Обзор стандартов и методических документов в области защиты информации

Лекция

Критерии безопасности компьютерных систем (“Оранжевая книга”)
TCSEC - Trusted Computer System Evaluation Criteria

Разработчики: МО США, 1983 год.

Цель разработки

- Определения требований безопасности, предъявляемых к аппаратному, программному и специальному обеспечению компьютерных систем и выработки соответствующей методологии и технологии анализа степени поддержки политики безопасности в компьютерных системах военного назначения.

Эволюция

- 1985 г. “Оранжевая книга” была принята в качестве стандарта МО США (DOD TCSEC).
- 1987 и 1991 гг. стандарт был дополнен требованиями для гарантированной поддержки политики безопасности в распределённых вычислительных сетях и базах данных.

- Впервые нормативно определено понятие, **“политика безопасности”,** TCB (*Trusted Computing Base* – вычислительная база защиты или ядро защиты).
- ***Безопасная компьютерная система*** – это система, поддерживающая управление доступом к обрабатываемой в ней информации таким образом, что только соответствующим образом авторизованные пользователи или процессы, действующие от их имени, получают возможность читать, писать, создавать и удалять информацию.
- **Предложены категории требований безопасности:**

  - политика безопасности;
  - аудит;
  - корректность.

*Предложенные концепции защиты и набор функциональных требований послужили **основой** для формирования всех появившихся впоследствии стандартов безопасности.*

Сформулированы базовые требования безопасности

1. Политика безопасности.

- *Система должна поддерживать точно определенную политику безопасности.*
- *Возможность осуществления субъектами доступа к объектам должна определяться на основании их идентификации и набора правил управления доступом.*

2. Метки.

- *С объектами должны быть ассоциированы метки безопасности, используемые в качестве атрибутов контроля доступа.*

3. Идентификация и аутентификация.

- *Все субъекты должны иметь уникальные идентификаторы.*
- *Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификация) и правил разграничения доступа.*
- *Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения.*

4. Регистрация и учет.

- *Все происходящие в системе события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе.*
- *Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность.*
- *Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.*

5. Контроль корректности функционирования средств защиты.

- *Все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учет, должны находиться под контролем средств, проверяющих корректность их функционирования.*
- *Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.*

Базовые требования безопасности

6. Непрерывность защиты.

- *Все средства защиты должны быть защищены от несанкционированного вмешательства и/или отключения.*
- *Защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом.*
- *Данное требование распространяется на весь жизненный цикл компьютерной системы.*
- *Его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.*

направлены непосредственно на обеспечение безопасности информации

1. ***Политика безопасности.***
2. ***Метки.***
3. ***Идентификация и аутентификация.***
4. ***Регистрация и учет.***
5. ***Контроль корректности функционирования средств защиты.***
6. ***Непрерывность защиты.***

направлены на качество самих средств защиты

Оранжевая

Приведена классификация систем

Класс D – минимальная защита. Зарезервирован для систем, не удовлетворяющих ни одному из других классов защиты.

Класс C1 – защита, основанная на разграничении доступа (DAC). Обеспечивается разграничение пользователей и данных.

Класс C2 – защита, основанная на управляемом контроле доступом.

Класс B1 – мандатная защита, основанная на присваивании меток объектам и субъектам, находящимся под контролем TCB.

Класс B2 – структурированная защита. Управление доступом распространяется на все субъекты и объекты системы.

Класс B3 – домены безопасности. Реализации концепции монитора обращений, который гарантированно защищен от доступа, порчи и подделки, обрабатывает все обращения, прост для анализа и тестирования

Класс A1 – верифицированный проект. Проект TCB должен быть представлен в виде формализованной и верифицированной математическими методами спецификации.

Разработчики стандарта

- Национальный институт стандартов и технологий США *(National Institute of Standarts and Technology)*
- Агентство национальной безопасности США *(National Security Agency)*.

Цель разработки

- одна из составляющих “Американского федерального стандарта по обработке информации” (Federal Information Processing Standart), призванная заменить **“Оранжевую книгу”**
- охват полного спектра проблем, связанных с защитой и обеспечением безопасности, включающих все аспекты обеспечения **конфиденциальности, целостности и работоспособности** *(доступности)*

Объекты применения требований безопасности “Федеральных критериев”

- **Продукты Информационных Технологий** (Information Technology Products) - *совокупность аппаратных и/или программных средств, которая представляет собой поставляемое конечному потребителю готовое к использованию средство обработки информации.*
- **Системы Обработки Информации** (Information Technology Systems).
- Вводится ключевое понятие концепции информационной безопасности **“Профиль защиты”** *(Protection Profile)* - нормативный документ, регламентирующий все аспекты безопасности **ИТ - продукта** в виде требований к его **проектированию, технологии разработки и квалификационному анализу**.
- Регламентируется **этап** разработки и анализа **Профиля защиты**.

Канадские критерии оценки доверенных компьютерных *продуктов*
Canadian Trusted Computer Product Evaluation Criteria

Разработчики стандарта

- Центр безопасности связи Канады *(Canadian System Security Center Communication Security Establishment).*

Цель разработки

- Национальный стандарт безопасности компьютерных систем.

Особенности

- возможность применения критериев к широкому кругу различных по назначению систем.
- реализован принцип дуального представления требований безопасности в виде ***функциональных критериев*** к средствам защиты и требований к ***адекватности их реализации***.

Функциональные критерии

частные метрики, предназначенные для определения показателей эффективности средств защиты в виде уровня их возможностей по отражению угроз соответствующего типа

группы критериев *(разделы стандарта)*

критерии конфиденциальности	**критерии целостности**	**критерии работоспособности**	**критерии аудита**
угрозы НСД к информации	угрозы несанкционированного изменения информации или ее искажения	угрозы работоспособности	угрозы, направленные на фальсификацию протоколов и манипуляции с внутрисистемной информацией

совокупность возможностей системы по отражению соответствующего ***класса угроз***

Приложения:

- подробное описание концепции обеспечения безопасности информации;
- руководство по применению функциональных критериев;
- руководство по применению критериев адекватности реализации;
- набор стандартных ***Профилей защиты*** *(типовые наборы требований к компьютерным системам, применяющимся в государственных учреждениях).*

Подход к оценке уровня безопасности

- отвергается подход к оценке с помощью универсальной шкалы;
- используется ***независимое ранжирование требований по каждому разделу, образующее множество частных критериев***, характеризующих работу подсистем обеспечения безопасности;
- уровень ***адекватности реализации*** политики безопасности характеризует качество всей системы в целом.

Разработчики стандарта

- соответствующие органы Франции, Германии, Нидерландов и Великобритании. *Опубликованы в июне 1991 года.*

Новое:

- **вводится** понятие **адекватности** средств защиты.
- определяется отдельная **шкала** для критериев адекватности. *адекватности средств защиты придаётся даже большее значение чем их функциональности этот подход используется во многих появившихся позднее стандартах информационной безопасности.*
- признаётся **возможность наличия недостатков** в сертифицированных системах *(что свидетельствует о **реалистичном** взгляде на существующее положение и признании того очевидного факта, что реальные системы еще весьма несовершенны и далеки от идеала).*

Критерии оценки безопасности информационных технологий
Evaluation Criteria for IT Security (ECITS)

Разработчики стандарта *(на общественных началах)*

- Рабочая группа 3 подкомитета 27 первого совместного технического комитета (JTC1/SC27/WG3) Международной организации по стандартизации (ISO) , в 1990 году.

Цель разработки

- собрать и увязать между собой мнения экспертов примерно из двух десятков стран;
- унификация национальных стандартов в области оценки безопасности ИТ;
- повышение уровня доверия к оценке безопасности ИТ;
- сокращение затрат на оценку безопасности ИТ на основе взаимного признания сертификатов.

Общие критерии безопасности информационных технологий
Common Criteria for Information Technology Security Evaluation

Разработчики стандарта *(финансирование правительств)*

- правительственные организации - Канады, США, Великобритании, Германии, Нидерландов и Франции, в 1993 году.

Цель разработки - объединить и развить:

- Гармонизированные критерии Европейских стран;
- Канадские критерии оценки доверенных компьютерных продуктов;
- Федеральные критерии безопасности информационных технологий;
- Оранжевую книгу *(по мнению разработчиков).*

Между коллективом "Проекта ОК" и Рабочей группой 3 установилось тесное взаимодействие

Эволюция “Общих критериев”

- С 1994 года ранние версии “*Общих критериев*” становятся рабочими проектами WG3.
- В 1996 году появилась **Версия 1.0** “*Общих критериев*” *(одобрена ISO и обнародована в качестве Проекта Комитета)*.
- Экспериментальная оценка и обсуждение документа.
- В мае 1998 года выходит **Версия 2.0** “*Общих критериев*”.
- В августе 1999 года выходит **Версия 2.1** “*Общих критериев*”, *учтены замечания WG3*.
- В декабре 1999 года принят международный стандарт ***ISO/IEC 15408:1999*** *(первая редакция - аналог ОК версии 2.1).*
- *Принят международный стандарт* ***ISO/IEC 15408:2005*** *(вторая редакция - аналог ОК версии 2.3).*
- В настоящее время осуществляется пересмотр ***ISO/IEC 15408:2005*** *(в соответствии с программой работы ISO/IEC JTC1/SC27 от 18.08.2008 г.)*.

Часть 1. *Введение и общая модель.*
Часть 2. *Функциональные требования безопасности.*
Часть 3. *Требования доверия к безопасности.*

Разработчики стандарта *аналога ISO/IEC 15408:1999*

- Центр безопасности информации, 4 ЦНИИ МО РФ, Центр «Атомзащитаинформ», ЦНИИАТОМИНФОРМ, ВНИИстандарт при участии экспертов WG3.

Устанавливает:

- общий подход к формированию требований и оценке безопасности (функциональные и доверия);
- основные конструкции (профиль защиты, задание по безопасности);
- представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ.

