	*		
Логическая защита компьютерной системы			*	
Физическая защита компьютерной системы			*	*
Самоконтроль компьютерной системы	*		*	
Инициализация и восстановление компьютерной системы			*	
Ограничение привилегий при работе с компьютерной системой		*		
Простота использования компьютерной системы	*			
Знак «*» указывает на какие свойства АС влияет реализация того или иного защитного механизма				

Federal Criteria for Information Technology Security – компонент Federal Information Processing Standard

Разработан National Security Agency совместно с National Institute of Standards and Technologies (США ,1992)

Развитие стандартов

- Federal Criteria for Information Technology Security (как составляющая Federal Information Processing Standard) США, 1992
- Common Criteria for Information Technology Security Evaluation, США/ Канада/Нидерланды/Великобритания/Франция/Германия,1998.
- ГОСТ Р ИСО/МЭК 15408-1,2,3-2002 «***Общие критерии*** оценки безопасности ИТ» (перевод ISO 15408). Вводится в действие с 1.01.2004

Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)

- Стандарт Common Criteria (“Общие Критерии …”) разрабатывался с целью облегчить заказчикам поиск продуктов, удовлетворяющих их требованиям.
  - представляет собой систему строгих независимых критериев безопасности (т. н. «профилей защиты» — Protection Profiles),
  - для оценки информационных продуктов устанавливает гарантированные уровни соответствия (Evaluations Assurance Levels, EAL) или оценочные уровни доверия - ОУД.
  - в СС главное внимание уделено защите от НСД. Модификации или потери доступа к информации в результате случайных или преднамеренных действий информационной безопасности остались не рассмотренными.
- Пример сертификации по «Общим критериям» - семейство систем Microsoft Windows 2000:
  - семейства систем Windows 2000 отвечают высшему уровню доверия для серийно выпускаемых систем - EAL4
  - Сертификат выдан на три года по правилам ГТК.
  - Шкала оценок подразумевает всего 7 уровней доверия, выше 4-го – особые требования конкретных государств
  - Был использован профиль защиты CAPP (Controlled access protection profile) «CAPP обеспечивает уровень защиты, подходящий в предположениях о невраждебном и хорошо управляемом сообществе пользователей, требующем защиты от неумышленных или случайных попыток нарушить безопасность системы.»
  - *Основные принципы ОК состоят в том, что следует сформулировать угрозы безопасности и положения политики безопасности организации, а достаточность предложенных мер безопасности должна быть продемонстрирована. Более того, следует предпринять меры по уменьшению вероятности наличия уязвимостей, возможности их проявления (т.е. преднамеренного использования или непреднамеренной активизации), а также степени ущерба, который может явиться следствием проявления уязвимостей. Дополнительно следует предпринять меры для облегчения последующей идентификации уязвимостей, а также по их устранению, ослаблению и/или оповещению об их использовании или активизации [3].*

Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)

- Первая часть «Общих критериев» содержит определение общих понятий, концепции, описание модели и методики проведения оценки безопасности ИТ. В ней вводится понятийный аппарат и определяются принципы формализации предметной области.
- Требования к функциональности средств защиты приводятся во второй части «Общих критериев» и могут быть непосредственно использованы при анализе защищенности для оценки полноты реализованных в АС (СВТ) функций безопасности.
- Третья часть «Общих критериев» содержит класс требований по анализу уязвимостей средств и механизмов защиты под названием AVA: Vulnerability Assessment. Данный класс требований определяет методы, которые должны использоваться для предупреждения, выявления и ликвидации определенных типов уязвимостей

Новые нормативные документы, базирующиеся на ГОСТ Р ИСО/МЭК 15408-2002

для продуктов и систем информационных технологий, предназначенных для обработки информации, отнесенной к информации ограниченного доступа

- Безопасность информационных технологий. Критерии оценки безопасности информационных технологий
- Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности
- Безопасность информационных технологий. Руководство по регистрации профилей защиты
- Безопасность информационных технологий. Руководство по формированию семейств профилей защиты
- Руководство по разработке профилей защиты и заданий по безопасности

Термины и определения нормативных документов, базирующихся на ГОСТ Р ИСО/МЭК 15408-2002

- ***Базовая стойкость функции безопасности:*** Уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от случайного нарушения безопасности ОО нарушителями с низким потенциалом нападения.
- ***Безопасность ИТ:*** Характеристика защищенности информации и изделий ИТ от воздействия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способности изделий ИТ выполнять предусмотренные функции без нанесения неприемлемого ущерба.
- ***Высокая стойкость функции безопасности:*** Уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от тщательно спланированного и организованного нарушения безопасности ОО нарушителями с высоким потенциалом нападения.
- ***Информационная технология:*** *Приемы, способы и методы* применения технических и программных средств при выполнении функций обработки информации.
- ***Изделие ИТ:*** Обобщенный термин для продуктов и систем ИТ.
- ***Продукт ИТ:*** Совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы ИТ.
- ***Система ИТ:*** Специфическое воплощение изделия ИТ с конкретным назначением и условиями эксплуатации.

