Лекция 6. Нормативная база по управлению рисками информационной безопасности

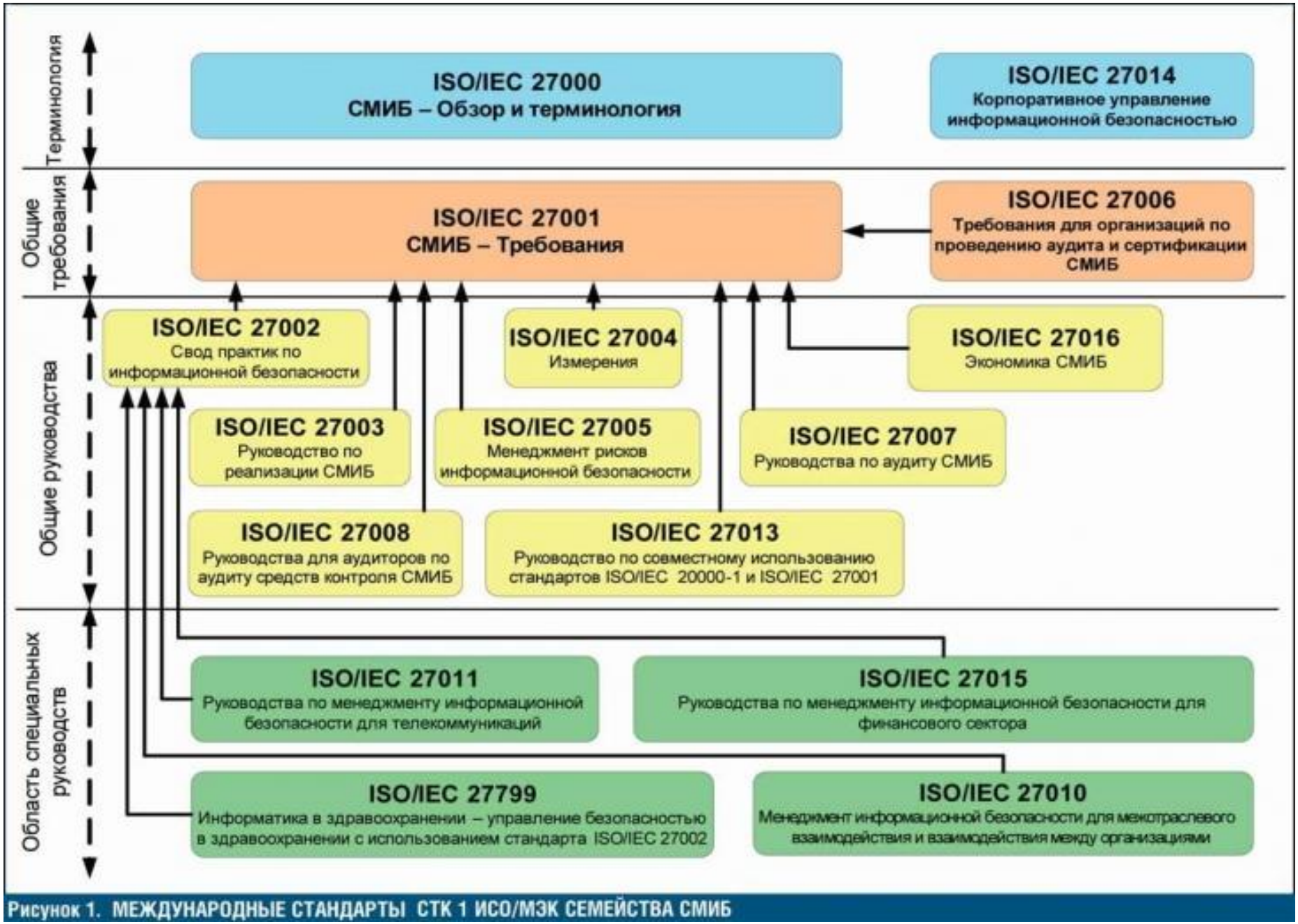


Рисунок 1. МЕЖДУНАРОДНЫЕ СТАНДАРТЫ СТК 1 ИСО/МЭК СЕМЕЙСТВА СМИБ

П Р О Б Л Е М А

Извечный вопрос: сколько тратить на безопасность?

