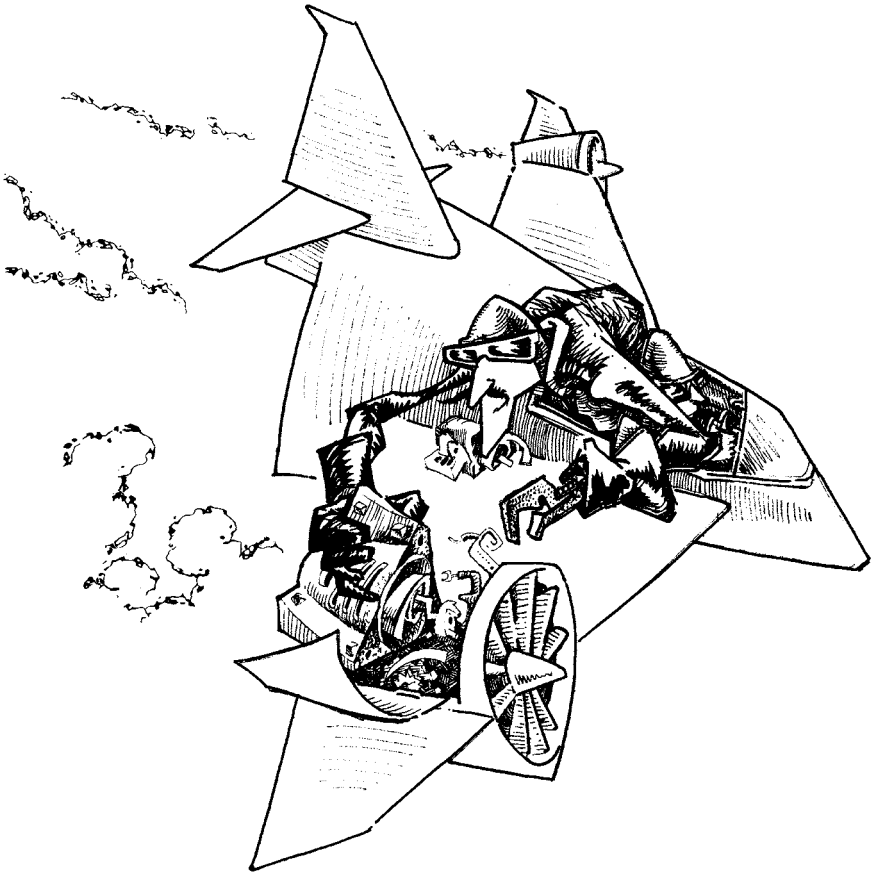
«...Зрелость – это не годы,
а состояние познания самого себя...»
Джон Роберт Фаулз



Обеспечение непрерывности бизнеса

Часть 4. Модель зрелости как инструмент управления совершенствованием непрерывности безопасности бизнеса

Эта статья завершает цикл публикаций на тему «Обеспечение непрерывности бизнеса». В первой статье цикла[1] были проанализированы проблемы применения стандартов, основанных на цикле PDCA, и описана модель управления процессами, опирающаяся на расширение цикла PDCA – цикл SDCA. Во второй статье цикла[2] мы разбирали проблемы стандартов в области непрерывности бизнеса и информационной безопасности, а также дали описание функциональной модели процесса «Управлять непрерывностью безопасности бизнеса». В третьей статье[3] были кратко рассмотрены стандарты де-юре в области информационной безопасности и методики тестирования защищенности предприятия. Подробно описана наиболее полно охватывающая модель тестирования – методика OSSTMM – и приведена декомпозиция блока «Выполнить тестирование внешнего проникновения» функциональной модели, описание которой было начато во второй статье цикла. В заключительной статье серии мы кратко рассмотрим ряд моделей зрелости в области информационной безопасности бизнеса и предложим адаптивную модель зрелости. Фактически в этой части мы определяем методологию управления непрерывностью безопасности бизнеса и комментируем её составляющие.

Владимир Алёшин
Профессор РАНХ и ГС при Президенте РФ.
С ним можно связаться
по e-mail: aleshin_vladimir@mail.ru.

Александр Баскаков
Начальник группы по ИБ ТЦ «Комус»,
выпускник Школы ИТ-менеджмента РАНХ и ГС.
С ним можно связаться
по e-mail: baskav@rbcmail.ru.

Евгений Ёрхов
Генеральный директор «Ай Экс Ай лаборатория
защиты информации», выпускник Школы
ИТ-менеджмента АНХ. С ним можно связаться
по e-mail: yy@ixi.ru.

История развития моделей зрелости

Устоявшегося понятия «зрелость» применительно к системам и процессам в русском языке пока нет. Оно широко используется в биологии, экологии. Мы же будем трактовать термин «зрелость» как полное, состоявшееся развитие той или иной системы, понимая при этом под развитием результат процесса. Для характеристики этого процесса будем использовать термин «совершенствование».

