Содержание

Введение

Развитие° информационных систем приносит компании очевидную пользу. Однако при некорректном использовании они становятся источником специфических рисков, реализация которых может не только свести к минимуму эффект от внедрения технологий, но и повлечь значительные убытки. Информационный аудит позволяет управлять этими рисками: выявить их, оценить эффективность информационной системы и выбрать направления для ее совершенствования.

Международные стандарты управления и аудита в области информационных технологий рекомендуют оценивать информационную систему с точки зрения совокупности иерархии IT-процессов, детализированных целей контроля и типовых процедур деятельности для того, чтобы определить соответствие системы задаче по минимизации рисков. С указанной целью детальному аудиту подвергается управление IT-процессами, отвечающими за минимизацию более чем 30 высокоуровневых ИТ-рисков.

CobiT (Control Objectives for Information and related Technology) – международный стандарт управления корпоративными информационными технологиями, который помогает согласовать стратегию бизнеса и ИТ, выстроить диалог между руководителями бизнес-подразделений и менеджментом информационной службы. Библиотека передового опыта ITIL (IT Infrastructure Library) – стандарт по управлению информационными технологиями, активно применяется во многих странах на протяжении последних 15 лет.

Цель - произвести расчет уровня зрелости и построения тренда зрелости ИТ-процесса.

Задачи:

1. Ознакомиться с методикой расчета уровня зрелости и построения тренда зрелости ИТ-процесса
2. На основе полученных знаний построить график влияния показателей уровня зрелости на тренд зрелости ИТ-процесса.
3. Составить отчет с выводами.

1. Ознакомиться с методикой расчета уровня зрелости и построения тренда зрелости ИТ-процесса

Ответом на вопрос "чем и как управлять" явилась разработка моделей зрелости, начатая в конце 80-х годов Институтом проектирования и разработки программного обеспечения, по заказу Министерства обороны США. Первоначальное предназначение — создание эффективного инструмента для классификации и оценки проектов, связанных с разработкой программного обеспечения и гарантированного соблюдения качества при выполнении этих проектов. В дальнейшем модели зрелости были доработаны для управления ИТ-сервисами и аудита процессов управления.

Maturity Models (MM) — "модели зрелости". Соответствие уровням "модели зрелости" означает, что компания готова к плановой модернизации или обновлению. MM — не технология, не стандарт, для нее нет формальных описаний, в ней нет жестких требований, и она не привязана к конкретным информационным технологиям.

Модели зрелости не подсказывают как улучшить работу компании и не объясняют, как работать с персоналом, также нет готовых руководств и по применению моделей зрелости. Рекомендуется каждой конкретной компании разработать подобное руководство для своего бизнеса или пригласить сторонних консультантов для решения этого вопроса. Модели зрелости предназначены для организации эффективного управления. Они определяют ключевые действия, которые указывают, что надо сделать для достижения требуемого качества и содержат способы контроля над правильностью выполнения ключевых ИТ-процессов и методы их корректировки.

Существуют модели зрелости, показывающие на каком этапе эволюции использования АИС, АИТ находится предприятие:

модели зрелости COBIT

модели зрелости по Р. Нолану.

Модели зрелости COBIT

0. Не существует. Полное отсутствие каких-либо процессов управления ИТ. Организация не признает существования проблем в ИТ, которые нужно решать, и, таким образом, нет никаких сведений о проблемах.

1. Начало (Анархия). Организация признает существование проблем управления ИТ и необходимость их решения. При этом не существует никаких стандартизованных решений. Существуют случайные одномоментные решения, принимаемые кем-то персонально или от случая к случаю. Подход руководства к решению ИТ-проблем хаотичен, признание существования проблем случайно и непоследовательно.

2. Повторение (Фольклор). Существует всеобщее осознание проблем управления ИТ. Показатели деятельности и ИТ-процессов находятся в развитии, охватывая процессы планирования, функционирования и мониторинга ИТ. Деятельность по управлению информационными технологиями описана и интегрирована в процесс управления организацией. Выбраны для улучшения и/или контроля те ИТ-процессы, которые влияют на основные бизнес-процессы предприятия. Эффективно выполняется планирование и управление инвестициями. Руководство организации регламентировало меры по управлению ИТ, а также методы управления и оценки, но процесс не был принят в организации. Не существует формализованного обучения, набора взаимосвязанных стандартных процедур управления, ответственность возложена на сотрудников. Сотрудники контролируют процессы управления с помощью проектов и ИТ-процессов. Ограниченные инструменты управления выбираются и внедряются для сбора метрик управления, но не используются в полном объеме из-за недостатков в оценке их функциональности.