Теория ИБ → абстрактные методы анализа, оценки и управление рисками

Принципы и рекомендации общего плана:

BS 7799-3:2006 “Information security management systems – Part 3: Guidelines for information security risk management” от 17 марта 2006 г.

НОРМАТИВНАЯ БАЗА УПРАВЛЕНИЯ РИСКАМИ

I. Потребность в национальном стандарте

II. Содержание британского стандарта

- Оценка риска
- Обработка риска
- Непрерывная деятельность по управлению

III. Международные стандарты

IV. Развитие

I. ПОТРЕБНОСТЬ В СТАНДАРТЕ

1. Апробация организационных стандартов по ИБ (ГОСТ 17799, ГОСТ 27001, СТО БР ИББС-1.0) в России

2. Работа секции ПК 27 СТК 1 ИСО/МЭК (ЕВРААС)

3. Работа ТК 362 «Защита информации»

Организационные стандарты по ИБ в РФ

ГОСТ Р ИСО 27001:2005	ГОСТ Р ИСО 17799:2005	СТО БР ИББС-1.0-2006
Требования по: - созданию СУИБ - внедрению и эксплуатации СУИБ - проведению мониторинга и анализа СУИБ - поддержке и совершенствованию СУИБ - документированию - ответственности руководства - управлению ресурсами (и обучению) - внутренним аудитам СУИБ - анализу СУИБ - совершенствованию СУИБ	Политика безопасности Организация ИБ Управление активами Безопасность кадровых ресурсов Физическая и экологическая безопасность Управление коммуникациями и операциями Контроль доступа Приобретение, разработка и сопровождение ИС Управление инцидентами ИБ Управление непрерывностью бизнеса Соответствие требованиям	Парадигма обеспечения ИБ, основные принципы, модель угроз Политика ИБ и требования по обеспечению ИБ (персонал, ЖЦ, управление доступом и регистрация, антивирусная защита, Интернет, криптография и др.) СУИБ (планирование, реализация, эксплуатация, проверка, совершенствование, непрерывность и восстановление, документирование, служба ИБ) Проверка и оценка ИБ Модель зрелости

Три источника, три составных части: историческая справка

- BS 7799-1: 2005. Information security management. Code of practice for information security management (Практические правила управления информационной безопасностью)

- BS 7799-2: 2005. Information security management. Specification for information security management systems (Требования к системам управления информационной безопасности)

- BS 7799-3: 2006. Information security management systems. Guidelines for information security risk management (Руководство по управлению рисками ИБ)

Взаимосвязь организационных стандартов

Британский стандарт	Международный стандарт	Российский стандарт
BS 7799-1: 2005	ISO 27002:2007 (ISO 17799: 2005)	ГОСТ 17799:2005
BS 7799-2: 2005	ISO 27001: 2005	ГОСТ 27001:2005
BS 7799-3: 2006	ISO 27005	- отсутствует

Потребность в национальном стандарте

- Требования ГОСТ 27001 к СУИБ

- Требования к документации при аудите и сертификации

- Потребности в методической и нормативной базах ИБ

Нормативные требования к СУИБ в соответствии с ГОСТ 27001

СУИБ - часть общей системы управления, основанной на оценке бизнес рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ

Раздел	Требования к управлению рисками
Создание СУИБ	c) Определить подход организации к оценке рисков d) Идентифицировать риски e) Проанализировать и оценить риски f) Идентифицировать и оценить возможности по обработке рисков g) Выбрать цели и механизмы контроля для обработки рисков h) Получить одобрение руководства для предложенных остаточных рисков
Внедрение и эксплуатация СУИБ	a) Разработать план обработки рисков b) Реализовать план обработки рисков c) Реализовать механизмы контроля d) Определить, как измерять эффективность выбранных механизмов контроля

Нормативные требования к СУИБ в соответствии с ГОСТ 27001 (продолжение)

Раздел	Требования к управлению рисками
Мониторинг и анализ СУИБ	d) Пересматривать оценки рисков, остаточные риски и идентифицированные уровни допустимых рисков
Сопровождение и совершенствование СУИБ	b) Предпринимать соответствующие корректирующие и превентивные действия c) Сообщать о предпринимаемых мерах и усовершенствованиях
Требования к документированию	d) Описание методологии оценки рисков e) Отчет об оценке рисков f) План обработки рисков
Ответственность руководства	f) Принятия решения о критериях принятия рисков и допустимом уровне риска
Анализ СУИБ руководством	b) Корректировка плана оценки и плана обработки рисков c) Внесение необходимых изменений об уровнях риска и/или критериях принятия рисков
...	...

