N.G. Miloslavskaya, R.A. Sagirov
Review of Information Security Processes' Maturity Models

Keywords: maturity model, maturity level, information security management processes, information security management system
The most commonly used maturity model as applied in the field of information security (IS) and information technologies (IT) are described. The results of a comparative analysis of selected models are given. Further, a universal maturity model for IS management processes will be developed on the basis of the results obtained.

Н.Г. Милославская, Р.А. Сагиров

ОБЗОР МОДЕЛЕЙ ЗРЕЛОСТИ ПРОЦЕССОВ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

«Нельзя управлять тем, что нельзя измерить»
П. Друкер

Введение

Управление информационной безопасности (ИБ) является неотъемлемой частью управления любой организации в независимости от ее сферы деятельности, размеров и т.п.

Управление ИБ состоит из совокупности тесно взаимосвязанных подпроцессов, вносящих существенный вклад в достижение основных целей управления ИБ и образующих систему управления информационной безопасностью (СУИБ). СУИБ определяется как та часть общей системы управления организации, основанной на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности [1]. СУИБ включает в себя организационную структуру, политики, планирование, должностные обязанности, практики, процедуры, процессы и ресурсы.

Управление ИБ базируется на процессном подходе, в основе которого лежит понятие процесса – последовательность шагов, направленная на достижение определенной цели или результата [2].Отдельные процессы, организации с их подразделениями и персоналом и даже страны постоянно эволюционируют, проходя различные этапы в своем развитии. Эволюционное развитие представляет собой движение от простого к сложному, однако иногда оно может оставаться в статическом состоянии, либо и вовсе делать шаги назад.

Задача внедрения процесса управления ИБ в организации должна соответствовать уровню ее организационного и технологического развития. Уровень развития информационных технологий (ИТ) организации часто оказывает значительное влияние на ее конкурентоспособность. Обеспечение конфиденциальности, целостности и доступности информации можно с уверенностью отнести к необходимым условиям непрерывности бизнеса. Требования к совершенствованию и реализации мер по обеспечению ИБ (ОИБ) формулируются на основе определения уровня зрелости этих процессов в организации. После получения оценки зрелости можно выработать необходимые меры для повышения уровня зрелости процессов и организации в целом.

В практике ОИБ для определения стадии организационного и технологического развития организации и её процессов применяется понятие модели зрелости (англ.

maturity model). Для измерения состояния процесса используется набор метрик, которые представляют собой определенные характеристики. Оценивание этих метрик по установленной шкале показывает состояние процессов, которое и будет характеризовать уровень их зрелости.

В зарубежной практике, в отличие от российской, применение модели зрелости для управления процессами ОИБ широко распространено. Примером этого может служить серия стандартов ISO27000, которая регулирует вопросы управления ИБ, реализуемых на основе СУИБ. Очевидно, что перед организацией, осуществляющей деятельность по управлению ИБ, рано или поздно встает вопрос о том, как выполнять эти требования, в каком объеме и на каком уровне детализации и т.п. Ответить на эти и другие вопросы может помочь модель зрелости, на основе которой будет проводится оценка уровня зрелости процессов ОИБ.

В России понятие «модель зрелости» известно сравнительно недавно, в то время как в зарубежных странах модели зрелости в области ИБ получили широкое распространение. Для оценки их применимости к российским реалиям в статье проводится сравнительный анализ наиболее распространенных и часто используемых моделей зрелости как в области ИБ, так и ИТ, а именно:

- Open Information Security Management Maturity Model (O-SIM3) – стандартимодельнезависимого консорциума The Open Group;
- ProcessCapabilityModel(PCM) – модель возможностей процессов стандарта CobIT 5 международной общественной ассоциации ISACA;
- Business Process Management Maturity Model (BPM MM) – модельзрелостиуправлениябизнес-процессамикомпанииGartner Group;
- CommunityCyberSecurityMaturityModel (CCSMM) – модель зрелости кибербезопасности одного из центров Университета Техаса.