Термины и определения нормативных документов, базирующихся на ГОСТ Р ИСО/МЭК 15408-2002

- ***Объект оценки:*** Подлежащие оценке продукт или система ИТ с руководствами администратора и пользователя.

- ***Профиль защиты:*** *Независимая от реализации совокупность требований безопасности* для некоторой категории изделий ИТ, отвечающая специфическим запросам потребителя.
- ***Семейство профилей защиты:*** *Совокупность упорядоченных взаимосвязанных ПЗ*, которые относятся к определенному типу изделий ИТ.

- ***Функция безопасности:*** Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных требований безопасности.
- ***Средняя стойкость функции безопасности:*** Уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения.
- ***Стойкость функции безопасности:*** Характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного поведения при прямой атаке на лежащие в ее основе механизмы безопасности.

- ***Пакет доверия:*** Предназначенная для многократного использования *совокупность компонентов доверия* для удовлетворения совокупности определенных целей безопасности. Примером ПД является оценочный уровень доверия.
- ***Функциональный пакет:*** Предназначенная для многократного использования *совокупность функциональных компонентов*, объединенных для удовлетворения совокупности определенных целей безопасности.

Требования AVA (по анализу уязвимостей средств и механизмов защиты)

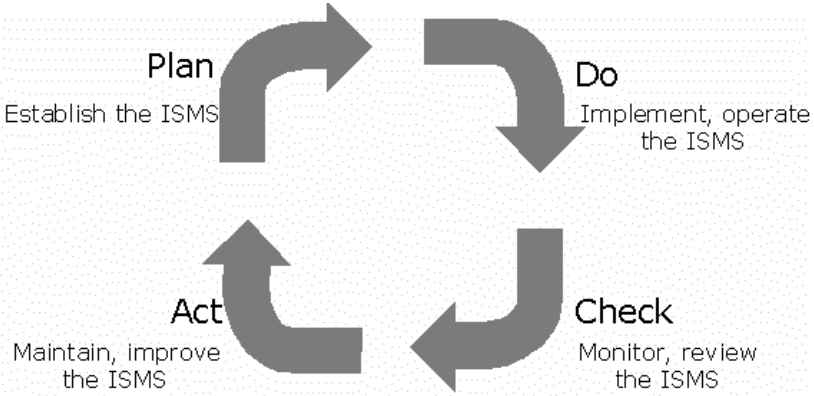
- методы, которые должны использоваться для предупреждения, выявления и ликвидации следующих типов уязвимостей:
  - Наличие побочных каналов утечки информации;
  - Ошибки в конфигурации, либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние;
  - Недостаточная надежность (стойкость) механизмов безопасности, реализующих соответствующие функции безопасности;
  - Наличие уязвимостей в средствах защиты информации, позволяющих пользователям получать НСД к информации в обход существующих механизмов защиты.

Требования гарантированности оценки уязвимостей

- Семейство AVA_CCA: Covert Channel Analysis (Анализ каналов утечки информации)
- Семейство AVA_MSU: Misuse (Ошибки в конфигурации, либо неправильное использование системы, приводящее к переходу системы в небезопасное состояние)
- Семейство AVA_SOF: Strength of TOE Security Functions (Стойкость функций безопасности, обеспечиваемая их реализацией)
- Семейство AVA_VLA: Vulnerability Analysis (Анализ уязвимостей)

PDCA (Plan – Do – Check – Act)

- У ISO существует мощная методологическая основа в области планирования, внедрения, мониторинга и поддержки систем ИБ, непрерывная последовательность которой базируется на т.н. «Цикле Деминга». В стандартах ISO принято использовать для обозначения этого цикла аббревиатуру PDCA (Plan – Do – Check – Act, Планирование – Внедрение – Мониторинг – Поддержка/улучшение) – модель Организации Экономического Сотрудничества и Развития (OECD). Т.о. используется процессный итеративный подход.

