

ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лекция № 8

**Особенности организации анализа
рисков информационной безопасности**

Особенности организации анализа рисков информационной безопасности

Цель занятия: **рассмотреть особенности информационных рисков организации в области информационной безопасности**

Учебные вопросы:

Введение

ВОПРОС **1.** Модель зрелости **Cartner Group**

ВОПРОС **2.** Модель **Carnegie Mellon University**

ВОПРОС **3.** Подготовка системы управления информационной безопасностью организации к сертификации в соответствии с ГОСТ Р ИСО/МЭК **27001-2006**

Этап **1.** Оценка текущего состояния СУИБ

Этап **2.** Оценка эффективности внедрения СУИБ

Этап **3.** Инспекции СУИБ

Введение

Введение

Оценка уровня безопасности корпоративной информационной системы влечет за собой определение по каким критериям и показателям производить оценку эффективности системы защиты информации и как оценивать и переоценивать информационные риски предприятия.

Вследствие этого, в дополнение к существующим требованиям, рекомендациям и руководящим документам ФСТЭК и ФСБ России приходится адаптировать к российским условиям и применять на практике методики международных стандартов BS ISO/IEC 27001:2005 BS 7799-2:2005, ISO/IEC TR 13335, ISO/IEC 10181-7:1996, ISO/IEC 15288:2002, ISO/IEC TR 15443, BSI, COBIT 4.1, ITIL V3, ISO/IEC 20000, ГОСТ Р ИСО/МЭК 15408-2002 и пр.

Введение

Основными целями разработки и внедрения корпоративных программ и методик управления информационными рисками являются:

— заполнение вакуума между топ-менеджерами компании, оперирующими терминами непрерывности и защищенности бизнеса, и техническими специалистами компании, использующими технические термины определения и парирования уязвимостей;

— создание мер (и, возможно, метрик) защищенности для надлежащего обеспечения информационной безопасности предприятия.

Введение

Ключевыми терминами в упомянутой области являются:

- риск (risk) - сочетание вероятности события и его последствий;**
- уязвимость (vulnerability) - ошибка или недочет в организации процессов, структуре или реализации технических средств, которые могут привести (случайно или преднамеренно) к нарушению политики безопасности системы;**
- угроза (threat) - потенциальная возможность реализации определенной уязвимости;**
- ущерб (impact) - степень и вид ущерба, нанесенного активу фактом реализации уязвимости.**

Введение

Оценивание рисков может производиться с помощью:

— экспертных оценок (непосредственно (явно) или косвенно - с использованием автоматических программных средств, в логику работы которых заложена некоторая база знаний о зависимости меры какого-либо риска от наблюдаемых условий);

— исторических сведений о вероятности реализации уязвимости и ущерба от ее реализации (недостатками метода являются потребность в достаточно большом объеме исторических данных (а для некоторых угроз их может просто не существовать) и невозможность точного оценивания тренда в случае меняющейся обстановки, что мы наблюдаем практически во всех сферах ИБ);

— аналитических подходов (находящихся в большей степени в академических разработках), например, с построением графов взвешенных переходов для определения величины ущерба от реализации уязвимости.

Введение

Меры, направленные на парирование рисков, могут включать в себя:

— **пассивные действия:**

— **принятие риска (решение о приемлемости наблюдаемого уровня данного риска без каких-либо контрмер);**

— **уклонение от риска (решение о трансформации деятельности, которая повлечет за собой данный уровень риска);**

— **активные действия:**

— **ограничение или снижение конкретного риска (состоит из набора организационных и технических мер, которые мы привыкли воспринимать в качестве мер по обеспечению информационной безопасности);**

— **передача риска (страхование) — довольно редкая в отечественных информационных технологиях процедура, которая, однако, постепенно завоевывает признание и в России.**

Введение

Постановка задачи обеспечения информационной безопасности может варьироваться в широких пределах. Соответственно, варьируются и постановки задач анализа рисков.

Основным фактором, определяющим отношение организации к вопросам информационной безопасности, является степень ее зрелости. Так, например известная аналитическая компания Cartner Group и университет Carnegie Mellon University предложили свои модели определения зрелости компании.

Различным уровням зрелости соответствуют различные потребности в области информационной безопасности.