Обзор моделей

Модель O-ISM3

Модель O-ISM3 описывает основные процессы управления ИБ, присущие большинству организаций.

Выделяются задачи процессов ОИБ и метрики, непосредственно вытекающие из бизнес-целей организации. Отмечается, что каждый процесс ОИБ вносит свой вклад в реализацию основных целей управления ИБ, которые определяются следующим образом:

- предотвращать и снижать число инцидентов ИБ, которые могут поставить под угрозу активы организации, поставляемую ею продукцию и предоставляемые сервисы, основанные на использовании информационных систем;
- оптимизировать использование информации, финансов, людей, времени и инфраструктуры.

Основная идея стандарта O-ISM3 как стандарта по управлению ИБ заключается в том, что ОИБ связано не только с предотвращением атак на активы, но и с достижением в рамках установленного бюджета бизнес-целей организации, несмотря на различные возможные инциденты ИБ (атаки, технические сбои, ошибки персонала и т.д.).

Модель O-ISM3 оценивает зрелость функционирования существующих процессов СУИБ организации. Отличительной особенностью модели O-ISM3 является то, что она основана на оценке зрелости каждого из применяемых в СУИБ процессов управления

ИБ, т.е. чтобы эффективно использовать это средство, необходимо оценивать уровень его зрелости.

Уровни зрелости в O-ISM3 – специальные комбинации процессов ISM3, применяющихся при определенных уровнях возможностей. Уровень зрелости определяется как совокупность процессов и возможности каждого из процессов. Если две системы управления базами данных (СУБД) имеют одинаковый набор процессов, но у одной из них больше возможностей, то она считается более зрелой. Если возможности одинаковы, а количество процессов различно, более зрелой считается СУБД с большим количеством процессов.

Согласно O-ISM3, СУИБ внедряется в рамках четырёх уровней управления ИБ организации, по которым производится оценка зрелости:

- базовый – для общего управления;
- стратегический (руководство и обеспечение), на котором устанавливаются стратегические цели, осуществляется координация деятельности и обеспечение ресурсами;
- тактический (внедрение и оптимизация), который связан с разработкой и реализацией СУИБ, установкой специфических целей и управлением ресурсами;
- операционный (исполнение и отчетность), который связан с достижением определенных целей посредством функционирования технических процессов.

Для каждого из этих уровней в модели определены процессы, которые их обслуживают.

ISM3 определяет следующие виды метрик [3]:

- деятельность (англ. *Activity*) – количество произведенных выходов, их средний срок жизни, среднее время между представлением выходов, среднее время на производство выхода после входа, худшее время на производство выхода после входа;
- область действия (англ. *Scope*) – доля всех входов, используемых процессом, и доля всех выбранных или тестируемых входов;
- недоступность (англ. *Unavailability*) – время, прошедшее с момента ожидаемого выполнения процесса после его запуска (время работы), частота и продолжительность перерывов;
- результативность (англ. *Effectiveness*) – количество входов, среднее время между входами и процент входов, породивших выход;
- эффективность (англ. *Efficiency*) – отношение числа произведенных выходов к реально доступным для процесса ресурсам;
- загрузка (англ. *Load*) – процент реально используемых ресурсов;
- качество (англ. *Quality*) – правильность, точность или другие измерения соответствия выхода начальным целям, если это применимо.

В O-ISM3 процессы системы управления классифицируются по пяти уровням зрелости: 1 – начальный (Initial); 2 – управляемый (Managed); 3 – определенный (Defined); 4 – контролируемый (Controlled); 5 – оптимизированный (Optimized).

В табл. 1 показано, какие метрики необходимо применять для процессов управления каждого уровня [3]. Видно, что для определения верного уровня зрелости требуется высокая детализация рассматриваемых процессов.

