

**Управление**  
**ИТ и информационной безопасностью**  
**в контексте международных стандартов,**  
**методик и лучших практик**

Владимир Булдыжов, CISM

# **Введение**

### Современные тенденции ИБ

#### **Постоянно расширяющееся взаимопроникновение и взаимосвязь угроз.**

Нарушение одного вида легко приводит к нарушениям другого:

а) вредоносное ПО скрытно отправляет конфиденциальную информацию в Интернет (взаимосвязь: нарушение целостности приводит к утечке), а также рассылает спам (взаимосвязь: затрата ресурсов),

б) утечка информации (например, паролей, адресов e-mail) обуславливает заражение вирусами, взлом, спам (взаимосвязь: утечка приводит к нарушению целостности, отказу в доступе, потере рабочего времени),

в) заражение вредоносным ПО происходит через развлекательные и другие неслужебные сайты (взаимосвязь: потери рабочего времени приводят к нарушению целостности информации и доступности служб и так далее).

# Социально-экономические аспекты ИБ

*– На чьей стороне перевес в борьбе?*

Ещё несколько лет назад отчеты о потерях компаний от нарушений информационной безопасности содержали суммы в сотни миллионов \$.

В начале 2009 года был опубликован [отчет McAfee](#), согласно которому за 2008 год этот ущерб составил уже 1 000 000 000 000 долларов (1 триллион).

Индустрия ИБ показывает невиданный прогресс, но потери растут быстрее. Ситуация напоминает положение с медициной: прогресс огромный, но болезни не исчезают. Верен ли подход? Нужна ли вообще борьба?

Целью индустрии является не ликвидация угроз, а зарабатывание денег. Поэтому ответственность за ИБ предприятия лежит только на сотрудниках его службы ИБ, не на поставщиках.

**Услуги ИБ оплачиваются бизнесом, а для бизнеса существует только один показатель эффективности чего бы то ни было – экономическая эффективность.**



### Введение. Управленческие аспекты ИБ

#### ***– ИТ-безопасность – то же самое ли это, что ИБ?***

Варианты подчинения службы ИБ (СБ, ИТ, фин. службе) имеют преимущества и недостатки. При концентрации управления ИБ в ИТ-подразделении ИБ рассматривается как чисто техническая дисциплина, игнорируются юридические, экономические, методологические, образовательные, социальные, психологические, мотивационные проблемы.

#### ***– Что это за проблемы и какова природа нарушений ИБ?***

Большинство нарушений ИБ рассматриваются как технические, например, вирусные атаки, спам или отказы жестких дисков. Но по величине материального ущерба критичными являются нарушения человеческой природы, такие как халатность, утечки информации и мошенничество.

Более того, любая техническая угроза имеет человеческие причины. Вирус – следствие нарушения работы с ПО, Интернет, email. Уничтожение информации – следствие халатности при резервировании.

**Угроз информационной безопасности не существует.  
Есть недостаточная зрелость процессов управления ИБ.**

## Предпосылки усиления стандартизации в области ИТ и ИБ

### 1. Неудачные проекты в области ИТ. Статистика:

Инициатор исследования	Результаты проектов внедрения ИС		
	Провал	Удовлетворительно	Полный, долгосрочный успех
Price Waterhouse (Проекты Пентагона 2001г.)	83%		17%
Standish Group (Европа 2001г.)	77%		23%
KPMG (США + Европа 2001г.)	40%	57%	3%
ИМИСП (Северо-Запад РФ, 2003г.)	78%	20%	2%

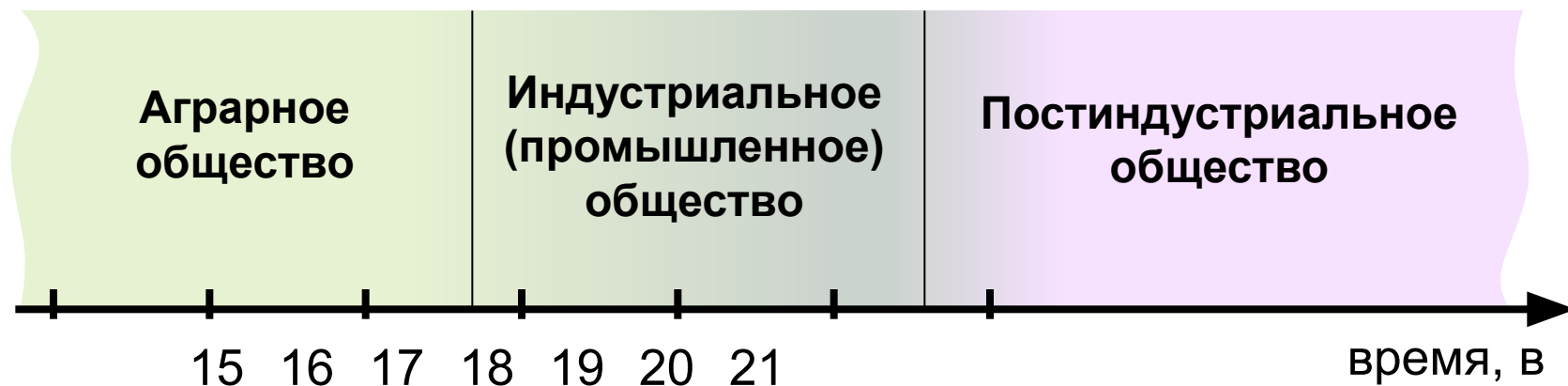
### 2. Громкие дела о банкротствах и махинациях.

Крупнейший корпоративный крах в истории США – банкротство энергетической компании Enron. С 1997 по 2000 год компания завышала свои прибыли, ее руководство тайком переводило деньги в другие компании на стороне. Отчеты искажались. Компания Arthur Andersen, отвечающая за бухгалтерский аудит Enron, признала, что ее сотрудники уничтожали документы Enron. Другие дела: HeathSouth, Adelphia, Tyco, WorldComm, Quest Communications и Global Crossing

### 3. Глобализационные процессы.

Глобализация и информационная революция связаны двунаправленными (слияния/поглощения, конкурентная борьба) причинно-следственными связями. Современная тенденция – повышение контроля государства над бизнесом (предлоги процесса: мошенничество, терроризм, кризис).

# Постиндустриальное глобализованное общество



**Изобретение паровой машины в 1769-76 гг.** Механизация труда, массовое производство, новые профессии и социальные группы, урбанизация, закрепление рыночной экономики.

⇒ **5-10% населения кормят продуктами питания всё общество.**

**Расширение корпораций во II половине XX в.** Становление экономики услуг, глобализация экономики, формирование научного знания как самостоятельного элемента производственных сил, повышение престижа образования и знаний, информационные услуги, экономика знаний.

⇒ **реальный сектор экономики – всего 20-30% ВВП на западе.**

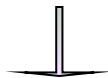
### Стандарты как вклад в глобализацию

Оценка пользы глобализации для человечества неоднозначна. Однако, это реальность, с которой трудно не считаться. Нужно извлекать пользу из нее.

Глобализация и конкуренция ускоряют бизнес-процессы, что обуславливает повышенные требования к:

- скорости принятия решений,
- непрерывности бизнеса,
- конфиденциальности обрабатываемой информации.

Повышение доли информации и других нематериальных активов ведет к повышению расходов на ИТ, что непрерывно ужесточает требование экономической эффективности ИТ и экономической безопасности бизнеса.



Данные требования являются главными предпосылками возникновения стандартов ИТ (ISO, ITIL, COBIT), которые в современном мире выполняют миссию, в некоторой степени аналогичную роли механизации и унификации процессов и средств труда в индустриальную эпоху.



# Внутренние проблемы корпоративных служб ИТ и ИБ

### Обоснование инвестиций и определение экономической эффективности.

- Подразделения ИТ и ИБ в коммерческой компании являются *затратным* (неприбыльным). С годами растет количество обрабатываемых данных, количество услуг, соответственно, затраты на ИТ.
- Бизнес не имеет достаточно инструментов управления инвестициями в ИТ/ИБ, а проще говоря, не видит, на что именно идут его деньги. Управление инвестициями во многих случаях строится на *доверии* к руководителю службы ИТ/ИБ (CIO/CISO).
- Формально обосновать деятельность ИБ труднее, чем ИТ, поскольку служба ИБ оперирует *абстрактными* для бизнеса понятиями (целостность, доступность, конфиденциальность).
- Особенности ИБ. Создаются *неудобства* пользователям и ИТ. Независимо от вида подчиненности службы ИБ, в случае её бездеятельности снижается её влияние, в случае неэффективной деятельности – доверие к ней. ИБ – это постоянный поиск компромиссов.

### Внутренние проблемы корпоративных служб ИТ и ИБ

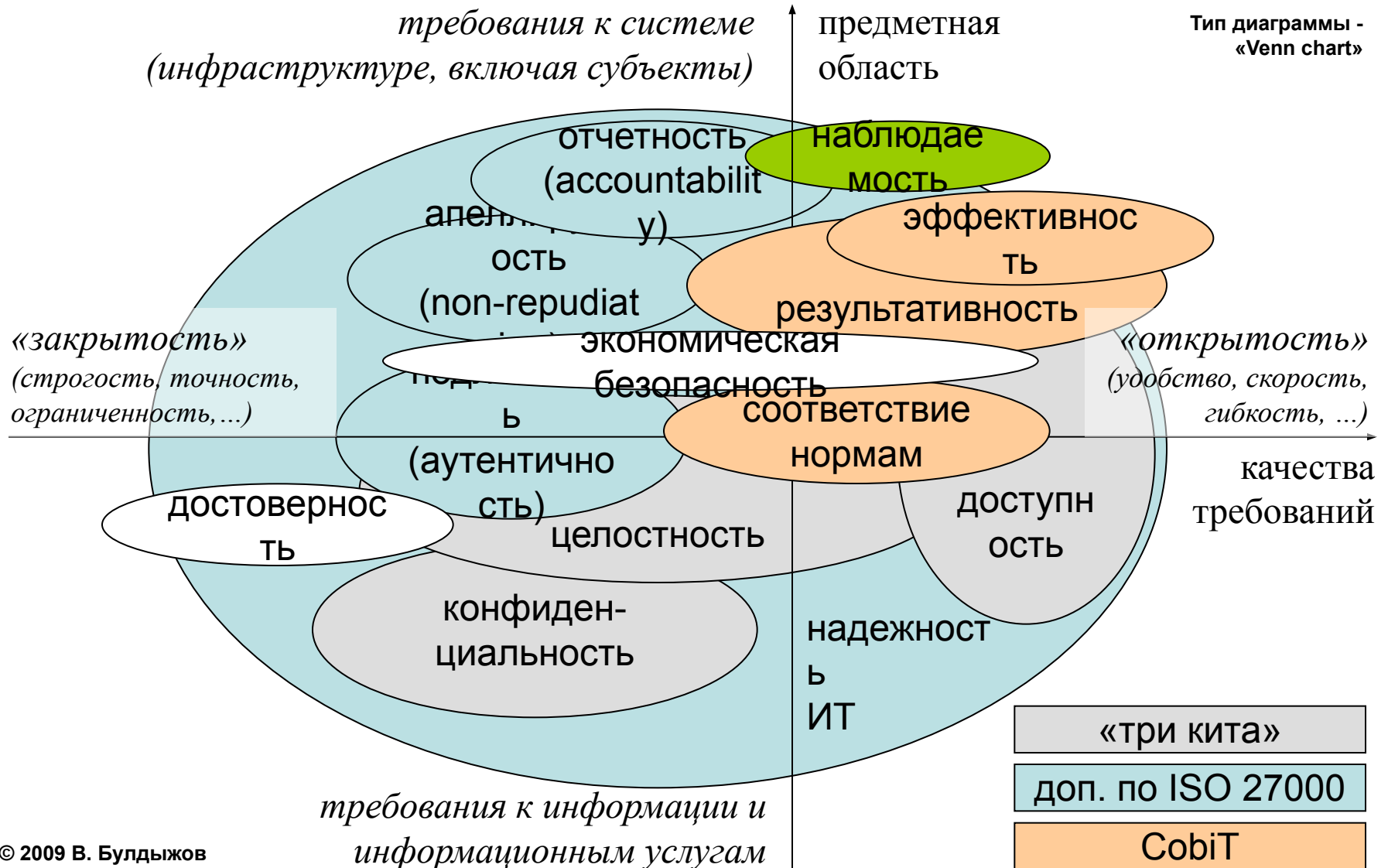
**Традиционный подход: управление, основанное на доверии (человеческом факторе).**

Получаемый кредит доверия (в том числе, в финансовом выражении), расходуется руководством службам ИТ и ИБ не только на прямо формулируемые цели бизнеса, но и на внутренние, косвенные цели, служебные сервисы.