ВОПРОС 1.**Модель зрелости Cartner Group**

Вопрос 1. Модель зрелости Cartner Group

Уровни зрелости	Характеристика уровня зрелости
0	<p>Проблема обеспечения ИБ управлением компании в должной мере не осознана и формально задачи обеспечения информационной безопасности компании не ставятся.</p> <p>Выделенной службы информационной безопасности нет.</p> <p>Служба автоматизации использует традиционные механизмы и средства защиты информации стека протоколов TCP/IP и сервисов Интранет, а также операционной среды и приложений (ОС, СУБД, CRM и др.).</p>
1	<p>Проблема обеспечения ИБ рассматривается управлением компании как исключительно техническая проблема.</p> <p>Выделенной службы защиты информации нет.</p> <p>Организационные меры обеспечения ИБ не используются.</p> <p>Финансирование осуществляется в рамках единого бюджета на IT-технологии.</p> <p>Служба автоматизации дополнительно к средствам защиты информации 0 уровня может использовать средства отказоустойчивости, резервного копирования информации, источники бесперебойного питания, а также межсетевые экраны, виртуальные частные сети (VPN), антивирусные средства.</p>

Модель зрелости Cartner Group

Уровни зрелости	Характеристика уровня зрелости
2	<p>Проблема обеспечения ИБ управлением компании осознана и рассматривается как взаимноувязанный комплекс организационных и технических мер.</p> <p>Используются методики анализа информационных рисков, отвечающие минимальному, базовому уровню защищенности КИС.</p> <p>В компании определены состав и структура штатной службы информационной безопасности.</p> <p>Принята корпоративная Политика информационной безопасности.</p> <p>Финансирование ИБ ведется в рамках отдельного бюджета на создание и поддержку корпоративной системы защиты информации.</p> <p>Служба информационной безопасности дополнительно к средствам защиты информации 0 и 1 уровней использует средства защиты от НСД, системы обнаружения вторжений (IDS), инфраструктуру открытых ключей (PKI), а также соответствующие политике безопасности компании организационные меры (внешний и внутренний аудит, разработка планов защиты, непрерывного ведения бизнеса, действия в штатных ситуациях и пр.)</p>

Вопрос 1. Модель зрелости Cartner Group

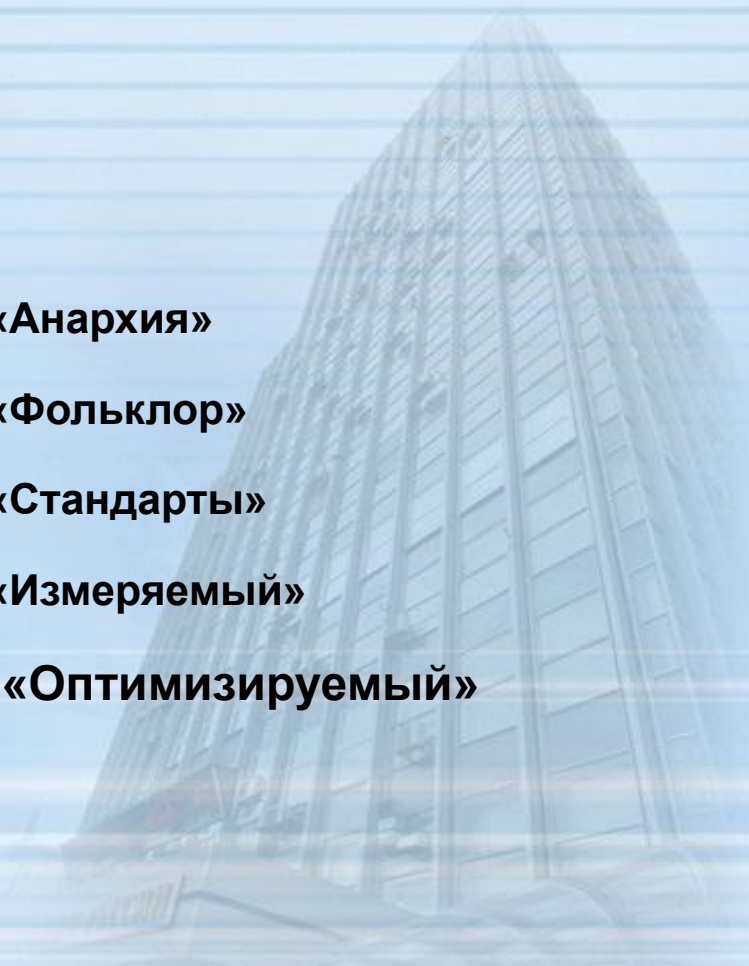
Уровни зрелости	Содержание уровня зрелости
3	<p>Проблема обеспечения ИБ управлением компании осознана в полной мере.</p> <p>Наряду с такими понятиями как бизнес культура существует понятие культуры информационной безопасности компании.</p> <p>Активно используются методики полного количественного анализа информационных рисков, а также соответствующие инструментальные средства.</p> <p>Назначен старший офицер по режиму информационной безопасности компании (CISO).</p> <p>Определена состав и структура группы внутреннего аудита безопасности КИС(CISA), группы предупреждения и расследования компьютерных преступлений, группы экономической безопасности.</p> <p>Руководством компании утверждены Концепция и Политика безопасности, План защиты и другие нормативно-методические материалы и должностные инструкции.</p> <p>Финансирование ведется исключительно в рамках отдельного бюджета.</p> <p>Служба информационной безопасности дополнительно к средствам защиты информации 0-2 уровней использует средства централизованного управления информационной безопасностью компании и средства интеграции с платформами управления сетевыми ресурсами</p>