Таблица 1. Взаимосвязь метрик с уровнем зрелости в модели O-ISM3

Уровень зрелости		Начальный	Управляемый	Определенный			Контролируемый	Оптимизированный
Процессы управления		Аудит, сертификация	Тестирование	Мониторинг	Планирование	Эффективная реализация	Оценка	Оптимизация
Документация		+	+	+	+	+	+	+
Тип метрики	Деятельность		+	+	+	+	+	+
	Область действия		+	+	+	+	+	+
	Недоступность		+	+	+	+	+	+
	Результативность		+	+	+	+	+	+
	Загрузка			+	+	+	+	+
	Качество						+	+
	Эффективность							+

Модель BPMMM

При оценке зрелости организации в области ОИБ также известен подход аналитической компании Gartner Group, которая выделяет четыре уровня – с нулевого по третий [4].

Нулевой уровень – необходимость ОИБ организацией в должной мере не осознана и формально такая задача не ставится. Выделенной службы ИБ нет. Служба автоматизации использует традиционные механизмы и средства защиты информации стека протоколов TCP/IP и сервисов интранета, а также операционной среды и приложений (операционные системы, СУБД, системы поддержки и принятия решений и т.д.).

Первый уровень – проблема ОИБ рассматривается управлением организации как исключительно техническая. Выделенной службы ИБ нет. Организационные меры поддержания ИБ не принимаются. Финансирование осуществляется в рамках единого бюджета на ИТ. Служба автоматизации дополнительно к средствам уровня 0 может привлекать средства отказоустойчивости, резервного копирования информации, источники бесперебойного питания, а также МЭ, виртуальные частные сети, антивирусные средства, средства прозрачного шифрования и электронные ключи для аутентификации.

Второй уровень – важность ОИБ организацией осознана и рассматривается как взаимно увязанный комплекс организационных и технических мер. Внедрены методики анализа рисков ИБ, отвечающие минимальному (базовому) уровню защищенности ИС. Определены состав и структура штатной службы ИБ. Принята корпоративная ПолИБ. Финансирование на создание и поддержку системы ОИБ (СОИБ) ведется в рамках отдельного бюджета. Служба ИБ дополнительно к средствам уровней 0 и 1 привлекает средства защиты от НСД, систем обнаружения вторжений, инфраструктуру открытых ключей, а также соответствующие ПолИБ организационные меры (внешний и внутренний аудит ИБ, разработка планов защиты и непрерывности бизнеса, действия во внештатных ситуациях и т.п.).

Третий уровень – проблема ОИБ организацией осознана в полной мере. Наряду с бизнес-культурой существует понятие культуры ИБ. Активно применяются методики полного количественного анализа рисков ИБ, а также соответствующие инструментальные средства. Введена штатная должность – директор службы ИБ (CISO). Определены состав и структура группы внутреннего аудита ИБ (CISA), группы предупреждения и расследования компьютерных преступлений, группы экономической безопасности. Руководством организации утверждены концепция и политика ИБ, план защиты и другие нормативно-методические материалы и должностные инструкции. Финансирование выделяется исключительно в рамках отдельного бюджета. Служба ИБ дополнительно к средствам уровней 0–2 обращается к средствам централизованного управления ИБ и средствам интеграции с платформами управления сетевыми ресурсами.

Модель BPM MM многомерна по своей сети и позволяет рассматривать процессы по нескольким направлениям – организационным факторам: стратегия, культура и лидерство, персонал, руководство, методики, ИТ.

Модель PCM

В стандарте Cobit 5, разработанном ISACA в 2012 г., четко выражен процессный подход к управлению ИТ. С точки зрения стандарта наиболее эффективным подходом к управлению ИТ является функциональное разделение обязанностей, полномочий и ответственностей персонала ИТ-подразделения.