Достижения идут в актив, неудачи – в пассив. Происходит алгебраическое сложение уровня доверия. В конечном итоге, руководство компании отстранено от принятия решений в ИТ/ИБ и может принять только одно решение: уменьшить или увеличить финансирование.

Данный подход **непрозрачен** для бизнеса, который готов полнее управлять своими инвестициями, однако, при этом не вдаваясь в технические детали ИТ и ИБ.

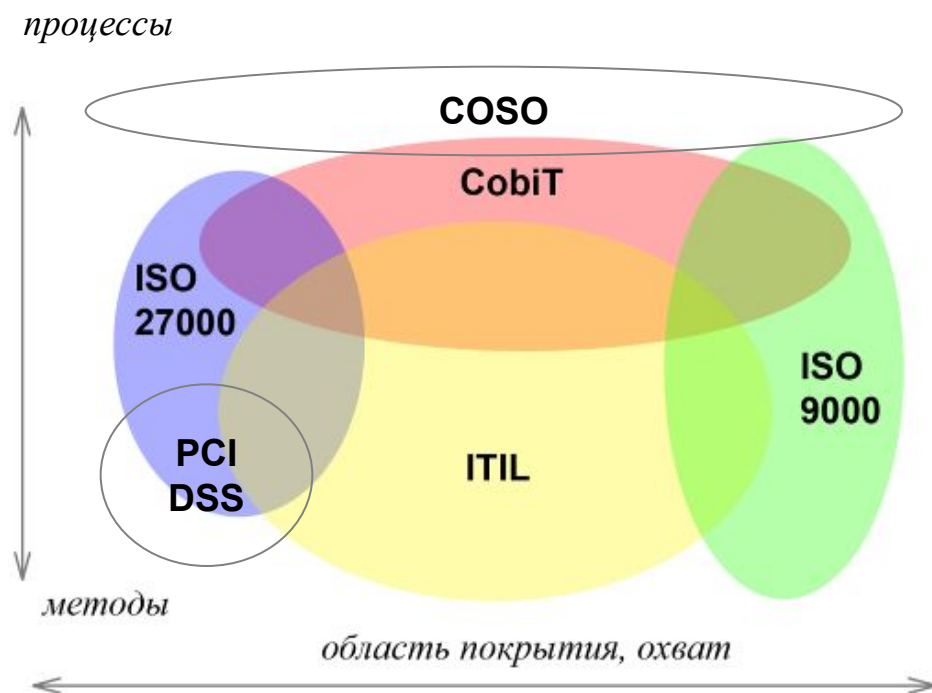
## Требования ИТ и ИБ как показатель области охвата методологии



### Области охвата и уровень абстракции стандартов

Управление ИБ не просто связано с управлением ИТ, а **тесно интегрировано**. Неэффективно рассмотрение отдельно управления ИБ и управления ИТ, а особенно рассмотрение данных двух областей отдельно от управления бизнесом.

Интеграцию условно можно представить по взаимосвязи международных стандартов. Области охвата стандартов и методологий, а также их роли при взаимодействии:



- **COSO** – корпоративное стратегическое управление и управление рисками, роль – структура управления бизнесом в целом;
- **CobiT** – стратегическое управление ИТ, эффективностью, управляемостью, прозрачностью, надежностью и т. д., роль – связь ИТ/ИБ с бизнесом, «зонтик» методологий ИТ, ИБ, BCM, BSC, MM, PM;
- **ITIL** – управление качеством ИТ-услуг, роль – «аккумулятор» первичных знаний, массовый инструмент;
- **ISO 27000** – управление ИБ, роль – формализация эталона СУИБ;
- **ISO 9000** – управление качеством, роль – связь процессов с т. з. качества.

# Международные стандарты – «опытный» подход

**Стандарты и методики.** Наиболее распространенные: ISO, COBIT, ITIL.

**Актуальность.** ITIL – двигатель COBIT и ISO. ITIL был создан *во время экономического кризиса* в Великобритании в конце 80-х. Главная цель – экономическая эффективность и прозрачность управления ИТ.

**Методики и стандарты – это удобные *инструменты*,** хорошо согласующиеся друг с другом и взаимно дополняющие друг друга. Каждая методика имеет свои сильные места, концентрируясь на своём уровне абстракции. COBIT и ISO говорят «что» нужно делать, ITIL – «как».

**Методические цели стандартов и лучших практик:**

- предоставить структурную основу, призванную упорядочить знания, облегчить их использование и передачу, в том числе, в условиях «текучки» персонала,
- обеспечить общий язык между специалистами, руководством, бизнесом, поставщиками.

**Стандарты – не панацея.** В каждой организации есть уникальные процессы или объекты, защита которых не описана в стандартах/практиках (или трудно найти).

### Методологическая роль западных стандартов

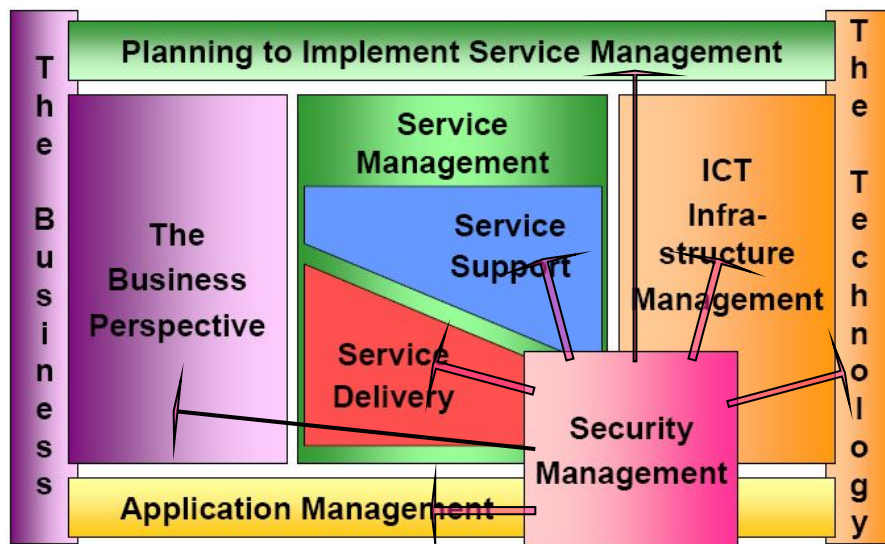
Западные стандарты, в отличие от привычных нам ГОСТ, часто носят методологический, обучающий, рекомендательный и даже, как это ни парадоксально, необязательный характер.

- **Предисловие к CobiT 4.1:** стандарт предназначен, прежде всего, для образовательных целей.
- **Как перевести ключевой глагол ISO 27002 «*should*»?**  
Зачастую он переводится неправильно как «должен». Однако, вариант «рекомендуется» искажает смысл ещё больше. Почти точно передает смысл русское слово «следует». Рекомендательный оттенок остается.
- **Закрепление понятийного аппарата.** «Средство управления», «апеллируемость», «перенос рисков» и т. д.

**ITIL**

## Библиотека ITIL. Внедрение реального проекта

### ITIL Publication Framework:



### Service Delivery:

- Управление уровнем обслуживания
- Финансовое управление ИТ
- Управление мощностями
- Управление непрерывностью
- Управление доступностью

### Service Support:

- Служба поддержки
- Управление инцидентами
- Управление проблемами
- Управление изменениями
- Управление релизами
- Управление конфигурациями

### Результаты начала интеграции:

- разрешительный механизм ИБ (ISO) реально заработал
- увеличился поток сообщений об уязвимостях и нарушениях ИБ

### Дальнейшие направления интеграции:

- SLA
- обеспечения непрерывности бизнеса и ИТ-услуг



## Библиотека лучших практик ITIL, структура v. 3

Service Strategy (SS)	Service Design (SD)	Service Transition (ST)	Service Operation (SO)	Continual Service Improvement (CSI)
<ul style="list-style-type: none"> <li>• Service management</li> <li>• Service life cycle</li> <li>• Service assets and value creation</li> <li>• Service provider types and structures</li> <li>• Strategy, markets and offerings</li> <li>• Financial management</li> <li>• Service portfolio management</li> <li>• Demand management</li> <li>• Organisational design, culture and development</li> <li>• Sourcing strategy</li> <li>• Service automation and interfaces</li> <li>• Strategy tools</li> <li>• Challenges and risks</li> </ul>	<ul style="list-style-type: none"> <li>• Balanced design</li> <li>• Requirements, drivers, activities and constraints</li> <li>• Service-oriented architecture</li> <li>• Business service management</li> <li>• SD models</li> <li>• Service catalogue management</li> <li>• Service level management</li> <li>• Capacity and availability</li> <li>• IT service continuity</li> <li>• Information security</li> <li>• Supplier management</li> <li>• Data and information management</li> <li>• Application management</li> <li>• Roles and tools</li> <li>• Business impact analysis</li> <li>• Challenges and risks</li> <li>• SD package</li> <li>• Service acceptance criteria</li> <li>• Documentation</li> <li>• Environmental issues</li> <li>• Process maturity framework</li> </ul>	<ul style="list-style-type: none"> <li>• Goals, principles, policies, context, roles and models</li> <li>• Planning and support</li> <li>• Change management</li> <li>• Service asset and configuration management</li> <li>• Release and deployment</li> <li>• Service validation and testing</li> <li>• Evaluation</li> <li>• Knowledge management</li> <li>• Managing communication and commitment</li> <li>• Stakeholder management</li> <li>• Configuration management system</li> <li>• Staged introduction</li> <li>• Challenges and risks</li> <li>• Asset types</li> </ul>	<ul style="list-style-type: none"> <li>• Balance in SO</li> <li>• Operational health</li> <li>• Communication</li> <li>• Documentation</li> <li>• Events, incidents and problems</li> <li>• Request fulfilment</li> <li>• Access management</li> <li>• Monitoring and control</li> <li>• Infrastructure and service management</li> <li>• Facilities and data centre management</li> <li>• Information and physical security</li> <li>• Service desk</li> <li>• Technical, IT operations and application management</li> <li>• Roles, responsibilities and organisational structures</li> <li>• Technology support to SO</li> <li>• Managing change, projects and risk</li> <li>• Challenges</li> <li>• Complementary guidance</li> </ul>	<ul style="list-style-type: none"> <li>• Goals, methods and techniques</li> <li>• Organisational change</li> <li>• Ownership</li> <li>• Drivers</li> <li>• Service level management</li> <li>• Service measurement</li> <li>• Knowledge management</li> <li>• Benchmarks</li> <li>• Models, standards and quality</li> <li>• CSI seven-step improvement process</li> <li>• Return on investment (ROI) and business issues</li> <li>• Roles</li> <li>• Authority matrix (RACI)</li> <li>• Support tools</li> <li>• Implementation</li> <li>• Governance</li> <li>• Communications</li> <li>• Challenges and risks</li> <li>• Innovation, correction and improvement</li> <li>• Best practices supporting CSI</li> </ul>