Имеются вариант ***ГОСТ Р ИСО/МЭК 15408-1-2007*** *(аналог* ***ISO/IEC 15408:2005)***

РД “Безопасность информационных технологий. Критерии оценки безопасности информационных технологий”

Часть 1. *Критерии оценки безопасности информационных технологий*
Часть 2. *Функциональные требования безопасности*
Часть 3. *Требования доверия к безопасности*

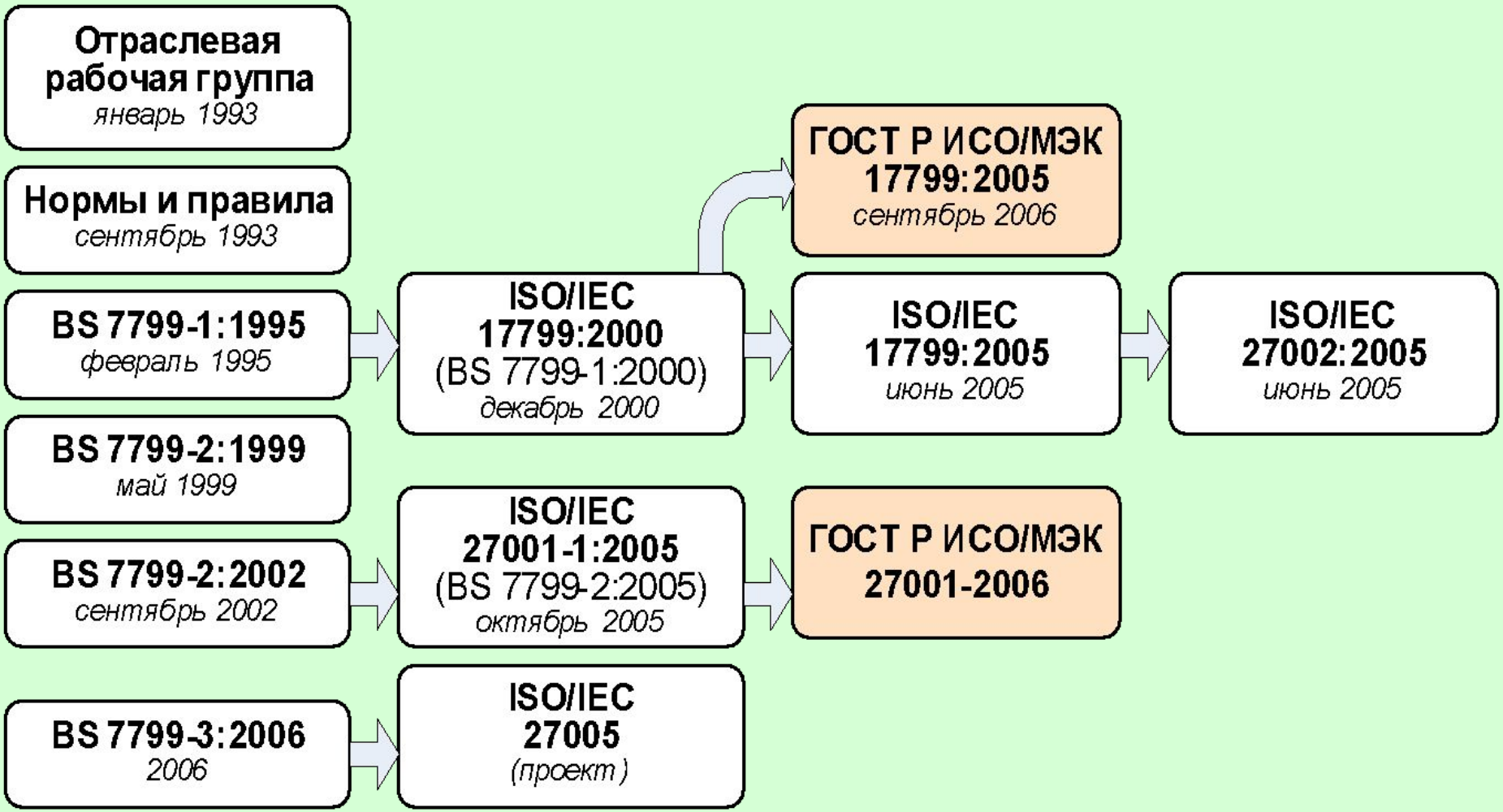
Цель разработки:

- обеспечение практического использования ***ГОСТ Р ИСО/МЭК 15408-2002*** в деятельности заказчиков, разработчиков и пользователей продуктов и систем ИТ при
  - *формировании ими требований,*
  - *разработке,*
  - *приобретении,*
  - *применении*

продуктов и систем информационных технологий, предназначенных для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями НМД или требованиями, устанавливаемыми собственником информации.

Приказ ГТК России от 19.06.02 г. №

Международные стандарты оценки информационной безопасности и управления ею



Международные стандарты оценки информационной безопасности и управления ею

BS 7799-1:1995 Code of Practice for Information Security Management *(Практические правила управления информационной безопасностью)*

Описывает *127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определенных на основе лучших примеров мирового опыта (best practices) в данной области.*

Служит *практическим руководством по созданию СУИБ.*

BS 7799-2:1999 Information Security Management – specification for information security management system *(Спецификация системы управления информационной безопасностью)*

Определяет *спецификацию СУИБ.*

Используется *в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.*

Международные и национальные стандарты оценки информационной безопасности и управления ею

ISO/IEC 17799:2000 Information technology — Code of practice for information security management (*Информационная технология - свод правил для информационного управления безопасностью).*

ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management *(Информационные технологии - Методики безопасности - Практические правила управления информационной безопасностью).*

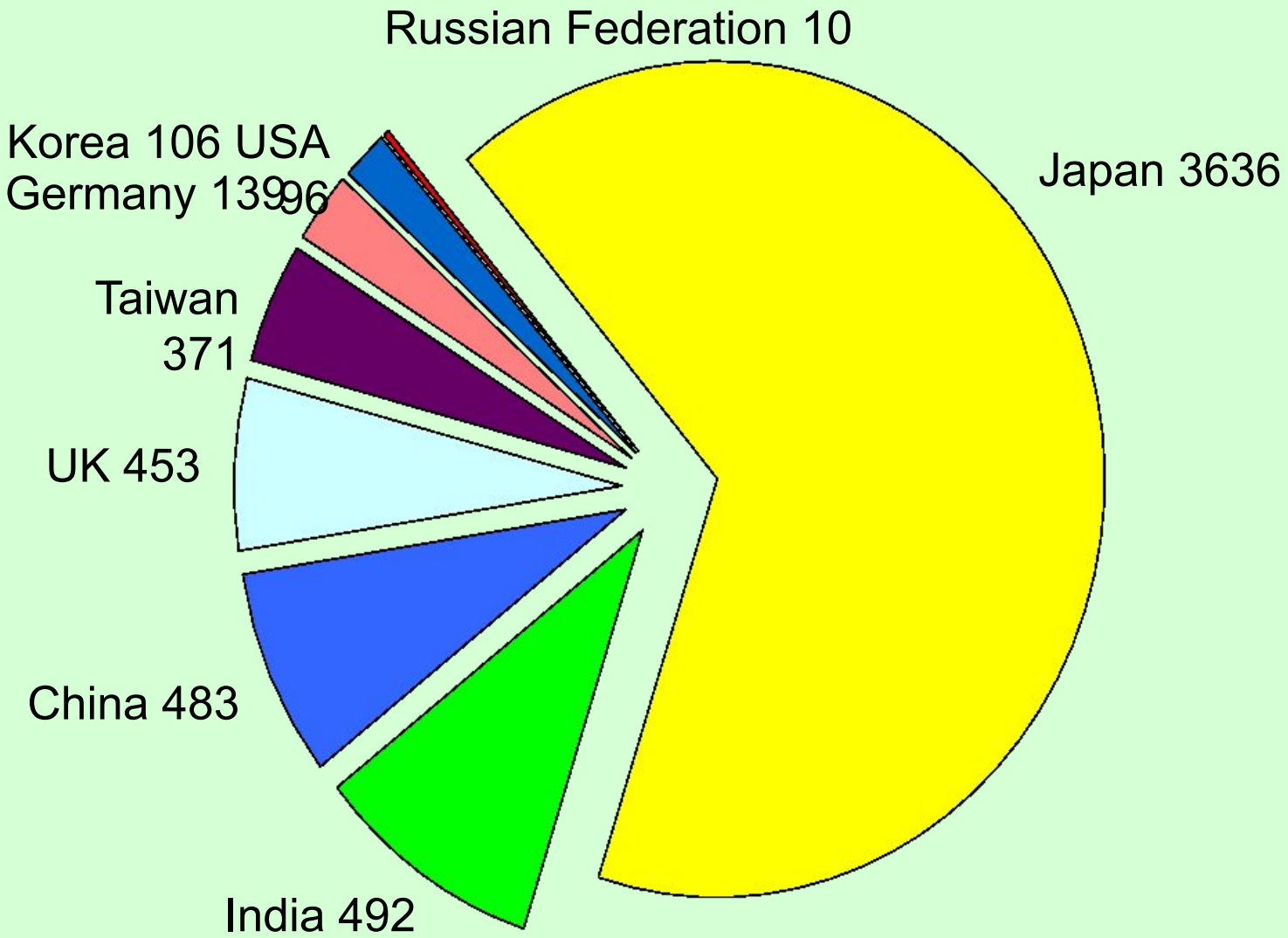
ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems - Requirements *(Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования).*