Модель PCM основана на модели зрелости, описанной в стандарте Cobit 4.1. В Cobit 5 введены следующие уровни зрелости процессов [5]:

- 0: Неполный процесс – такой процесс еще не внедрен или не способен соответствовать своему назначению; на этом уровне отсутствуют свидетельства систематического достижения процессом своих целей или таких свидетельств мало;
- 1: Осуществленный процесс – процесс внедрен и соответствует своему назначению;
- 2: Управляемый процесс – осуществленный процесс предыдущего уровня теперь управляем (т.е. планируется, отслеживается и корректируется);создаются, контролируются и поддерживаются рабочие продукты процесса;
- 3: Установленный процесс – управляемый процесс теперь способен получать ожидаемые результаты;
- 4: Предсказуемый процесс – установленный процесс теперь получает результаты в условиях заданных ограничений;
- 5: Оптимизируемый процесс– предсказуемый процесс теперь постоянно совершенствуется, чтобы достигать текущих и будущих целей организации.

Уровень зрелости определяется на основании наличия и полноты базовых атрибутов процессов: производительность процесса (Уровень 1); управление производительностью (Уровень 2); управление рабочими продуктами (Уровень 2); определение процесса (Уровень 3); внедрение процесса (Уровень 3); управление процессом (Уровень 4); контроль процесса (Уровень 4); инновационность процесса (Уровень 5); оптимизация процесса (Уровень 5).

Важно заметить, что переход на новый уровень возможностей осуществляется лишь при исполнении всех атрибутов предыдущего уровня. В соответствии с этим оценщик должен последовательно рассмотреть каждый из девяти атрибутов и далее выявить свидетельства всех атрибутов возможностей процесса и выставить каждому процессу рейтинг в соответствии со следующей шкалой [6]:

- N (not achieved, не достигается) – в оцениваемом процессе не существует или существует мало свидетельств того, что определенный атрибут достигается (от 0до 15% реализованных практик);
- P (partially, частично достигается) – в оцениваемом процессе есть свидетельства того, что существует подход к достижению и происходит частичное достижение заданных целей; некоторые аспекты достижения цели (атрибута) непредсказуемы (от 15 до 50% реализованных практик);
- L (largely, в основном достигается) – в оцениваемом процессе существуют свидетельства системного подхода и системного достижения заданных целей; существуют некоторые недостатки достигаемых результатов (от 50 до 85% реализованных практик);
- F (fully, полностью достигается) – в оцениваемом процессе существуют свидетельства полного системного подхода и фактического достижения заданных целей; значительных недостатков, связанных с полученным результатом, не выявлено (от 85до 100% реализованных практик).

Модель CCSMM

Модель CC SMM основана на опыте использования двух моделей зрелости.

1. Пятиуровневая модель Software Capability Maturity Model для программного обеспечения (SW-CMM), разработанная институтом Software Engineering Institute – подразделением Университета Carnegie Mellon и предложенная в 1987 г. Выделены следующие уровни зрелости: Initial – начальный (процесс спонтанен и во многом хаотичен; успех зависит от индивидуальных способностей участников и не может быть повторен без их привлечения); Repeated – повторяемый (организация применяет лучшей практики для управления процессами; возможно повторное использование успешных решений); Defined – определенный (процесс документирован, стандартизован, утвержден, последовательно применяется в рамках всей организации); Managed – управляемый (для процессов предложены специальные метрики, которые позволяют количественно определить организацию процесса); Optimizing – оптимизированный (процессы направленным образом изменяются для достижения новых целей);

2. Шестиуровневая модель Systems Security Engineering – Capability Maturity Model (SSE-CMM) для разработки программных систем безопасности. Выделены следующие уровни: Initial – начальный; Performed informally – выполняемый без официального указания (за счет самых необходимых основных действий); Planned & Tracked – планируемый и отслеживаемый; Well-defined – хорошо определенный (с координацией основных действий); Quantitatively controlled – контролируемый на основе количественных показателей; Continuously improving – постоянно совершенствуемый (включая вопросы эффективности).

Модель CC SMM ориентирована на содействие взаимодействию различных организаций сообщества между собой в направлении эффективного противодействия киберпреступности.