## Основные процессы ИБ в ITIL

1. **Стратегия услуг (SS).** Трудности и риски. Активы сервисов и создание ценности, управление портфолио сервисов.
2. **Проектирование услуг (SD).** Собственно информационная безопасность, трудности и риски, непрерывность сервисов ИТ, мощность и доступность. Детализация: SLA, BIA, управление приложениями, роли и инструменты, документация, управление каталогом сервисов, *управление поставщиками и третьими сторонами.*
3. **Развертывание услуг (ST).** Трудности и риски, *управление изменениями*, цели/ принципы/ политики/ контекст/ роли/ модели, типы активов. Доп.: управление конфигурациями и CMDB/CMS, управление коммуникациями и согласованиями, внедрение и развертывание сервисов.
4. **Оказание услуг (SO).** Информационная и физическая безопасность, роли/ обязанности и орг. структуры, управление доступом, события/ инциденты/ проблемы, *управление изменениями/ проектами/ рисками*, отслеживание и управление. Доп.: коммуникации, техническое/ операционное управление/ управление приложениями, диспетчерская служба, документация.
5. **Постоянное улучшение услуг (CSI).** Трудности и риски, матрица полномочий RACI, роли. Доп.: коммуникации, измерения сервисов, управление знаниями, ROI и вопросы бизнеса.

# Управление непрерывностью бизнеса (BCM)

### Простой вариант формализации BCM в SLA.

- ИТ-услуги разделяются на *разовые* и *постоянные* (разовых больше). Кроме того, услуги могут группироваться по признакам.
- Определяются *параметры качества* каждой группы ИТ-услуг. Для разовых: время реакции на заявку, время частичного предоставления, время выполнения. Для постоянных: время реакции на инцидент, время частичного восстановления услуги в случае её прекращения или недопустимого снижения качества, время полного восстановления.
- Определяются *индивидуальные параметры качества* каждой услуги (пропускная способность интернет, скорость реакции сайта, доступное дисковое пространство на файловом сервере, доля спама среди писем, количество ложных срабатываний антивируса, максимальный размер группы на занятиях по повышению квалификации).
- Если требования качества у разных клиентов разные (то есть, если есть "богатые" и «бедные» клиенты), определяются разные наборы параметров качества, по сути, *разные SLA* (normal/ VIP, silver/ gold/ platinum support).

### Анализ воздействия на бизнес (ВИА), ВСП/DRP

- ВИА является аналогом анализа рисков в области непрерывности бизнеса.
- ВИА – это управление рисками, привязанное к ресурсам и бизнес-угрозам. Включает определение ресурсов для восстановления и приоритизацию восстановления процессов.
- ВИА используется для расчета приоритетов мероприятий ВСП/DRP по восстановлению ресурсов при аварии.
- После ВИА разрабатывается ВСП (включая DRP) и Incident Response Plan (IRP). ВИА/ВСП фокусируются на доступности, IRP – на других рисках ИБ.

### Параметры BSM, фиксируемые в SLA и BCP

- **RPO – Recovery Point Objective** – цель восстановления, максимальной допустимый срок последнего известного приемлемого состояния данных или системы, т. е. наиболее старый допустимый «возраст» восстановления; иначе говоря, максимально допустимые потери;
- **RTO – Recovery Time Objective** – допустимое полное время восстановления.
- **AIW Acceptable Interruption Window** – максимально допустимое время простоя, то есть, время после возникновения аварии, через которое сервис будет доступен в ограниченном или аварийном режиме, либо
- **MTO – Maximal Tolerable Outages** – максимально допустимое время работы в аварийном режиме, исходя из соотношения  $RTO = AIW + MTO$ .
- **Service Delivery Objective (SDO)** – это SLA аварийного режима, длительность которого =  $RTO = AIW + MTO$ .
- **Recovery criteria** – это часть BCP, описывающая, что считается аварией, что нет, когда нужно начинать восстанавливать данные/сервисы.

### Методы резервирования ИТ-инфраструктуры

- **Hot site** («горячая площадка») – резервная площадка (серверная комната, находящаяся не в одном здании с основной серверной) с дублированием ключевой, часто не всей, ИТ-инфраструктуры.
- **Warm site** («тёплая площадка») – более дешёвый метод, резервная площадка без ИТ-инфраструктуры, но с подготовленной инфраструктурой связи, электропитания и кондиционирования, а также, опционально, с кабельной системой и мебелью.
- **Дублирующий ВЦ/ЦОД** – наиболее дорогой метод ВСМ, полное дублирование сервисов основной ИТ-инфраструктуры, иногда с синхронизацией в реальном времени или репликацией состояния.



### Мероприятия ВСМ

- Основными методами, используемыми при ВСМ, являются организационные мероприятия по исключению зависимости от ключевых (уникальных) сотрудников, оборудования, программного обеспечения и сервисов, а также мероприятия по дублированию, всевозможные системы резервирования и кластеры, подготовка или аренда резервных площадок «теплого» или «горячего» типа, либо использование полнофункциональных дублирующих вычислительных центров или центров обработки данных.
- Стоимость системы ВСМ с высокими требованиями отказоустойчивости сравнима с капитальной частью основного ИТ-баланса.
- Согласование с клиентом параметров качества RPO, RTO и AIW/MTO выполняется итеративно, поскольку изменение одного из параметров может вызвать изменение требуемого метода ВСМ, а значит, весьма значительное изменение стоимости проекта внедрения ВСМ и периодических затрат на поддержание системы ВСМ.

# Управление и реагирование на инциденты ИБ

- **Registering.** Крайне важно вести учет инцидентов. Не имея статистики инцидентов, трудно обосновать вложения в ИБ, а в дальнейшем – правильно рассчитать риски и оптимизировать вложения.
- **Reporting.** В рамках данного процесса каждый сотрудник организации должен знать, куда ему обращаться в случае нарушения или подозрения. Если в организации внедрена диспетчерская служба ИТ (Service Desk), лучше всего использовать принцип «единой точки входа». Диспетчерская служба должна уметь отличить, выражаясь языком ITIL, инцидент ИТ от инцидента ИБ и, в случае необходимости, эскалировать событие на команду реагирования на инциденты (Incident Response Team, IRT).
- **Response.** IRT должна уметь: отсеять ложные срабатывания, подтвердить инцидент, оценить серьезность инцидента, принять меры сдерживания (ограничения области его охвата), защитить улики, классифицировать и зарегистрировать инцидент, оценить допустимые сроки ликвидации инцидента и принять решение о дальнейшей эскалации, ликвидировать и закрыть инцидент, проанализировать его.



# Управление и реагирование на инциденты ИБ

Состояния инцидента:

- **Alert** – эскалация инцидента.
- **Emergency** – начало инцидента.
- **Resolution** – окончание.

*Правильная обработка скомпрометированного устройства:*

- изоляция, локализация ущерба,
- побитная копия памяти,
- физическое выключение,
- перемещение в сейф,
- при решении руководства – передача следственным органам.

**ISO 27002**

### ISO 27002 (бывший ISO 17799, BS 7799)

#### Этапы становления британской методологии управления корпоративной ИБ.

**1999** – публикация стандарта BS 7799

**2000** – появление его международной редакции ISO 17799

**2005** – выпуск второй, расширенной версии ISO 17799, выпуск стандарта ISO 27001, соответствующего BS 7799-2.

**2007** – объединение всех стандартов системы управления ИБ в семейство под единой нумерацией ISO 27000.

**Семейство ISO 27000 является стандартом де-юре и де-факто в корпоративной ИБ. Причины мгновенного, по меркам стандартов, развития методологии:**

- системность, удобная структура, широкая область охвата,
- удачное сочетание простоты и подробности,
- согласованность и гармоничность со стандартами систем управления в других областях, таких, как управление качеством

# ISO 27002 (бывший ISO 17799, BS 7799), продолжение

### Полноценный подход

(согласно ISO 27000):

- Управление ИБ выполняется по ISO 27001 на основе цикла PDCA.
- Проводится количественный анализ рисков заданной области охвата.
- Высшим руководством принимается решение по приемлемому уровню **остаточного** риска.
- Принимается решение по обработке каждого риска: **уклонение, снижение, перенос, принятие.**
- Для каждого риска, который решено снижать, выбираются средства управления из ISO 27002.