Истоки моделей зрелости во многом лежат в теории стадийности, исходящей из предположения, что «… всякая система (экономическая, социальная и т.д.), развиваясь, проходит определенные стадии, которые

[1]«Обеспечение непрерывности бизнеса. Часть 1. Модель управления процессами». Information Management №2 2013.

[2]«Обеспечение непрерывности бизнеса. Часть 2. Функциональная модель «Управлять непрерывностью безопасности бизнеса». Information Management №3 2013.

[3]«Обеспечение непрерывности бизнеса. Часть 3. Верификация информационной безопасности бизнеса». Information Management №4 2013.

могут быть систематизированы на абстрактном уровне. В соответствии с этой теорией, можно утверждать, что каждая бизнес-система проходит за время своей жизни определенные стадии, независимо от того, когда она начала первую – становление бизнеса. Понимание теории стадийности применительно к управлению компанией может помочь ей сократить путь от становления до зрелости»[4].

Впервые о модели зрелости разработки программного обеспечения (ПО) заговорили в середине 80-х годов XX века, когда возникла острая необходимость повысить качество разрабатываемого ПО, реализовать проекты в условленные сроки с заданными бюджетом и качеством. Другими словами, речь шла о переходе от разработки ПО программистами-одиночками (программистами-«кустарями») к индустриальному производству ПО. В 1987 года Software Engineering Institute (SEI) выпустил краткий обзор процессов разработки ПО с описанием их уровней зрелости, а также опросник, предназначавшийся для выявления в организации тех областей, где необходимы улучшения. Первая версия модели – Capability Maturity Model for Software (CMM) – появилась в 1991 году. Важно отметить, что уже эта модель зрелости базировалась на процессном подходе[5].

В России 90-х годов в силу ряда причин интереса к индустриальному производству ПО практически не было. Это следствие привычки делать всё своими силами и убеждения, что мы сами сделаем лучше, низкого платежеспособного спроса заказчиков и т.д. Вопросам организации процесса создания ПО: планированию, тестированию, взаимодействию участников проекта, управлению конфигурацией – практически не уделялось должного внимания. Затем начали появляться российские программные продукты массового спроса. Управление процессом разработки стало важным фактором бизнеса, появилась необходимость в индустриальном подходе к производству программного обеспечения. Компании, сумевшие усовершенствовать процесс разработки программного обеспечения, использовавшие на практике индустриальный подход к разработке программ и, соответственно, вышедшие на высокие уровни зрелости, начали выигрывать конкурентную борьбу.

По аналогии с моделями зрелости в области промышленной разработки ПО, модели зрелости стали применяться и в других областях (секторах экономики[6]). В 1998 году были приняты первые стандарты ISO, посвященные оценке ПО – ISO/IEC TR 15504:1998 Information Technology – Software Process Assessment. COBIT 3, вышедший в 2000 году, уже содержал модель зрелости. Как инструмент управления модели зрелости получили широкое применение и развитие.

В бизнес-сообществе принят подход, согласно которому в качестве инструмента совершенствования конкурентоспособности организации используется зрелость ее бизнес-процессов

Менеджмент давно осознал, что внедрение и продвижение всего нового в организации должно соответствовать уровню ее организационного, технологического развития и т.д. Нельзя внедрить эффективную современную технологию, если уровень организации не соответствует уровню этой технологии. Практически всегда современные технические средства требуют высочайшего уровня обслуживания. Если персонал в целом не обладает необходимой производственной и корпоративной культурой, то, как правило, оборудование быстро выходит из строя.

Модели зрелости в области ИБ

Не является исключением и внедрение процессов обеспечения безопасности. Требования к реализации мероприятий по безопасности должны формулироваться с учетом уровня зрелости этих процессов в конкретной организации. В качестве

[4]Гантер Р. Методы управления проектированием программного обеспечения. Мир, 1981.

[5]Первая подробная публикация на русском языке, посвященная модели CMM и ISO 15504 «Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем (ISO/IEC TR 15504-CMM)». Книга и бизнес, 2001.

[6]В качестве примера сошлемся на модель зрелости закупок, предложенную компанией KPMG для российского бизнеса.

примера рассмотрим серию стандартов по управлению информационной безопасностью 27xxx. В стандарте ISO 27001:2005 существует требование по наличию в организации процедуры анализа рисков. При реализации требований стандарта в конкретной организации всегда возникает множество вопросов: как выполнить это требование, в каком объеме и на каком уровне детализации для разных по величине компаний. Очень часто менеджеры по безопасности обращают внимание именно на размер организации и практически никогда – на уровень ее организационного и технологического развития. Ответить на этот вопрос помогает модель зрелости. Если уровень зрелости организации низкий, детальная проработка процедуры оценки рисков не имеет смысла – достаточно экспертной оценки рисков и определения приоритетных направлений безопасности. В организациях с высоким уровнем зрелости процессов ИБ процедура оценки рисков должна не только функционировать, но и постоянно совершенствоваться.

