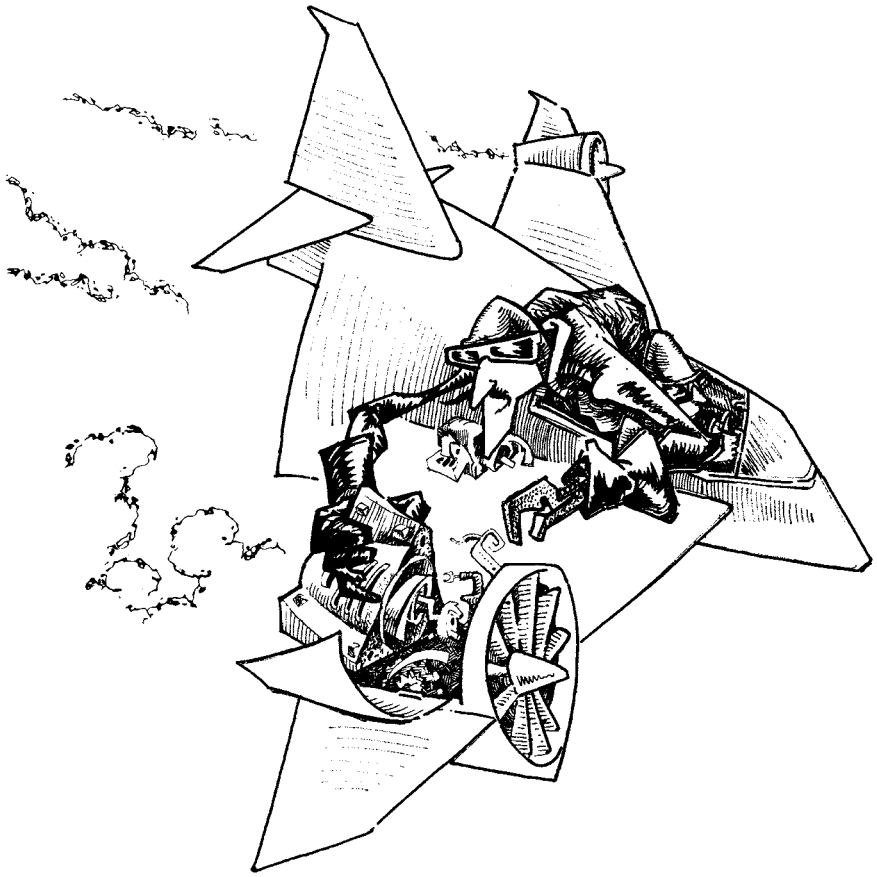
Тот, кто не закладывает фундамент изначально, может огромными усилиями сделать это затем... Но с большой сложностью для архитектора и опасностью для строения.
Никколо Макиавелли



Обеспечение непрерывности бизнеса

Часть 2. Функциональная модель «Управлять непрерывностью безопасности бизнеса»

В первой статье цикла «Обеспечение непрерывности бизнеса»[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 описаны проблемы стандартов в области непрерывности бизнеса и информационной безопасности, а также дано описание функциональной модели «Управлять непрерывностью безопасности бизнеса». Используемая нами формулировка моделируемого процесса требует развернутых пояснений и обоснования.

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».
С ним можно связаться по e-mail: baskav@rbcmail.ru.

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

Рост требований к системе управления информационной безопасностью

В условиях обострения конкуренции и при многочисленных фактах информационных утечек бизнес все больше зависит от качества процесса обеспечения безопасности. В любой отрасли любого масштаба бизнес может столкнуться с самыми различными инцидентами. Об остроте ситуации можно судить по описанным ниже инцидентам, корректирующими действиями которых занимались авторы статьи.

Инцидент 1. Нефтедобывающая компания имеет договор подряда на оказание услуг по доработке системы отслеживания технологического процесса в АСУ ТП с разработчиками мнемосхем. Сотрудники подрядчика находятся на площадке компании в операторском центре. Доработка мнемосхем осуществляется на ноутбуках сотрудников подрядчика, ноутбуки не подключены к технологической сети АСУ ТП. Перенос доработок осуществляется с помощью USB-накопителя через инженерную станцию АСУ ТП. Сотрудники подрядчика организовали выход в Интернет со своих ноутбуков через GSM-модемы. Не озаботившись обновлением антивирусных баз, они заразили собственный USB-накопитель вирусом. Далее через указанный накопитель зараженные файлы попали на инженерную станцию АСУ ТП. Вирус проник в компьютеры операторской смены. При этом в нефтедобывающей компании функционировала «Политика обращения с мобильными носителями информации». Были организованы «Процесс постоянно контроля оказания услуг третьей стороной», «Процесс проверки новых разработок», «Процесс подключения третьих лиц к сети компании», где прописан запрет на использование GSM-модемов без согласования со службой безопасности. А сама компания имела действующий сертификат о соответствии требованиям стандарта ISO 27001:2005.