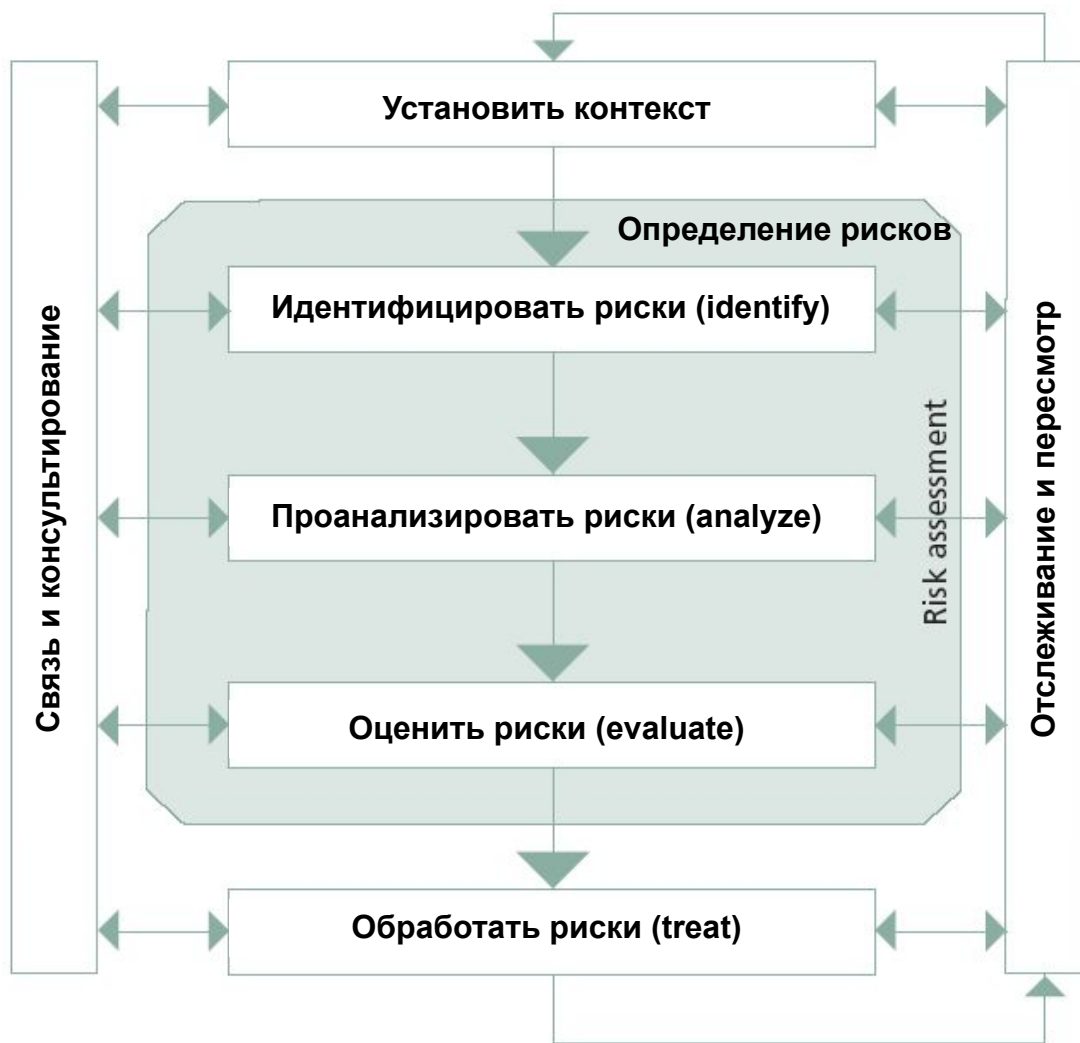
### Упрощенный подход

(на основе п. 0.6 ISO 27002):

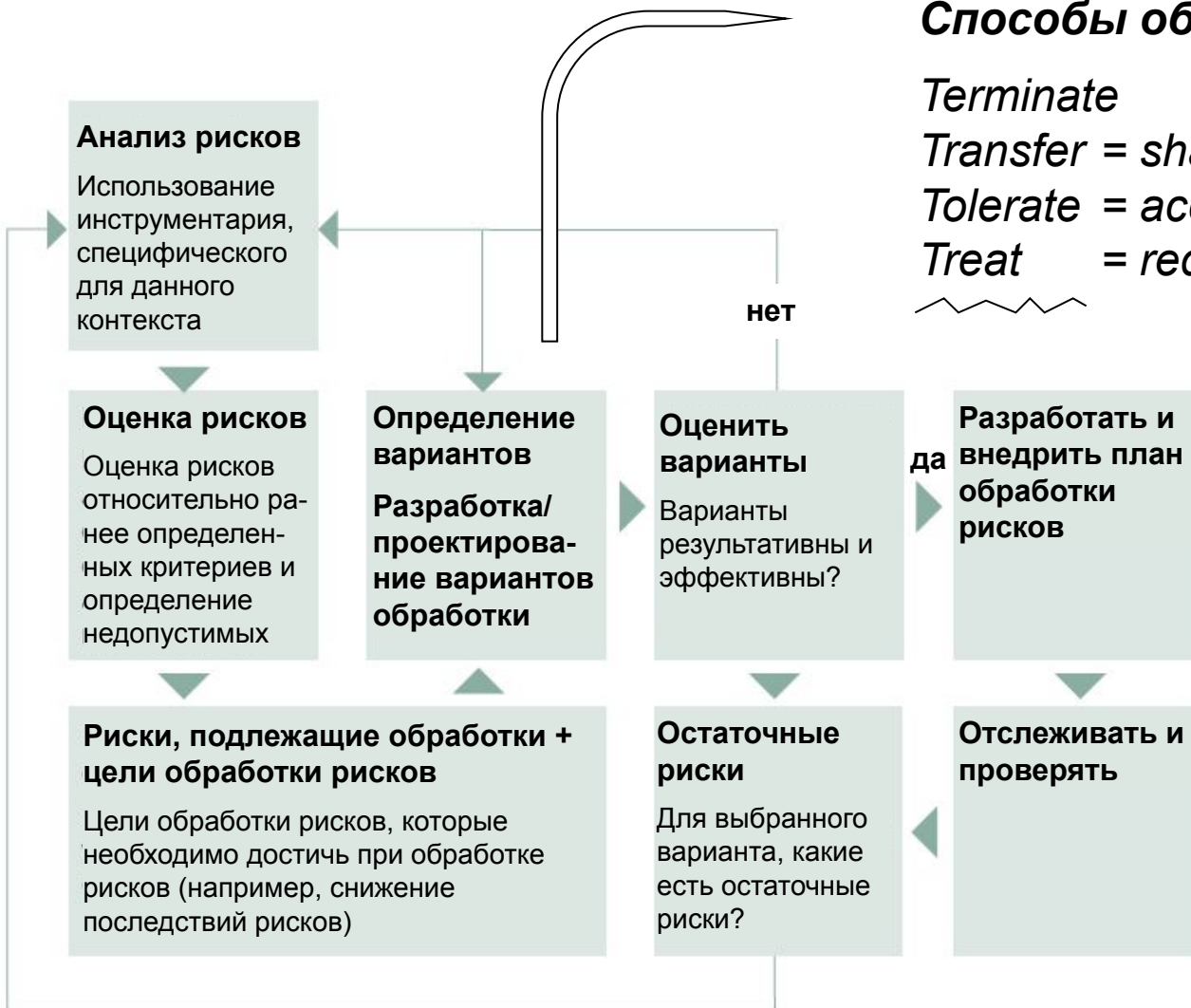
- Анализ рисков не выполняется, либо неполный / неколичественный / качественный.
- Высшее руководство вовлекается в процесс управления ИБ постепенно, начиная с наиболее необходимых обязанностей по санкционированию.
- ISO 27001 не применяется. Используется ISO 27002, как справочник средств управления, начиная с **базовой безопасности.**

**Упрощенный подход позволяет построить необходимое отношение к стандартам, привить культуру их использования.**

## Полноценный подход. Управления рисками (AS/NZS)



# Управление рисками, продолжение



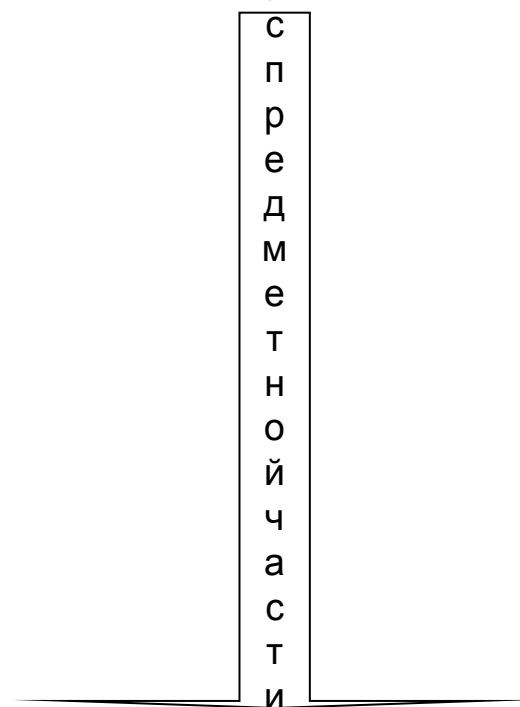
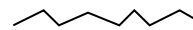
## Способы обработки рисков (4Т):

*Terminate* = *avoid* = уклонение

*Transfer* = *share* = перенос

*Tolerate* = *accept* = принятие

*Treat* = *reduce* = снижение



### Снижение рисков – основной фокус предмета ISO 27002

Стандарт состоит из общей (р. 1-4) и предметной (рр. 5-15) частей, в т. ч.: 34 главные категории (цели управления), 133 средства управления:

5. **Security Policy** (1) – политика безопасности;
6. **Organizing Information Security** (2) – организация ИБ;
7. **Asset Management** (2) – управление активами;
8. **Human Resources Security** (3) – управление персоналом;
9. **Physical and Environmental Security** (2) – физическая безопасность и безопасность окружения;
10. **Communications and Operations Management** (10) – управление коммуникациями и операциями;
11. **Access Control** (7) – управление доступом;
12. **Information Systems Acquisition, Development and Maintenance** (6) – приобретение, разработка и поддержка информационных систем;
13. **Information Security Incident Management** (2) – управление инцидентами ИБ;
14. **Business Continuity Management** (1) – управление непрерывностью бизнеса;
15. **Compliance** (3) – соответствие законодательству.

## Управление рисками ИБ (методология BSI).

Отчет по анализу рисков – основной документ при управлении рисками.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Код риска	Группа активов	Угроза	целостность	доступность	конфиденц.	BCMDRM	Уязвимости	Ценность группы активов	Доля актива в группе	Кол-во требований ИБ	Ценность актива	Степень уязв. (простога осущ. угрозы)	Вероятность (статист. + мировой опыт)	Риск-фактор
2	3	Документы / Информация	Сбой резервирования. Авария в системе резервного копирования, повреждение лент	+	+		+	Чувствительность носителей данных к повреждениям, износ / дефекты оборудования	4	2	2	9	4	4	144
3	18	Документы / Информация	Повреждение жестких дисков	+	+			Чувствительность носителей данных к повреждениям	4	3	2	9	4	4	144
4	82	Сервисы	Неуправляемые конфигурации. Снижение эффективности управления ИТ-процессами из-за отсутствия сведений о конфигурации		+			Неадекватное управление конфигурацией	4	4	1	9	4	4	144
5	28	Оборудование	Отказ ядра сети. Выход из строя или снижение производительности центрального коммутатора. Зависание коммутационной фабрики.		+		+	Устаревшее / изношенное, некачественное / дефектное оборудование	3	3	1	8	4	3	96
6	29	Оборудование	Авария электроснабжения. Долговременное отсутствие электропитания в сети		+		+	Нестабильное электропитание, неполадки и неадекватное управление дизель-генератором (техническое состояние, топливо)	3	4	1	9	3	3	81
7	68	Сервисы	Отказ 1С		+		+	Неадекватное управление (ошибки, недостатки) оборудованием, ОС, СУБД, устаревшее / дефектное оборудование	4	3	1	9	3	3	81
8	69	Сервисы	Отказ ERP		+		+	Неадекватное управление (ошибки, недостатки) оборудованием, ОС, кластером, СУБД, устаревшее / дефектное оборудование	4	3	1	9	3	3	81
	36	Оборудование	Неавторизованное оборудование. Снижение безопасности сети вследствие подключения неавторизованного / небезопасного оборудования			+		Отсутствие аутентификации оборудования, отсутствие карантина для небезопасного оборудования, наличие пользовательских (незащищенных) точек доступа	3	1	1	5	4	4	80



## Управление рисками ИБ (BSI, ISO 27000).

Средства управления (controls) = Положение о применимости согласно ISO 27001.