Гармонизация российских стандартов

Требования ГОСТ 27001:2005 к СУИБ в части управления рисками

BS 7799-3:2006*:* принципы и рекомендации по реализации требований, относящихся к процессам управления рисками и связанным с ними мероприятиям

ГОСТ 17799:2005*:* примеры по политике ИБ, активам, угрозам, уязвимостям, целям и механизмам контроля

ГОСТ 9001:2001*:* требования к документам

ГОСТ 13335-3:2007*:* примеры стратегий оценки рисков

Международные стандарты 27000-серии

ISO 27000	Основные положения и термины
ISO 27001:2005	*Требования к системам управления информационной безопасности*
ISO 27002:2007	*Практические правила управления информационной безопасностью*
ISO 27003	Руководство по внедрению системы управления информационной безопасностью
ISO 27004	Измерение эффективности системы управления информационной безопасностью
ISO 27005	*Руководство по управлению рисками информационной безопасности*
ISO 27006:2007	Требования для органов, выполняющих аудит и сертификацию систем управления информационной безопасности

Международные стандарты 27000-серии

ISO 27007	Руководство по аудиту систем управления информационной безопасности
ISO 27031	Руководство по обеспечению непрерывности бизнеса
ISO 27032	Руководство по обеспечению компьютерной безопасности
ISO 27033	Руководство по обеспечению безопасности сетевых технологий
ISO 27034	Руководство по обеспечению безопасности программных приложений
…	…

II. СОДЕРЖАНИЕ BS 7799-3

0-4. Вводная часть

5. Оценка рисков

6. Обработка риска и принятие решения руководством

7. Непрерывные действия по управлению рисками

Приложения. Примеры активов, угроз, уязвимостей, методов оценки рисков

Термины и определения

Риск - комбинация вероятности события и его последствий

Управление риском (Risk Management) - скоординированные действия по управлению и контролю организации в отношении риска. Обычно включает в себя оценку риска, обработку риска, принятие риска и сообщение о риске