[1]Часть 1. Модель управления процессами. Information Management №2 2013.

В первой статье цикла фотографии авторов были перепутаны по вине редакции. Приносим свои извинения.

Инцидент 2. Вертикально интегрированный холдинг пищевой промышленности. Бухгалтер, работающий с клиент-банком, заходит на сайт, посвященный изготовлению кулинарных изделий в домашних условиях. Сайт содержит ряд баннеров, один из которых представляет собой фрагмент HTML-кода, зараженного вирусом типа Dropper. Вирус подкачивает основной модуль в рабочую станцию и определяет наличие программного обеспечения клиент-банк. Уже на следующий день зафиксирована попытка вывода 500 тыс. руб. через зараженный компьютер. Следы вируса вели в одну из стран Восточной Европы.

Инцидент 3. Крупный телеком-оператор, работающий на территории всей России и сертифицированный по ISO 27001. Технологическая сеть содержит тысячи систем и считается очень хорошо защищенной. В результате действий внутреннего злоумышленника, имевшего доступ к офисной сети, недостаточно проработанных механизмов разграничения доступа, а также использования администраторами технологической сети небезопасных методов управления ИТ–инфраструктурой, большая часть систем технологической сети была скомпрометирована.

Один из ключевых выводов, который можно сделать из приведенных примеров:

Время от момента проникновения злоумышленника в бизнес до момента выполнения опасных для бизнеса действий существенно сокращается и в дальнейшем будет только сокращаться.

Обоснованием этой тенденции служит рост в Интернете числа сайтов, размещающих на своих страницах не только методики проникновения, но и инструментальные (программные) средства для реализации проникновения. Следствием этого становится, с одной стороны, понижение требований к квалификации злоумышленников, с другой – их количественный рост. По нашему мнению, можно говорить о новой тенденции: через эти сайты готовят новых членов для криминальных структур (из числа хакеров-самоучек). Цель – извлечение прибыли от нарушений безопасности. А в части промышленных систем речь идет и о целенаправленных атаках для влияния в масштабе страны. Серьезные атаки нацелены на серьезный бизнес [2].

Даже если существуют внедренные процедуры обеспечения безопасности, без их постоянного совершенствования и регулирования нельзя гарантировать, что они сработают в нужный момент

Другой вывод из приведенных примеров – даже если уже существуют внедренные процедуры обеспечения безопасности, без их постоянного совершенствования и регулирования нельзя гарантировать, что они сработают в нужный момент. **Со временем технологии атак совершенствуются, а уровень зашиты деградирует.**

Учитывая зависимость как бизнеса, так и государственных структур от качества и целостности информации, используемых автоматизированных систем, грамотная организация защиты приобретает важное значение и заставляет говорить о том, что обеспечение информационной безопасности нужно рассматривать как непрерывный процесс.

Это выдвигает серьезные требования к системе управления информационной безопасностью, она должна выстраиваться на основе целостного системного подхода. Стандарты информационной безопасности, о которых говорилось выше, идут во многом от ИТ, от реакции на прошедшие инциденты (в стандартах подчеркивается, что они разработаны специалистами-практиками). Нам представляется, что этап первоначального накопления проблем и знаний в этой области заканчивается.

[2] В качестве примеров можно указать на вирусы, специально разработанные под заказ: Stuxnet, Duqu, Flame…

Обеспечение информационной безопасности как составляющая часть непрерывности бизнеса

Информационная безопасность – один из элементов, от которого зависит бизнес, его устойчивость и непрерывность.

Business Continuity Management (BCM) – целостный процесс управления, в рамках которого идентифицируются потенциальные угрозы деятельности организации, def оцениваются возможные воздействия на бизнес-операции в случае осуществления этих угроз, а также создается основа для обеспечения способности организации восстанавливать свою деятельность и эффективно реагировать на инциденты, что гарантирует соблюдение интересов заинтересованных сторон, обеспечивает защиту репутации, бренда и создающих стоимость операций[3].

Однако, управление информационной безопасностью до самого последнего времени (до появления стандарта ISO/IEC 27031:2011[4]) рассматривалось в отрыве от управления непрерывностью бизнеса. Одним из первых исключений был стандарт по информационной безопасности в банковской сфере[5]. В него включен пункт, рассматривающий информационную безопасность во взаимосвязи с управлением непрерывностью бизнеса (9.6. «Обеспечение непрерывности бизнеса (деятельности) и восстановление после прерываний»)[6].