3. Описание (Стандарты). Необходимость действовать в соответствии с принципами управления ИТ понимается и принимается. Развивается базовый набор показателей управления ИТ: определена связь между результатом и показателями производительности, она зафиксирована и внедрена в стратегические процессы планирования и мониторинга. Процедуры стандартизованы и документированы, проводится обучение сотрудников по выполнению этих процедур. Показатели производительности всех видов деятельности зафиксированы и отслеживаются, что приводит к повышению эффективности работы всей организации. Процедуры не сложны, они являются формализацией существующей практики. Идеи сбалансированных карт оценки бизнеса принимаются организацией. Ответственность за обучение, выполнение и применение стандартов возложена на сотрудников организации. Анализ первопричин применяется время-от-времени. Большинство процессов управляются в соответствии с некоторыми основными метриками, и, как правило, отдельными сотрудниками, поэтому ни о каких отклонениях руководители не знают. Однако всеобщая отчетность о выполнении ключевых процессов является четкой, и руководство премирует сотрудников на основе измерения ключевых результатов.

4. Управление (Измеряемый). Существует полное понимание проблем управления ИТ на всех уровнях организации, постоянно происходит обучение сотрудников. Определены и поддерживаются в актуальном состоянии соглашения об уровне обслуживания. Четко распределена ответственность, установлен уровень владения процессами. Процессы ИТ соответствуют бизнесу и стратегии ИТ. В первую очередь улучшения в процессах ИТ основываются на измеряемых количественных показателях. Существует возможность управлять

процедурами и метриками процессов, измерять их соответствие. Все совладельцы процесса осознают риски, важность ИТ и возможности, которые они предоставляют. Руководство организации определило допустимые отклонения, при которых процессы должны работать. Если процессы не работают эффективно и продуктивно, действия предпринимаются во многих (но не всех случаях). Процессы постоянно совершенствуются, их результаты соответствуют "лучшим практикам". Формализован порядок анализа первопричин. Присутствует понимание необходимости постоянного совершенствования. Ограниченно применяются передовые технологии, основанные на современной инфраструктуре и модифицированных стандартных инструментах. Все необходимые ИТ-специалисты вовлечены в бизнес-процессы. Управление ИТ превращается в процесс уровня всей организации. Деятельность управления ИТ интегрируется в процесс управления организацией.

5. Оптимизация (Оптимизируемый). В организации существует углубленное понимание управления ИТ, проблем и решений ИТ, а также перспектив. Обучение и коммуникация поддерживаются на должном уровне, самыми современными средствами. В результате непрерывного улучшения процессы соответствуют моделям зрелости, построенным на основании "лучшей практики". Внедрение этих процедур привело к появлению организаций, людей и процессов, максимально адаптируемых к изменяющимся условиям, а также полностью соответствующих требованиям управления ИТ. Первопричины всех проблем и отклонений тщательно анализируются, по результатам анализа выполняются результативные действия. Информационные технологии интегрированы в бизнес-процессы, полностью их автоматизируют, предоставляя возможность повышать качество и эффективность работы организации.

2. На основе полученных знаний построить график влияния показателей уровня зрелости на тренд зрелости ИТ-процесса.

Международные стандарты управления и аудита в области информационных технологий рекомендуют оценивать IT-систему с точки зрения совокупности иерархии IT-процессов, детализированных целей контроля и типовых процедур деятельности для того, чтобы определить соответствие системы задаче по минимизации рисков. С указанной целью детальной экспертизе подвергаются IT-процессы, отвечающие за минимизацию более чем 30 высокоуровневых IT-рисков.

Фрагмент перечня IT-рисков и процессов, в рамках которых осуществляется деятельность по их минимизации, представлен в табл. 1.