Оценка риска (Risk Assessment) - общий процесс анализа и оценивания риска

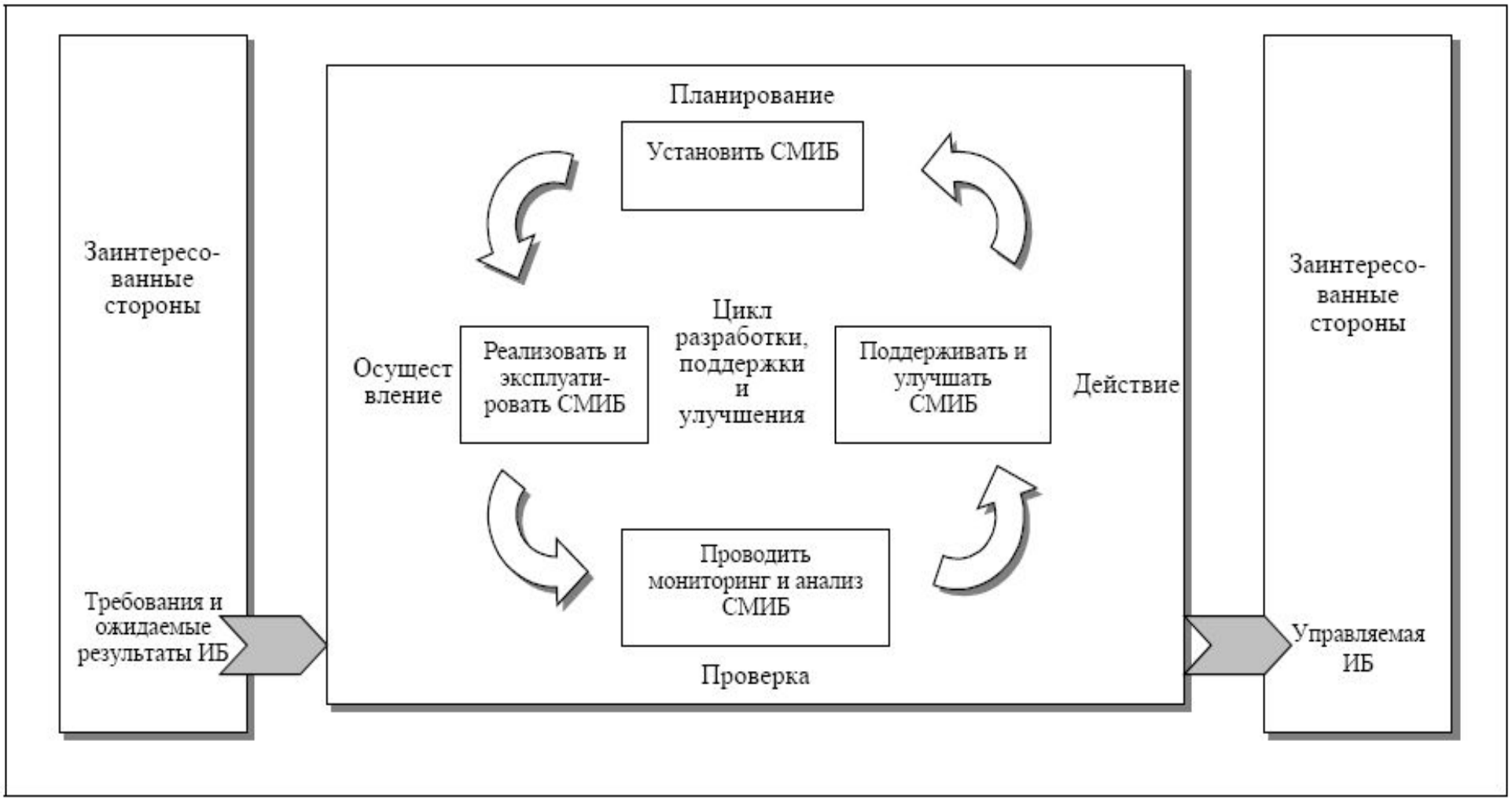
Анализ риска (Risk Analysis) - систематическое использование информации для идентификации источников и оценки величины риска

Оценивание риска (Risk Evaluation) - процесс сравнения оценочной величины риска с установленным критерием риска с целью определения уровня значимости риска

Обработка риска (Risk Treatment) - процесс выбора и реализации мер по модификации риска. Меры по обработке риска могут включать в себя избежание, оптимизацию, передачу или сохранение риска

Процессный подход (ISO 27001)

Процессная 4-х фазная модель менеджмента систем (Plan-Do-Check-Act) применительно к СУИБ