Совершенствование механизмов, инструментов и стандартов обеспечения непрерывности бизнеса и информационной безопасности развивается интенсивно. Это отразилось в появлении большого количества стандартов, посвященных управлению непрерывностью бизнеса, где бизнес рассматривается как первооснова. Один из наиболее известных стандартов в этой области – британский BS 25999[7]. В книге «Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться» авторы (Петренко С.А. и Беляев А.В.) указывают, что: «**... основной целью BCM является поддержание в актуальном состоянии достаточного количества структур, операций и ресурсов (активов), необходимых для стабильного функционирования организации в чрезвычайных ситуациях. Данное представление BCM существенно отличается от понятия аварийного восстановления после катастрофы, которое тесно, если не исключительно, связывается с информационными технологиями.** Сегодня фокус внимания концепции непрерывности смещается на организацию в целом, на критически важные для бизнеса процессы, расширяя горизонты прежнего рассмотрения проблемы **за пределы исключительно информационных систем**, несмотря на их важность для современных компаний»[8].

По данным Стивена Росса, приведенным в книге Петренко С.А. и Беляева А.В., системы управления информационной безопасностью являются одними из самых эффективных инструментов (рис. 1). Однако проблема в том, что этот инструмент требует больших затрат.

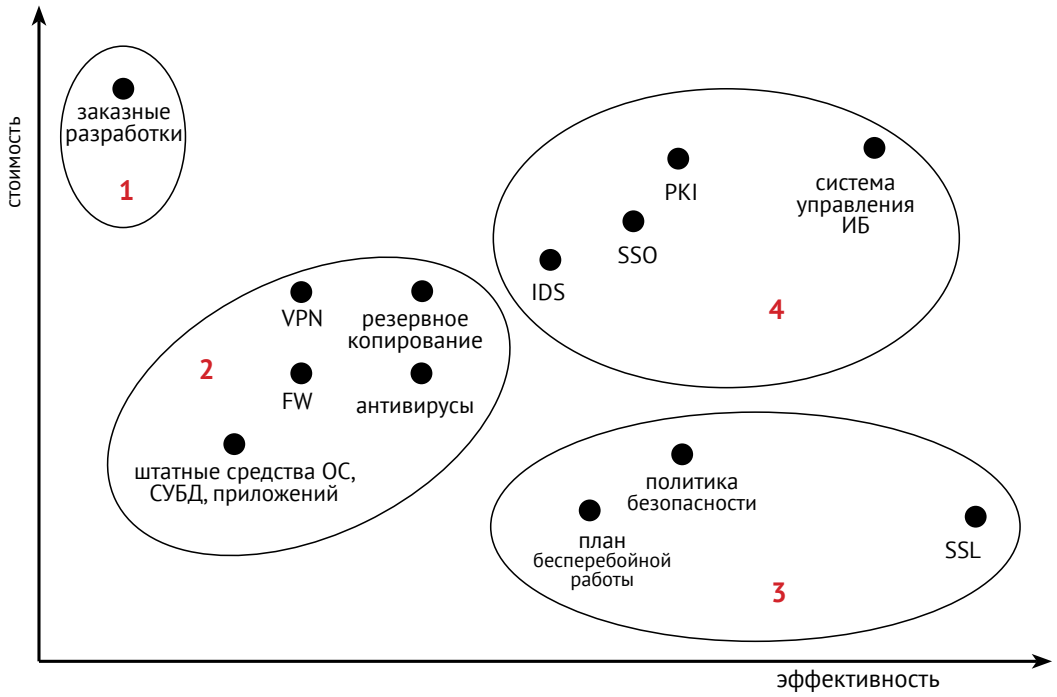


Рис. 1. Оценка эффективности/цены решения в области BCM.

[3]Мусатов К. Непрерывность бизнеса. Подходы и решения. Jet Info N 5, 2007.

[4]ISO/IEC 27031:2011 Информационные технологии. Методы обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий для обеспечения непрерывности бизнеса.

[5]Стандарт Банка России СТО БР ИББС-1.0–2006 Обеспечение информационной безопасности организаций банковской системы Российской Федерации (вступил в действие 01.01.2006).

[6]Нужно подчеркнуть, что в стандарте 27001 есть раздел, где говорится о непрерывности бизнеса.

[7]Стандарт BS 25999 состоит из двух частей:
- BS 25999-1:2006. Code of Practice (Часть 1: Кодекс лучших практик);
- BS 25999-2:2007. Specification. (Часть 2: Спецификации системы BCM).

[8]Петренко С.А., Беляев А.В. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров. ДМК Пресс, Компания АйТи, 2011.

Рис. 2. Жизненный цикл BCM[9].