Национальные стандарты

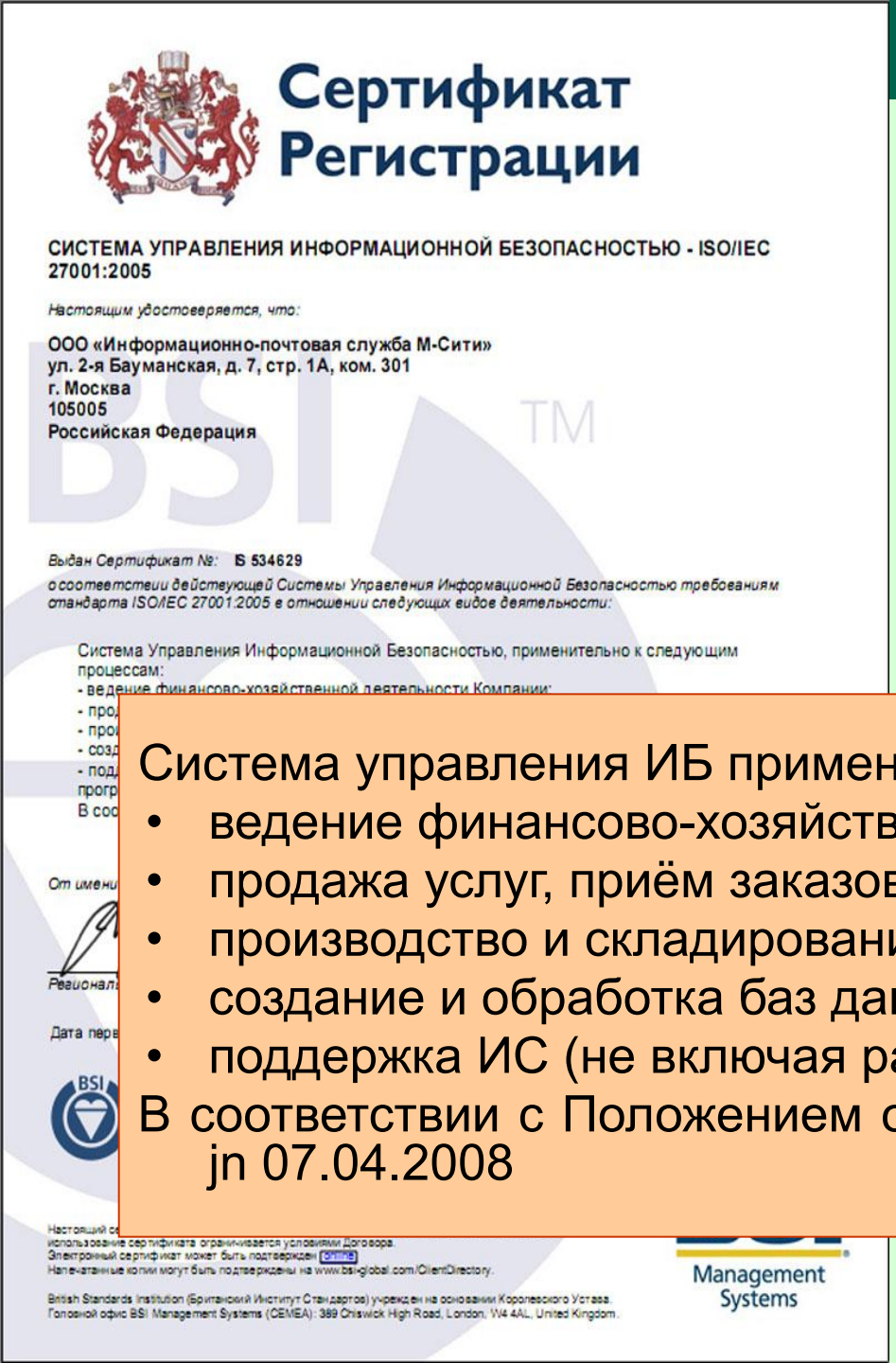
ГОСТ Р ИСО/МЭК 17799:2005 Информационная технология практические правила управления информационной безопасностью.

ГОСТ Р ИСО/МЭК 27001:2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

International ISMS Register в 80 странах мира на сентябрь 2010 года = 6826



http://www.iso27001certificates.com/



Сертификат Регистрации

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ - ISO/IEC 27001:2005

Настоящим удостоверяется, что:

ООО «Информационно-почтовая служба М-Сити»
ул. 2-я Бауманская, д. 7, стр. 1А, ком. 301
г. Москва
105005
Российская Федерация

Выдан Сертификат №: **IS 534629**

о соответствии действующей Системы Управления Информационной Безопасностью требованиям стандарта ISO/IEC 27001:2005 в отношении следующих видов деятельности:

Система Управления Информационной Безопасностью, применительно к следующим процессам:
- ведение финансово-хозяйственной деятельности Компании;
- про
- про
- созд
- под

прогр
В соо

От имени

Региональ

Дата пер

Настоящий се
использование сертификата ограничивается условиями Договора.
Электронный сертификат может быть подтвержден online.
Напечатанные копии могут быть подтверждены на www.bsi-global.com/ClientDirectory.

British Standards Institution (Британский Институт Стандартов) учрежден на основании Королевского Устава.
Головной офис BSI Management Systems (CEMEA): 389 Chiswick High Road, London, W4 4AL, United Kingdom.

Management Systems

Система управления ИБ применительно к следующим процессам:

- ведение финансово-хозяйственной деятельности компании
- продажа услуг, приём заказов, согласование условий и макетов
- производство и складирование готовой продукции
- создание и обработка баз данных
- поддержка ИС (не включая разработку специализированного ПО)

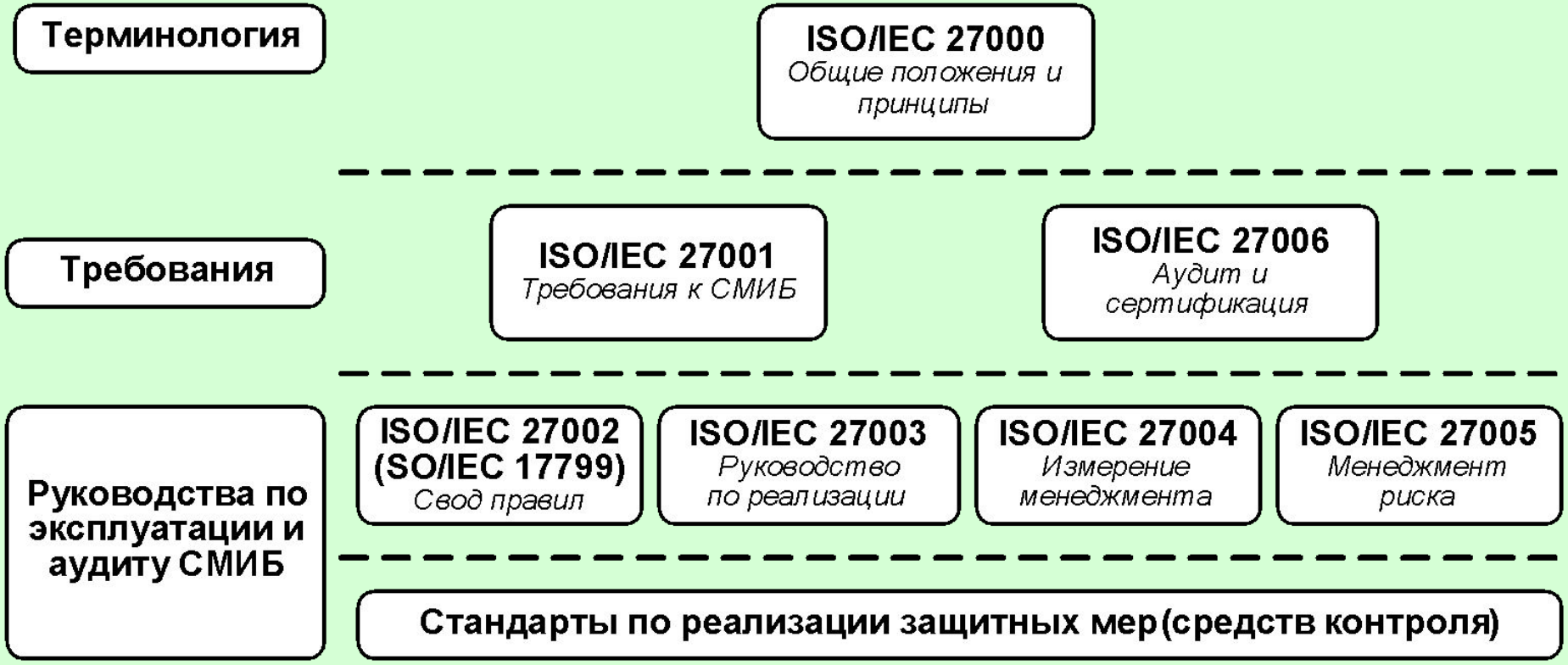
В соответствии с Положением о применимости контролей (SoA v.4) jn 07.04.2008

Выписка из International ISMS Register на 6 сентября 2010 года

Name of the Organization	Country	Certificate Number	Certification Body	Standard BS 7799-2:2002 or ISO/IEC 27001:2005
Bank24.ru, Ekaterinburg	Russian Federation	231663	Bureau Veritas Certification	ISO/IEC 27001:2005
CMA Small Systems AB	Russian Federation	IS 97256		ISO/IEC 27001:2005
CROC incorporated, CSC	Russian Federation	IS 95689		ISO/IEC 27001:2005
LANIT, CSC	Russian Federation	IS 516523		ISO/IEC 27001:2005
Lukoil-Inform, LLC	Russian Federation	IS 502464		ISO/IEC 27001:2005
Luxsoft, Moscow	Russian Federation	LRQ4002352	LRQA	ISO/IEC 27001:2005
Multiregional TransitTelecom, OJSC	Russian Federation	IS 512669		ISO/IEC 27001:2005
Rosno, SC	Russian Federation	IS 515437		ISO/IEC 27001:2005
Rutenia, JSC	Russian Federation	IS 517942		ISO/IEC 27001:2005
TransTeleCom	Russian Federation	HU08/3058	SGS	ISO/IEC 27001:2005

http://www.iso27001certificates.com/

Структура международных стандартов СМИБ



Перспективы развития международных стандартов СМИБ

ISO/IEC 27000 (проект) *Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.* ***Общие положения и терминология.***

Начало разработки проекта **май 2006 года**
Возможный срок принятия **май 2010 года**

ISO/IEC 27001:2005 *Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.* ***Требования.***

Введён в действие **в октябре 2005 года**
Предварительный пересмотр **в 2010 году**

Программа работы ISO/IEC JTC1/SC27 от 18.08.2008 г. принята 14.04.2008 г ., на пленарном заседании в Киото