	A	B	C	D	E
1	Подраздел (главная категория) ISO 27002	№№№	Средство управления рисками	Комментарий	Документация
2	Политика ИБ	5.1.1	Документ политики информационной безопасности	Стратегическая позиция высшего руководства	Политика ИБ
3	Политика ИБ	5.1.2	Пересмотр политики информационной безопасности	Поддержка и обновление политики ИБ	Политика ИБ
4	Внутренняя организация	6.1.1	Выполнение обязательств руководства по отношению к информационной безопасности	Общие обязанности менеджмента среднего звена	Политика организации обеспечения ИБ
5	Внутренняя организация	6.1.2	Координация обеспечения информационной безопасности	Управление и централизация в области защиты информации	Положение об отделе информационной безопасности
6	Внутренняя организация	6.1.3	Распределение обязанностей по информационной безопасности	Ответственность за процессы и средства управления ИБ	Положения о ДИТ, об отделах ДИТ, Политика управления инф. активами, Положение о поддержке сервисов и серверов
7	Внутренняя организация	6.1.4	Процесс санкционирования новых средств обработки информации	Новое ПО и аппаратура подлежит анализу. Внедрение согласовывается.	Положение по управлению изменениями, Инструкция по использованию ПО, Процедура внедрения нестандартного ПО
8	Внутренняя организация	6.1.5.	Соглашения о соблюдении конфиденциальности	Юридическая и психологическая мера сдерживания персонала и партнеров	Обязательство соблюдения информационной безопасности физ. лица, юр. лица, ИТ-специалиста
9	Внутренняя организация	6.1.6	Связи с государственными органами	Обработка крупных инцидентов и инцидентов, выходящих за рамки ГКФ	Политика организации обеспечения информационной безопасности, Инструкция по управлению инцидентами ИБ
10	Внутренняя организация	6.1.7	Связи с тематическими группами	Отслеживание тенденций, угроз, появляющихся уязвимостей	Инструкция по поддержанию актуальности программного обеспечения
11	Внутренняя организация	6.1.8	Независимая проверка информационной безопасности	Внутренний и внешний аудит информационной безопасности	Положение об аудите информационной безопасности, Положение об управлении рисками ИБ
12	Внешние стороны	6.2.1	Определение рисков, связанных с внешними сторонами	Доступ партнеров и контрагентов к информации и системам ГКФ	Политика управления коммуникациями и операциями, Обязательство ИБ физ. лица, юр. лица, ИТ-специалиста
13	Внешние стороны	6.2.2	Принятие мер безопасности при отношениях с клиентами	Доступ клиентов к информации и системам ГКФ	Политика управления коммуникациями и операциями
14	Внешние стороны	6.2.3	Принятие мер безопасности в соглашениях с третьими сторонами	Доступ партнеров и контрагентов к информации и системам ГКФ	Политика управления коммуникациями и операциями, Обязательство ИБ физ. лица, юр. лица, ИТ-специалиста
15	Ответственность за активы	7.1.1	Опись активов	Инвентаризация информации, сервисов, аппаратуры, ПО	Политика управления информационными активами, Положение о поддержке сервисов и серверов, Инструкция по использованию ПО
	Ответственность за активы	7.1.2	Выполнение активизации	За каждый набор данных сервис сервер и ПК	Политика управления инф. активами, Положение о поддержке

# Упрощенный вариант. Базовая ИБ согласно ISO 27002

1. *Разработка и внедрение документов политик ИБ.*
  2. *Распределение обязанностей по ИБ.*
  3. *Повышение осведомленности, обучение и тренинги по ИБ.*
  4. *Правильная обработка в приложениях.*
  5. *Управление техническими уязвимостями.*
  6. *Управление непрерывностью бизнеса.*
  7. *Управление инцидентами ИБ.*
- +
1. *Защита личной информации.*
  2. *Защита записей организации.*
  3. *Защита прав интеллектуальной собственности.*

См. статью «Сохранение информационных активов» в журнале «Корпоративные системы» за 12/2008, либо на сайте [www.cism.com.ua](http://www.cism.com.ua), раздел «Аналитика».

### Классификация средств управления рисками (ISACA)

- **preventive**, предотвращающие (снижают уязвимости, делают невозможными атаки, снижают воздействие: управление доступом, шифрование, аутентификация),
- **corrective** (recovery), корректирующие (снижающие воздействие: резервирование и восстановление),
- **detective**, обнаруживающие (обнаруживающие атак или сканирования и включающие превентивные или корректирующие средства: журналы аудита, IDS, контрольные суммы).

Также выделяют средства управления:

- **compensatory**, компенсирующие (компенсация возрастающего риска, либо добавление доп. средств в дополнение к существующим слабым),
- **deterrent**, сдерживающие (снижают вероятность угроз или восприимчивость к ним, либо мотивирование пользователя путем предупреждений),

# Контрмеры и средства управления рисками информационной безопасности (ISACA)

- Отличие контрмеры (countermeasure) от средства управления (control) в том, что контрмера направлена на снижение конкретного риска или небольшого количества рисков, а одно средство управления снижает одновременно большое количество рисков.
- Свойство контрмеры – целевая направленность на угрозу или уязвимость (прекращение рискованной деятельности, разделение сетей, диверсификация поставщиков), а не на компонент системы.
- Контрмерами и средствами управления являются технические и организационные мероприятия.
- Выбор между контрмерами и средствами управления, а также выбор между средствами управления нужно делать на основании экономических оценок, например, **ROI**, Return On Investment – коэффициент возврата инвестиций, один из наиболее важных показателей экономической эффективности проектов, равный разности дохода и инвестиций, деленной на инвестиции.

### Структура процесса управления ИБ (ISACA)

- 1. Стратегическое управление ИБ.** Цель: внедрение и поддержка структурной основы для гарантирования соответствия стратегии ИБ целям бизнеса, законодательству и нормативным требованиям.
- 2. Управление информационными рисками.** Цель: определение рисков ИБ и управление ими для достижения бизнес-целей.
- 3. Разработка программы (портфеля проектов) ИБ.** Цель: создание и поддержка программы внедрения стратегии ИБ.
- 4. Управление программой (портфелем проектов) ИБ.** Цель: надзор за мероприятиями по информационной безопасности с целью выполнения программы ИБ.
- 5. Управление инцидентами и реагирование на инциденты.** Цель: планирование, разработка и управление мощностями по выявлению и реагированию на инциденты ИБ, а также по восстановлению после них.

**COBIT**

### Риски ИТ как часть множества бизнес-рисков

Структура операционных рисков согласно соглашению Basel II («Международная конвергенция измерения капитала и стандартов капитала: новые подходы» Базельского комитета по банковскому надзору) с примерами:

- **Внутреннее мошенничество** – завладение активами, уклонение от уплаты налогов, умышленное неправомерное назначение должностей, взяточничество.
- **Внешнее мошенничество** – кража информации, ущерб от хакерства, кража и подделка третьими сторонами.
- **Практики трудоустройства и безопасность рабочего места** – дискриминация, зарплата работников, здоровье и безопасность работников.
- **Клиенты, продукты и практика бизнеса** – манипулирование рынком, антимонопольные риски, незаконная торговля, дефекты продукции, нарушения доверительных сторон, «накрутка» счетов.
- **Ущерб физическим активам** – естественные катастрофы, терроризм, вандализм.
- **Прерывания бизнеса и системные сбои** – прерывания коммунального обслуживания, сбои программного и аппаратного обеспечения.
- **Исполнительные, снабженческий и процессный менеджмент** – ошибки ввода данных, бухгалтерские ошибки, невыполнение обязательной отчетности, халатная утрата клиентских активов.

### Источники IT Governance

#### **Прародители стандартов IT Governance:**

- Strategic Planning for MIS (McLean and Soden 1977),
- Business Systems Planning (IBM 1981),
- SISP (Lederer and Sethi 1988).
- Strategic Alignment Model of the MIT90s Research Program (Henderson et al 1992),
- Strategic Grid (Cash et al 1998)

**Разработчики закрытых стандартов.** Вендоры: Microsoft, WallMart, Siemens, UTC; консалтинговые компании: Gartner, KPMG, PWC, Forrester Research.

**Разработчики открытых стандартов.** US General Accounting Office, IT Governance Institute, UK Office of Government Commerce, The Institute of Internal Auditors, ISACA, IT Governance Institute.



### Концепция IT Governance как модель миграции управления ИТ от технического персонала в менеджмент

**IT Governance** – это ответственность исполнительных директоров и совета директоров, состоящая из лидерства, организационных структур и процессов, гарантирующих, что информационные технологии предприятия поддерживают и расширяют его стратегию и цели. (определение из CobiT)

Концепция IT Governance была предложена фондом ISACF, ассоциацией ISACA и созданным ей институтом ITGI. Это формально признанная сфера управления, которая рассматривается как неотъемлемая часть корпоративного управления, регулирующая отношения между ИТ-менеджерами и руководством организации и распределяющая ответственность между директором информационной службы (CIO) и советом директоров с топ-менеджментом.

Corporate governance – концепция, появившаяся в 90-х. Законодатель – Организация Экономического Сотрудничества и Развития (OECD). В 1999 OECD разработала «Принципы корпоративного управления». Они были поддержаны Министрами финансов Большой семерки и включены в Руководящие принципы OECD для многонациональных предприятий (MNE) в раздел, посвященный раскрытию информации и прозрачности.

### Стандарт COBIT – основа IT Governance.

Собит предлагает структуру внутренней системы управления ИТ путем:

- создания связей с требованиями бизнеса,
- организации работы в области ИТ в виде общепринятой процессной модели,
- определения основных ресурсов ИТ, подлежащих усилению,
- определения целей управления, которые необходимо рассматривать.