Сказанное выше указывает на необходимость начать движение в сторону сближения управления информационной безопасностью и управления непрерывностью бизнеса. Это нашло отражение в появлении стандарта ISO/IEC 27031:2011. Однако, он был опубликован совсем недавно – лишь в апреле 2012 года. Тогда как один из наиболее известных стандартов в области управления непрерывностью бизнеса – BS 25999. Поэтому рассмотрим кратко его положительные и отрицательные аспекты.

[9]Мусатов К. Непрерывность бизнеса. Подходы и решения. Jet Info N 5, 2007.

Проблема трактовки и использования понятия жизненного цикла в стандарте BS 25999

Как отмечалось выше, стандарт BS 25999 можно трактовать как стандарт, ориентированный на бизнес. Подтверждением тому служит требование внедрения BCM в культуру организации, предполагающее понимание потребностей бизнеса в части обеспечения его непрерывности. Важными чертами стандарта являются построение системы управления общими рисками организации, постоянное совершенствование BCM, проведение учений, аудит и т.д. В отличие от стандартов по ИБ и других стандартов ISO, в стандарте BS 25999 не ограничились циклом PDCA, а ввели две важные составляющие: обратную связь от цикла PDCA, указывающую на необходимость совершенствования управления непрерывностью бизнеса, и жизненный цикл BCM (рис. 2).

Анализируя рис. 2, важно заметить явное указание на необходимость анализа организации (т.о. все построения определяются бизнесом) и определение стратегии обеспечения непрерывности бизнеса, которая должна строиться на основании стратегии бизнеса. Петренко С.А. и Беляев А.В. особо подчеркивают, что:

def **...под управлением непрерывностью бизнеса понимается системный процесс оценки текущего уровня зрелости компании в области непрерывности бизнеса и его приведение к более зрелому уровню, в соответствии с целями и задачами бизнеса.**

Если первый компонент сомнений не вызывает, а наоборот, подчеркивает выводы, сделанные в первой части нашей статьи, то корректность использование понятия «жизненный цикл» сомнительна. Поясним нашу мысль.

Совокупность процессов и этапов развития организмов живой природы, технических систем, продуктов производства от момента зарождения или появления потребности их создания и использования до прекращения функционирования или применения принято называть жизненным циклом[10]. Близкое по смыслу определение жизненного цикла системы дается в ГОСТ Р ИСО/МЭК 15288:2005:

def **Жизненный цикл – развитие рассматриваемой системы во времени, начиная от замысла и заканчивая списанием.**

В NATO CALS Handbook[11] жизненный цикл (life-cycle) определяется аналогично: «Life-cycle in this context covers concept, design/develop, build, maintain, and dispose of a defense system (DS)». Другими словами, жизненный цикл ограничен во времени.

В результате почти 20-летнего периода развития рынков и технологий термин Product Lifecycle Management (PLM)[12] стал применяться для обозначения процесса управления полным циклом изделия – от его концепции, через проектирование и производство до продаж, послепродажного обслуживания и утилизации. Важно подчеркнуть, что эта методология – одно из центральных направлений развития управления бизнесом. Таким образом, методология PLM и инструментальные средства, поддерживающие ее, вступают в противоречие со стандартом BS 25999. Как это несоответствие можно решить на уровне одной компании? Решать эту проблему придется, ибо первичен именно бизнес, но не подход BCM и тем более не его жизненный цикл.

Нам представляется, что приведенных примеров более чем достаточно для понимания причин нашего принципиального несогласия с использованием в стандарте BS 25999 понятия жизненный цикл BCM. Зачем же оно понадобилось? Полагаем, что введение данного понятия – попытка решить проблему построения системы управления непрерывностью бизнеса, базируясь только на цикле PDCA. Слова Никколо Макиавелли (использованные Петренко С.А. и Беляевым А.В. в качестве эпиграфа) хорошо проиллюстрируют и нашу трактовку взаимосвязи циклов PDCA и SDCA при построении системы управления:

> **Тот, кто не закладывает фундамент изначально, может огромными усилиями сделать это затем... Но с большой сложностью для архитектора и опасностью для строения.**

Функциональная модель «Управлять непрерывностью безопасности бизнеса»

Перейдем к описанию функциональной модели. В данной версии модели мы подчеркиваем необходимость анализа организации и определения стратегии информационной безопасности, которая должна строиться на основе стратегии организации. Разработка же политик информационной безопасности должна строиться на основе стратегии. Вместе с тем в данной версии модели мы не коснемся вопроса восстановления деятельности организации после серьезного инцидента, оставаясь в этом смысле в рамках стандартов серии ISO 2700X.