Из этого следует, что:

- решение задачи совершенствования управлением непрерывности безопасности бизнеса следует строить на основе модели зрелости;
- при построении модели зрелости необходимо учитывать мировой опыт создания моделей зрелости.

Модели зрелости в области ИБ на западе получили широкое распространение. Для оценки их применимости к российским условиям авторы статьи провели сравнительный анализ нескольких моделей зрелости как в области ИБ, так и ИТ-процессов и бизнес-процессов[7]:

- Open Information Security Management Maturity Model[8] (O-ISM3);
- Enterprise Information Management Maturity Model[9] (EIM MM);
- NISTIR-7358 методология PRISMA[10];
- Community Cyber Security Maturity Model[11] (CCSMM);
- Business Process Management Maturity Model[12] (BPM MM).

Анализ указанных моделей показал, что:

- единой трактовки понятия зрелости нет. Каждая из моделей зрелости разрабатывалась для решения конкретных задач на основе своей модели, которую можно назвать базовой. Например, модель зрелости Open Information Security Management Maturity Model решает вопросы оценки состояния существующих процессов системы управления информационной безопасностью. Хотя она полностью совместима с требованиями стандартов ISO 27001, COBIT, ITIL, но описание лежащей в ее основе базовой модели не приводится;
- применение моделей зрелости предполагает высокий уровень менеджмента в организации. Например, в модели NIST и методологии PRISMA уровни управления названы согласно общей теории стратегического управления и отражают эволюцию управления в организации;
- одним из центральных условий применения моделей является требование развитости и стабильности процессов управления, а также их высокой детализации;
- как правило, в моделях выдвигаются высокие требования к квалификации менеджеров по информационной безопасности;
- все рассмотренные модели не учитывают обеспеченность ресурсами процессов управления информационной безопасности бизнеса, что немаловажно для практического применения в российских условиях;
- наблюдается тенденция построения комплексных моделей зрелости, в которых, помимо уровней зрелости, рассматриваются организационные факторы (например, в модели Business Process Management Maturity Model рассматриваются стратегическая линия, культура и лидерство, персонал, руководство, методики, ИТ). Эти факторы должны сбалансировано развиваться по мере перехода от стадии к стадии.

[7]Все перечисленные ниже модели разработаны и применяются в основном в США. Подробнее смотрите в статье «Модель зрелости как инструмент развития процесса безопасности в организации», Баскаков А. В. http://journal.itmane.ru/node/913.

[8]Разработана консорциумом The Open Group.

[9] Разработана Gartner.

[10]Разработана National Institute of Standards and Technology.

[11]Разработана The Center for Infrastructure Assurance and Security The University of Texas.

[12]Предложена Gartner.

Примечание:
СМЗИ – Система менеджмента защиты информации.

Рис. 8. PDCA-модель системы управления информационной безопасностью, предлагаемая стандартом ISO/IEC 27001:2005.

Адаптивная модель зрелости в области управления напрерывностью безопасности бизнеса

Очевидно, что при построении модели зрелости необходимо использовать базовую модель, адекватную российским условиям. В качестве базовой модели мы воспользуемся функциональной моделью «Управлять непрерывностью безопасности бизнеса», подробное описание которой было приведено в частях 2 и 3 цикла статей. Подчеркнем еще раз, что предложенная нами модель строилась на основе положений стандарта ISO/IEC 27001:2005, но при этом мы внесли ряд дополнений. Обсудим их подробнее.

Базовая модель

На рис. 8 показана модель системы управления информационной безопасностью, предлагаемая стандартом ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management Systems – Requirements[13]. Согласно ей, входом процесса управления информационной безопасностью в стандарте являются требования и ожидаемые результаты в области информационной безопасности, выходом – управляемая информационная безопасность. В соответствии с предложенной нами трактовкой цикла PDCA[14] представленная в стандарте ISO/IEC 27001:2005 модель системы управления информационной безопасностью – это модель стратегического уровня управления.

Какие же трудности вызывает практическое применение указанного стандарта? Во-первых, не понятно, каким образом (с помощью каких механизмов) «требования и ожидаемые результаты в области информационной безопасности» должны быть сформулированы и чем при этом нужно руководствоваться? Кто должен участвовать в этой работе? Каковы роли владельцев бизнеса, руководителя службы ИБ и его подчиненных при формулировании этих требований и ожиданий?