Перспективы развития международных стандартов СМИБ

ISO/IEC 27002:2005 *Информационные технологии. Методы и средства обеспечения безопасности.* ***Свод правил для менеджмента информационной безопасности.***

Введён в действие **в июне 2005 года**
Пересмотр первого издания **в октябрь 2008 года**
Возможный выход второй редакции **май 2011 года**

ISO/IEC 27003 (проект) *Информационные технологии. Методы и средства обеспечения безопасности.* ***Руководство по реализации систем менеджмента информационной безопасности.***

Начало разработки проекта **ноябрь 2005 года**
Возможный срок принятия **ноябрь 2010 года**

Программа работы ISO/IEC JTC1/SC27 от 18.08.2008 г. принята 14.04.2008 г ., на пленарном заседании в Киото

Перспективы развития международных стандартов СМИБ

ISO/IEC 27004 (проект) *Информационные технологии. Методы и средства обеспечения безопасности.* ***Измерение менеджмента информационной безопасности.***

Начало разработки проекта **ноябрь 2004 года**
Возможный срок принятия **май 2010 года**

ISO/IEC 27005 *Информационные технологии. Методы и средства обеспечения безопасности.* ***Менеджмент риска информационной безопасности.***

Введён в действие в **июне 2008 года**
Пересмотр первого издания начнётся в **2011 году**

Программа работы ISO/IEC JTC1/SC27 от 18.08.2008 г. принята 14.04.2008 г ., на пленарном заседании в Киото

Перспективы развития международных стандартов СМИБ

ISO/IEC 27006:2007 *Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.* ***Требования для органов осуществляющих аудит и сертификацию систем менеджмента информационной безопасности.***

Введён в действие в **марте 2007 года**

Пересмотр первого издания начнётся в **2010 году**

ISO/IEC 27007 (проект) *Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.* ***Руководство для аудиторов систем менеджмента информационной безопасности.***

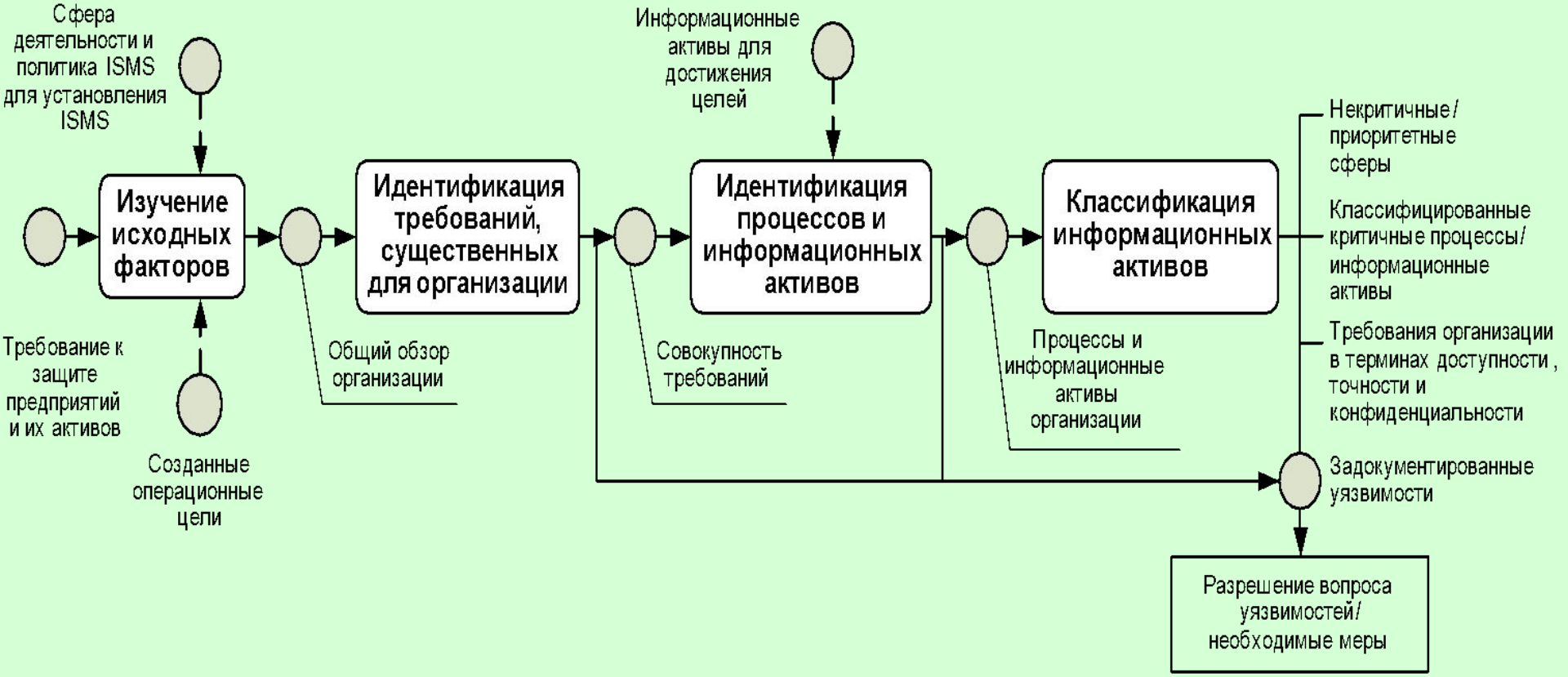
Сведения отсутствуют

Программа работы ISO/IEC JTC1/SC27 от 18.08.2008 г. принята 14.04.2008 г ., на пленарном заседании в Киото

Общий подход к разработке отраслевых стандартов”

Основной принцип:

- дополнение ISO/IEC 27002:2005 (ISO/IEC 17799:2005) “Свод правил менеджмента ИБ” специфичными для отрасли практиками



Information Security Management System (ISMS) – система управления информационной безопасностью

Предварительный вариант (отвергнут)

Концепция ИБ АС БС РФ

Основополагающие стандарты: Группа 0 "Основные требования"

ОСТ хх.0.0-хх Обеспечение ИБ АС БС РФ **Общие положения**	**ОСТ хх.0.1-хх** Обеспечение ИБ АС БС РФ **Термины и определения**	**ОСТ хх.0.2-хх** Обеспечение ИБ АС БС РФ **Требования ИБ в процессах ЖЦ**	**ОСТ хх.0.3-хх** Обеспечение ИБ АС БС РФ **Управление ИБ в процессах ЖЦ**

Группа 1 "Обеспечение ИБ в процессах ЖЦ"

ОСТ хх.1.0-хх Обеспечение ИБ АС БС РФ **Процесс стратегического планирования ИБ АС БС РФ**	**ОСТ хх.1.1-хх** Обеспечение ИБ АС БС РФ **ИБ на стадии создания АС БС РФ**	**ОСТ хх.1.2-хх** Обеспечение ИБ АС БС РФ **ИБ на стадии эксплуатации АС БС РФ**	**ОСТ хх.1.3-хх** Обеспечение ИБ АС БС РФ **ИБ на стадии вывода из эксплуатации**
ОСТ хх.1.4-хх Обеспечение ИБ АС БС РФ **ИБ в процессах соглашения (приобретения поставки)**	**ОСТ хх.1.5-хх** Обеспечение ИБ АС БС РФ **ИБ в процессах проекта**	**ОСТ хх.1.6-хх** Обеспечение ИБ АС БС РФ **ИБ на стадии сопровождения**	**ОСТ хх.1.2-хх** Обеспечение ИБ АС БС РФ **ИБ в процессах предприятия**

Группа 2 "Оценка, аудит и инспектирование ИБ"

ОСТ хх.2.0-хх Обеспечение ИБ АС БС РФ **Оценка АС БР и КО**	**ОСТ хх.2.1-хх** Обеспечение ИБ АС БС РФ **Аудит АС БР и КО**	**ОСТ хх.2.2-хх** Обеспечение ИБ АС БС РФ **Инспектирование АС БР и КО**

Группа 3 "Система разработки, оценки и сертификации"

ОСТ хх.3.0-хх Обеспечение ИБ АС БС РФ **Основы системы разработки, оценки и сертификации ПЗ и АС**	**ОСТ хх.3.1-хх** Обеспечение ИБ АС БС РФ **Порядок разработки профилей защиты**	**ОСТ хх.3.3-хх** Обеспечение ИБ АС БС РФ **Порядок разработки заданий по безопасности**

Комплекс стандартов отрасли "Обеспечение ИБ АС БС РФ"

Требования к стандартам безопасности

Что делать?

- Простота и понятность;
- Непротиворечивость терминов и определений;
- Открытость;
- Стандарт должен быть прямого действия;
- Стандарт должен быть гармонизирован с отечественными и международными документами, стандартизирующими (или представляющими наилучшие практики) области ИБ и безопасности ИТ;
- Стандарт должен содержать механизмы его актуализации.

Форма организации работ по разработке стандарта ИБ

- стандарт должен разрабатываться коллегиально, специальной рабочей группой (состоящей из подкомиссий) в состав которой должны входить представители всех сфер жизнедеятельности отрасли;
- целесообразно включить в состав рабочей группы представителей ФСТЭК и других государственных организаций занимающихся вопросами защиты информации;
- руководители организаций, представители которых включены в состав рабочей группы, должны дать согласие своим сотрудникам на участие в данных работах, то есть должно быть оформлено специальное соглашение.

Основные тезисы

- Язык текста стандарта должен быть ясным.
- Цель стандарта – сформировать требования и обеспечить возможность аудита их выполнения.
- Необходимо учесть требования международных и национальных стандартов ИБ.
- Основа парадигмы – контроль над активами, управление ими, стратегия борьбы брони и снаряда.
- Технические риски – часть операционных.
- Должно быть указано, что политика безопасности – это основной документ. Определена иерархия политик *(корпоративная и т.д.).*
- Без приложений. Все детали в последующих документах.
- Служба ИБ *(подразделение должно быть организационно обособлено, свой бюджет, наличие подразделений на местах).*
- Наличие непрерывного контроля. Все процессы подчиняются бизнес - целям.
- Оценка должна быть на уровне подходов.