ВОПРОС 2.

Модель **Carnegie Mellon University**

ВОПРОС 2.

Модель **Carnegie Mellon University**

- Уровень 1. «Анархия»
 - Уровень 2. «Фольклор»
 - Уровень 3. «Стандарты»
 - Уровень 4. «Измеряемый»
 - Уровень 5 «Оптимизируемый»
- 

ВОПРОС 2.

Модель **Carnegie Mellon University**

Уровень 1. «Анархия»

Признаки:

- сотрудники сами определяют, что хорошо, а что плохо
- затраты и качество не прогнозируются
- отсутствуют формализованные планы
- отсутствует контроль изменений
- высшее руководство плохо представляет реальное положение дел.

Политика в области ИБ не формализована, руководство не занимается этими вопросами.

Обеспечением информационной безопасности сотрудники могут заниматься по своей инициативе, в соответствии со своим пониманием задач по должности.

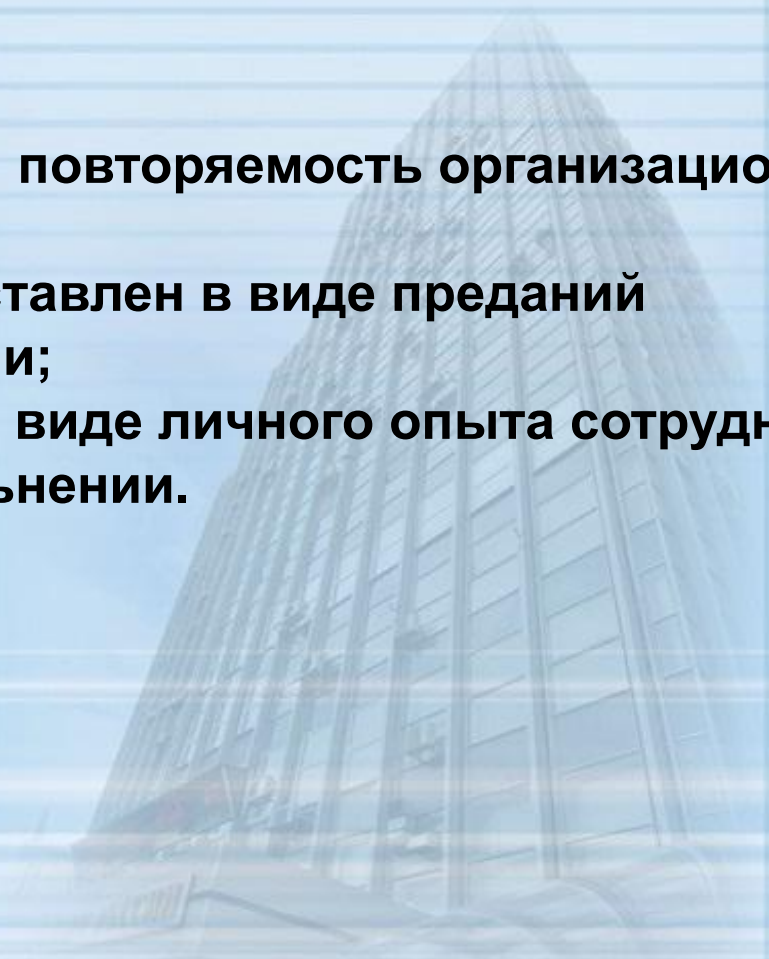
ВОПРОС 2.