Во-вторых,– и, пожалуй, это самое главное – каким образом в организации должна быть реализована работа по локализации инцидентов, связанных с внешними проникновениями? Каковы должны быть процессы (механизмы) оперативной работы службы ИБ? Фактически в стандарте ISO/IEC 27001:2005 (и идентичном ему ГОСТ Р ИСО/МЭК 27001–2006) отсутствует явное описание процесса регулирования непрерывности безопасности бизнеса. Это, подчеркнем еще раз, является следствием использования только цикла PDCA и игнорирования связанного с ним цикла SDCA.

[13] В 2013 году вышла новая редакция этого стандарта. В России действует стандарт ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», идентичный предыдущей редакции стандарта ISO/IEC 27001:2005.

[14] «Обеспечение непрерывности бизнеса. Часть 1. Модель управления процессами». Information Management №2 2013.

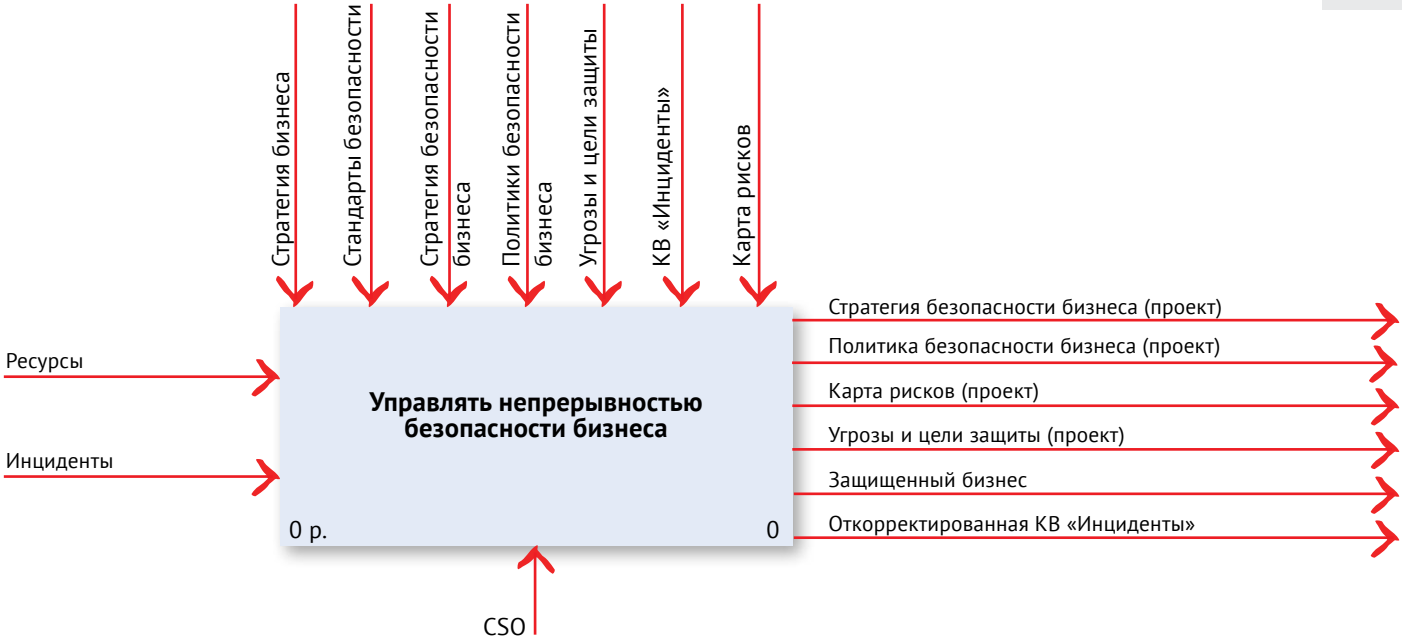


Рис. 9.
Композиционная модель «Управлять непрерывностью безопасности бизнеса» (контекстная диаграмма A-0).

Ответ на эти вопросы дает функциональная модель «Управлять непрерывностью безопасности бизнеса» (рис. 9). В функциональной модели мы расширили границы моделируемой системы. Поясним соображения, которыми мы руководствовались.

Ранее отмечалось, что сформулировать и представить на утверждение владельцу бизнеса (топам компании) требования и ожидаемые результаты в области информационной безопасности в состоянии только специалисты по ИБ организации во главе с CSO. В этой связи в нашей модели одним из входов являются «ресурсы». Эти ресурсы необходимы для формулирования требований и ожидаемых результатов в области информационной безопасности. В силу российской специфики данное требование представляется нам необходимым. Другим входом, который мы рассмотрели, является вход «инциденты». Это следствие нашего желания расширить модель за счет описания процессов, реализующих оперативную работу по защите бизнеса.