Для измерения текущего состояния уровня безопасности и определения зрелости в этой модели учитываются не только метрики, но и технологии, уязвимости, тесты, которые могут быть использованы вместе с метриками.

В табл. 2 представлено описание уровней зрелостей модели CC SMM [6].

Таблица 2. Уровни зрелости модели CCSMM

Уровень зрелости	Описание уровней
1: О безопасности известно	Уровень зрелости предполагает, что отдельные лица и руководство организации осознает угрозы, проблемы и вопросы, связанные с безопасностью
2: Развитие процессов	Уровень зрелости предполагает, что элементы безопасности разработаны, есть необходимость в совершенствовании процессов безопасности
3: Установлено информирование	Уровень зрелости указывает, что все организации в рамках сообщества знакомы с вопросами, связанными с безопасностью, и имеют процессы и механизмы, позволяющие идентифицировать безопасность соответствующих мероприятий. Целью на этом уровне является улучшение механизмов обмена информацией в рамках сообщества для того, чтобы оно эффективно соотносило разрозненные фрагменты информации. Следуя этому, могут быть выявлены факты готовящегося нападения
4: Развитие тактики	На этом уровне действия направлены на развитие, улучшение методов обнаружения и реагирования на атаки. Также должны быть внедрены методы профилактики
5: Полная безопасность эксплуатируемых возможностей	Представляет собой наличие всех необходимых элементов безопасности, которые должны существовать для оперативного решения любых типов киберугроз. Это не означает, что организация на этом уровне будет защищена от любой атаки, а означает, что служба безопасности сделала все, что могла, в целях предотвращения и обнаружения атак. Организация способна эффективно реагировать в случае, если она не смогла предотвратить нападение на первой итерации. Организация должна взаимодействовать с соответствующими лицам других организаций, информируя их об атаках и совместно реагируя на них. Это позволит всему сообществу, совместно работая, устранить угрозы кибербезопасности

Сравнительный анализ

Перечисленные модели зрелости объединяет процессный подход к определению уровня зрелости. Однако отсутствует единая трактовка понятия зрелости, в силу того, что каждая модель решает собственную задачу:

- O-ISM3 – оценка зрелости СУИБ на основе анализа внедренных процессов;
- PCM – оценка возможностей процессов, интегрированных в ИТ организации;
- BPMMM – оценка уровня реализации процессов организации;
- CCSMM – сравнение зрелости различных организаций для координации общих усилий по обеспечению желаемого уровня безопасности.

Для определения уровня зрелости необходимо учитывать конкретный набор метрик, которые позволяют раскрыть уровень зрелости процессов. Каждая модель предлагает свой набор метрик/атрибутов для оценки зрелости процессов, совпадений среди которых практически нет. Это обусловлено различием целей и решаемых задач для разных моделей.

Одним из центральных условий применения моделей является требование развитости и стабильности процессов управления. Все рассмотренные модели зрелости разработаны и применяются в основном в зарубежных странах. В России применение этих моделей затруднено в силу того, что развитие ИБ в организациях находится на низком уровне и требования, рассматриваемые в моделях, не реализованы. Развитие и стабиль-

ность процессов управления зарубежных организаций и российских сильно различаются.

Итоги краткого сравнительного анализа исследованных моделей по таким критериям, как тип модели, количество уровней зрелости, масштаб модели и профессиональная подготовка персонала, представлены в табл. 3.

Таблица 3. Сравнение рассмотренных моделей зрелости

Характеристики моделей	O-ISM3	PCM	BPMMM	CC SMM
Тип модели	Описательная	Рекомендательная	Описательная	Описательная
Количество уровней	5	6	4	5
Масштаб модели	СУИБ организации	ИТ-инфраструктура	Все процессы организации	Процессы ИБ организации
Профессиональная подготовка персонала	Высокая	+	-	-

Заключение

Для эффективного управления ИБ необходимо использовать модель зрелости. Результаты зрелости процесса СУИБ показывают следующее:

- определен ли в конкретной организации этот процесс;
- документирован ли процесс;
- выполняются ли требования документов для процесса;
- насколько процесс управляем и соответствует лучшим практикам.