Модель **Carnegie Mellon University**

Уровень **2. «Фольклор»**

Признаки:

- выявлена определенная повторяемость организационных процессов;
- опыт организации представлен в виде преданий корпоративной мифологии;
- знания накапливаются в виде личного опыта сотрудников и пропадают при их увольнении.



ВОПРОС 2.

Модель **Carnegie Mellon University**

На уровне руководства существует определенное понимание задач обеспечения информационной безопасности.

Существуют стихийно сложившиеся процедуры обеспечения информационной безопасности, их полнота и эффективность не анализируются.

Процедуры не документированы и полностью зависят от личностей вовлеченных в них сотрудников.

Руководство не ставит задач формализации процедур защиты информации.

ВОПРОС 2.

Модель **Carnegie Mellon University**

Уровень **3.** «Стандарты»

Признаки:

- корпоративная мифология записана на бумаге;
- процессы повторяемы и не зависят от личных качеств исполнителей;
- информация о процессах для измерения эффективности не собирается;
- наличие формализованного описания процессов не означает, что они работают;
- организация начинает адаптировать свой опыт к специфике бизнеса;
- производится анализ знаний и умений сотрудников с целью определения необходимого уровня компетентности;
- вырабатывается стратегия развития компетентности.

ВОПРОС 2.

Модель **Carnegie Mellon University**

Руководство осознает задачи в области информационной безопасности.

В организации имеется документация (возможно неполная), относящаяся к политике информационной безопасности.

Руководство заинтересовано в использовании стандартов в области информационной безопасности, оформлении документации в соответствии с ними.

Осознается задача управления режимом ИБ на всех стадиях жизненного цикла информационной технологии.

ВОПРОС 2.

Модель **Carnegie Mellon University**

Уровень **4. «Измеряемый»**

Признаки:

- процессы измеряемы и стандартизованы

Имеется полный комплект документов, относящихся к обеспечению режима информационной безопасности, оформленный в соответствии с каким-либо стандартом.

Действующие инструкции соблюдаются, документы служат руководством к действию соответствующих должностных лиц.

Регулярно проводится внутренний (и возможно внешний) аудит в области ИБ.

Руководство уделяет должное внимание вопросам информационной безопасности, в частности имеет адекватное представление относительно существующих уровней угроз и уязвимостей, потенциальных потерях в случае возможных инцидентов.

ВОПРОС 2.

Модель **Carnegie Mellon University**

Уровень **5** «Оптимизируемый»

Признаки:

- основное внимание уделяется повторяемости, измерению эффективности, оптимизации;
- вся информация о функционировании процессов фиксируется;

Руководство заинтересовано в количественной оценке существующих рисков, готово нести ответственность за выбор определенных уровней остаточных рисков, ставит оптимизационные задачи построения системы защиты информации.

Проблема обеспечения режима информационной безопасности будет ставиться (хотя бы в неявном виде) и решаться для организаций, находящихся на разных уровнях развития, по-разному.

ВОПРОС 3.

Подготовка системы управления информационной безопасностью организации к сертификации в соответствии с ГОСТ Р ИСО/МЭК **27001-2006**

Этап **1.** Оценка текущего состояния СУИБ

Этап **2.** Оценка эффективности внедрения СУИБ

Этап **3.** Инспекции СУИБ

ВОПРОС 3.

Подготовка системы управления информационной безопасностью организации к сертификации в соответствии с ГОСТ Р ИСО/МЭК **27001-2006**

Целью такого проекта является подготовка и сертификация системы управления информационной безопасностью, СУИБ компании согласно требованиям гармонизированного стандарта ГОСТ Р ИСО/МЭК 27001-2006 **"Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности"**.

Подготовка системы управления информационной безопасностью к сертификации в соответствии с ГОСТ Р ИСО/МЭК 27001-2006 осуществляется по следующим этапам.

Этап 1. Оценка текущего состояния СУИБ

Этап 2. Оценка эффективности внедрения СУИБ

Этап 3. Инспекции СУИБ

ВОПРОС 3.

Подготовка системы управления информационной безопасностью организации к сертификации в соответствии с ГОСТ Р ИСО/МЭК **27001-2006**

Этап 1.