Таблица 1 - Фрагмент перечня IT-рисков и процессов, в рамках которых осуществляется деятельность по их минимизации

№ п/п	IT-процесс	
	IT-риск	Возможные признаки рисковой ситуации
Стратегическое планирование IT		
1	На стадии стратегического бизнес-планирования не рассматриваются вопросы IT-стратегии, что не позволяет в проактивном режиме оптимизировать работу IT-подразделения под фактические бизнес-требования	Стратегическое планирование IT-деятельности выполняется по мере необходимости в ответ на конкретное требование бизнеса, и поэтому результаты являются эпизодичными и непоследовательными. Вопросы стратегического планирования иногда обсуждаются на встречах только на уровне руководства департамента IT, а не руководителей бизнес-подразделений. Настройка приложений и технологий под потребности бизнеса является реакцией на внешнее воздействие, например на предложения поставщиков, а не осуществляется на базе стратегии, разработанной в компании. Оценка стратегического риска не формализована и осуществляется от проекта до проекта
Планирование IT-архитектуры		
2	Не оптимизирована структура информационных систем, что повышает избыточность данных (дублирование) в корпоративной системе, а также снижает уровень совместимости систем и приложений	Идет разрозненная разработка компонентов информационной структуры. Имеется частичная реализация схем данных, документации и правил синтаксиса данных. Определения относятся скорее в данным, чем к информации, и обусловлены предложениями поставщиков приложений. Разъяснение сотрудникам необходимости информационной архитектуры проводится хаотично и бессистемно
Управление персоналом		
3	Не оптимизирована политика в отношении найма и сохранения (мотивирования) квалифицированного персонала, что не позволяет обеспечивать максимальный вклад персонала в результат IT-деятельности	Используется неформальный подход к найму и управлению персоналом, обусловленный скорее потребностями конкретных проектов, чем направлением развития технологии и продуманным соотношением предложений

		квалифицированных сотрудников внутри организации и на стороне. Осуществляется неформальное обучение новых сотрудников
Управление проектами		
4	Не оптимизированы подходы к управлению проектами, что приводит к невыполнению обязательств по срокам и стоимости работ. Решение об использовании методики и подходов к управлению проектами в области IT оставлено на усмотрение отдельных менеджеров	Принципиальные решения по управлению проектами принимаются без управления пользователями и исходных данных клиента. Клиенты и пользователи не принимают участия в определении IT-проектов или их участие носит незначительный характер. IT-проекты плохо организованы: роли и обязанности участников, а также график выполнения проектов не определены, не отслеживаются трудозатраты
Приобретение IT-инфраструктуры		
5	Не оптимизирована и не стандартизирована деятельность по приобретению и обслуживанию инфраструктуры IT. При эксплуатации это приводит к снижению производительности систем и возникновению рисков безопасности в отношении данных и программ, хранящихся в системе	Для каждого нового приложения в инфраструктуру вносятся изменения без какого-либо общего плана. Обслуживание организовывается как реакция на краткосрочные потребности. Средой для тестирования является производственная среда. Приобретение и обслуживание IT-инфраструктуры не базируется на какой-либо определенной стратегии и не учитывает потребности бизнес-приложений, которые необходимо поддерживать. Графики обслуживания не разработаны в полном объеме, и деятельность не координируется.
Управление услугами поставщиков		
6	Не установлены четкие договорные отношения (соглашения) с поставщиками IT-услуг, включая определение ролей, ответственности и ожиданий, а также проведение проверок и мониторинга соответствующих соглашений с точки зрения эффективности и соответствия, что повышает угрозу возникновения ущерба для случаев невыполнения поставщиками своих обязательств	Отсутствует формальная политика и порядок заключения договоров со сторонними организациями. Не осуществляется оценка деятельности сторонних организаций. Сторонние организации не предоставляют отчетность. В отсутствие обязательство предоставлении отчетности высшее исполнительное руководство не владеет информацией о качестве предоставляемых услуг. Отсутствуют типовые условия договоров с поставщиками услуг. Оценка предоставляемых услуг осуществляется произвольно и фрагментарно. Методика зависит от индивидуального опыта отдельно взятого лица и от поставщика (например, по