Таким образом можно охарактеризовать полноту, адекватность, результативность и эффективность всех процессов управления ИБ, выполняемых в рамках функционирования СУИБ, что позволит помочь повысить качество используемых процессов управления ИБ и, следовательно, улучшить СУИБ.

Однако, организации следует подобрать и применить под свои потребности, а, возможно, и разработать собственную модель зрелости с подходящими для нее метриками, используя рассмотренные модели в качестве образца.

Также уровни зрелости могут быть использованы различными сертифицирующими органами и аудиторами для разработки схемы сертификации, специфической для данного органа сертификации (аудитора).

Ни одна из рассмотренных моделей в полной мере не отражает всех современных требований по ОИБ для организаций различного размера и сферы деятельности. Поэтому представляется актуальным разработка обобщенном и более уточненной по процессам и возможностям модели зрелости управления ИБ.

СПИСОК ЛИТЕРАТУРЫ:

1. Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов /Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая Линия-Телеком, 2014. – 166 с.

2. ITIL® The key to Managing IT services Office of Government Commerce. London: TSO. 2005. – 418 c. ISBN 0-11-330948-1 (Поддержка услуг. Перевод на русский язык компании «Ай-Теко»,www.i-teco.ru).

3. Open Information Security Management Maturity Model (O-ISM3), The Open Group, February 2011. 121 c. ISBN 1-931624-86-0.

4. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. [Электронныйресурс]. – URL: http://www.isaca.org/COBIT/Pages/default.aspx?utm_source= informz-25-January-2013-COBIT-Focus-Vol-1&utm_medium=email&utm_campaign=cobit- focus (датаобращения:24.02.2015).

5. **Нарыжный К**. Cobit 5: **модель оценки процессов** [**Электронный ресурс**]. – URL:http://www.cleverics.ru/ru/subject-field/articles/554-cobit5-pam(**датаобращения**: 24.02.2015).
6. **Баскаков А.В**. **Модель зрелости как инструмент развития процесса безопасности в организации процессов** [**Электронный ресурс**]. – URL: http://journal.itmane.ru/node/913 (**дата обращения**: 24.02.2015).

REFERENCES:

1. Proverka i otsenka deyatel'nosti po upravleniyu informatsionnoy bezopasnost'yu. Uchebnoe posobie dlya vuzov /N.G. Miloslavskaya, M.Yu. Senatorov, A.I. Tolstoy. – M.: Goryachaya Liniya-Telekom, 2014. – 166 s.
2. ITIL® The key to Managing IT services Office of Government Commerce. London: TSO. 2005. – 418 c. ISBN 0-11-330948-1 (**Поддержкауслуг**. **Перевод на русский язык компании** «**Ай-Теко**», www.i-teco.ru).
3. Open Information Security Management Maturity Model (O-ISM3), The Open Group, February 2011. 121 c. ISBN 1-931624-86-0.
4. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. [**Электронныйресурс**]. – URL: http://www.isaca.org/COBIT/Pages/default.aspx?utm_source= informz-25-January-2013-COBIT-Focus-Vol-1&utm_medium=email&utm_campaign=cobit- focus (**дата обращения**: 24.02.2015).
5. Naryzhnyy K. Cobit 5: model' otsenki protsessov [Elektronnyy resurs]. – URL:http://www.cleverics.ru/ru/subject-field/articles/554-cobit5-pam(dataobrashcheniya: 24.02.2015).
6. Baskakov A.V. Model' zrelosti kak instrument razvitiya protsessa bezopasnosti v organizatsii protsessov [Elektronnyy resurs]. – URL: http://journal.itmane.ru/node/913 (data obrashcheniya: 24.02.2015).