**Оценка текущего состояния
СУИБ**

ВОПРОС 3.**Этап 1.**

Оценка текущего состояния СУИБ

На данном этапе проводятся все необходимые мероприятия для идентификации и документирования целей и мер контроля в соответствии с ГОСТ Р ИСО/МЭК 27001-2006.

1. Должны быть определены цели и задачи проекта, а также политика ИБ для СУИБ, выдвигаемой на сертификацию по требованиям ГОСТ Р ИСО/МЭК 27001-2006.

2. Должна быть определена область применения системы управления информационной безопасностью. Ее границы следует определить, исходя из характеристики организации, ее местоположения, информационных активов и используемых технологий.

3. Должна быть осуществлена проверка адекватности и полноты системы оценки рисков. Система оценки рисков должна выявлять угрозы для информационных активов предприятия, уязвимые места и их последствия для организации, а также определять величину риска.

4. На основе политики ИБ организации и с учетом степени необходимой гарантии определяются те области рисков, которые должны быть управляемыми.

5. Из подробного списка рекомендуемых международным стандартом ГОСТ Р ИСО/МЭК 27001-2006 целей контроля следует выбрать цели контроля, необходимые для внедрения; отбор следует обосновать.

6. Должен быть подготовлен документ о применимости стандарта. В нем следует изложить выбранные цели и средства контроля, а также причины их выбора. Кроме того, в этом отчете необходимо указать средства контроля из списка стандарта ГОСТ Р ИСО/МЭК 27001-2006, которые не были приняты.

ВОПРОС 3.**Этап 1.**

Оценка текущего состояния СУИБ

Проверяется имеющаяся в компании документация по системе управления информационной безопасностью на основе критериев, определенных стандартом ГОСТ Р ИСО/МЭК 27001-2006. Документация по системе управления ИБ должна содержать следующую информацию.

1. Свидетельства о предпринятых мерах в соответствии с принципами системы управления информационной безопасностью.

2. Общие принципы управления ИБ, включая политику в области информационной безопасности, цели и применяемые средства контроля, описанные в документе о применимости стандарта.

3. Описание процедур, принятых в целях эффективного применения средств контроля и проверенных на соответствие политике в области безопасности. При этом должны быть указаны обязанности ответственных лиц и их действия.

4. Описание процедур по управлению и использованию системы управления информационной безопасности. При этом должны быть указаны обязанности ответственных лиц и их действия.

ВОПРОС 3.**Этап 1.**

Оценка текущего состояния СУИБ

Компания должна определять и реализовывать процедуры контроля всей требуемой документации, чтобы выполнить следующие требования в отношении последней:

- документация готова к использованию;
- производится периодическая проверка документации и внесение необходимых изменений в соответствии с политикой безопасности организации;
- производится управление обновлениями и обеспечение доступности документации везде, где осуществляется деятельность, имеющая важное значение для эффективного функционирования системы управления информационной безопасностью;
- устаревшая информация своевременно удаляется;
- устаревшая документация, требуемая тем не менее для юридических целей и/или сохранения знаний, определяется и сохраняется.

ВОПРОС 3.**Этап 1.**

Оценка текущего состояния СУИБ

Документация должна быть удобной в обращении, содержать даты подготовки (включая даты внесения изменений) и быть легко узнаваемой, вестись в установленном порядке и храниться в течение определенного срока.

Следует определить и выполнять процедуры и обязанности по разработке и введению изменений в различные виды документов.

Документация может быть представлена в любой форме: печатной или электронной.

Проверяются все существующие процедуры ведения учетных записей в соответствии с критериями стандарта ГОСТ Р ИСО/МЭК 27001-2006.

Данные, полученные в результате функционирования системы управления информационной безопасностью, должны сохраняться в документированном виде с целью демонстрации соответствия требованиям стандарта ГОСТ Р ИСО/МЭК 27001-2006 применимо к самой системе и организации в целом (например, книга посетителей, аудиторская документация и санкционирование доступа).

ВОПРОС 3.**Этап 1.**

Оценка текущего состояния СУИБ

Нормативные документы организации целесообразно скомплектовать в группы.

Таблица 4

Группы разрабатываемых нормативных документов организации

№	Группы разрабатываемых нормативных документов организации
1	Документы работников
2	Делопроизводство
3	Приказы
4	Протоколы и решения совещаний
5	Политики информационной безопасности
6	Положения
7	Регламенты и методологии
8	Стандарты
9	Договоры и соглашения
10	Аудит ИБ

ВОПРОС 3.**Этап 1.**

Оценка текущего состояния СУИБ

Компания должна самостоятельно определить и выполнять процедуры по выявлению, учету, хранению и использованию данных, свидетельствующих о соответствии предъявляемым требованиям.