Следующим отличием нашей модели от модели системы управления информационной безопасностью, описанной в ISO/IEC 27001:2005, является то, что в качестве выходов модели мы определили «защищенный бизнес» и «откорректированную базу данных «Инциденты»[15] (рис. 9). Включение первого из них указывает на то, что мы не только описываем процессы создания системы управления информационной безопасностью, но и детализируем процессы обеспечения непрерывности безопасности бизнеса.

Процесс «Управлять непрерывностью безопасности бизнеса» должен быть одним из процессов управления организацией. Его основной результат – «Защищенный бизнес». Другие результаты процесса интегрируются в смежные процессы управления организацией либо в качестве управляющих воздействий, либо в качестве входов (исходных материалов для работы других управленческих процессов):

- «Стратегия безопасности бизнеса» должна использоваться в совокупности с другими стратегиями бизнеса, такими как маркетинговая, производственная, человеческого капитала и т.п., детализирующими рыночную стратегию организации. На их основе организация выстраивает свою систему стратегического управления;
- «Политики безопасности» используются в качестве управляющих воздействий и исходного материала для работы в процессах управления инфраструктурой, в процессах управления персоналом;
- «Карта рисков»/«Угрозы и цели защиты» используется в процессах управления рисками организации;
- «Откорректированная база знаний об инцидентах и сценариях атак» интегрируется в систему управления знаниями в области управления ИТ-услугами[16] на основе подходов и практик ITIL/ITSM. Информация об инцидентах и защищенности систем необходима для процессов «Управление инцидентами», «Управление проблемами», «Управление изменениями», «Управление релизами» и «Управление конфигурациями».

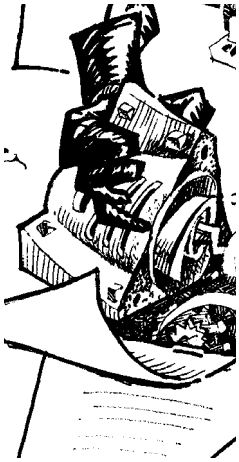
Рис. 10. Модель оценки зрелости процессов безопасности бизнеса.

Назначение адаптивной модели зрелости

Адаптивная модель зрелости организаций в области непрерывности бизнеса и его информационной безопасности предназначена для:

- понимания понятия «зрелость» как инструмента совершенствования непрерывности безопасности бизнеса;
- комплексной оценки организационного и технологического уровней развития бизнеса с точки зрения его непрерывности и информационной безопасности;
- понимания того, что нужно сделать для совершенствования процесса «Управлять непрерывностью безопасности бизнеса» в своей организации.

Описание адаптивной модели зрелости



В бизнес-сообществе принят подход, согласно которому в качестве инструмента совершенствования конкурентоспособности организации используется зрелость ее бизнес-процессов. Модели зрелости помогают бизнесу выполнять бенчмаркинг, сравнивая свои показатели с показателями других подобных организаций. Очевидно, что для такого сравнения необходима широкая информационная база, созданием которой занимаются ведущие мировые консалтинговые компании. Однако, по понятным причинам организации не открывают свои процессы в области ИБ. В этой связи, адаптивная модель зрелости может помочь при проведении одного из вариантов внутреннего бенчмаркинга, состоящего в сравнении своих же показателей на предыдущих этапах развития организации.

Предлагаемая адаптивная модель зрелости процессов безопасности бизнеса включает два направления оценки базового процесса «Управлять непрерывностью безопасности бизнеса»:

1. **Оценка обеспеченности условиями, необходимыми для внедрения базового процесса.**
2. **Оценка подпроцессов базового процесса.**

Как правило, при построении моделей зрелости в качестве шкал используют словесные оценки. Далее мы будем использовать 5–6 бальную шкалу словесных оценок, руководствуясь традиционным инженерным подходом: «Настолько точно, насколько надо; настолько грубо, насколько можно». Схематически модель зрелости показана на рис. 10. Обращаем внимание на то, что при оценке зрелости подпроцессов базовой модели используется одна и та же шкала зрелости, при оценке же обеспеченности условиями, не-

обходимыми для внедрения базового процесса, для каждого из используемых атрибутов используется своя шкала зрелости. Рассмотрим элементы модели зрелости более подробно.