Фазы управления рисками

1) Оценка рисков, включающая анализ и оценивание рисков

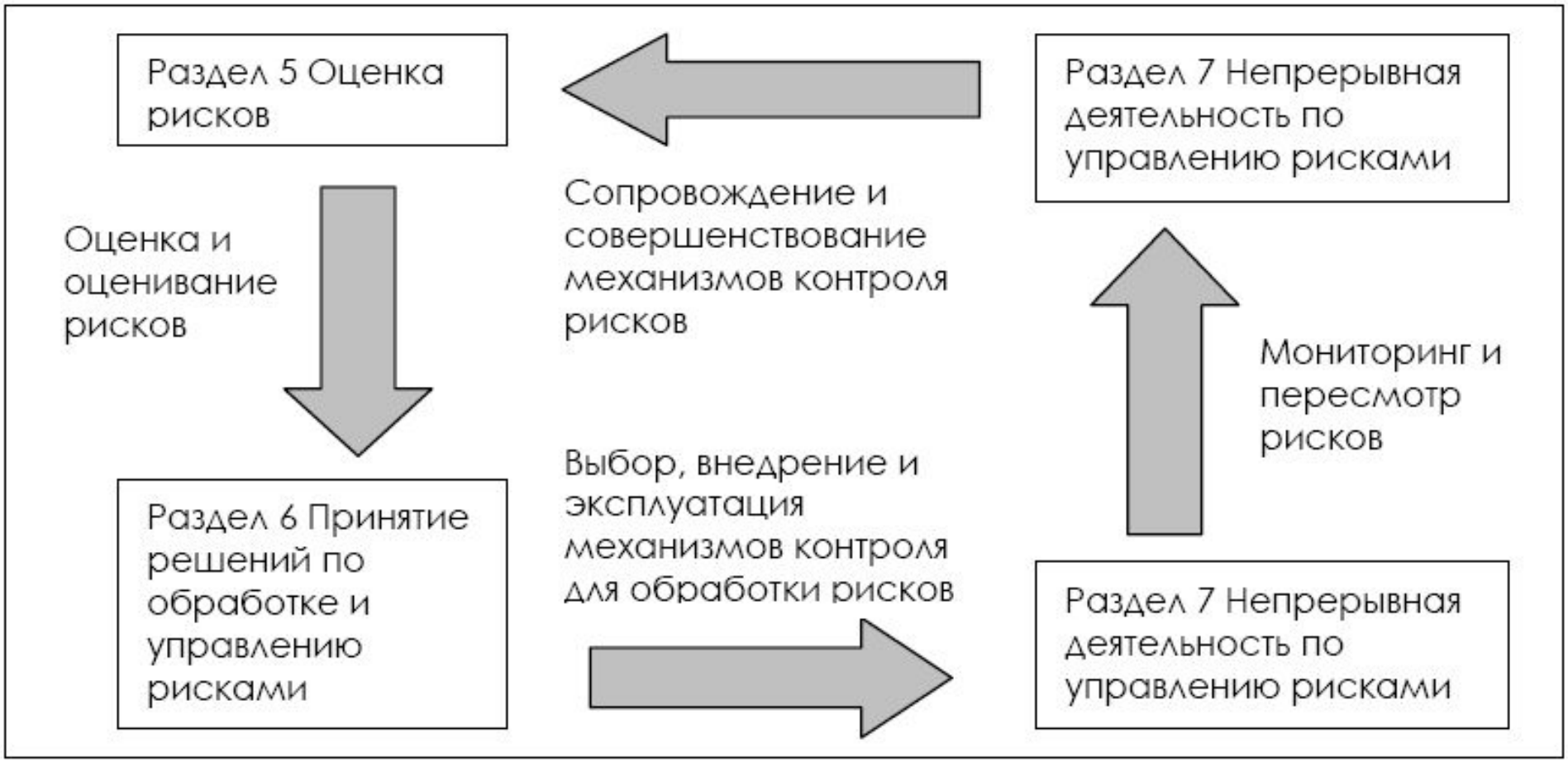
2) Обработка риска – выбор и реализация мер и средств безопасности

3) Контроль рисков путем мониторинга, тестирования, анализа механизмов безопасности, а также аудита системы

4) Оптимизация рисков путем модификации и обновления правил, мер и средств безопасности

Процессный подход (BS 7799-3)

Процессная модель применительно к управлению рисками



Методики оценки и анализа рисков

Не содержит требований к использованию ***конкретных*** *методик!*

Общие требования к методике:

- Возможность определения критериев для принятия риска
- Возможность идентификации приемлемых уровней риска
- Возможность проведения и идентификации и оценки рисков
- Покрытие всех аспектов СУИБ

2.1. ОЦЕНКА РИСКА

АНАЛИЗ РИСКА

- Инвентаризация и категорирование ресурсов
- Идентификация требований (нормативных, договорных, технических) к ресурсам
- Оценивание идентифицированных ресурсов с учетом идентифицированных требований законодательства и бизнеса, а также последствий нарушения конфиденциальности, целостности и доступности
- Идентификация значимых угроз и уязвимостей для идентифицированных ресурсов
- Вычисление вероятности реализации угроз и уязвимостей

ОЦЕНИВАНИЕ РИСКА

- Вычисление рисков
- Сопоставление рисков с заранее определенной шкалой риска

Величина риска может быть определена на основе стоимости ресурса, вероятности осуществления угрозы и величины уязвимости по следующей формуле :

$$Риск = \frac{(стоимость\ ресурса \times вероятность\ угрозы)}{величина\ уязвимости}$$