Документы должны быть удобными в обращении, узнаваемыми и указывать на конкретные действия. Их следует хранить и поддерживать в таком состоянии, чтобы можно было легко восстановить и защитить от повреждения или потери.

В результате выявляются любые недостатки СУИБ в соблюдении стандартов ГОСТ Р ИСО/МЭК 27001-2006 и подготовка плана их устранения. На данном этапе выполняются предусмотренные стандартом ГОСТ Р ИСО/МЭК 27001-2006 мероприятия, связанные с оценкой документации по внедрению общих принципов системы управления ИБ и ознакомление с текущим состоянием дел в рамках проекта.

Этап 2.

Оценка эффективности внедрения СУИБ

ВОПРОС 3.**Этап 2.**

Оценка эффективности внедрения СУИБ

На данном этапе работ, согласно требованиям стандарта ГОСТ Р ИСО/МЭК 27001-2006, проводится оценка, подтверждающая эффективность внедрения системы управления информационной безопасностью и ее соответствие установленным требованиям, а также выбранным мерам и средствам контроля стандарта ГОСТ Р ИСО/МЭК 27001-2006.

По итогам выполнения работ составляется отчет, в котором будет высказано мнение относительно сертификации, в частности в отчете будет отражена оценка деятельности по управлению информационной безопасностью на объектах организации на предмет соответствия международному стандарту ГОСТ Р ИСО/МЭК 27001-2006.

ВОПРОС 3.

Подготовка системы управления информационной безопасностью организации к сертификации в соответствии с ГОСТ Р ИСО/МЭК **27001-2006**

Этап 3.**Инспекции СУИБ**

ВОПРОС 3.**Этап 3.**

Инспекции СУИБ

В соответствии с правилами сертификации необходимо проводить регулярную оценку объекта на соответствие требованиям международного стандарта ISO 27001:2005.

Критерии периодичности таких посещений основаны на действующих критериях получения аккредитации UKAS.

Как правило, проводится две инспекции в год до истечения трех лет с момента сертификации, после чего срок действия сертификации продлевается.

По истечении трех лет с момента сертификации может потребоваться дополнительный день для возобновления срока действия сертификации.

ВОПРОС 3.

Этап 3.

Инспекции СУИБ

Предусматривается, что на третьем этапе инспекционные визиты будут проводиться один раз в шесть месяцев представителями, например, BSI Россия, начиная с момента получения сертификации на протяжении первых трех лет срока действия сертификации, данные проверки будут осуществляться в соответствии с согласованным планом оценки.

Национальный стандарт Российской Федерации
ГОСТ Р ИСО/МЭК 27001-2006

**«Информационная технология.
Методы и средства обеспечения безопасности.
Системы менеджмента информационной
безопасности»**

(утв. приказом Федерального агентства по техническому
регулированию и метрологии от 27 декабря 2006 г. N 375-ст)

**Information technology. Security techniques. Information security
management systems.
Requirements**

Дата введения - 1 февраля 2008 г.
Введен впервые

Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 27001-2006

Настоящий стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ).

Внедрение СМИБ является стратегическим решением организации.

На проектирование и внедрение СМИБ организации влияют:

- потребности и цели организации,
- требования безопасности,
- используемые процессы,
- масштабы деятельности и структура организации.