Состав комплекса стандарта

Комплекс документов
в области стандартизации Банка России
“Обеспечение информационной безопасности организаций банковской системы Российской Федерации”
(Комплекс “БР ИББС”)

СТО БР ИББС-1.0-2008
Общие положения

СТО БР ИББС-1.1-2007
Аудит информационной безопасности

СТО БР ИББС-1.2-2009
Методика оценки соответствия

РС БР ИББС-2.0-2007
Документы по обеспечению информационной безопасности

РС БР ИББС-2.1-2007
Руководство по самооценке

Комплекс “БР ИББС” (перспектива)

СТО БР ИББС -0.0-xxxx Классификатор

СТО БР ИББС -0.1-xxx Термины и определения

СТО БР ИББС -1.0-2008 Общие положения

СТО БР ИББС -1.1-2007 Аудит информационной безопасности

СТО БР ИББС -1.2-2009 Методика оценки соответствия

РС БР ИББС -2.0-2007 Документы по обеспечению информационной безопасности

РС БР ИББС -2.1-2007 Руководство по самооценке

РС БР ИББС -2.3-xxxx Методика классификации активов

Есть проект

РС БР ИББС -2.2-xxxx Методика оценки рисков

Есть проект

РС БР ИББС -2.3-xxxx Методика назначения описания

Проект формируется

BSI *(Германия, 1998 г.)*
Руководство по защите информационных технологий для базового уровня защищенности

- **Методология управления ИБ;**
- **Компоненты информационных технологий:**
  - *основные компоненты (организационный и процедурный уровень ИБ, организация защиты данных, планирование действий в чрезвычайных ситуациях);*
  - *инфраструктура (здания, помещения, кабельные сети, организация удаленного доступа);*
  - *клиентские компоненты различных типов (DOS, Windows и пр.);*
  - *сети различных типов (соединение "точка-точка", разнородные сети и т.д.);*
  - *элементы систем передачи данных (электронная почта, модемы, МЭ и т.д.);*
  - *Телекоммуникации (факсы, автоответчики и пр.);*
  - *стандартное ПО;*
  - *базы данных;*

- **Каталоги угроз безопасности и контрмер.**

Угрозы по классам:

- *Форс-мажорные обстоятельства;*
- *Недостатки организационных мер;*
- *Ошибки человека;*
- *Технические неисправности;*
- *Преднамеренные действия.*

Около **600** наименований в каждом из каталогов

Контрмеры по классам:

- *Улучшение инфраструктуры;*
- *Административные контрмеры;*
- *Процедурные контрмеры;*
- *Программно-технические контрмеры;*
- *Уменьшение уязвимости коммуникаций;*
- *Планирование действий в чрезвычайных ситуациях.*

Достоинства: 

- Детальный учет специфики различных элементов информационных систем.
- Детальное рассмотрение особенностей обеспечения ИБ в современных сетях.
- Возможность оперативно вносить изменения и корректировать связи между частями стандарта.

Недостатки: 

- Невозможность с одним уровнем детализации описать всё многообразие различных элементов информационных систем.

COBIT - контрольные объекты для информационных и смежных технологий

Control Objectives for Information and related Technology

Набор документов, в которых изложены принципы управления и аудита информационных технологий





Резюме для руководителя. *Описание стандарта CobiT, ориентированное **на топ-менеджеров** организации для принятия ими решения о применимости стандарта в конкретной организации.*

Описание структуры. *Развернутое описание структуры стандарта, высокоуровневых целей контроля и пояснения к ним, необходимые для эффективной навигации и результативной работы со стандартом.*

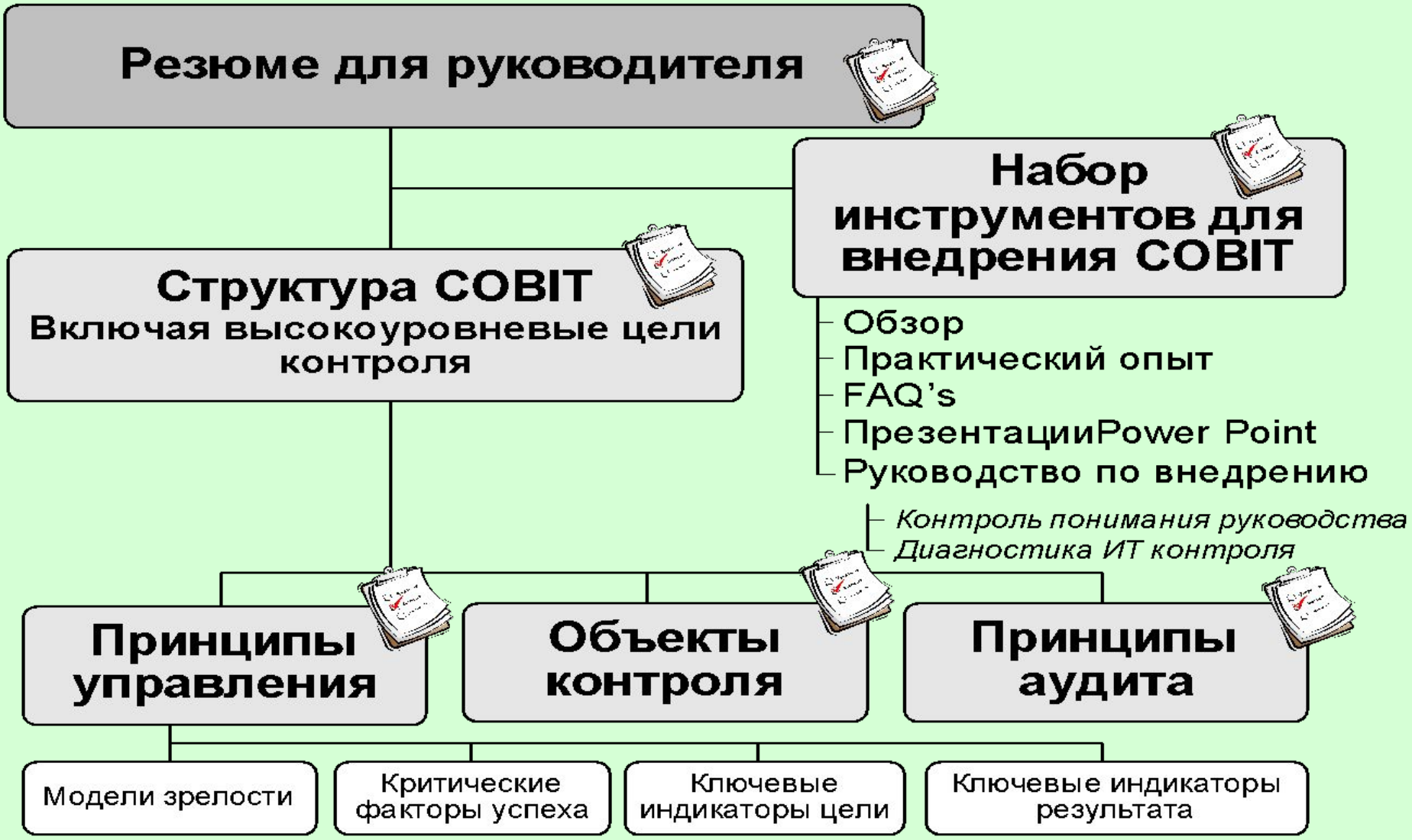
Объекты контроля. *Детальные описания объектов контроля, содержащие расшифровку каждого из объектов.*

Принципы управления. *Ответы на вопросы как управлять ИТ, как правильно поставить достижимую цель, как ее достичь и как проконтролировать полноту ее достижения. **Предназначена для руководителей ИТ-служб.***

Принципы аудита. *Правила проведения ИТ-аудита. Описание того, у кого можно получить необходимую информацию, как ее проверить, какие вопросы задавать? **Для внутренних и внешних аудиторов ИТ, а также консультантов в сфере ИТ.***

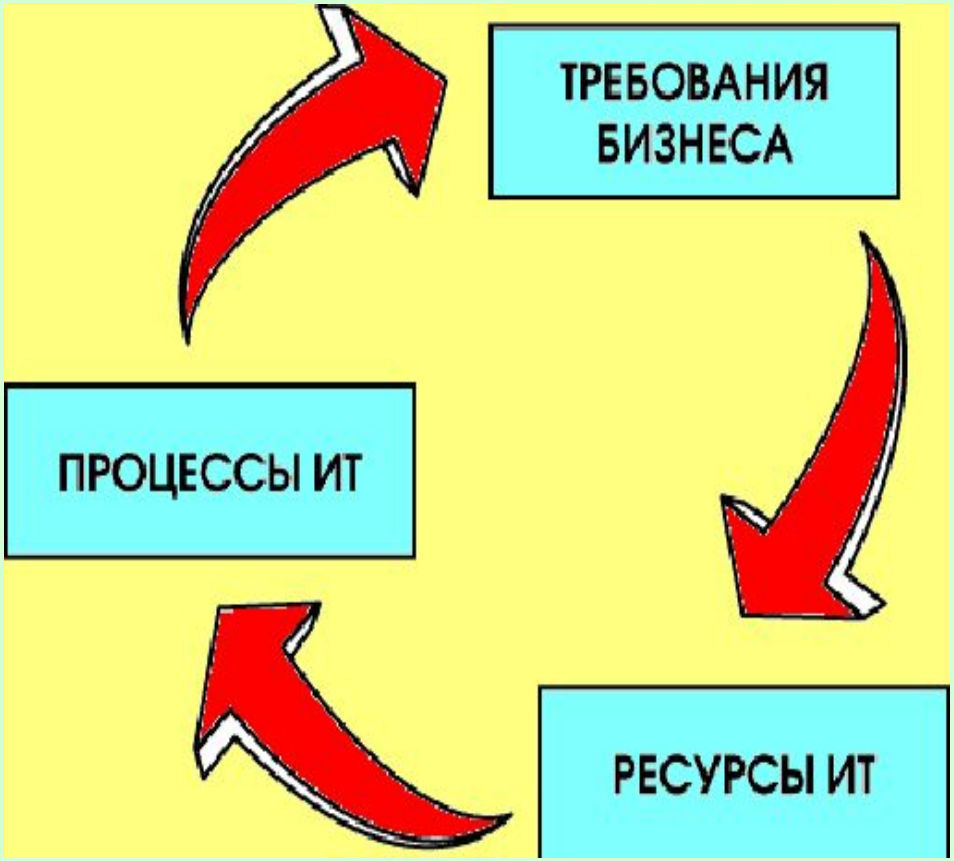
Набор инструментов внедрения стандарта - *практические советы по ежедневному использованию стандарта в управлении и аудите ИТ. **Книга предназначена для внутренних и внешних аудиторов ИТ, консультантов в сфере ИТ.***