#### Рассматриваемые области:



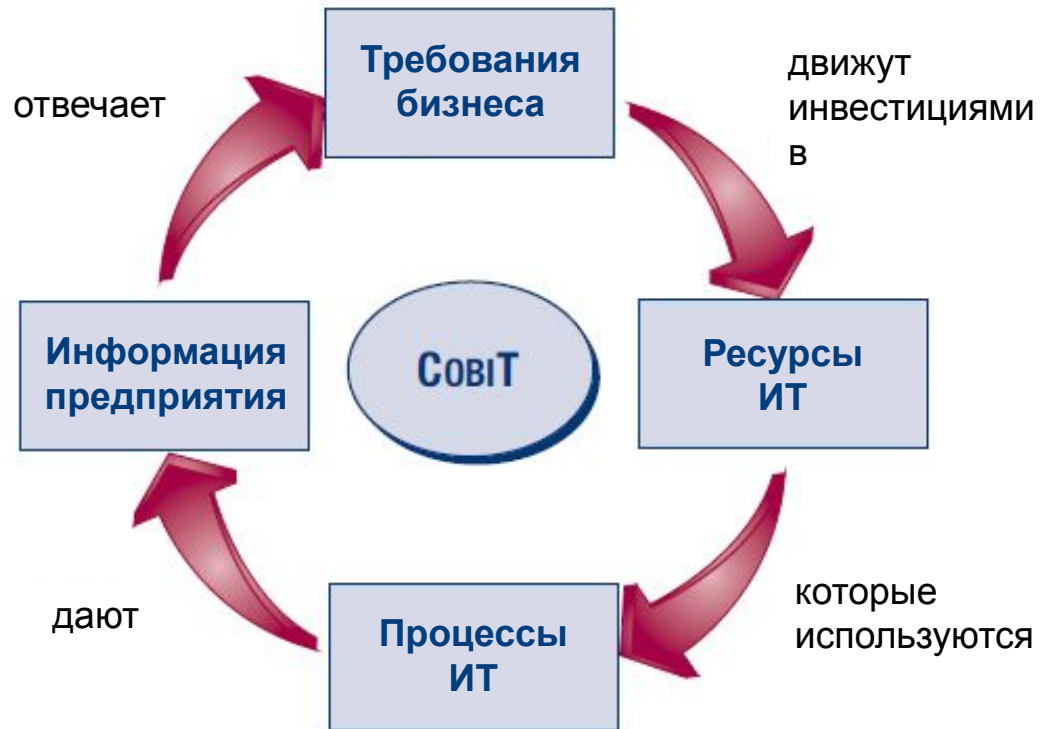
- **Стратегическое соответствие** бизнес-целям;
- **Предоставление ценности** предприятию со стороны ИТ, извлечение ожидаемых выгод;
- **Управление ресурсами** – приложениями, информацией, инфраструктурой, людьми;
- **Управление рисками** на основе анализа рисков и уровня приемлемого риска;
- **Измерение производительности** – отслеживание проектов, процессов, ресурсов.

# Миссия и базовый принцип СОВІТ.

**Миссия.** Исследовать, разрабатывать, публиковать и продвигать авторитетную, актуальную, всемирно признанную структурную основу для принятия её предприятиями и повседневного использования руководителями бизнеса, профессионалами в области ИТ и корпоративного обеспечения.

### Базовый принцип.

Для получения информации, которая необходима предприятию для достижения его целей, предприятию необходимо инвестировать в ресурсы ИТ, а также управлять данными ресурсами с помощью структурированного набора процессов, что необходимо для предоставления услуг, дающих необходимую предприятию информацию.



## Стандарт COBIT. Метрики

---

Как ответственные руководители удерживают «судно на курсе»?

ПАНЕЛИ  
ИНДИКАТОРОВ



Индикаторы?

---

Как предприятие может достичь результатов, удовлетворяющих наиболее крупному из возможных сегменту заинтересованных лиц?

СИСТЕМЫ  
ПОКАЗАТЕЛЕЙ



Мерки?

---

Как оперативно можно адаптировать предприятие к тенденциям и изменениям в его окружении

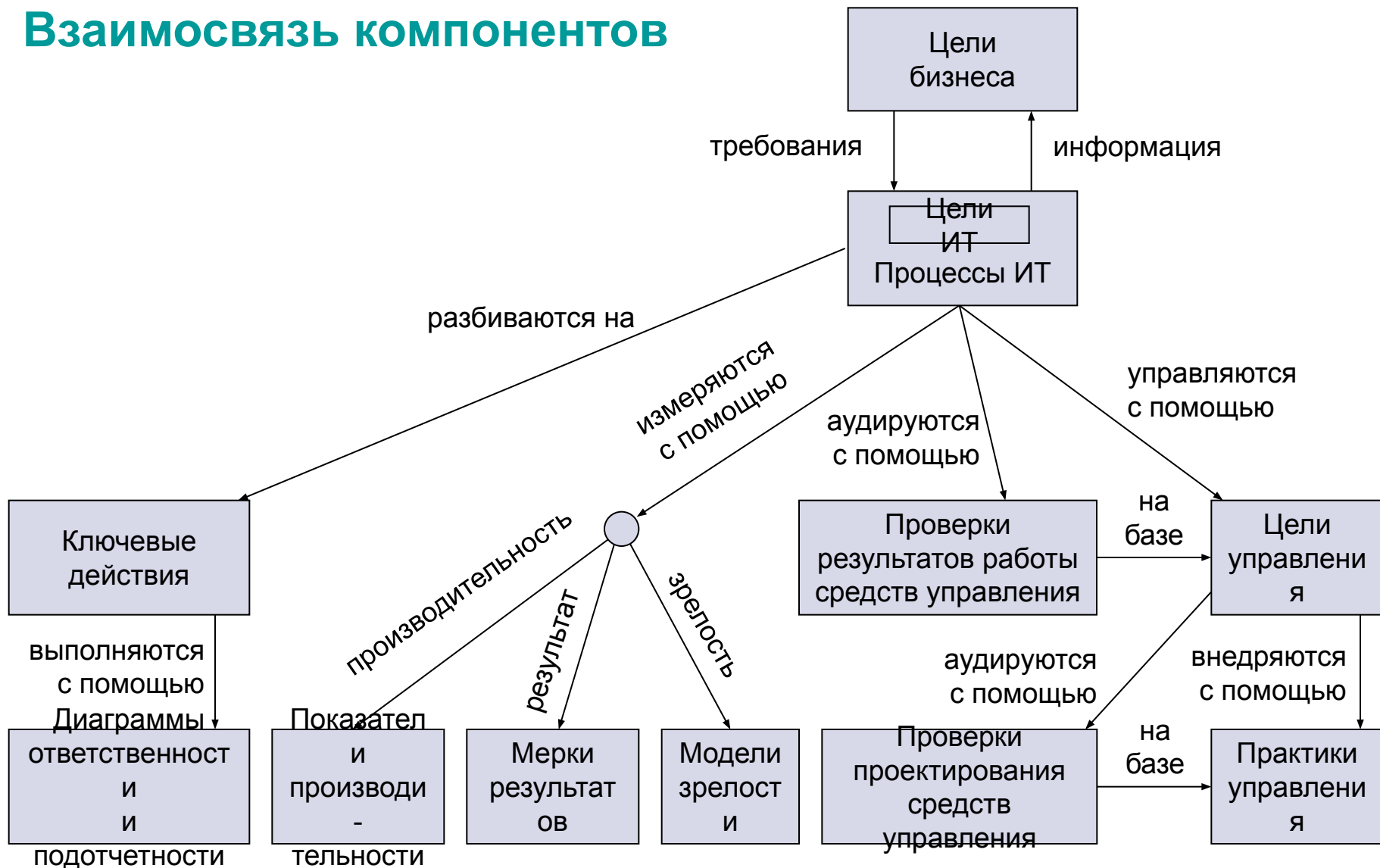
СРАВНЕНИЕ  
ЭФФЕКТИВНОСТИ



Шкалы?

- **Сравнение эффективности** с эталоном (benchmarking) выполняется на основе моделей зрелости CMM, разработанной Software Engineering Institute.
- **Цели и метрики** процессов ИТ определяются по принципам Balanced Scorecards (система сбалансированных показателей).
- **Цели деятельности** определяются на основе целей управления.

## Стандарт COBIT. Взаимосвязь компонентов



## Особенность COBIT – хорошо структурированные связи

«Основной принцип структурной основы» COBIT («куб COBIT»):

- ресурсы ИТ управляются
- процессами ИТ для достижения целей,
- удовлетворяющих **требованиям бизнеса**

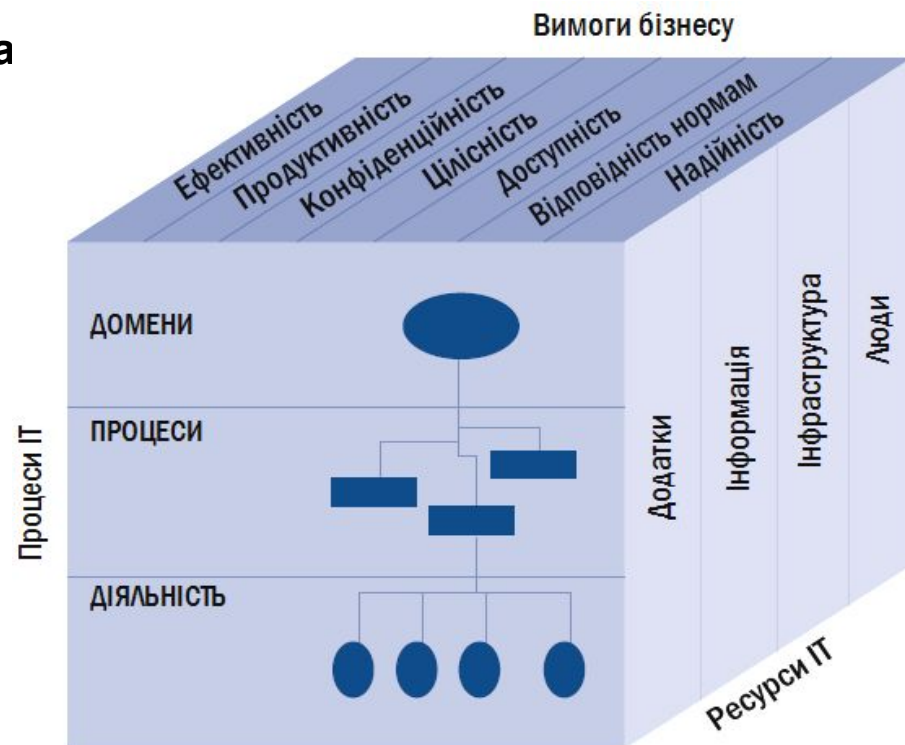
**Домены** ≡ стадии жизненного цикла.

**Процессы** – повторяемые технологические действия по преобразованию входа в выход.

**Деятельность** = операции.

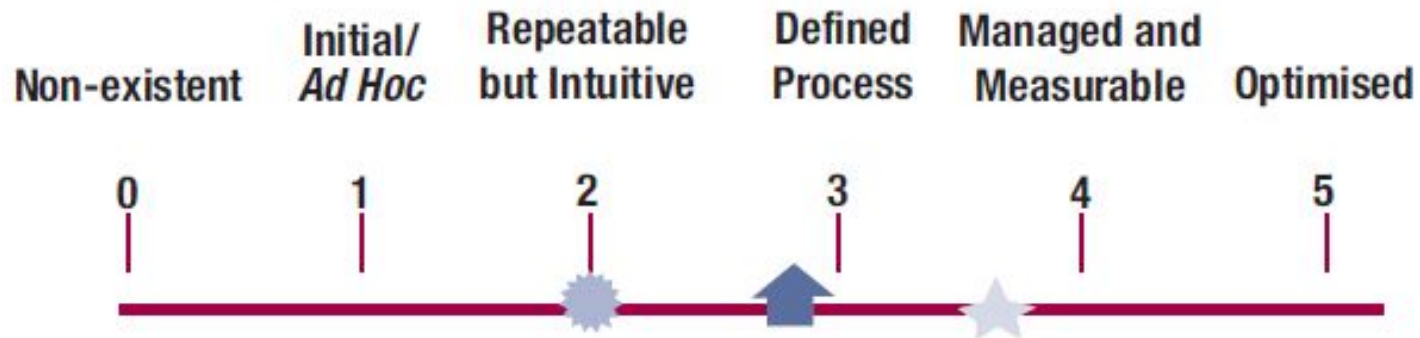
**Требования бизнеса** – стандартные требования информационной безопасности, плюс результативность, эффективность, соответствие нормам, надежность.