Введение понятия «жизненный цикл BCM» в стандарте BS 25999 – это попытка решить проблему построения системы управления непрерывностью бизнеса, базируясь только на цикле PDCA

Ключевым условием, которым нужно руководствоваться при чтении функциональной модели, является отказ от причинно-следственного мышления. Необходимо исходить из следующей трактовки как модели, так и каждого из ее блоков: что нужно иметь на входе для того, чтобы получить требуемый результат на выходе, чем при этом нужно руководствоваться и что является механизмом, посредством которого получается требуемый результат. Другими словами:

> **Вход (I) при наличии управления (C) преобразуется в выход (O) посредством (при помощи) механизма (исполнителя) (M)[13].**

[10] Толковый словарь по вычислительным системам. М.: Машиностроение, 1990, Липаев В.В. Программная инженерия. Методологические основы. Курс лекций. М.: Теис, 2006.

[11] NATO CALS Handbook. Ver. 2, June 2000.

[12] PLM - это стратегия ведения бизнеса на основе системных бизнес-решений, поддерживающих коллективную разработку, управление, распространение и использование информации о спецификации изделия в рамках расширенного предприятия от концепции до конца жизненного цикла изделия; PLM обеспечивает интеграцию персонала, производственных процессов, бизнес-систем и информации. http://www.cimdata.com, http://plmpedia.ru

[13] Марка Д., МакГоуэн К. Методология структурного анализа и проектирования.М.: МетаТехнология, 1993.

Если при этом некоторый вход одновременно является и управляющими воздействиями, то в соответствии со стандартом IDEF0 мы показываем его только как управление.

1. **Цель моделирования и точка зрения.**

   Цель моделирования: формализовать и описать процесс обеспечения непрерывности безопасности бизнеса, понять функции участников этого процесса и их роли для того, чтобы в дальнейшем использовать эту модель в качестве референсной.

   Точка зрения. Модель строилась с точки зрения владельца бизнеса[14], который:
   - определяет стратегию бизнеса;
   - утверждает проект стратегии ИБ;
   - утверждает проект политик (и) ИБ;
   - утверждает проект угроз и целей защиты;
   - утверждает проект карты рисков;
   - выделяет ресурсы на обеспечение этой стратегии;
   - назначает владельца процесса.

2. **Композиционная диаграмма[15].**

   Входы (I) модели:
   - ресурсы[16];
   - инциденты.

   Управляющие воздействия (C):
   - стратегия бизнеса;
   - стратегия безопасности бизнеса;
   - стандарты безопасности;
   - политики безопасности бизнеса;
   - угрозы и цели защиты;
   - база данных «Инциденты»;
   - карта рисков.

   Выходы (O):
   - стратегия информационной безопасности бизнеса (проект);
   - политика (и) безопасности бизнеса (проект);
   - карта рисков (проект);
   - угрозы и цели защиты (проект);
   - откорректированная база данных «Инциденты»;
   - защищенный бизнес (как конечный результат).

   В качестве механизма (исполнителя) выступает CSO.

3. **Общие замечания.** По композиционной диаграмме A0 нужно сделать следующие замечания:
   - В стандарте ISO/IEC 27001:2005 входом процесса являются требования и ожидаемые результаты в области информационной безопасности. По нашему мнению, сформулировать и представить на утверждение владельцу бизнеса (топам компании) требования и ожидаемые результаты в области информационной безопасности в состоянии только специалисты по ИБ во главе с CSO. В этой связи в нашей модели одним из входов являются ресурсы, выделяемые для управления непрерывностью безопасности бизнеса. Другим входом – инциденты, так как важно явно показать, каким образом реализуется непрерывность безопасности бизнеса.
   - Выходами процесса являются проекты документов, утверждать которые должен владелец бизнеса как постановщик задачи и владелец выделяемых ресурсов. Мы исходим из того, что CSO не может нести ответственность за бизнес. Это полностью соответствует требованию п. 1.2 стандарта ISO/IEC 27001:2005:

Подпроцесс «Регулировать обеспечение непрерывности безопасности бизнеса» (блок A4) реализует цикл SDCA

[14]Из приведенного ниже описания понятно, что означает участие высшего руководства в процессе управления непрерывностью безопасности бизнеса. Вопрос же собственно утверждения указанных проектов ниже проектов документов по управлению непрерывностью информационной безопасности остается вне рамок нашей модели. Вне рамок модели и стратегия бизнеса, выделение ресурсов (временных, финансовых, людских) и назначение владельца процесса.

[15]В статье мы не приводим рисунок композиционной диаграммы по той причине, что все элементы представлены на декомпозиционной диаграмме A0.

[16]Временные, финансовые, людские.