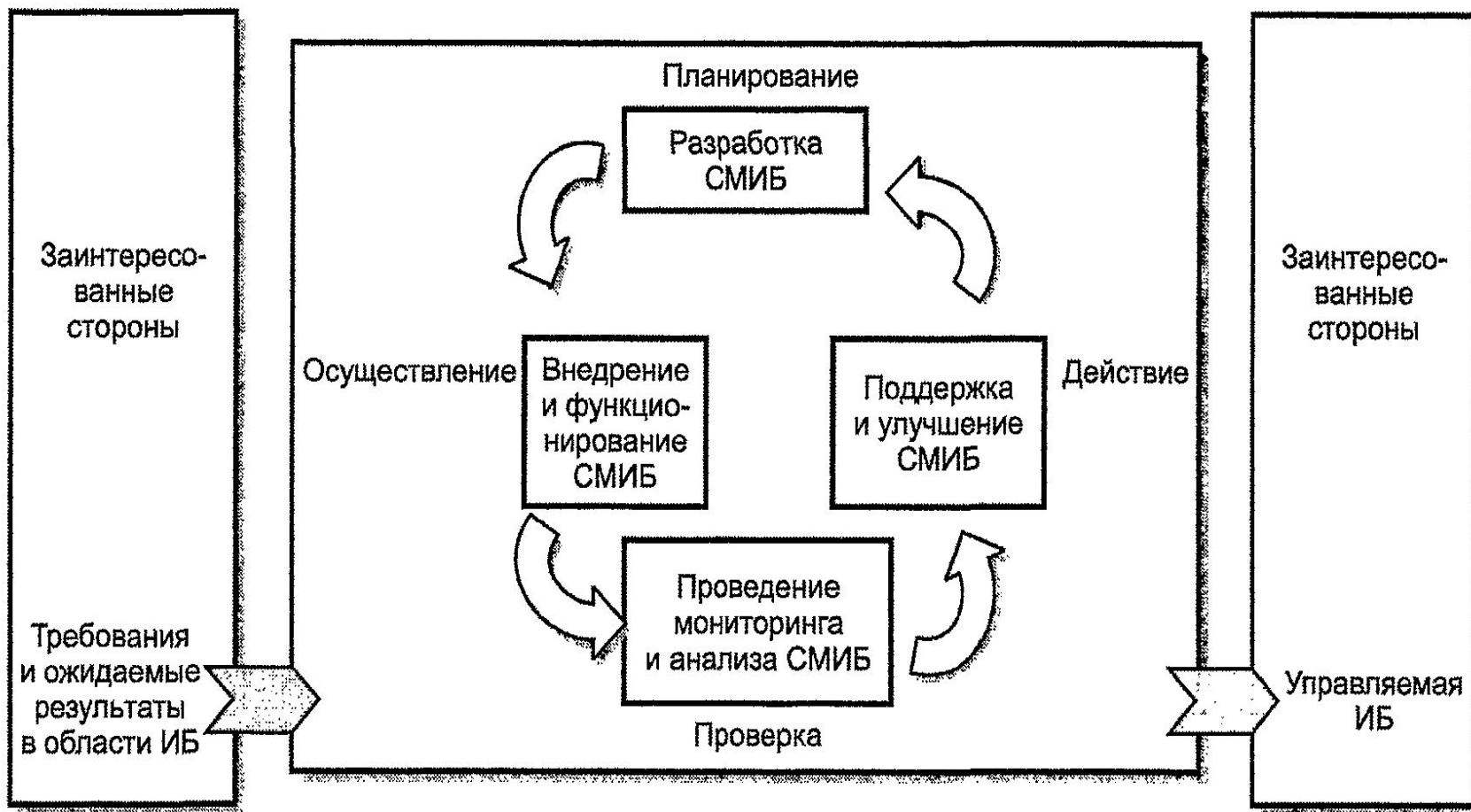
Предполагается, что вышеуказанные факторы и поддерживающие их системы будут изменяться во времени.

Предполагается также, что СМИБ будет изменяться пропорционально потребностям организации, т.е. для простой ситуации потребуется простое решение по реализации СМИБ.

В настоящем стандарте представлена модель **"Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)" (PDCA)**, которая может быть применена при структурировании всех процессов СМИБ.

На рисунке 1 показано, как СМИБ, используя в качестве входных данных требования ИБ и ожидаемые результаты заинтересованных сторон, с помощью необходимых действий и процессов выдает выходные данные по результатам обеспечения информационной безопасности, которые соответствуют этим требованиям и ожидаемым результатам.

Рисунок 1 иллюстрирует также связи между процессами



Совместимость с другими системами менеджмента

Стандарт 27001-2006 согласован со стандартами [ИСО 9001:2000](#) "Системы менеджмента качества. Требования" и [ИСО 14001:2004](#) "Системы управления окружающей средой. Требования и руководство по применению" в целях поддержки последовательного и интегрированного внедрения и взаимодействия с другими подобными взаимосвязанными стандартами в области менеджмента.

Таким образом, **одна правильно построенная система менеджмента в организации может удовлетворять требованиям всех этих стандартов.**

Настоящий стандарт позволяет организации регулировать СМИБ или интегрировать ее с соответствующими требованиями других систем менеджмента.



**Благодарю за
внимание!**