где *уязвимость* – **слабость в средствах защиты**, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, **которая может быть использована для проникновения в систему.**

Пример метода оценки рисков (приложение С.5). Шкала оценивания

Шкала оценивания уровня стоимости ресурсов:

{ «незначительный», «низкий», «средний», «высокий», «очень высокий»}

Шкала оценивания уровня вероятности угроз:

{«низкий», «средний», «высокий»}

Шкала оценивания уровня вероятности уязвимостей:

{«низкий», «средний», «высокий»}

Примеры методов оценки рисков (приложение С.5). Таблица расчета уровня риска

Таблица, использующая стоимость ресурсов и величины угроз и уязвимостей (R=F(A,T,V))

Стоимость ресурса	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимости								
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Примеры методов оценки рисков (приложение С.5). Ранжирование инцидентов по величине риска

Таблица категорирования инцидентов по величине уровня риска

Дескриптор инцидента (a)	Ущерб (стоимость ресурса) (b)	Вероятность осуществления (c)	Величина риска (d)	Категория инцидента (e)
Инцидент A	5	2	10	2
Инцидент B	2	4	8	3
Инцидент C	3	5	15	1
Инцидент D	1	3	3	5
Инцидент E	4	1	4	4
Инцидент F	2	4	8	3

План управления рисками

1. Ограничения и зависимости между механизмами контроля
2. Приоритеты
3. Сроки и ключевые промежуточные этапы реализации
4. Требуемые ресурсы
5. Ссылки на разрешения использования требуемых ресурсов
6. Критические маршруты выполнения плана

2.2. ОБРАБОТКА РИСКА

1. Уменьшение риска
2. Осознанное и обоснованное принятие риска
3. Передача риска
4. Избежание (отказ) риска

2.3. НЕПРЕРЫВНЫЕ ДЕЙСТВИЯ ПО УПРАВЛЕНИЮ РИСКАМИ

1. Сопровождение и мониторинг
2. Анализ со стороны руководства
3. Пересмотр и переоценка риска
4. Аудиты
5. Механизмы контроля документации
6. Корректирующие и превентивные меры
7. Отчеты и коммуникации
8. Менеджер рисков безопасности

Сопровождение и мониторинг: примеры

- Анализ файлов системных журналов
- Модификация параметров, связанных с произошедшими в системе изменениями
- Повторный анализ корректности использования механизмов контроля
- Обновление механизмов контроля, политик и процедур

Пересмотр и переоценка риска

- Результаты первоначальной оценки рисков должны регулярно пересматриваться
- Результаты повторного анализа рисков, проводимого с учётом возникших изменений, должны накапливаться в специальной базе данных, позволяющей отследить динамику происходящих изменений

Факторы возникновения изменений

- Изменения в бизнес-модели организации
- Появление новых данных относительно корректности и эффективности используемых сервисов безопасности
- Изменения, связанные с политической обстановкой, социальными факторами или окружающей средой
- Возникновение новых, ранее неизвестных угроз и уязвимостей

2.4. ПРИНЦИП ОСВЕДОМЛЕННОСТИ

1. Информирование на каждом этапе
2. Документирование событий
3. Обязанности персонала

Требования к документам

- план обеспечения непрерывности бизнеса
- описание методологии оценки рисков
- отчет об оценке рисков
- план обработки рисков
- план управления рисками
- рабочая документация: реестры ресурсов, реестры рисков, декларации применимости, списки проверок, протоколы процедур и тестов, журналы безопасности, аудиторские отчеты, планы коммуникаций, инструкции, регламенты и др.

