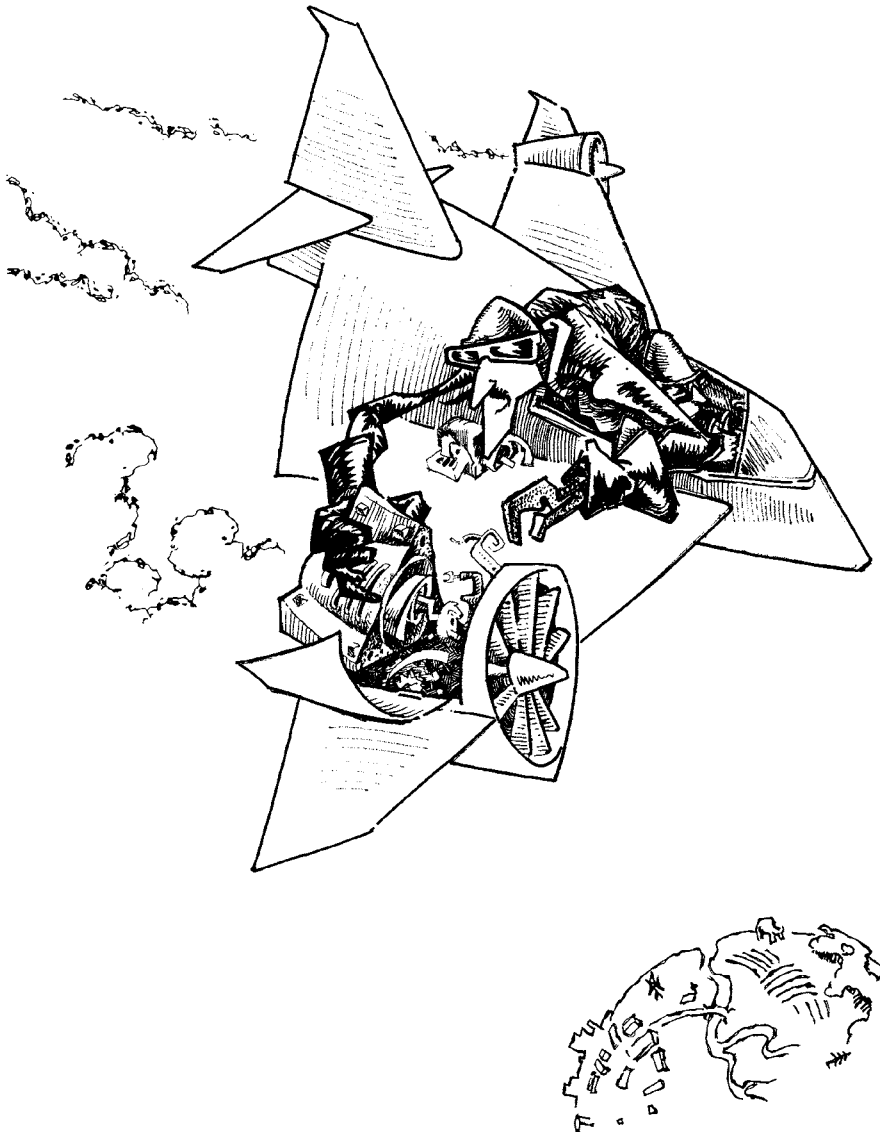
Правило ведения войны заключается в том, чтобы не полагаться на то, что противник не придет, а полагаться на то, с чем я могу его встретить; не полагаться на то, что он не нападет, а полагаться на то, что я сделаю нападение на себя невозможным для него.

Сунь Цзы[1] Искусство войны



Обеспечение непрерывности бизнеса

Часть 3. Верификация информационной безопасности бизнеса

Мы продолжаем цикл статей «Обеспечение непрерывности бизнеса». В первой статье цикла[2] 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[3] были описаны проблемы стандартов в области непрерывности бизнеса и информационной безопасности, а также дано описание функциональной модели процесса «Управлять непрерывностью безопасности бизнеса». В данной, третьей, статье мы кратко рассмотрим стандарты де-юре в области информационной безопасности и методики тестирования защищенности предприятия. Более подробно описывается наиболее полно охватывающая модель тестирования методика OSSTMM. Также дается декомпозиция блока «Выполнить тестирование внешнего проникновения» функциональной модели.