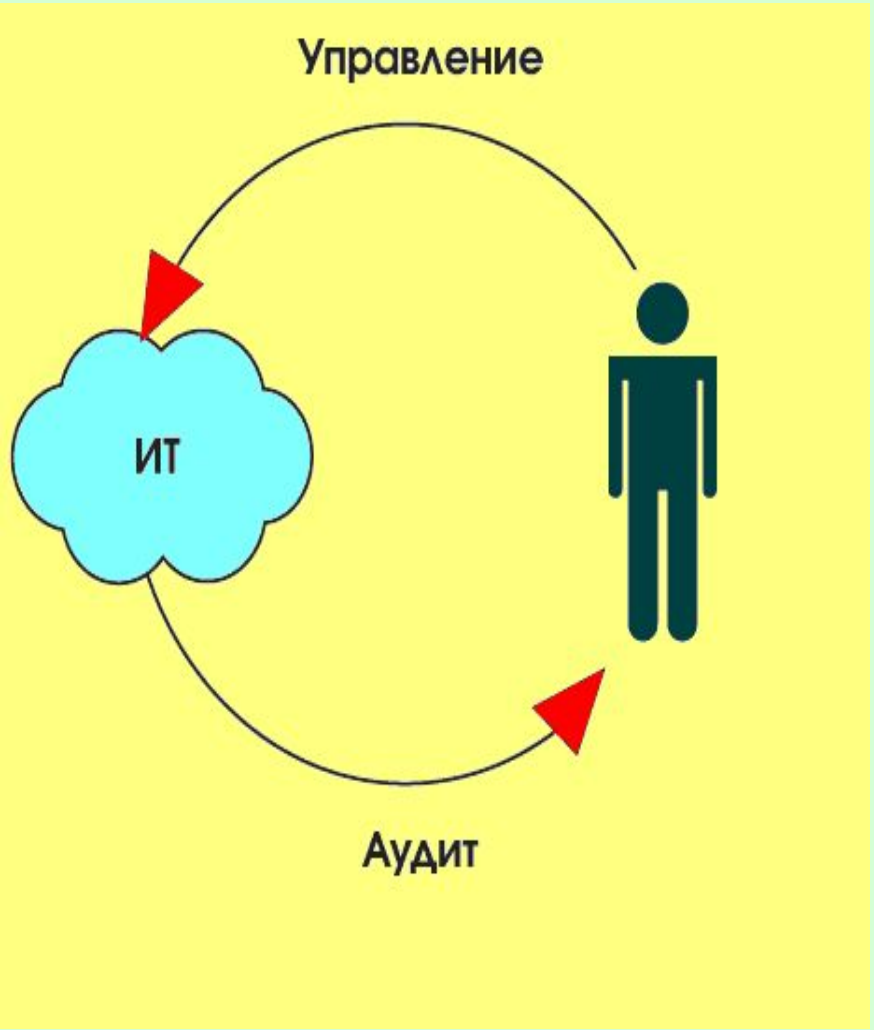
Состав книг COBIT



COBI

В основу стандарта COBIT положено следующее утверждение: ***для предоставления информации, необходимой организации для достижения ее целей, ресурсы ИТ должны управляться набором естественно сгруппированных процессов.***





Цикл COBIT, отражающий непрерывность соответствия ИТ требованиям бизнеса

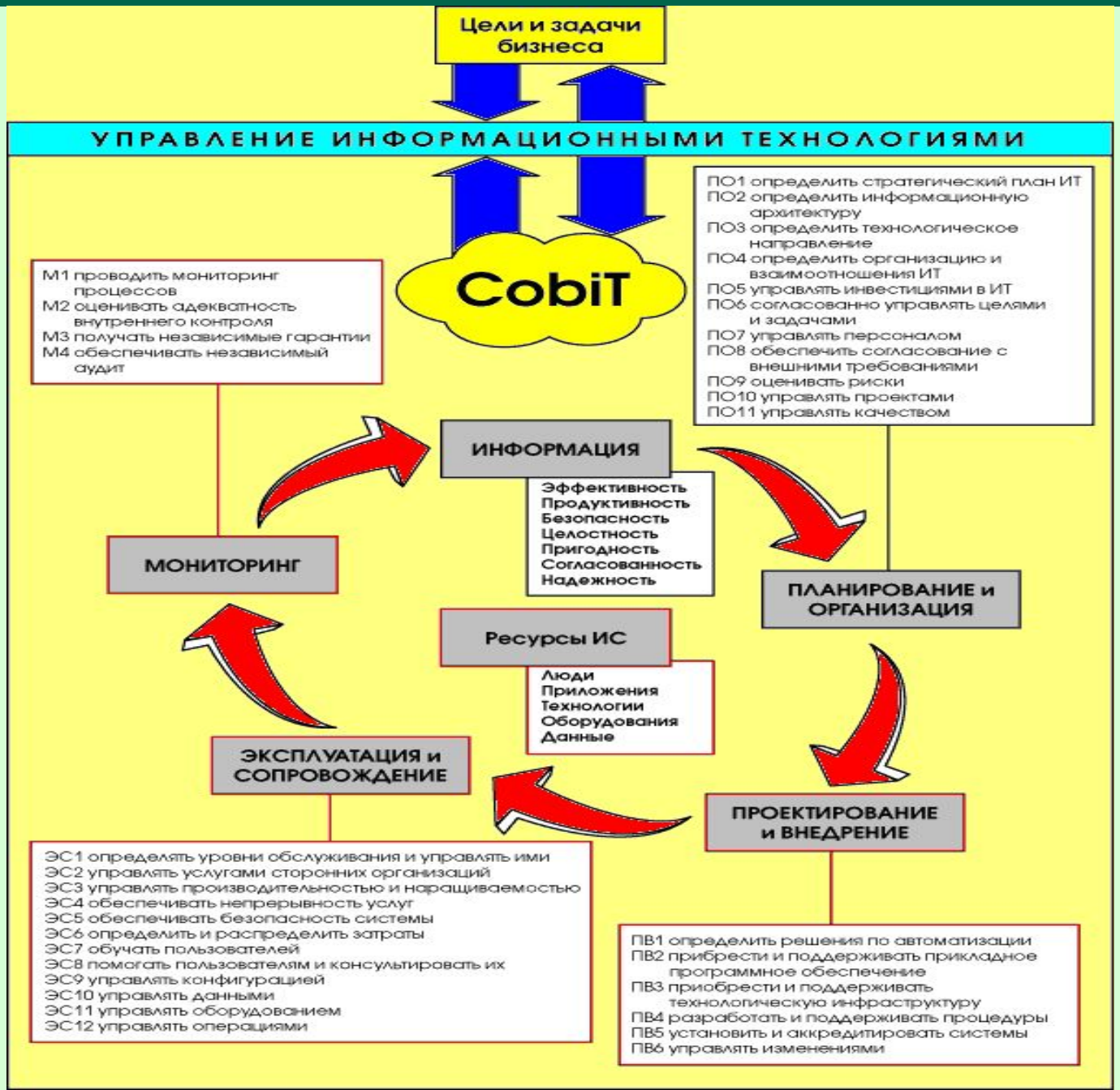
Ресурсы ИТ в COBIT

- **Данные** - объекты в широком смысле (то есть внутренние и внешние), структурированные и неструктурированные, а также графика, звук и т.д.
- **Приложения** - совокупность автоматизированных и выполняемых вручную процедур.
- **Технология** - аппаратное обеспечение, программное обеспечение, операционные системы, системы управления базами данных, сетью и мультимедиа.
- **Оборудование** - все ресурсы, создающие и поддерживающие информационные технологии.
- **Люди** - персонал, его навыки: умение планировать и организовывать, комплектовать, обслуживать и контролировать информационные системы и услуги.

Критерии оценки информации:

- **Эффективность** - актуальность информации, соответствующего бизнес-процесса, гарантия своевременного и регулярного получения правильной информации.
- **Продуктивность** - обеспечение доступности информации с помощью оптимального (наиболее продуктивного и экономичного) использования ресурсов.
- **Конфиденциальность** - обеспечение защиты информации от неавторизованного ознакомления.
- **Целостность** - точность, полнота и достоверность информации в соответствии с требованиями бизнеса.
- **Пригодность** - предоставление информации по требованию бизнес-процессов.
- **Согласованность** - соответствие законам, правилам и договорным обязательствам.
- **Надежность** - доступ руководства организации к соответствующей информации для текущей деятельности, для создания финансовых отчетов и оценки степени соответствия.

Модель управления информационной технологией



COBI

Модель зрелости

Анархия *Фольклор* *Стандарты* *Измеряемый* *Оптимизируемый*

Текущий статус организации

Требования международных стандартов

“Лучшая практика” индустрии

Стратегия организации

0 Не существует	Процессы управления не применяются
1 Начало	Процессы специализированны и неорганизованны
2 Повторение	Процессы повторяются на регулярном основании
3 Описание	Процессы документированы и взаимосвязаны
4 Управление	Процессы наблюдаются и измеряются
5 Оптимизация	Процессы соответствуют “лучшей практике” и автоматизированы

- Модели зрелости предназначены для стратегического выбора и эталонного сравнения.

Критические Факторы Успеха (КФУ)

Определяют наиболее важные проблемы или действия руководителей, направленные на достижение контроля над ИТ-процессами.