Требования и обязанности персонала

- эксперты по оценке рисков
- менеджеры безопасности
- менеджеры рисков безопасности
- владельцы ресурсов
- руководство организации

III. СООТНОШЕНИЕ С МЕЖДУНАРОДНЫМИ СТАНДАРТАМИ

1. Гармонизация BS 7799-3 с ISO 27001:2005 (ГОСТ 27001) и ISO 27002:2007 (ГОСТ 17799)

2. Преемственность с рекомендациями NIST SP 800-30:2002 Risk Management Guide for Information Technology Systems (Руководство по управлению рисками в системах информационных технологий)

3. Рекомендации ISO 13335-3 Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT security (Руководство по управлению информационной безопасностью – Часть 3: Технологии управления информационной безопасностью)

4. Проект ISO 27005

Гармонизация российских стандартов

Требования ГОСТ 27001:2005 к СУИБ в части управления рисками

BS 7799-3:2006*:* принципы и рекомендации по реализации требований, относящихся к процессам управления рисками и связанным с ними мероприятиям

ГОСТ 17799:2005*:* примеры по политике ИБ, активам, угрозам, уязвимостям, целям и механизмам контроля

ГОСТ 9001:2001*:* требования к документам

ГОСТ 13335-3:2007*:* примеры стратегий оценки рисков

Рекомендации NIST SP 800-30:2002

Порядок оценки риска	Варианты обработки риска	Порядок обработки риска
1. Сбор сведений о системе 2. Идентификация угроз 3. Идентификация уязвимостей 4. Анализ механизмов защиты 5. Оценка вероятности 6. Оценка ущерба 7. Вычисление рисков 8. Рекомендации по выбору контрмер 9. Отчетная документация	Рассмотрение риска Избежание риска Ограничение риска Планирование риска Принятие к сведению и проведение исследований Передача риска	1. Распределение приоритетов действий по реализации контрмер 2. Оценка рекомендуемых параметров контрмер 3. Анализ экономической эффективности предлагаемых контрмер 4. Выбор контрмер 5. Распределение ответственности 6. Разработка плана реализации механизмов защиты 7. Реализация окончательно выбранных контрмер