		запросу)
Управление непрерывностью		
7	Отсутствует формализованный подход к созданию (поддержанию и тестированию) планов обеспечения непрерывности IT-деятельности (в том числе планов резервного хранения данных), что делает в случае наступления чрезвычайной ситуации высоковероятным возникновение значительных перерывов в предоставлении IT-услуг по ключевым направлениям и процессам бизнеса	Реакции на крупные нарушения заранее не продуманы и не подготовлены. Практикуются плановые отключения системы для обеспечения нужд IT-обслуживания без учета выполнения требований бизнеса. Подходы, применяемые к обеспечению непрерывности предоставления услуг, характеризуются неполнотой и фрагментарностью. Поступающая информация относительно доступности системы не учитывает состояние бизнеса. Нет документального обеспечения в отношении действий пользователя или в отношении обеспечения непрерывной работы

Данная деятельность рассматривается как по вопросам, специфичным для каждого отдельного процесса, так и по стандартным элементам процессного управления, а именно:

- распределение ответственности между всеми уровнями управления и обеспечение адекватного взаимодействия между ними;
- наличие и эффективность механизмов поддержания компетенции персонала на необходимом уровне;
- поддержание в полном и актуальном состоянии процессной документации на всех уровнях;
- наличие и полнота механизмов измерения производительности и формирования внутренней отчетности для каждого IT-процесса, позволяющая руководству IT-службы оценивать степень достижения целевых показателей и, как следствие, принимать эффективные управленческие решения;
- наличие процедур оперативного мониторинга текущей деятельности, обеспечивающих своевременную идентификацию операционных сбоев линейными менеджерами, например невыполнение сотрудниками штатных процедур;
- наличие процедур информационного обмена между смежными IT-процессами;
- методы и специальные инструменты, позволяющие повысить эффективность деятельности, например использования средств автоматизации для регистрации и учета обращений пользователей;

- совершенствование деятельности на основе анализа текущей эффективности и планов развития информационных технологий.

- предварительное ранжирование перечня IT-процессов и связанных IT-рисков, подлежащих оценке;

- согласование границ аудита: IT-сервисы, системы, программно-аппаратное обеспечение, подразделения и специалисты, в отношении которых будет проведен анализ;

- формирование и согласование детального плана аудита.

Аудитором обычно формируется эталонный перечень IT-рисков, которые согласно международным стандартам присущи стадиям планирования, разработки, внедрения и эксплуатации информационных автоматизированных систем. Инициатор аудита (заказчик) на основе указанного перечня определяет приоритеты для оценки. Если заказчиком IT-аудита выступают представители руководства компании, то для получения более точного результата рекомендуется формировать анкеты и бизнес-терминах (табл. 2).

Таблица 2 - Выдержка из анкеты для проведения интервью с руководством компании и ключевыми пользователями

Описание IT-риска (из каталога рисков компании "ИТ Эксперт")	Оценка важности управления IT-риском	Выбранный вариант отметить "+"
На этапе стратегического бизнес-планирования не рассматриваются вопросы IT-стратегии. Последствия: несвоевременное реагирование IT-службы на бизнес-инициативы (открытие новых офисов, автоматизация бизнес-процессов); увеличение финансовых затрат на перевод бизнес-инициатив в конкретные IT-решения (неоптимальные и ошибочные решения, принимаемые IT в спешном порядке)	Риск несущественный Пояснения к интервью: риск носит гипотетический характер и малозначим для деятельности компании (затраты на управление риском будут выше, чем полученный эффект)	+/-
	Риск умеренный (приемлемый) Пояснения к интервью: признается важность управления указанным риском в стратегической перспективе (на данном этапе допускается предварительная проработка вопроса, не требующая привлечения финансовых инвестиций и затраты существенных временных ресурсов бизнес-руководителей)	+/-
	Риск выше среднего Пояснения к интервью: признается важность управления указанным риском (в том числе выделение временных и финансовых ресурсов)	+/-

	уже в краткосрочной перспективе	
	Риск высокий Пояснения к интервью: допускается, что реализация данного риска не только возможна в краткосрочной перспективе, но и уже происходила	+/-
	Дополнительный параметр оценки	
	Признается необходимость совместного участия IT и бизнеса в управлении данным риском	+/-

С учетом временных и ресурсных параметров проведения аудита определяются границы аудита (сервисы, системы, подразделения и т.п.). При этом рекомендуется рассматривать наиболее значимые для целей бизнеса и/или распространенные сервисы и системы, чтобы иметь возможность на основе оценки определенной (ключевой) области аудита сделать объективные выводы о системе IT-управления в целом.