Примеры КФУ:

- *Управление ИТ сосредоточенно на целях организации: стратегических инициативах, использовании технологий для развития бизнеса, достаточности ресурсов и удовлетворения бизнес-требований;*
- *Действия по управлению ИТ ясно определены, формализованы и осуществляются на основе потребностей предприятия с соответствующей отчетностью;*
- *Методы аудита определены таким образом, чтобы избежать сбоев и ошибок в системе внутреннего контроля;*
- *Учрежден контрольный комитет, назначающий и наблюдающий за независимым аудитом, уделяющий пристальное внимание ИТ при составлении планов аудита, а также принимающий во внимание результаты исследований сторонних организаций и аудиторов.*

Предназначены для организации контроля ИТ - процессов.

Ключевые Индикаторы Цели *(КИЦ)*

Описывают комплекс измерений, которые по факту сообщают руководству, что ИТ-процесс достиг предъявляемых бизнес - требований.

Выражается в терминах информационных критериев:

- Пригодность информации, необходимой для поддержки бизнеса;
- Риски отсутствия целостности и конфиденциальности;
- Рентабельность процессов и операций;
- Подтверждение надежности, эффективности и согласованности.

Примеры КИЦ:

- *Улучшение управления производительностью и стоимостью;*
- *Увеличение дохода от инвестиций в ИТ;*
- *Сокращение времени запуска в продажу нового продукта или услуги;*
- *Улучшение управления качеством, новшествами и рисками;*

•Предназначены для контроля достижения целей ИТ - процессов.

Ключевые Индикаторы Результата *(КИР)*

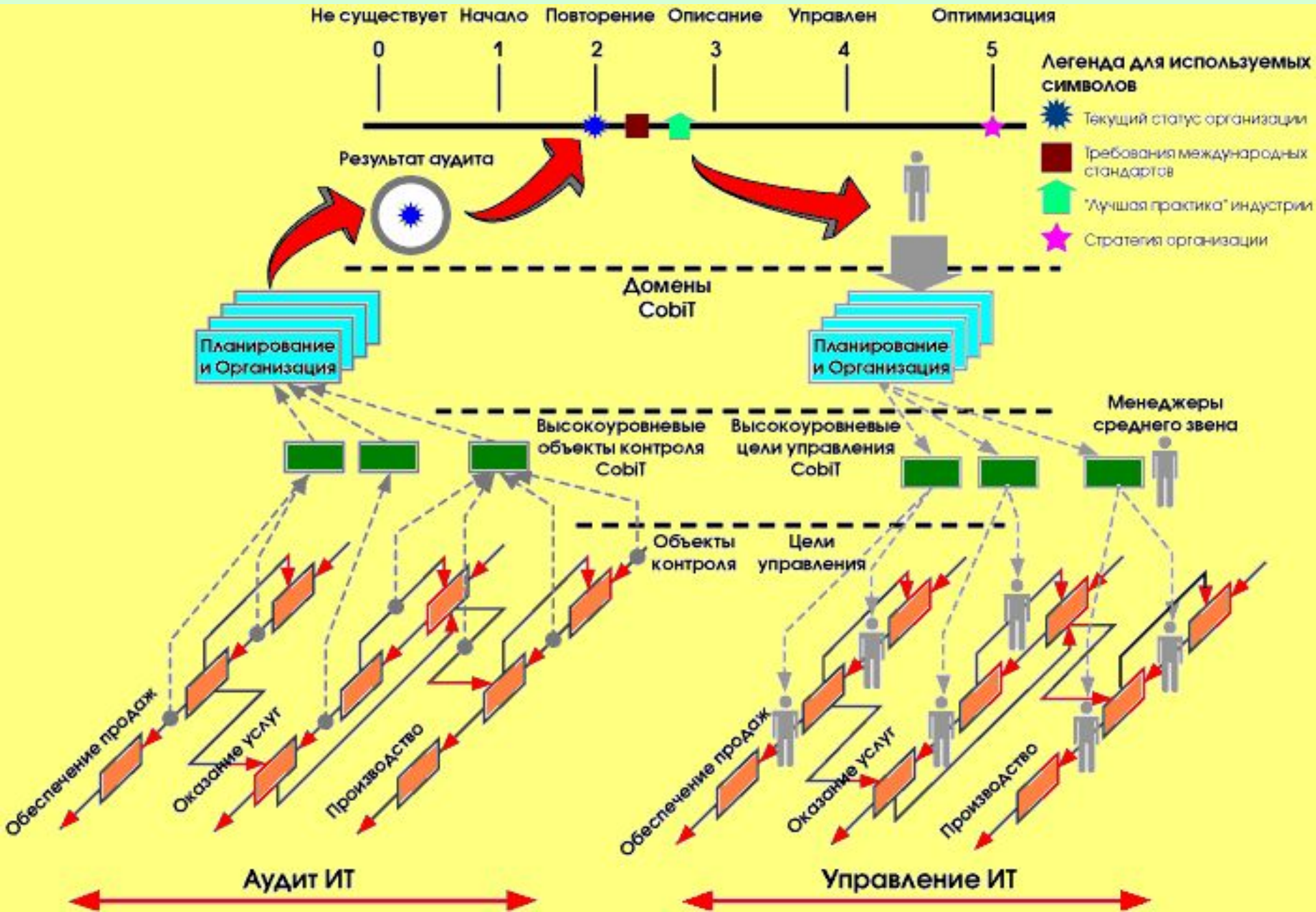
Описывают комплекс действий, необходимых для определения, насколько ИТ-процессы достигают поставленных целей.

Примеры КИР:

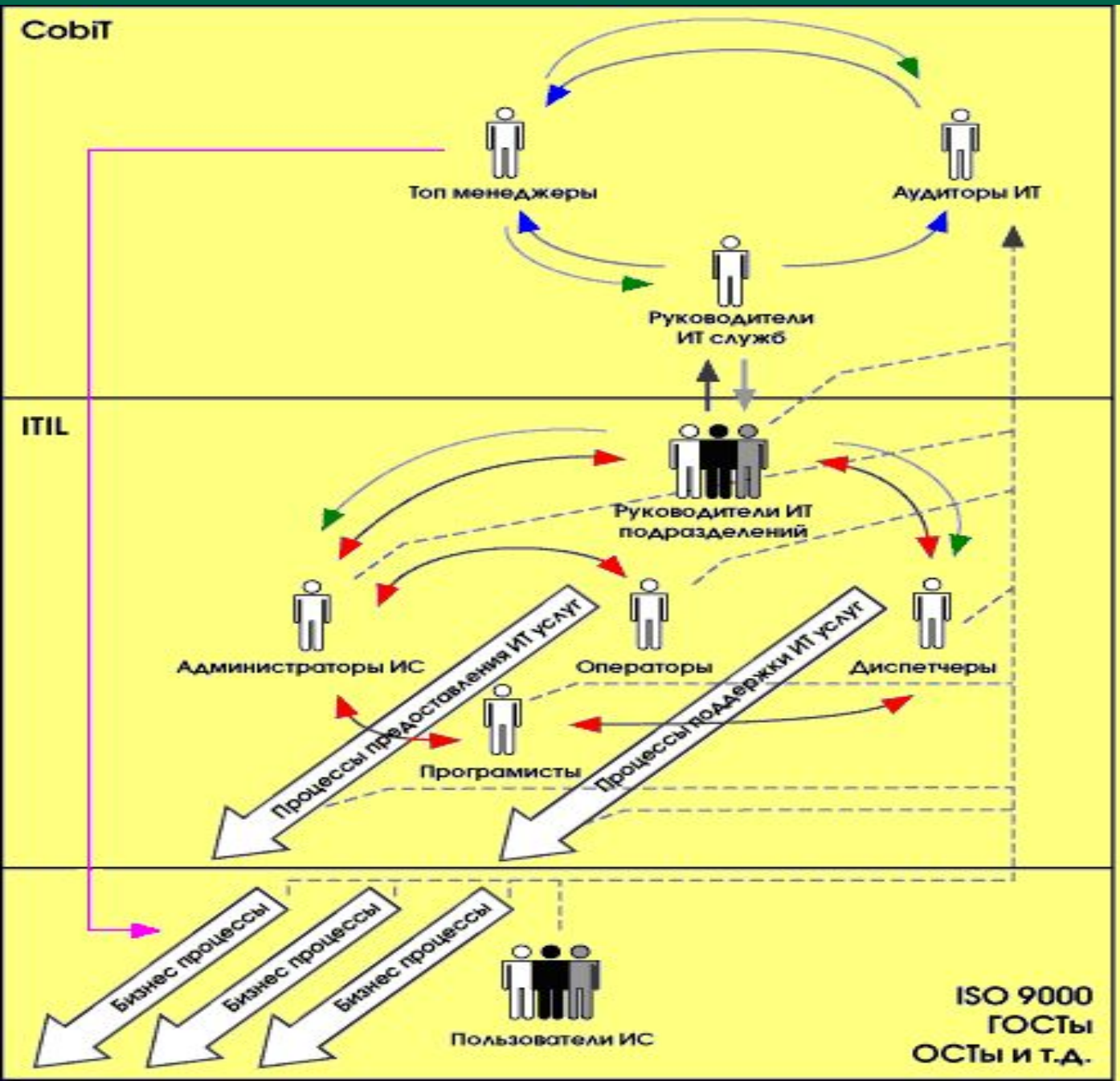
- *Увеличение рентабельности ИТ-процессов;*
- *Улучшение работы и планирования действий по совершенствованию ИТ-процессов;*
- *Увеличение нагрузки на ИТ-инфраструктуру;*
- *Повышение степени удовлетворения пользователей (опросы пользователей и количество жалоб);*
- *Улучшение взаимодействия и коммуникаций между руководителями ИТ и руководством организации*
- *Повышение производительности сотрудников (в том числе, повышение морального духа).*

•Предназначены для контроля результатов каждого ИТ - процесса.

Процессы управления и аудита



Взаимосвязь COBIT и других требований и стандартов



ITIL - библиотека лучшего практического опыта в части предоставления ИТ-услуг.

COBIT специализируется и на управлении и на аудите ИТ.

Процессы **ITIL**, как и любые другие процессы, могут управляться и контролироваться стандартом CobiT.