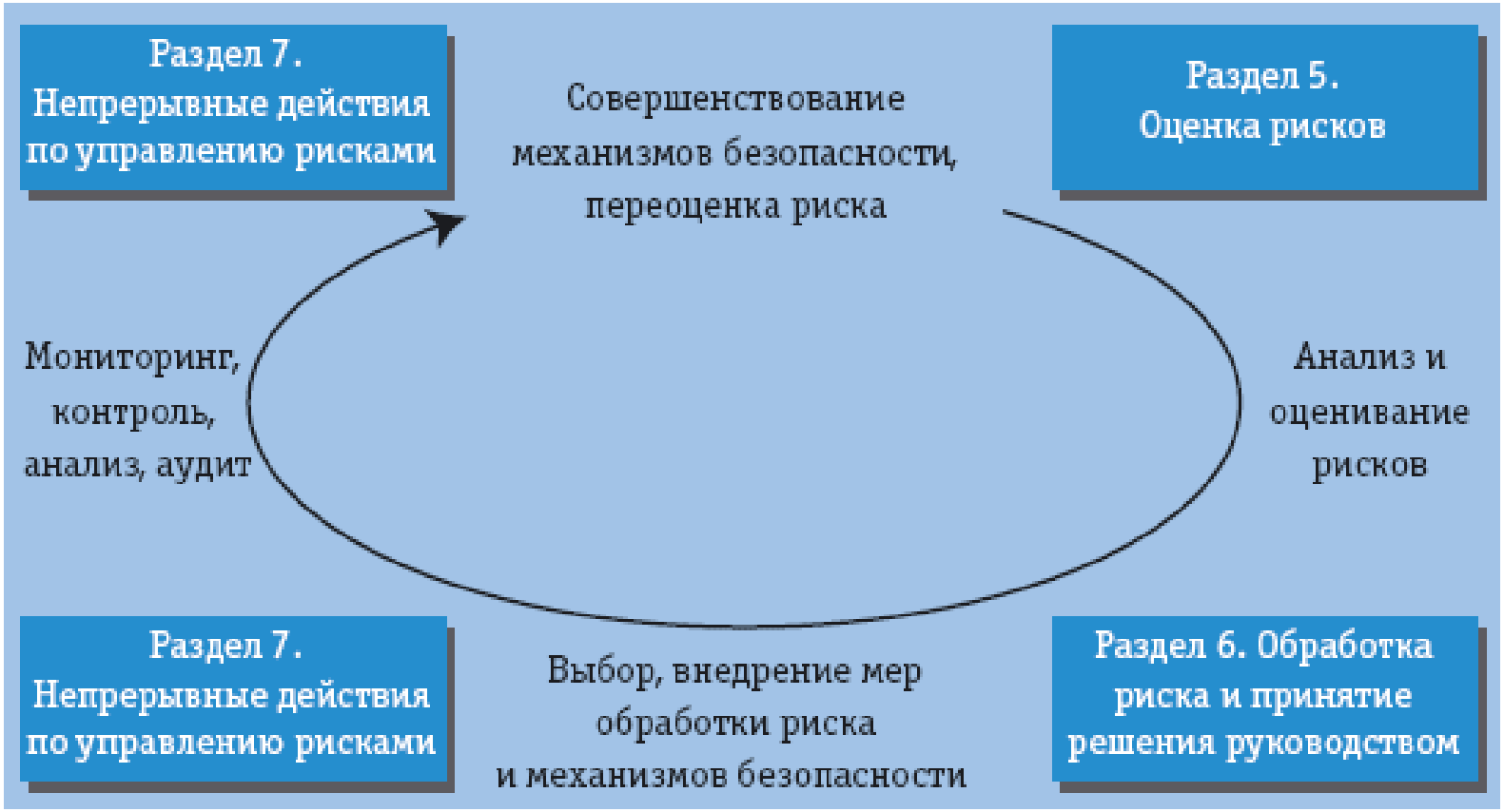


Управление ИБ

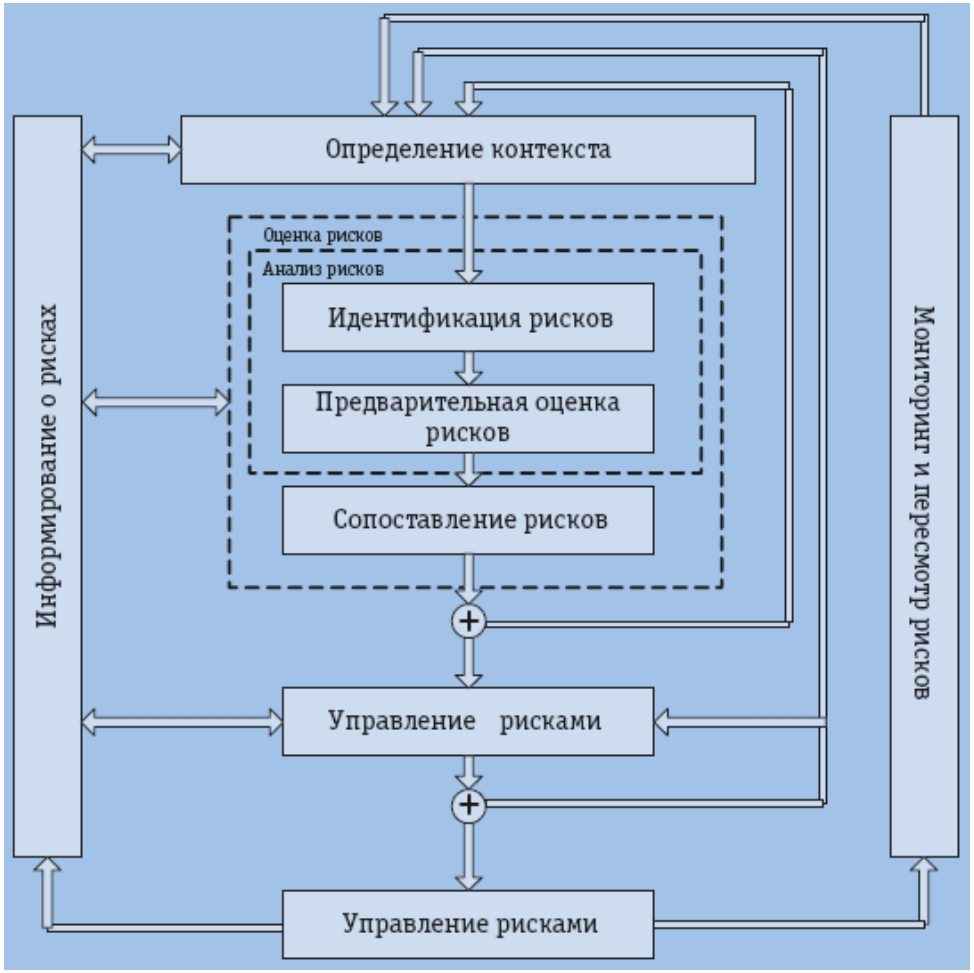
- ISO находится в процессе реорганизации стандартов по ИБ: во-первых они объединяются в серию ISO27000, во-вторых сама серия «гармонизируется» с другими стандартами управления – ISO9001, ISO14000.

- В настоящее время, серия 27000 включает в себя следующие важные стандарты:
- 1. Стандарт ISO27001 (основан на британском BS7799-2, есть российский перевод ГОСТ27001:2005) - определяет требования к системе управления ИБ (ISMS, Information Security Management System) по ее определению, внедрению, работе, мониторингу, поддержки и улучшению.
- 2. Стандарт ISO27002 (основан на британском BS7799-1, есть российский перевод ГОСТ17799:2005) – определяет правила и средства управления.
- 3. Проект ISO27003 (выход в 2009г.) – руководство по внедрению ISMS.
- 4. Проект ISO27004 – определяет метрики и измерения эффективности ISMS.
- 5. Проект ISO27005 (основан на BS7799-3 и ISO13335) – посвящен управлению рисками (УР).
- 6. Стандарт ISO27007 – руководство по аудиту ISMS.

Фазы управления рисками стандарта ISO 27005



Модель управления рисками ISO 27005



Международный стандарт ISO/IEC 17799

- ISO 17799: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) содержит:
  - Основные понятия и определения информационной безопасности
  - Политика информационной безопасности компании
  - Организация информационной безопасности на предприятии
  - Классификация и управление корпоративными информационными ресурсами
  - Кадровый менеджмент и информационная безопасность
  - Физическая безопасность
  - Администрирование безопасности корпоративных информационных систем
  - Управление доступом
  - Требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения
  - Управление бизнес-процессами компании с точки зрения информационной безопасности
  - Внутренний аудит информационной безопасности компании