С учетом полученной информации аудитор формирует анкеты, в которых указывает параметры аудиторских процедур по каждому IT-процессу, в том числе наименование детализированных целей контроля и примерное количество уточняющих вопросов.

Чтобы оценка системы IT-управления была всесторонней, формируется иерархия вопросов от частных до высокоуровневых. Для анализа оценки уровня зрелости IT-процессов рассматриваются частные вопросы, сгруппированные в детализированные цели контроля. При этом учитывается полнота и достоверность предоставленных аудиторам данных и свидетельств.

Для примера приведем структуру анкеты для оценки IT-процесса "Управление услугами подрядчиков":

Риски недостижения целей процесса:

- отсутствие четких договорных отношений (соглашений) с поставщиками IT-услуг (включая определение ролей, ответственности и ожиданий, проведение проверок и мониторинга соответствующих соглашений с точки зрения эффективности и соответствия) повышает угрозу возникновения ущерба для случаев невыполнения поставщиками своих обязательств.

Влияние на достижение целей IT-деятельности:

- обеспечение результативности IT-деятельности - умеренное влияние;
- обеспечение рациональности IT-деятельности - высокое влияние;
- обеспечение безопасности IT-деятельности - высокое влияние.

Детализированные цели контроля:

- определение политик процесса и процедур деятельности;

- распределение ролей;
- менеджмент документов;
- анализ контрактов;
- управление договорными разногласиями;
- передача прав;
- ответственность и подотчетность;
- инструментарий;
- охват процесса;
- отчетность и метрики.

Следующий этап - аудит на месте, в рамках которого проводятся интервью с сотрудниками компании-заказчика и верифицируются их результаты (табл. 3).

Таблица 3 - Фрагмент анкеты для самооценки процесса "управление конфигурациями"

№ п/п	Критерии аудита	Самооценка от 0 до 3 или да/нет
1	Положение о подразделении содержит указание на задачи, связанные с управлением конфигурациями	да
2	В должностные инструкции сотрудников, отвечающих за управление конфигурациями, включены соответствующие записи	да
3	Определен и адекватен охват CMDB (конфигурационной базы данных): серверы, ПЭВМ, СУБД, ПО, ЛВС	3
4	Определена и адекватна степень детализации атрибутов конфигурационной единицы (наименование, тип, место, владелец, инвентарный номер, статус, документация, лицензия и др.)	2
5	Регистрируются взаимоотношения (взаимосвязи) между конфигурационными единицами на физическом и логическом уровне	3
6	Применяется порядок регистрации базисной конфигурации	2
7	Определены и выполняются процедуры контроля над добавлением конфигурационной единицы	
8	Определены инициирующие события и периодичность проведения аудита CMDB (проверки того, насколько точно отражена текущая ситуация в CMDB)	да
9	Применяются инструментальные средства аудита, которые могут автоматически выполнять анализ рабочих станций и формировать отчеты о текущей ситуации и статусе IT-инфраструктуры	1

На этом этапе рекомендуется решать следующие задачи:

- провести процедуры самооценки с использованием разработанных ранее анкет;

- провести интервьюирование ключевых сотрудников объекта аудита для уточнения результатов самооценки;

- провести верификацию результатов интервью и самооценки в рамках процедур наблюдения за деятельностью и детализированного тестирования предоставленных свидетельств (в том числе регламентов, положений, отчетов, записей о событиях и т.п.).

Заказчик определяет сотрудников, которые будут в рамках интервью по рассматриваемому IT-процессу давать официальную оценку (самооценку) степени соответствия фактического положения дел изложенным в анкете критериям. Аудитор проводит интервьюирование, в рамках которого анализируются и уточняются результаты самооценки.

Анализируется перечень свидетельств, подтверждающих высокие результаты самооценки, в том числе оценивается фактическая готовность предоставить соответствующие свидетельства (табл. 4).

Таблица 4 - Фрагмент перечня представленных свидетельств

№ п/п	документ	Отметка аудитора
1	Положение по управлению серверов, баз данных и виртуальных машин	+
2	Положение по управлению конфигурациями активного сетевого оборудования	+
3	Положение по ведению конфигурационной базы данных персональных компьютеров	+
4	Положение по ведению конфигурационной базы данных персональных компьютеров, на которых производится обработка, хранение и передача конфиденциальных сведений	+

Каждый вопрос анкеты может быть рассмотрен по следующим параметрам: компетенция персонала, фактическая деятельность, документирование, мониторинг и автоматизация.