**Ресурсы** – приложения, информация, инфраструктура, люди.



### СОБИТ. Модели зрелости.

Модель зрелости процессов **разработки** программного обеспечения Capability Maturity Model (CMM), разработанная институтом SEI, была адаптирована ассоциацией ISACA для процессов **управления** информационными системами.



#### LEGEND FOR SYMBOLS USED

-  Enterprise current status
-  Industry average
-  Enterprise target

#### LEGEND FOR RANKINGS USED

- 0—Management processes are not applied at all.
- 1—Processes are *ad hoc* and disorganised.
- 2—Processes follow a regular pattern.
- 3—Processes are documented and communicated.
- 4—Processes are monitored and measured.
- 5—Good practices are followed and automated.

## Сравнение модели зрелости CMM и Gartner

Уровень зрелости	CMM (CobiT, ITIL)
0	Не существующий
1	Начальный
2	Повторяющийся
3	Документированный
4	Управляемый
5	Оптимизируемый

Год

2003

2005

2008

Уровень зрелости	Gartner (ИБ)
0	нулевой ( <i>штатные средства</i> )
1	<i>тех. проблема (простые средства)</i>
2	<i>орг. проблема (политика, аудит)</i>
3	<i>корп. культура (CISO, CSIRT, SLA)</i>

Год

2005

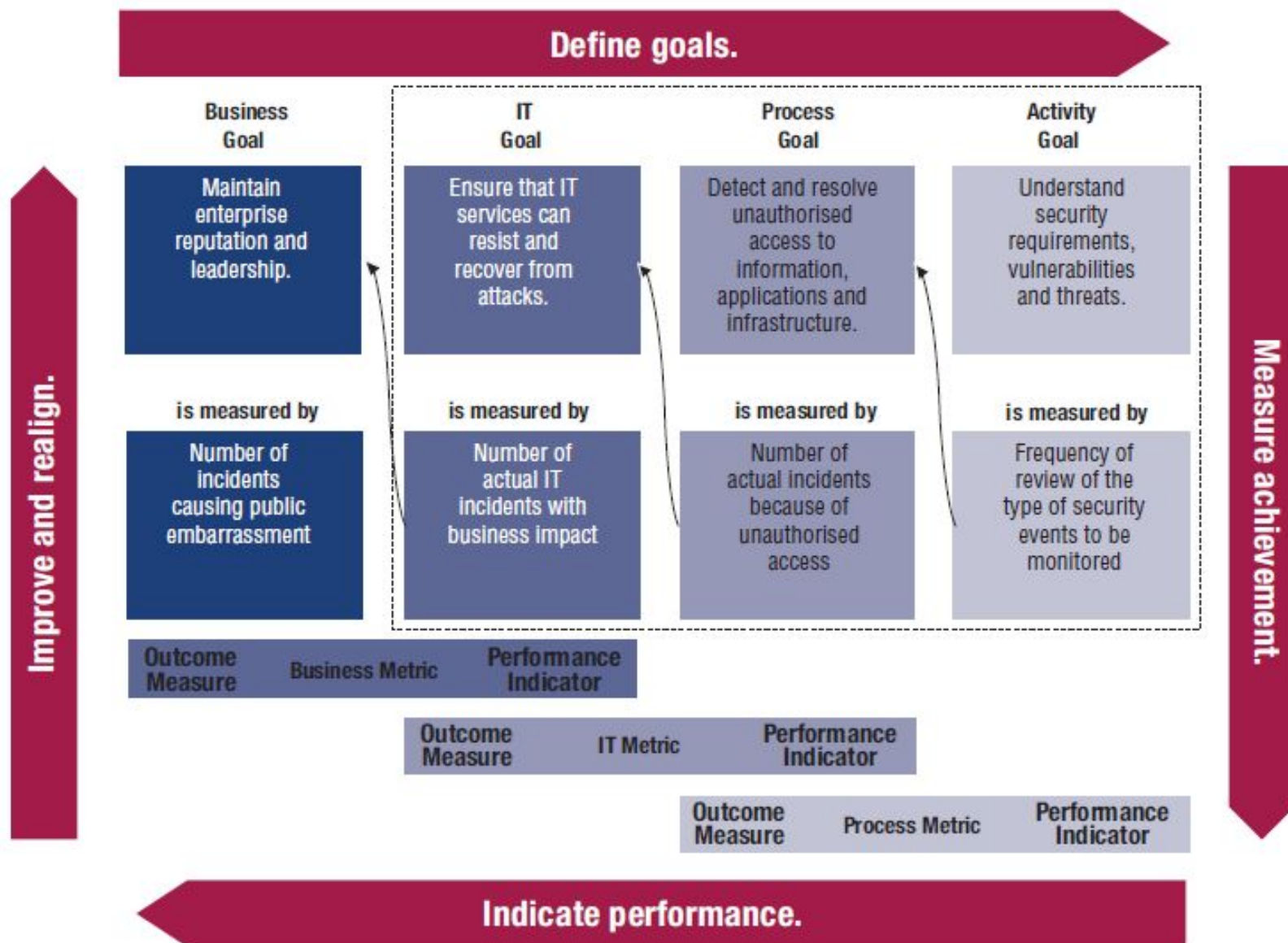
2006

2008





## СОBIT. Отношения между процессами, целями и метриками.



## Общая структура COBIT

### Процессы:

- PO1 Define a strategic IT plan.
- PO2 Define the information architecture.
- PO3 Determine the business requirements.
- PO4 Define the information systems.
- PO5 Manage the information systems.
- PO6 Comply with external requirements.
- PO7 Manage the information systems.
- PO8 Manage the information systems.
- PO9 Assess the information systems.
- PO10 Manage the information systems.

- DS1 Определить уровни обслуживания и управлять ими.
- DS2 Управлять обслуживанием третьими сторонами.
- DS3 Управлять производительностью и мощностями.
- DS4 Обеспечивать непрерывность обслуживания.
- DS5 Обеспечивать безопасность систем.

- AI1 Определить автоматизированные решения.
- AI2 Приобрести и поддерживать прикладное ПО.
- AI3 Приобрести и поддерживать технологическую инфраструктуру.
- AI4 Сделать возможными операции и использование.
- AI5 Снабжать ресурсами ИТ.
- AI6 Управлять изменениями.
- AI7 Внедрять и санкционировать решения и изменения.

DS13 Управлять операциями.

PO9 Определять риски ИТ и управлять ими.

PO10 Управлять проектами.

- DS1 Define the information systems.
- DS2 Manage the information systems.
- DS3 Manage the information systems.
- DS4 Educate and train users.
- DS5 Educate and train users.
- DS6 Identify and manage risks.
- DS7 Educate and train users.
- DS8 Manage service desk and incidents.
- DS9 Manage the configuration.
- DS10 Manage problems.
- DS11 Manage data.
- DS12 Manage the physical environment.
- DS13 Manage operations.

- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal control.
- ME3 Ensure compliance with external requirements.
- ME4 Provide IT governance.

- DS7 Educate and train users.
- DS8 Manage service desk and incidents.
- DS9 Manage the configuration.
- DS10 Manage problems.
- DS11 Manage data.
- DS12 Manage the physical environment.
- DS13 Manage operations.

- AI5 Procure IT resources.
- AI6 Manage changes.
- AI7 Install and accredit solutions and changes.

# Общая структура КобиТ



### Ассоциация ISACA

**ISACA** – авторитетный источник знаний и лучших практик, автор стандартов **COBIT** и **ValIT**, концепции **IT Governance**, методик аудита и управления ИТ, обучающих, исследовательских и аналитических материалов. Издаётся журнал, проводятся конференции, в том числе в режиме онлайн. В **70** странах **175** официальных филиалов. В **160** странах **75** тыс. членов организации. В Украине формируется филиал.

Ранее ISACA расшифровывалось как **Information Systems Audit and Control Association**. Затем сфера компетенции была расширена. Поэтому сейчас акроним ISACA не раскрывается.

**Обучение** – приоритет ISACA International и Kyiv chapter-in-formation. Проводится сертификация специалистов в области аудита (**CISA**), информационной безопасности (**CISM**) и управления ИТ (**CGEIT**). На базе Kyiv chapter-in-formation и компании Ernst&Young плодотворно функционирует сертификационный центр CISA/CISM.



### Общие проблемы рынка специалистов по ИБ

*Невозможно управлять тем, что нельзя измерить.*

- Знания и видение проблем ИБ специфичны. Те и другие трудно показать, стандартизовать и классифицировать по стоимости. Рынок не развит.
- Работа в области ИБ трудно поддается дискретному учёту. Эту работу не видно, достойно оценить её обычно может только специалист. Клиент не видит, за что именно он платит, наполняя фонд зарплаты службы ИБ.
- Стратегия карьерного роста специалиста по информационной безопасности неясна не только его работодателю, но и самому специалисту.

**Необходима единая, общепринятая шкала, мерило, через призму которого преломлялись бы все оценки для принятия правильных решений. Такой шкалой является сертификация специалистов.**



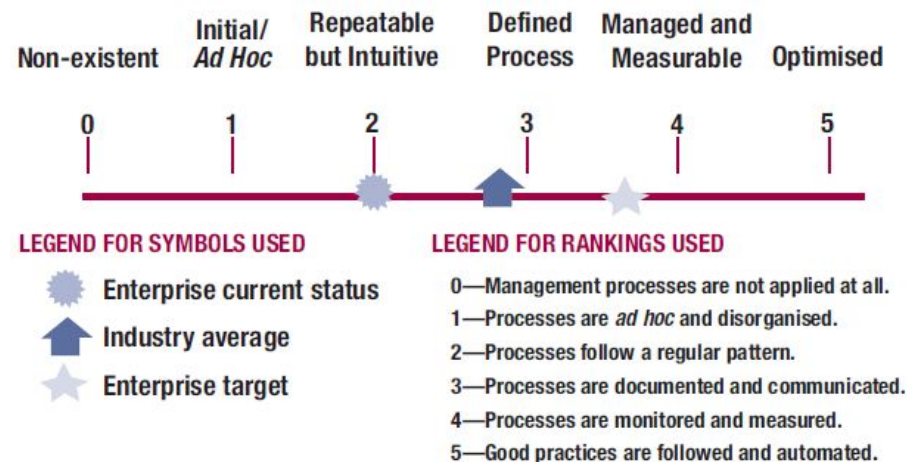
# **Модель управления инфраструктурой**

## Зрелость методологий управления корпоративными ИТ/ИБ

Модель зрелости процессов разработки СММ адаптирована для процессов управления информационными системами.