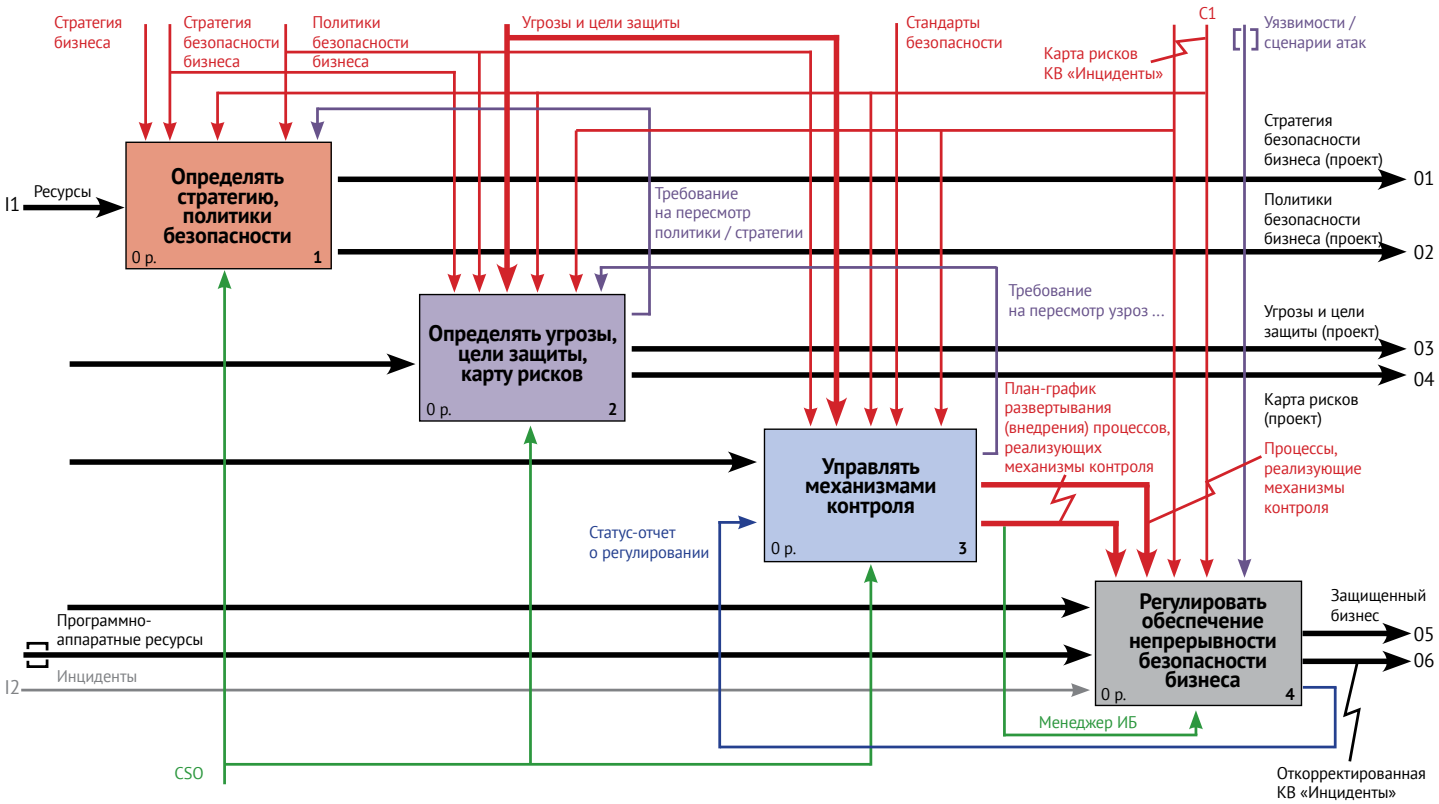


Рис. 3.
Декомпозиция процесса «Управлять непрерывностью безопасности бизнеса».

«Любые исключения механизмов контроля, которые сочли необходимыми для удовлетворения критериям принятия рисков, должны быть обоснованы, а также должны быть представлены свидетельства того, что соответствующие риски были приняты ответственными лицами».

- Еще одним отличием нашей модели от модели, описанной в ISO/IEC 27001:2005, стали выходы «защищенный бизнес» и «откорректированная база данных «Инциденты», что является результатом управления описываемым процессом. Этим мы «покрываем» термин «управляемая информационная безопасность», используемый в стандарте ISO/IEC 27001:2005.

Описание декомпозиционной диаграммы A0

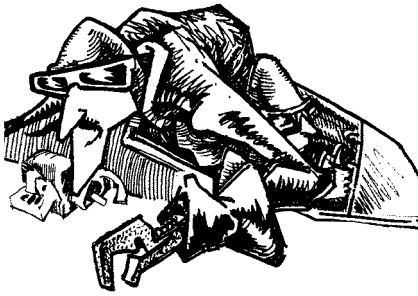
Основываясь на разделе 4 «Система управления информационной безопасностью» стандарта ISO/IEC 27001:2005, при декомпозиции процесса «Обеспечить непрерывность безопасности бизнеса» будем выделять следующие подпроцессы (блоки) (рис. 3):

1. Определять стратегию и политику безопасности бизнеса (A1);
2. Определять угрозы, цели защиты, карту рисков (A2);
3. Управлять механизмами контроля (A3);
4. Регулировать обеспечение непрерывности безопасности бизнеса[17] (A4).