Оценка показателей осуществляется по пятибалльной шкале, распределенной, например, для показателя "деятельность" следующим образом:

0 - деятельность не осуществляется и не признается необходимой;

1 - деятельность не осуществляется, но признается необходимой;

2 - деятельность осуществляется фрагментарно и имеет минимальный охват, подтвердить ее свидетельствами невозможно, вероятные отклонения выявить сложно;

3 - деятельность осуществляется на периодической основе, однако имеет небольшой охвать и может быть подтверждена свидетельствами только в отдельных случаях или посредством демонстрации в режиме "наблюдения за деятельностью";

4 - деятельность осуществляется на постоянной основе. Охват процесса находится на удовлетворительном уровне и запланирован к увеличению, в большинстве случаев имеются документальные свидетельства деятельности;

5 - деятельность осуществляется на постоянной основе, имеет полный охват, имеются свидетельства в электронном и бумажном виде, которые пригодны как для внутреннего контроля, так и для аудита.

При выставлении оценки необходимо учитывать адекватность документарных свидетельств (аудиторский след), на основании которых можно дать заключение по оцениваемой деятельности. К этой группе документов относятся, например, реестры и описи, регистрационные журналы, протоколы, листы ознакомления, акты и/или отчеты, свидетельствующие о выполнении работы (наряда).

Полученные ответы ранжируются по весовым характеристикам и результатам (баллам) самооценки. Далее происходит верификация анкет. Оценки с наибольшим весом и результатом самооценки проходят экзамен на соответствие в первую очередь. В любом случае данной процедуре должно быть подвергнуто не менее 50% свидетельств/ответов с высшим баллом и не менее 30% остальных.

Если выясняется, что самооценка завышена, аудитор проставляет свою оценку, которая затем и является основной для последующих расчетов. Верификация производится на основании наблюдения за деятельностью и условиями работы; запроса документов, записей (актов, протоколов) проверок, протоколов совещаний, отчетов (актов) по аудитам, итоговых данных, показателей анализа и результативности, отчетов; обращения к электронным базам данных и веб-сайтам.

При необходимости аудитор оперативно формирует анкету детализированного тестирования для проведения аудиторских процедур по существу (выборочный анализ совокупности свидетельств аудита по отдельным вопросам для получения дополнительных гарантий результатов самооценки).

На заключительном этапе аудита проводится анализ собранных свидетельств, формируются детальные оценки и итоговые выводы аудита. Международный стандарт CobiT характеризует данный этап как "творческий", так как перед аудитором стоит непростая задача провести многоступенчатое

преобразование оценок от отдельных частных вопросов до формирования итоговых выкладок о состоянии системы IT-управления организации в целом.

Ключевой задачей аудитора на данном этапе является обеспечение транспарентности механизма формирования итоговых выводов как основного условия доверия к результатам аудита. Все заинтересованные стороны должны иметь возможность отследить причинно-следственную связь в цепочке преобразования результатов аудита от частных к итоговым оценкам. Остановимся на наиболее специфичных этапах преобразования оценок.

Расчет уровня зрелости IT-процесса проведен с использованием методологии CobiT, предлагающей определять пять ключевых характеристик зрелости процесса (табл. 5). Аудитор проводит группировку частных вопросов по указанным характеристикам процесса (компетенция, фактическая деятельность, документирование, измерение, совершенствование) и рассчитывает оценку для каждой группы. При этом рекомендуется учитыватьвесовые характеристики как вопросов внутри группы, так и самих групп. Определение конкретных значений выполняется экспертным путем и согласуется с заказчиком аудита в начале работы.

Таблица 5 - Формула расчета итоговой оценки уровня зрелости L=L1+L2+L3+L4+L5

Уровень зрелости по разделу	Наименование	К - вес раздела (сумма баллов равняется 5)	R(Tn) - базовая оценка от 0 до 1 по итогам анкетирования и верификации (фактическая сумма оценок/максимально возможная сумма оценок)
L=KxR(T1)	Компетенция	0,75	R(T1)
L2=KxR(T2)	Деятельность	1,45	R(T2)
L3=KxR(T3)XR(T2)	Документирование	1,15	R(T3)
L4=KxR(T4)XR(T2)	Измерение	0,9	R(T4)
L5=KxR(T5)XR(T2)	Совершенствование	0,7	R(T5)

Расчет позволяет построить тренд уровня зрелости IT-процесса.