1. **Оценка обеспеченности условиями, необходимыми для внедрения базового процесса.** По этому направлению (измерению[17]) состояние обеспеченности условиями, необходимыми для внедрения базового процесса, характеризуется по пяти атрибутам:
   - **Стратегия бизнеса.** Вводя этот атрибут, мы хотим подчеркнуть, что ИБ организации должна обеспечивать стратегию бизнеса путем ее детализации в виде стратегии ИБ. Говоря о стратегии ИБ, нужно иметь в виду необходимость ее разработки, превращения (через политики ИБ) в рабочий инструмент организации и постоянное совершенствование в соответствии с изменением рыночной стратегии организации и возникающими угрозами.
   - **Выделение ресурсов на ИБ.** Этот атрибут нам представляется особо значимым для российского бизнеса. Его введение указывает, что необходимы ресурсы на обеспечение ИБ организации и на создание процессов, их поддержание и совершенствование. Немаловажно учитывать регулярность выделения ресурсов и формирования в виде отдельного бюджета или в составе бюджета ИТ.
   - **Учет инцидентов ИБ.** При введении этого атрибута мы полагали необходимым подчеркнуть то, как организация работает с инцидентами, а именно: как они фиксируются, ведется ли и как учет инцидентов по ИБ, как они влияют на совершенствование процесса управления непрерывностью безопасности бизнеса (эскалация).
   - **Распределение ролей и ответственности за ИБ.** Вводя этот атрибут, мы хотим указать на важность рассмотрения того, как определяются роли. Не менее важно как распределены роли «разработчика стратегии и политики ИБ», «аналитика по оценки рисков», «специалиста по развертыванию контрмер», «тестировщика контрмер».
   - **Учет стандартов в области ИБ.** При введении этого атрибута мы полагали необходимым подчеркнуть то, как в организации ведется работа по изучению, применению стандартов по ИБ, как проводится аттестация на соответствие требованиям стандартов. Кроме того, учитывается работа как с «базовыми» стандартами (например, ISO/IEC 27001), так и с отраслевыми (например, PCI DSS).

[17]Измерение – процедура присвоения символов наблюдаемым объектам в соответствии с некоторым правилом. Новейший философский словарь, 2009.

Даже если в организации уже функционируют ряд подпроцессов по обеспечению непрерывности бизнеса, но в то же время нет условий, необходимых для базового процесса, то полноценное управление непрерывностью бизнеса невозможно

Как указывалось выше, для оценки каждого из атрибутов используем 5-бальную шкалу словесных оценок от 1 до 5. Описание уровней оценки для описанных атрибутов приведено в таблице 5.

На рис. 11 в качестве примера представлена диаграмма уровней зрелости для направления «Оценка обеспеченности условиями, необходимыми для внедрения базового процесса» некоей гипотетической организации. Из рисунка следует, что уровень ее зрелости по атрибуту «Стратегия бизнеса» равен 1. По атрибутам «Выделение ресурсов на ИБ», «Распределение ролей и ответственности за ИБ» и «Учет стандартов в области ИБ» равен 2, а по атрибуту «Учет инцидентов ИБ» равен 3. В предлагаемой модели зрелость организации в целом определяется по тому атрибуту, который имеет наименьший уровень. Т.е. уровень зрелости этой гипотетической компании по направлению «Обеспеченность условиями, необходимыми для внедрения процесса» равен 1.

Уровни зрелости / Атрибуты	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5
Стратегия бизнеса	Стратегия бизнеса отсутствует или ее нет в виде документа	Стратегия бизнеса есть, но не считается необходимым разрабатывать стратегию безопасности бизнеса	Стратегия бизнеса определяет ИБ как центр затрат	Стратегия бизнеса определяет ИБ как одну из функциональных стратегий	Стратегия бизнеса учитывает необходимость управлять и совершенствовать непрерывность бизнеса
Выделение ресурсов на ИБ	Выделять какие-либо ресурсы не признается необходимым	Ресурсы на ИБ выделяются хаотично, на основе информации, получаемой владельцем бизнеса	Ресурсы на ИБ выделяются только на поддержание функционирующих систем ИБ. Бюджет на ИБ отдельно не формируется, а входит в состав бюджета ИТ	Ресурсы на ИБ выделяются в соответствии со стратегией ИБ, но не на регулярной основе. Бюджет на ИБ отдельно не формируется, а входит в состав бюджета ИТ	Ресурсы на ИБ выделяются на регулярной ежегодной основе в соответствии со стратегией бизнеса. Бюджет на ИБ формируется отдельно
Учет инцидентов ИБ	Вести учет инцидентов ИБ не признается необходимым	Фиксирование инцидентов ИБ существует на нерегулярной основе, инциденты не влияют на изменение процесса управления непрерывностью бизнеса	Учет инцидентов ИБ ведется в созданной БД, влияние на изменение процесса управления непрерывностью бизнеса инциденты не оказывают	Учет инцидентов ИБ ведется в БД, как основа для выработки контрмер	Учет инцидентов ведется. Если зафиксированный инцидент ИБ не был отражен развернутыми контрмерами, то он запускает механизм обратной связи, который может изменить весь процесс управления непрерывностью бизнеса*
Распределение ролей и ответственности за ИБ	Отсутствует	За ИБ ответственно одно лицо, на которого возложена ответственность за все вопросы по обеспечению непрерывностью бизнеса	Выделенного подразделения ИБ нет, но есть рабочая группа, положение о которой задокументировано. В составе рабочей группы есть ответственные лица и распределены роли в области ИБ	Есть выделенное подразделение по ИБ. Есть ответственные лица и распределены роли в области ИБ	Сформировано выделенное подразделение по ИБ или рабочая группа, положение о которой задокументировано, в ней участвуют выделенные специалисты со специализацией по требуемым направлениям ИБ
Учет стандартов в области ИБ	Отсутствует	Стандарты в области ИБ изучаются частично (не в полной мере), применяются только основополагающие (ISO 27001). Аттестация на соответствие требованиям стандартов не проводится	Изучаются и применяются только основополагающие стандарты в области ИБ (ISO 27001) или только отраслевые (например, СТО БР ИББС). Аттестация на соответствие требованиям стандартов не проводится	Применяются не только основополагающие или отраслевые, но и другие стандарты в области ИБ (например, 27002, 27005). Аттестация на соответствие требованиям стандартов проводится нерегулярно	Применяются не только основополагающие или отраслевые, но и другие стандарты в области ИБ (например, ISO 27002, ISO 27005). Аттестация на соответствие требованиям стандартов проводится регулярно.