Опишем их более подробно.

1. В соответствии со стратегией бизнеса (под руководством CSO) в блоке A1 разрабатывается проект стратегии безопасности бизнеса и затем направляется владельцу (владельцам) бизнеса на утверждение. По утвержденной стратегии безопасности бизнеса на его основе разрабатывается проект политик безопасности, который в свою очередь направляется на утверждение.
2. В блоке A2 последовательно разрабатываются проекты угроз, целей защиты и карта рисков.
3. На основе проектов перечисленных документов, утвержденных владельцами бизнеса, в блоке A3 разрабатываются процессы, регулирующие механизмы контроля, и план-график развертывания (внедрения) процессов, регулирующих механизмы контроля.

[17] В отличие от ISO/IEC 27001:2005 мы говорим о регулировании, а не о мониторинге и анализе.



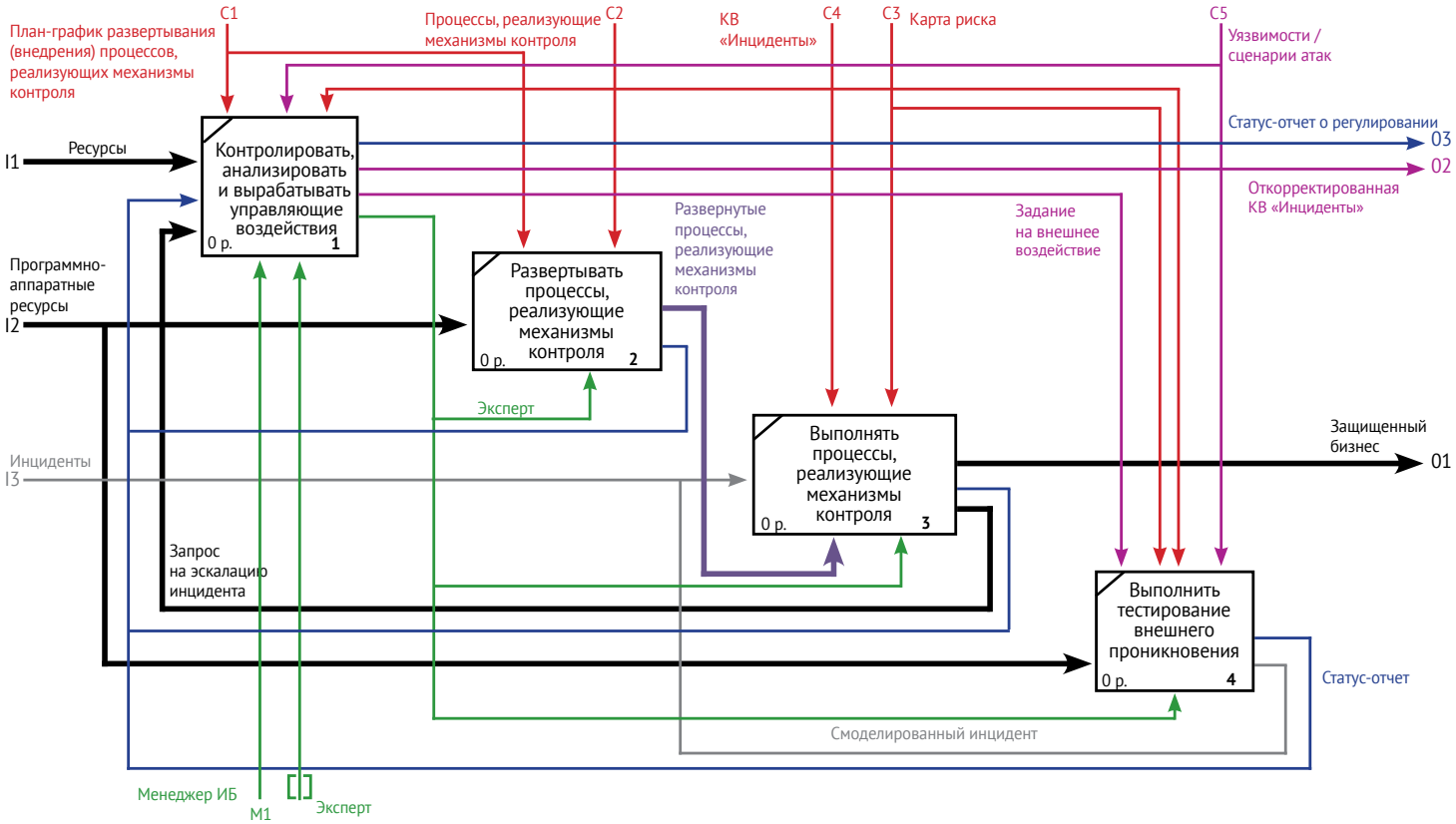


Рис. 4. Декомпозиция подпроцесса «Регулировать обеспечение непрерывности безопасности бизнеса»