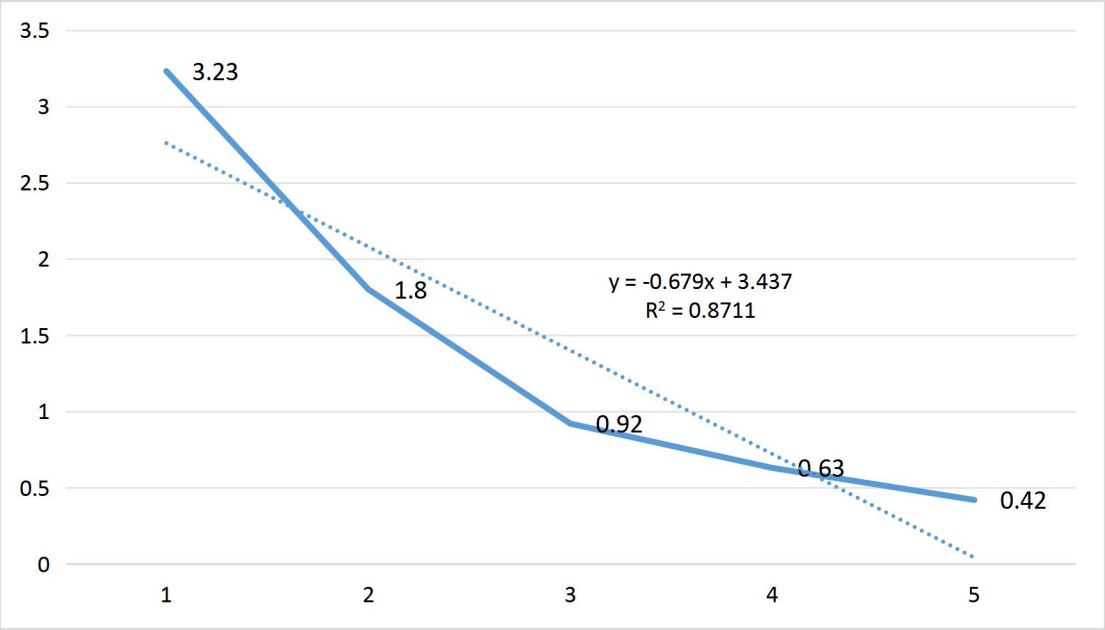

Рисунок 1 - Тренд уровня зрелости IT-процесса

Отрицательный вектор тренда строится с учетом уровня документирования (итоговая оценка для данной группы вопросов). Чем ниже уровень документирования, тем больше вероятность в случае утраты ключевого персонала или изменений условий деятельности не достигнуть целей IT-деятельности (например, новые сотрудники не могут получить информацию о том, как должны выполняться те или иные процедуры). Соответственно для положительного тренда учитываются измерение и совершенствование как основа улучшения деятельности.

Длительность постпроверочного периода (времени между аудитами) на практике в большинстве случаев составляет от года до трех лет и определяется с учетом законодательных и нормативных требований по периодичности, а также принципа разумной достаточности - исследуется период, который представляет наибольший интерес для целей формирования прогнозов на будущее.

Речь идет об уровне риска после его обработки, например после применения контрмер, направленных на его снижение. В рамках данной процедуры аудитор составляет ранжированный перечень выявленных рисков и сопоставляет базовый уровень риска с уровнем зрелости IT-процесса, отвечающего за управление данным параметром (табл. 6).

Таблица 6 - Оценка остаточного уровня IT-риска

IT-риск	Уровень неотъемлемого риска от 0 до 5 (экспертная	Влияние уровня зрелости IT-процесса (в рамках которого	Оценка остаточного риска

	оценка)	управляется риск) от 0 до 5	
	R1	L	S=5xR1-L2
Риск увеличения времени от начала разработки до готовности систем из-за отсутствия гибкой инфраструктуры	5	2	21
Риск увеличения времени простоя инфраструктуры	3	2	11
Риск увеличения проблем, связанных с производительностью работы приложений и вызванных несоответствиями в технологической инфраструктуре	4	2	16
Риск нехватки мощностей при внедрении новых IT-решений	3	3	6
Риск повышения затрат на IT-инфраструктуру вследствие создания необоснованных резервов "про запас"	2	3	1

Допустимым считается остаточный риск (S) 6 и менее. Умеренным - от 7 до 11. Высоким - от 12 до 16. Критическим - от 17 до 25.