По аналогии, можно оценить зрелость самих современных методологий в целом. Сейчас это примерно уровень 2-3,5:

*повторяемые, интуитивные, определенные методы, управляемые, измеряемые и оптимизированные не в полной мере.*



**Направление современного менеджмента ИТ и ИБ как научной дисциплины - повышение методологической зрелости.**

# Формализация проблем управления ИТ и ИБ

- 1. Недостаточное соответствие целей ИТ и целей ИБ целям бизнеса.** Пример. Службы ИТ и ИБ имеют собственное представление об относительной важности процессов и активов. Другой пример – стратегическое планирование бизнеса (географии, направлений деятельности, структуры связей и т. п.) несвоевременно корректирует стратегические планы ИТ и ИБ. При построении базовой защиты это допустимо. Проблемы возникают при возникновении задачи распределения ресурсов пропорционально ценности активов и важности процессов.
- 2. Отсутствие стратегии построения безопасности.** Концентрация на статичном описании требуемого состояния ИБ (унаследованный недостаток методологий ITIL, ISO, PCI DSS), недостаточное внимание на методологии и технологии достижения требуемого состояния приводит к снижению эффективности ИБ и неполному удовлетворению требований ИБ. Нет стратегии обработки рисков.



### Формализация проблем управления, продолжение

- 3. Проблемы определения и анализа рисков.** Трудно выявить все риски в большой информационной системе со множеством сервисов. Трудно ранжировать риски по важности из-за смешивания природы и уровней абстракции разных рисков. Данные процессы субъективны, выполняются в головах сотрудников ИБ и исчезают при ротации персонала.
- 4. Несвоевременное реагирование на изменения рисков.** Внесение изменений в проекты с целью оптимизации приоритетов, ресурсов и сроков их выполнения. Инструментарий для предоставления бизнесу возможности принимать решения по отмене неактуальных проектов, увеличению/уменьшению инвестиций, сдвигу сроков и т. д.

### Формализация проблем управления, продолжение

- 5. Неправильное распределение внимания персонала службы ИБ.** Распределение внимания должно быть пропорционально важности операционных и стратегических задач. Проблемы классификации и приоритизации большого количества задач различных типов, областей охвата, масштабов. Данная функциональность выполняется вручную руководителем службы ИБ.
- 6. Недостаток оперативной информации.** Неудобная форма предоставления информации, необходимой для оперативного принятия правильных решений по мелким изменениям в инфраструктуре, процессах и операциях, например, определение и применение корректирующих воздействий при снижении риска в ходе нестандартного запроса пользователя.

### Формализация проблем управления, продолжение

7. **Недостатки «опытных» методик и стандартов.** Методики и стандарты по ИБ и ИТ – ISO, ITIL, COBIT, Risk IT, разнообразны и гармонизированы между собой, но не предоставляют:
- последовательности их применения и внедрения,
  - способов определения относительной важности тех или иных мероприятий в рамках внедрения,
  - методов повышения оперативности принятия решений в области информационной безопасности и непрерывности бизнеса.

### Подход к моделированию управления ИТ и ИБ

Предлагаемая модель работает на нескольких уровнях. Уровни и цели на каждом:

1. *бизнес-стратегия* (цели организации),
2. *ИТ- и ИБ-стратегия* (политики ИТ и ИБ),
3. *проектный* (цели проектов),
4. *архитектурный* (требования ИБ к инфраструктуре),
5. *процессный* (требования ИБ к бизнес-, ИТ и ИБ-процессам),
6. *операционный* (требования ИБ к операциям).

На каждом уровне взаимосвязанная с другими уровнями схема процесса.

## Предлагаемая модель управления ИТ и ИБ

№	Уровень	Входы	Выходы (цели)
1.	бизнес-стратегия	(в модели не рассматривается)	критичность всех групп ресурсов, в том числе нематериальных (включая репутацию), подразделений, планы развития и изменений, параметры BCM/DRP SLA, конфиденциальность
2.	ИТ- и ИБ-стратегия	бизнес-цели, проекты, архитектура, текущий анализ рисков	политика ИБ, требования ИБ (Ц, Д, К) на основе требований бизнеса (BCM, грифы), изменения в политике и анализе рисков, либо констатация их неадекватности (проблемы знания политики)
3.	проектный	бизнес-цели, политика и требования ИБ	планы проектов ИБ, цели проектов ИБ (должны ставиться в нескольких вариантах: программа-минимум, оптимум, максимум для учета возможных изменений стратегии в ходе выполнения проекта)
4.	архитектурный (инфраструктурный)	текущее состояние архитектуры и процессов, цели проектов, политика и требования ИБ	требуемые и несанкционированные изменения архитектуры, управление инфраструктурой в ручном и автоматическом режиме
5.	процессный	текущее состояние процессов и архитектуры, цели проектов, политика и требования ИБ, <i>анализ трафика КЕ</i>	требуемые и несанкционированные изменения процессов, отклонения от нормального функционирования КЕ, <i>нахождение слабых (незрелых) мест с помощью статистич. анализа</i>
6.	операционный	текущее состояние операций и архитектуры, политика и требования ИБ, статистика инцидентов, <i>анализ трафика КЕ</i>	требуемые и несанкционированные изменения в анализ рисков, влияние инцидента на цели бизнеса (формирование входной информации для дополнения и корректировки целей бизнеса)

# Предлагаемая модель управления ИТ и ИБ

- 1. Общие входы:** зрелость организации, запросы на изменения и т. д.
- 2. Общие выходы:** отслеживание несанкционированных изменений, отслеживание и повышение уровня зрелости, динамика изменения зрелости процессов и т. д.

**Цель модели** – гармоничность развития (одинаковость уровня зрелости различных процессов). Это даёт оптимизацию затрат.

Стандарты должны быть согласованы с корпоративными аудиторами. Это один из шагов по внедрению. Вообще, ценность методики в том, что она даёт пошаговый способ внедрения системы управления, в отличие от стандартов.

### Extended CMS (расширенная БД конфигураций)

CMDB (CMS) – важнейший элемент корпоративной системы управления ИТ согласно ITIL. Представляет собой базу данных / систему баз данных конфигурационных единиц (КЕ) – всех пользователей, оборудования, программного обеспечения и сервисов информационной системы. Есть много успешных реализаций данной идеи в виде программных решений.

**Предлагается использование расширенной системы управления конфигурациями (условно, ECMS). Характерные особенности:**

- 1. ECMS – это CMS, содержащая, кроме традиционных КЕ, также информацию о группах информационных активов, орг. структуре предприятия и о пользователях. Изменения КЕ (как минимум, серверов) должны предлагать изменения групп активов и наоборот. Изменения в орг. структуре должны предвидеть и предлагать изменения мощностей сервисов. Таким образом, ECMS будет статической моделью информационной системы, в которой будут отражаться не только состояние инфраструктуры, но и состояние и процессы информационных активов и субъектов доступа к ним.**

### Характеристики ЕСМС. Продолжение

- 2. Каждая КЕ содержит информацию о её стоимости (критичности).**  
Для информации – это ущерб от утечки или простоя соответствующего бизнес-процесса, как вариант – доля критичности в бизнесе в целом, оцениваемом, например, оборотом или прибылью. Стоимость участвует в расчете величины ущерба нарушений и рисков. И наоборот, стоимость сама корректируется, если введен конкретный ущерб от конкретного нарушения. Удобный принцип – стоимость задаётся на высшем уровне иерархии КЕ и распределяется вначале пропорционально между всеми составляющими, затем при необходимости корректируется с помощью GUI.
- 3. Самообучение ЕСМС.** Связи КЕ влияют на процесс анализа рисков. Обучение должно происходить при изменениях в КЕ и наступлении нарушения. Построение связей КЕ ЕСМС – сложная проблема.



### Предлагаемый подход к анализу рисков

- 1. Традиционный подход к управлению рисками BSI:** аудит и анализ рисков (2 недели), определение уровня приемлемого (остаточного) риска, определение стоимости программы по снижению рисков, коррекция значения приемлемого риска, утверждение отчета по анализу рисков и программы (2 недели). Неизменность отчета и программы, по крайней мере, 6-12 мес. Недостатки – низкая оперативность реагирования на изменения (в т. ч. уточнения анализа рисков), потеря адекватности проектов снижения рисков, затраты средств и времени на ненужные результаты.
- 2. Предлагаемый подход к управлению рисками.** Утверждение методики анализа рисков и диапазона уровней (допустимых скоростей изменения) приемлемого риска для каждой группы ресурсов. Непрерывный анализ рисков и коррекция отчета и программы. Изменение методики и уровня приемлемого риска при необходимости чаще, чем раз в 6-12 мес., с ограничением на скорости такого изменения (производные величин рисков).

### Угрозы, уязвимости, риски. Зрелость.

- 1. Недостатки рисков в методологии BSI** – в кучу смешаны риски различных уровней абстракции. Модель неформальная. Классификация рисков должна быть строгой, это необходимое условие формальной модели. В идеале, подлежащий формализации риск представляет собой обобщенное нарушение ИБ – совокупность КЕ, связанного с нарушением, уязвимости (кстати, они тоже обычно смешиваются в кучу), величины ущерба и частоты нарушения (?).
- 2. Понятие угрозы в риске не должно участвовать**, так как при правильно построенной системе исключается возможность для какой-либо реализации угроз. Исключением упоминания чего-либо мы подрываем его право на существование.
- 3. Уязвимость (незрелость)** – это отсутствие/неполнота того или иного средства управления. В ответ на изменение риска модель должна предлагать внедрение соответствующих средств управления. Должны предлагаться варианты таких средств, соотв. параметры проектов и прогнозируемое снижение риска по каждому варианту. CISO или CEO выбирает подходящий вариант снижения рисков.

### Угрозы, уязвимости, риски. Зрелость.

4. Снижение одного риска может вызывать увеличение другого. Риски нужно обрабатывать в комплексе, обращая внимание на такие моменты обратных эффектов.
5. Соответствие средства управления – КЕ. Большинство СУ связаны с процессами, обязанностями. То есть, с людьми. Основная мысль – при внедрении СУ снижается уязвимость процессов и людей. Следовательно, снижается соотв. риск.
6. Зрелость процессов рассчитывается по критериям COBIT.
7. Отчетность для топ-менеджмента должны показывать эффективность работы службы ИБ – график зависимости от времени отношений ущерб ИБ / доход и риск / доход (ущерб и риск / прибыль, ущерб и риск / полная стоимость предприятия), график зрелости ИБ.

### Требования ИБ и требования бизнеса должны не просто соответствовать, а быть гармоничными

**Разные требования ИБ несут разную относительную важность с точки зрения бизнеса.** Некоторые являются первичными, другие – вторичными. В классической тройце "целостность, доступность, конфиденциальность" требование целостности информации с точки зрения бизнеса является неоднозначным и не первичным. Вместо понятия целостности следует использовать требования аутентичности и доступности.

**Ключевым требованием ИБ является доверие к информации и системе.** Доверие к конфиденциальности информации – это уверенность в том, что она недоступна посторонним. Доверие к аутентичности информации – уверенность в подлинности. Доверие к доступности системы – уверенность в возможности получить нужный сервис. Оценка компонентов доверия пользователей может дать ценную обратную связь, которая может быть использована в оценке текущего состояния ИБ.