Таблица 5. Атрибуты и уровни зрелости направления «Обеспеченность условиями, необходимыми для внедрения процесса».

** Т.е. его выходом является запрос на эскалацию инцидента для выработки управляющего воздействия на процесс управления контрмерами и возможно далее наверх.*

2. **Оценка подпроцессов базового процесса.** Отталкиваясь от идей модели зрелости Capability Maturity Model for Software (CMM), выделим процессы базовой модели «Управлять непрерывностью безопасности бизнеса», зрелость которых необходимо оценивать. В этом качестве будут выступать подпроцессы:
   - «Определять стратегию, политики безопасности»;
   - «Определять угрозы, цели защиты, карту рисков»;
   - «Управлять механизмами контроля»;
   - «Регулировать обеспечение непрерывности безопасности бизнеса».

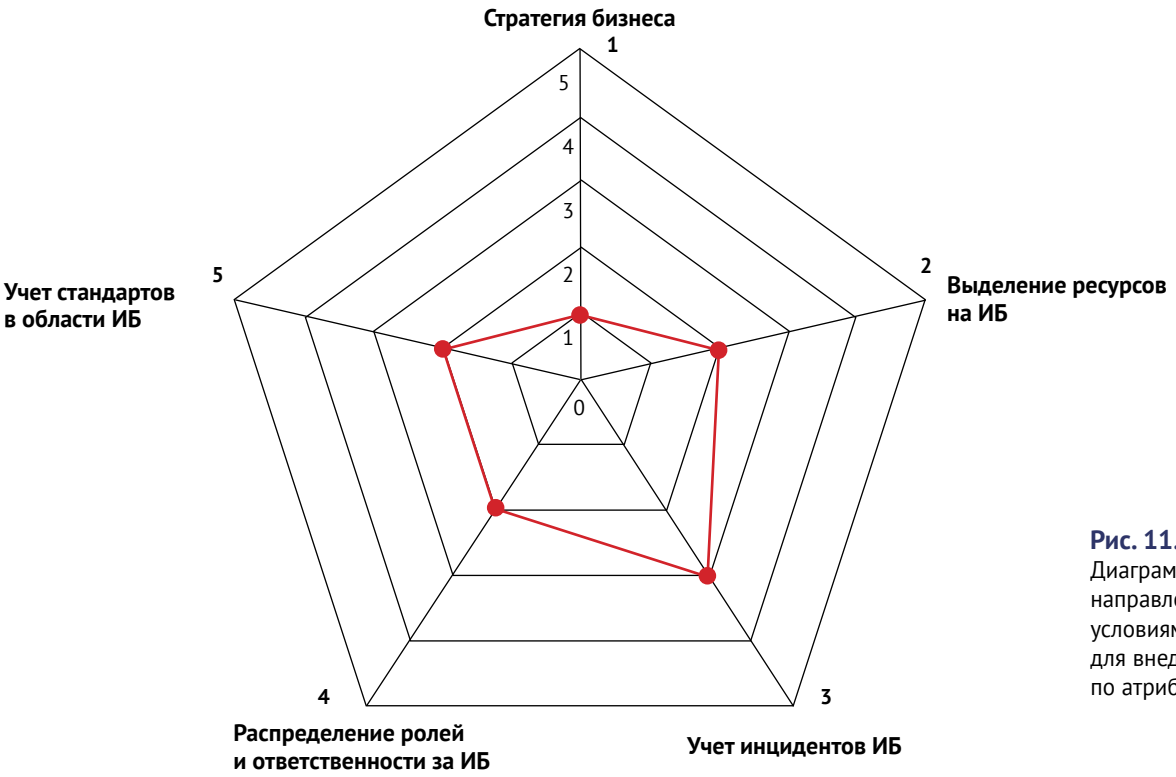


Рис. 11.
Диаграмма уровней зрелости направления «Обеспеченность условиями, необходимыми для внедрения процесса» по атрибутам.