4. В блоке А4 реализуется развертывание (внедрение) процессов, регулирующих механизмы контроля; процессы, регулирующие механизмы контроля, применяются для выполнения корректирующих действий по инцидентам. О дополнительной функции («Выполнить тестирование внешнего проникновения»), реализуемой в нашей модели, но отсутствующей в стандарте ISO/IEC 27001:2005, речь пойдет в третьей статье цикла.

Таким образом, блоки А1, А2 и А3 выполняют роль целеполагания – стратегическое управление, а блок А4 – это оперативное управление. Механизмы обратной связи:

- от блока А4 к блоку А3 – «Статус отчет о регулировании»;
- от блока А3 к блоку А2 – «Требование на пересмотр угроз»;
- от блока А2 к блоку А1 – «Требование на пересмотр политик/стратегии».

Эти механизмы являются ключевым и обеспечивают реализацию поддержания и совершенствования. Это полностью соответствует принципу стандартов ISO «Вовлечение работников».

На рис. 3 для каждого из блоков обозначены роли исполнителей. Это позволяет определить ролевое распределение обязанностей в процессе обеспечения непрерывности безопасности бизнеса, четко формализовать задачи и зоны ответственности участников процесса.

Описание подпроцесса «Регулировать обеспечение непрерывности безопасности бизнеса»

Подпроцесс «Регулировать обеспечение непрерывности безопасности бизнеса» (блок А4) реализует цикл SDCA. Его входами являются (рис. 4):

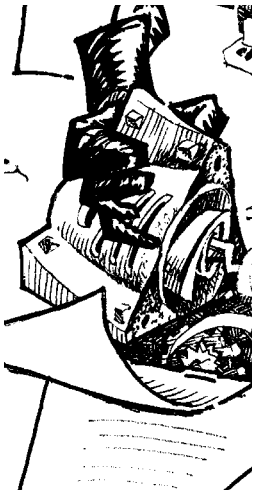
- программно-аппаратные ресурсы, на базе которых развертываются и выполняются процессы, реализующие механизмы контроля;
- инциденты.

Инциденты должны быть нейтрализованы с помощью процессов, реализующих механизмы контроля. Основными результатами блока являются:

- защищенный бизнес;
- откорректированная база данных «Инциденты»;
- статус-отчет о регулировании.

При декомпозиции этот блок может быть представлен следующими подпроцессами (рис. 4):

1. Контролировать, анализировать и вырабатывать управляющие воздействия (A41);
2. Развертывать процессы, реализующие механизмы контрмер (A42);
3. Выполнять процессы, реализующие механизмы контроля (A43);
4. Выполнять тестирование внешнего проникновения[18] (A44).



В блоке A41 реализуется оперативное управление (регулирование) обеспечением непрерывности безопасности бизнеса (этапы Check и Adjust (Act) цикла SDCA). Этап Do цикла SDCA реализуется в блоках A42 и A43. Процессы в этих блоках протекают параллельно. Результат блока A42 (стрелка «Развёрнутые процессы, реализующие механизмы контроля») далее выступает в качестве механизма блока A43.

В блоке A44 выполняется верификация развернутых процессов, реализующих механизмы контроля.

По заданию менеджера безопасности один из экспертов выполняет тесты, направленные на преодоление систем защиты и механизмов контроля, используя модели внутреннего и внешнего злоумышленника, а также различные векторы атак. В качестве методологической основы при этом выступают стандарты де-факто: выполнение тестов – стандарт PTES[19], построение методик измерения результатов верификации – стандарт OSSTMM[20].

Результаты (выход статус-отчета блока A44) направляются менеджеру безопасности. К нему же поступают статус-отчеты эксперта, выполняющего процессы, реализующие механизмы контроля. Сравнивая полученные статус-отчеты, менеджер безопасности принимает решение (в случае, если смоделированный инцидент не был зафиксирован) о необходимости эскалации проблемы, готовя статус-отчет о регулировании.

В третьей статье цикла будет дано детальное описание блока «Выполнить тестирование внешнего проникновения».

[18]Под внешним проникновением понимается деятельность экспертов по тестированию защищенности с использованием различных моделей внешних и внутренних злоумышленников.

[19]Penetration Test Execution Standard (PTES) www.pentest-standard.org.

[20]Open Source Security Testing Methodology Manual (OSSTMM) www.osstmm.org.