Заключение

Структурирование оценок на всех этапах формирования выводов аудита позволяет сформировать статистическую основу для расчета предполагаемой динамики изменения различных процессных показателей в постпроверочном периоде.

Полученные результаты могут быть использованы для формирования перспективного плана инвестиций в информационные технологии, взаимоувязанного с повышением уровня зрелости системы управления рисками. Как уже было сказано, чем сложнее информационная система, тем более зрелая система IT-управления ей должна соответствовать. Но существует и обратная зависимость. Например, если у компании несложная локальная система, то максимальной эффективности она достигнет при уровне зрелости 2,8-3,2. Более высокий уровень не даст решающего преимущества, но может привести к дополнительным расходам на менеджмент.

Помимо стандартных рекомендаций по устранению выявленных в ходе аудита несоответствий (замечаний), результаты аудита могут быть использованы для разработки ключевых рекомендаций по тактике и стратегии совершенствования системы IT-управления в целом и отдельных IT-процессов, а также для формирования методической основы систем внутреннего контроля и аудита за информационными технологиями организации.

Применение рассмотренной выше методики аудита позволяет компании взглянуть на свою систему IT-управления через призму международных стандартов и практического опыта и, как следствие, получить профессиональную экспертную оценку:

- степени ее соответствия требованиям стандартов, что может быть использовано для определения готовности организации к прохождению сертификационного аудита;
- ее адекватности целям эффективного формирования добавочной ценности для бизнеса при использовании информационных технологий;
- ее устойчивости при реализации различных сценариев, например, если рассматривается расширение бизнеса, то оценивается готовность службы IT масштабировать свою деятельность, если речь идет о масштабном переходе на новые информационные системы, анализируется готовность обеспечить надежный переход на новые системы в оптимальный срок, для изменения объемов финансирования оценивается степень адаптивности к соответствующим условиям.

На основании проведенной работы вырабатываются рекомендации по стратегии развития управления подразделениями IT, в том числе конкретных процессов управления, предотвращению рисков, совершенствованию работы.

Список литературы

1. Григорьева, Е. С., Максимова, Е. А., Александров, А. Х. Технические документы по критической информационной инфраструктуре / Е. С. Григорьева, Е. А. Максимова, А. Х. Александров // Состояние и перспективы развития ИТ- образования: сб. науч. тр. – Чебоксары:Изд-во Чуваш. ун-та, 2019. – С. 67-71.

2. Корнин, И. Требования для программного обеспечения: рекомендации по сбору и документированию / И. Корнин. – Москва: Нобель Пресс, 2014. – 118 с.

3. Пакин, А. И. Информационная безопасность информационных систем управления предприятием [Электронный ресурс]: учебное пособие / А. И. Пакин. – Москва:Моск. гос. акад. водного транспорта, 2012. – 41 с.

4. Поляков, А. В. Информационная безопасность организации: социально-управленческий анализ // Социально-гуманитарные знания. – 2010. – № 5. – С. 173-179.

5. Скокова И. К., Романенко Н. А., Макашова В. Н., Давлеткиреева Л. З. Оценка уровня зрелости для ИТ-компании // International Journal of Open Information Technologies. 2017. №5.

6. Стасышин, В. М.Проектирование информационных систем и баз данных [Электронный ресурс]: учебное пособие / В. М. Стасышин. – Новосибирск: Новосиб. гос. техн. ун-т, 2012. – 100 с.

7. Торпошян, Е. А. Подсистема управления инцидентами информационной безопасности в системе управления процессами защиты информации / Е. А. Торпошян // Актуальные проблемы математических и технических наук: сб. науч. тр. – Чебоксары: Чуваш. гос. пед. ун-т, 2017. – С. 135-138.

8. Чистов, Д. В. Проектирование информационных систем: учеб. и практикум для академ. бакалавриата / под общ. ред. Д. В. Чистова. – Москва: Юрайт, 2016. – 258 с.