Следуя техническому отчету ISO/IEC TR 15504[18] будем характеризовать зрелость процесса или подпроцесса набором атрибутов, совместно дающих возможность реализовать его значительно лучше. Для оценки зрелости каждого атрибута будем использовать 6-бальную шкалу словесных оценок от 0 до 5:

- Уровень 0: Неполный (Incomplete);
- Уровень 1: Выполняемый (Performed);
- Уровень 2: Управляемый (Managed);
- Уровень 3: Устоявшийся (Established);
- Уровень 4: Предсказуемый (Predictable);
- Уровень 5: Оптимизируемый (Optimizing).

[18]ГОСТ Р ИСО-МЭК 15504-1-2009 «Информационные технологии. Оценка процессов. Часть 1. Концепция и словарь». Является частью серии стандартов ИСО/МЭК 15504.

Методика применения адаптивной модели зрелости

Оценка зрелости организации будет состоять из определения значений зрелости по двум указанным направлениям. Понимание этих значений позволяет понять текущее состояние обеспеченности условиями, необходимыми для внедрения процесса и степень реализации подпроцессов.

Важно понимать, что без обеспеченности необходимыми условиями говорить о полноценном управлении процессом обеспечения непрерывности бизнеса невозможно. Даже если в организации уже функционируют ряд подпроцессов по обеспечению непрерывности бизнеса, но в то же время нет условий (ресурсного обеспечения), то невозможно полноценное управление базовым процессом. И нет гарантий того, что подпроцессы базового процесса будут совершенствоваться в соответствии с изменяющимися условиями. Демонстрация этих диспропорций руководителям бизнеса или его владельцам формирует понимание необходимости изменений в отстающих направлениях.

Модель зрелости процесса «Управлять непрерывностью безопасности бизнеса» производится по двум направлениям (измерениям): оценка обеспеченности условиями, необходимыми для внедрения процесса и оценка подпроцессов базового процесса

Определив текущее состояние обеспеченности условиями, необходимыми для внедрения процесса, следует сформировать план по развитию отстающих атрибутов направления, как минимум, до следующего уровня. Затем, необходимо разработать план и мероприятия по выравниванию атрибутов до общего уровня. Для подпроцессов после определения уровня их зрелости действует тот же принцип: «сначала работаем с элементами с минимальной оценкой, а затем развиваем остальные». Такой подход гарантирует баланс развития всех составляющих процесса.

Таким образом, по мнению авторов, формируется комплексный подход в управлении непрерывностью безопасности бизнеса. Это позволяет не только заложить основу для создания управляемого процесса, но и представляет инструмент для принятия соответствующих решений по корректировке уже созданного процесса или объединения отдельных внедренных практик в единый процесс.

Заключение

Итак, мы завершили цикл статей «Обеспечение непрерывности бизнеса». Мы предложили методологию управления непрерывностью безопасности бизнеса. В завершении статьи еще раз перечислим компоненты методологии, которые лежат в ее основе:

1. модель управления процессами, включающая:
   - модель взаимосвязи циклов PDCA & SDCA (модели стратегического и оперативного управлений);
   - модель ролевого распределения в циклах PDCA & SDCA;
2. стандарты управления ИБ серии ISO/IEC 27xxx;
3. стандарты тестирования защищенности OSSTMM[19] и PTES[20];
4. функциональная модель «Управлять непрерывностью безопасности бизнеса», построенная в соответствии с методологией функционального моделирования IDEF0[21];
5. методология применения системы тестов OSSTMM;
6. адаптивная модель зрелости организаций в области непрерывности бизнеса и его информационной безопасности;
7. методика применения адаптивной модели зрелости.

[19]Open Source Security Testing Methodology Manual (OSSTMM) v.3. http://www.osstmm.org.

[20]Penetration Test Execution Standard (PTES). http://www.pentest-standard.org.

[21]ISO/IEC/IEEE 31320 - 1:2012 «Информационные технологии. Языки моделирования. Часть 1. Синтаксис и семантика для IDEF0. Методология функционального моделирования IDEF0». С 2001 года в РФ действуют рекомендации по стандартизации Р 50.1.028-2001 «Информационные технологии поддержки жизненного цикла продукции методология функционального моделирования».