Подход к анализу рисков ISO 13335-3

Проект ISO 27005

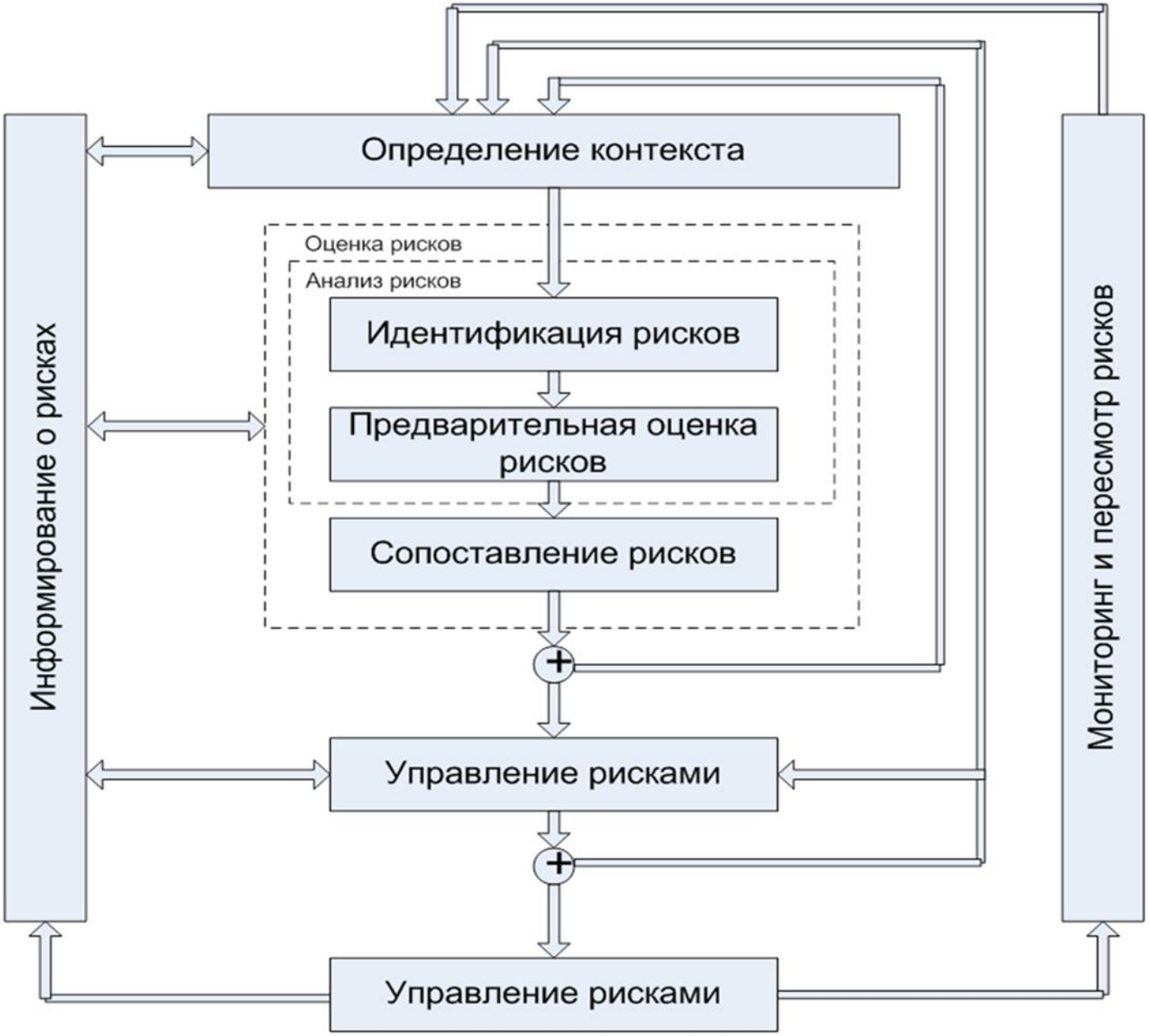
Сходство с BS 7799-3

- Процессная 4-фазная модель риск-менеджмента
- Доминирует логико-вероятностный подход к анализу и оцениванию уровня риска, допускаются качественные и количественные методики, конкретные методы и методики не навязываются
- Этапы носят итерационный характер, правила и рекомендации – общего плана
- Все процессы управления связаны с информированием о рисках

Развитие

- Порядок каждого этапа детально описан
- Большую половину стандарта составляют примеры и рекомендации

Порядок управления рисками по ISO 27005



ВЫВОДЫ (1)

I. BS 7799-3 и ISO 27005 отражают один и тот же сложившийся в международной практике процессный подход к организации системы управления рисками.

Управление рисками представляется как базовая часть системы менеджмента качества организации

ВЫВОДЫ (2)

II. Стандарты носят откровенно концептуальный характер, что позволяет экспертам по ИБ реализовать любые средства и технологии оценки, отработки и управления рисками. С другой стороны, стандарты не содержат рекомендаций по выбору какого-либо аппарата оценки риска, а также синтезу мер, средств и сервисов безопасности, используемых для минимизации рисков, что снижает полезность стандартов как технологических документов.

ВЫВОДЫ (3)

III. Потребность в национальном стандарте по управлению рисками определяется не только популяризацией экономически оправданных подходов к ИБ, но и требованиями и рекомендациями, заданными ГОСТ 27001:2005 и ГОСТ 17799:2005, а также вытекает из требований к организации бизнес-процессов, определенных в актуальных стандартах серии 9000.

ВЫВОДЫ (4,5)

IV. Можно предположить, развитие нормативной базы в стране пойдет по пути принятия ГОСТ, аутентичного ISO 27005 или BS 7799-3.

V. Недостатки стандарта (отсутствие конкретных методик) возможно исправить путем выпуска руководящего документа ФСТЭК России.

ВЫВОДЫ (6)

VI. Реальные стимулы в развитии данного нормативного направления, как и всех организационных стандартов ИБ:

- становление национальной сертификации СУИБ;
- развитие системы сертификации систем менеджмента качества в направлении выполнения требований по ИБ;
- широкое внедрение практики аудита систем ИБ

Источники:

BS 7799-3:2006 “Information security management systems – Part 3: Guidelines for information security risk management”.

Information Security Management Handbook. Fifth Edition. – CRC Press, 2004 г.

ISO/IEC TR 13335-3:1998 “Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT security”.

Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. - Special Publication 800-30, 2002.

О внедрении ГОСТ ИСО/МЭК 17799 и 27001 / С.А.Леденко, А.С. Марков и др. //InformationSecurity, 2006 -№3/4.

Управление рисками – нормативный вакуум / Марков А.С., Цирлов В.Л. // Открытые системы, 2007. №7.