Легенда:

- управление Cobit
- аудит Cobit
- управление и котроль ITIL
- стандарты бизнес процессов

Сравнение некоторых стандартов и концепций аудита

	COBIT	SAC	COSO	SAS 55/78
Целевая аудитория	TOP-менеджеры, пользователи, аудиторы информационных систем	Внутренние аудиторы компании	TOP-менеджеры	Внешние аудиторы
Понятие аудита	Системный процесс проверки на соответствие декларируемым целям политики безопасности, организации обработки данных, норм эксплуатации	Системный процесс проверки на соответствие декларируемым целям бизнес - процессов, политики безопасности и кадровой политики	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, а также политики безопасности компании	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, а также политики безопасности компании
Цели аудита	Развитие бизнеса, повышение его эффективности и рентабельности, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе
Область применения	Планирование и организация, постановка задач и выполнение, эксплуатация и сопровождение, мониторинг	Управление производством, эксплуатация автоматизированных и автоматических систем управления	Управление производством, риск-менеджмент, управление информационными системами, мониторинг корпоративных информационных систем	Управление производством, управление рисками, мониторинг и управление корпоративными информационными системами
Акцент	Менеджмент информационных технологий	Менеджмент информационных технологий	Менеджмент	Финансовый менеджмент
Срок действия сертификата аудита	Интервал времени	Время проверки	Интервал времени	Интервал времени
Заинтересованные лица	TOP-менеджеры компании	TOP-менеджеры компании	TOP-менеджеры компании	TOP-менеджеры компании
Объем документов, регламентирующих проведение аудита	4 документа общим объемом 187 страниц	12 частей общим объемом 1193 страницы	4 тома общим объемом 353 страницы	2 документа общим объемом 63 страницы

Стандарт безопасной электронной коммерции PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) - стандарт защиты информации в индустрии платежных карт, разработанный международными платежными системами Visa и MasterCard, объединяет в себе требования ряда программ по защите информации, в частности:

Основные области контроля и требования безопасности

PCI DSS определяет следующие 6 областей контроля и 12 основных требований по безопасности:

1. Построение и сопровождение защищенной сети:

Требование 1: создание и сопровождение конфигурации межсетевого экрана для защиты данных держателей карт;

Требование 2: неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности.

2. Защита данных держателей карт:

Требование 3: обеспечение защиты данных держателей карт в ходе их хранения;
Требование 4: обеспечение шифрования данных держателей карт при их передаче через общедоступные сети.

3. Поддержка программы управления уязвимостями:

Требование 5: использование и регулярное обновление антивирусного программного обеспечения;
Требование 6: разработка и поддержка защищенных систем и приложений.

4. Реализация мер по строгому контролю доступа:

Требование 7: разграничение доступа к данным по принципу служебной необходимости;
Требование 8: присвоение уникального идентификационного номера каждому лицу, располагающему доступом к компьютеру;
Требование 9: ограничение физического доступа к данным держателей карт.

5. Регулярный мониторинг и тестирование сети:

Требование 10: отслеживание всех сеансов доступа к сетевым ресурсам и данным владельцев карт;
Требование 11: регулярное тестирование систем и процессов обеспечения безопасности.

6. Поддержка политики информационной безопасности:

Требование 12: наличие и исполнение в организации политики информационной безопасности.

Документы ФСТЭК России

Положение по аттестации объектов информатизации по требованиям безопасности информации, *утверждено председателем Гостехкомиссии России 25 ноября 1994 г.*
Устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

Типовое положение об органе по аттестации объектов информатизации по требованиям безопасности информации. *утверждено председателем Гостехкомиссии России 25 ноября 1994 г.*

РД Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. *Гостехкомиссия России, 1992.*

РД Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. *Гостехкомиссия России, 1992.*

РД Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. *Гостехкомиссия России, 1992.*

РД Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. *Гостехкомиссия России, 1992.*

РД Защита от несанкционированного доступа к информации. Термины и определения. *Гостехкомиссия России, 1992.*

РД Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. *Гостехкомиссия России, 1997.*

РД Защита информации. Специальные защитные знаки. Классификация и общие требования. *Гостехкомиссия России, 1997.*

РД Защита от несанкционированного доступа. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. *Утвержден приказом Гостехкомиссии России от 4 июня 1999 г. № 114.*

РД Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. *Утвержден приказом Гостехкомиссии России от 19 июня 2002 г. № 187 (часть 1, часть 2, часть 3).*

«Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации», *Гостехкомиссия России, Москва, 2002.*[*]

«Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации», *Гостехкомиссия России, Москва, 2002.*[*]

«Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам», *Гостехкомиссия России, Москва, 2002.*[*]

«Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах», *Гостехкомиссия России, Москва, 2002.*[*]

НМД «Специальные требования и рекомендации по технической защите конфиденциальной информации». *Утвержден приказом Гостехкомиссии России от 30 августа 2002 г. № 282.*

Приказ ФСТЭК России «Об утверждении форм документов, используемых ФСТЭК России в процессе лицензирования деятельности по технической защите конфиденциальной информации и деятельности по разработке и (или) производству средств защиты конфиденциальной информации» *от 7 июля 2006 г. № 222, (зарегистрирован Минюстом России 27 июля 2006 г., регистрационный № 8114).*

** - Документ ограниченного распространения*

РД Методические рекомендации по технической защите информации, составляющей коммерческую тайну. *2007.*

1. Основные понятия и сокращения.
2. Понятие коммерческой тайны.
3. Порядок определения сведений, составляющих КТ.
4. Категорирование объектов информатизации по уровням защищенности и группам коммерческой ценности информации.
5. Методические рекомендации по общему порядку организации ЗИ, составляющей КТ, на ОИ.
6. Методические рекомендации по порядку выявления актуальных угроз безопасности информации, составляющей коммерческую тайну.

7. Рекомендации по применению мер и средств технической защиты информации, составляющей коммерческую тайну.

7.1. Общие рекомендации.

Стандарты

ГОСТ 17168-82. Фильтры электронные октавные и третьоктавные. Общие технические требования и методы испытаний.

ГОСТ 12.1.003-83. Система стандартов безопасности труда. Шум. Общие требования безопасности.

ГОСТ 21552-84. Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортировка и хранение.

ГОСТ 12.1.050-86. ССБТ. Методы измерения шума на рабочих местах.

ГОСТ 27296-87. Защита от шума в строительстве. Звукоизоляция ограждающих конструкций. Методы измерений.

ГОСТ 27201-87. Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования.

ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем.

ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

ГОСТ 28806-90. Качество программных средств. Термины и определения.

ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

ГОСТ 2.503-90. ЕСКД. Правила внесения изменений.

ГОСТ 34.601-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.

ГОСТ 29216-91. Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационной техники. Нормы и методы испытаний.

ГОСТ 34.603-92. Информационная технология. Виды испытаний автоматизированных систем.

ГОСТ Р ИСО 9127-94. Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов.

ГОСТ 30373-95/ГОСТ Р 50414-92. Совместимость технических средств электромагнитная. Оборудование для испытаний. Камеры экранированные. Классы, основные параметры, технические требования и методы испытаний.

ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

ГОСТ Р 50752-95. Информационная технология. Защита информации от утечки за счёт побочных электромагнитных излучений при её обработке средствами вычислительной техники. Методы испытаний.

ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

ГОСТ Р ИСО 9001-96. Системы качества. Модель обеспечения качества при проектировании, разработке, производстве, монтаже и обслуживании.

ГОСТ Р ИСО 9002-96. Системы качества. Модель обеспечения качества при производстве, монтаже и обслуживании.

ГОСТ Р ИСО 9003-96. Системы качества. Модель обеспечения качества при окончательном контроле и испытаниях.

ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

ГОСТ Р 50923-96. Дисплеи. Рабочее место оператора. Общие эргономические требования и требования к производственной среде. Методы измерения.

ГОСТ 22505-97. Совместимость технических средств электромагнитная. Радиопомехи индустриальные от радиовещательных приемников, телевизоров и другой бытовой радиоэлектронной аппаратуры. Нормы и методы испытаний.

ГОСТ Р 51188-98. Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

ГОСТ Р 51171-98. Качество служебной информации. Правила предъявления информационных технологий на сертификацию.

ГОСТ Р 51275-99. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

ГОСТ Р 51320-99. Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств - источников индустриальных радиопомех.

ГОСТ Р 51319-99. Совместимость технических средств электромагнитная. Приборы для измерения индустриальных радиопомех. Технические требования и методы испытаний.

ГОСТ Р 51583-2000. Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения, (дсп).

ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования, (дсп).

ГОСТ Р 50628-2000. Совместимость -технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний.

ГОСТ Р ИСО 9000-2001. Системы менеджмента качества. Основные положения и словарь.

ГОСТ Р ИСО 9001-2001. Системы менеджмента качества. Общие требования.

ГОСТ Р ИСО 9004-2001. Системы менеджмента качества. Рекомендации по улучшению качества.

ГОСТ Р 50948-2001. Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности.

ГОСТ Р 50949-2001. Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности.

ГОСТ ИСО/МЭК 15408-1-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ ИСО/МЭК 15408-2-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий Часть 2. Функциональные требования безопасности.

ГОСТ ИСО/МЭК 15408-3-2002. Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

РД 50-682-89. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Основные положения.

На сайте Федерального агентства по техническому регулированию и метрологии размещены

ГОСТ Р 52447-2005	Защита информации. Техника защиты информации. Номенклатура показателей качества
ГОСТ Р 52069.0-2003	Защита информации. Система стандартов. Основные положения
ГОСТ Р 50922-2006	Защита информации. Основные термины и определения
ГОСТ Р 52448-2005	Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения
ГОСТ Р 51275-2006	Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
ГОСТ Р 52633-2006	Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации
ГОСТ Р 52863-2007	Защита информации. Автоматизированные системы в защищенном исполнении испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования
ГОСТ Р 34.10-2001	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
ГОСТ 34.311-95	Информационная технология. Криптографическая защита информации. Функция хэширования
ГОСТ Р 34.11-94	Информационная технология. Криптографическая защита информации. Функция хэширования
ГОСТ Р 51188-98	Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство

Спасибо за внимание