10 правил ISO 17799 по управлению информационной безопасностью

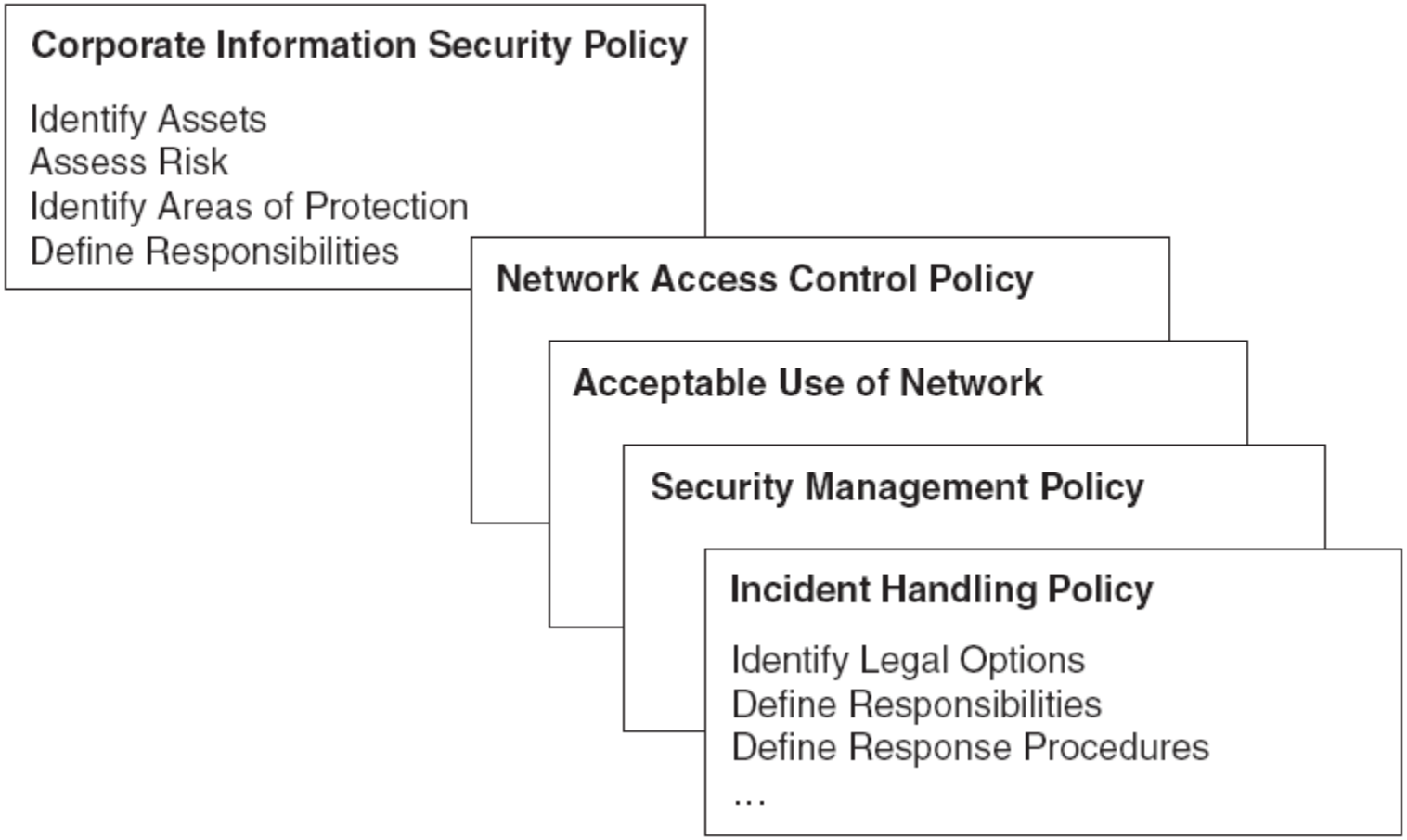
- ISO/IEC 17799:2000: Code of Practice for Information Security Management (Практические правила управления информационной безопасностью)
  - Политика безопасности
  - Организация защиты
  - Классификация ресурсов и их контроль
  - Безопасность персонала
  - Физическая безопасность
  - Администрирование компьютерных систем и вычислительных сетей
  - Управление доступом
  - Разработка и сопровождение информационных систем
  - Планирование бесперебойной работы организации
  - Контроль выполнения требований политики безопасности

10 ключевых средств контроля ISO 17799

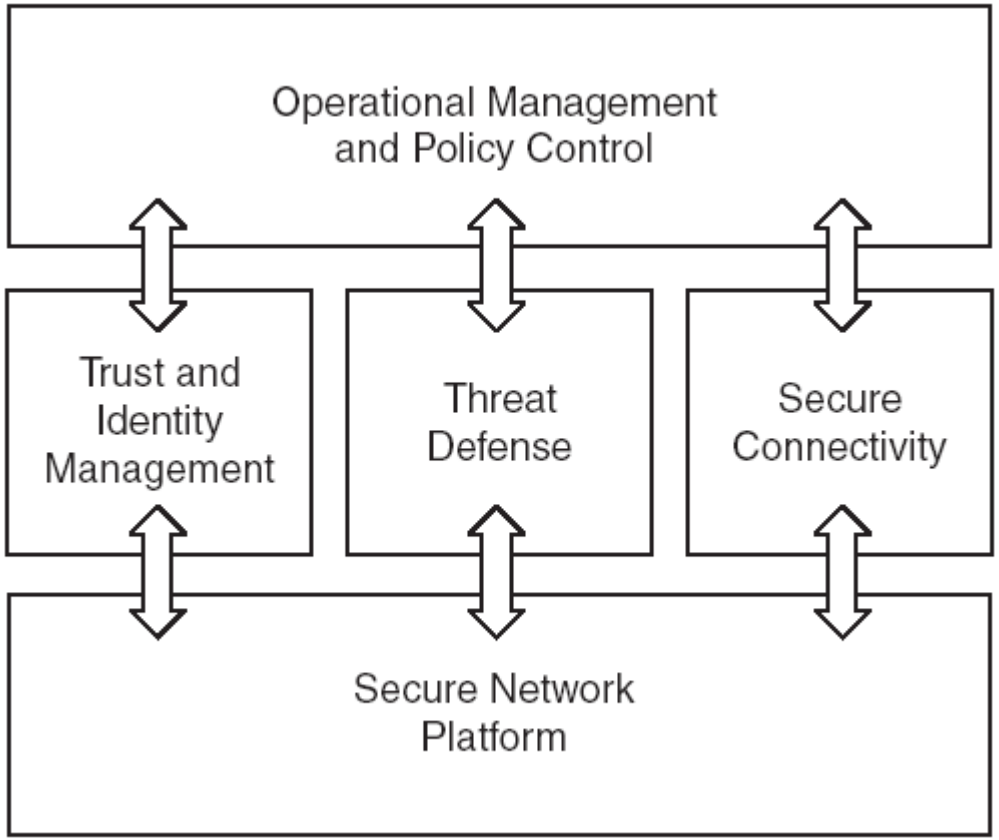
- документ о политике информационной безопасности;
- распределение обязанностей по обеспечению информационной безопасности;
- обучение и подготовка персонала к поддержанию режима информационной безопасности;
- уведомление о случаях нарушения защиты;
- средства защиты от вирусов;
- планирование бесперебойной работы организации;
- контроль над копированием программного обеспечения, защищенного законом об авторском праве;
- защита документации организации;
- защита данных;
- контроль соответствия политике безопасности

Сетевая политика, документы

Network Security Policy Documents



Cisco Self-Defending Network



Уязвимости ОС и ПО

- Команды быстрого реагирования
  - CERT(tm) - первая computer security incident response team (USA/DARPA/)
  - RU-CERT - это CSIRT (Computer Security Incident Response Team) РФ. Создан РосНИИРОС, является официальным CSIRT сервисом для пользователей опорной сети RBNET. С 2002 года RU-CERT является полным членом (full member) FIRST (Forum of Incident Response Team, first.org).
  - Common Vulnerabilities & Exposures(CVE)
  - Bugtraq, bugtraq.ru (публикация сообщений об уязвимостях ПО различных фирм-разработчиков) (→SecurityFocus) Symantec

Ссылки

1. Девянин П.Н. и др. Теоретические основы компьютерной безопасности: Учебное пособие для вузов. - М.: Радио и связь, 2000. - 192 с.
2. Федеральная служба по техническому и экспортному контролю (ФСТЭК), http://www.fstec.ru/
3. Консалтинговая группа «ЛЕКС», http://www.osnovi-bezopasnost.ru/
4. Марков А., Цирлов В. Управление рисками — нормативный вакуум информационной безопасности - http://www.osp.ru/os/2007/08/4492873/
5. L:\Лекции\4 курс\ИБИС => GOST-17799-2005.pdf