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.

Развитие технологий кибернападения предполагает необходимость совершенствовать технологии и процессы защиты бизнеса. В первой статье цикла мы отмечали, что сегодня стремительно сокращается временной разрыв между проникновением и реализацией угрозы, представляющей собой, например, вывод денежных средств либо кражу конфиденциальной информации. По этой причине во всех стандартах, разработанных для управления информационной безопасностью (ИБ), присутствуют требования регулярно проводить анализ ИБ для подтверждения адекватности ее функционирования и определения направлений совершенствования.

То есть организация должна регулярно выявлять возможности по улучшению управления информационной безопасностью, предпринимать необходимые корректирующие и предупреждающие действия. Для выполнения этих требований необходим процесс верификации защитных механизмов в организации. Поэтому с нашей точки зрения требуется проводить регулярные проверки защищенности информационной безопасности бизнеса (подробнее об этом ниже).

К сожалению, существуют организации, прошедшие сертификацию на соответствие стандартам, но которые по каким-либо причинам больше не проходят сертификационные аудиты. Они считают, что все необходимые мероприятия уже выполнены. Понятие «деградация сервиса» в отношении безопасности в этом случае не рассматривается.

[1]Китайский стратег и мыслитель.

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

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

[4]Макконнелл С. Профессиональная разработка программного обеспечения. Символ&Плюс, 2006.

[5]Ричард Фейнман, лауреат Нобелевской премии по физике.

Не напоминает ли такая ситуация «культ карго», описанный Стивом Макконнеллом в главе «Культ карго в разработке ПО»[4]. В качестве эпиграфа к этой главе он использует цитату Ричарда Фейнмана[5], в которой последний пишет: «У народностей, населяющих регионы южных морей, бытует «культ карго». В войну к ним прилетали самолеты с массой полезных вещей. Теперь люди хотят, чтобы так было опять. Поэтому они устраивают некое подобие взлетно-посадочной полосы, вдоль нее разжигают костры, строят будку, в которой сидит человек, изображающий диспетчера (с деревяшками вместо наушников и бамбуковыми палочками-антеннами), и ждут приземления самолета. Они все делают как нужно, по форме все правильно и выглядит так, как было раньше. Вот только самолеты не приземляются. Я называю такие вещи наукой «культа карго»: соблюдаются все внешние признаки и рецепты научного исследования, но нет чего-то очень важного, потому что самолеты так и не приземляются». Разве не так же поступают компании, внедрившие все лучшие рекомендации из стандартов ISO 27xxx, но не выполняющие процедуры проверки созданной системы? Чем это отличается от ситуации, описанной Фейнманом?

По нашему мнению, необходимо привлекать лучшие практики, реализованные в стандартах де-факто, предназначенные для верификации ИБ, и дополнить стандарты серии ISO 27xxx методами и методиками верификации. Задача верификации информационной безопасности бизнеса на современном этапе предполагает наличие в проекте многопрофильных специалистов, которые должны обладать всё более глубокими знаниями и навыками в таких смежных областях, как техники преодоления систем защиты, нормативно-правовая база, техники социальной инженерии, методы анализа бизнес-процессов и понимание используемых технологий. Это сложная задача, которая требует наличия системного подхода и выверенных методик проведения процесса верификации безопасности, позволяющих получить результат, который будет понятен владельцу бизнеса или заказчику. В нынешних условиях CSO следует противопоставить злоумышленникам, помимо глубоко эшелонированной технической обороны, отлаженные бизнес-процессы управления непрерывностью безопасности бизнеса, обучение и постоянную тренировку персонала службы информационной безопасности.

На сегодняшний день используется два принципиально разных подхода к оценке защищённости организации, основанные на двух различных взглядах (рис. 5):

- проверка на соответствие требованиям стандартов информационной безопасности (сертификационные аудиты) – внутренний взгляд на созданную систему обеспечения непрерывности бизнеса;
- тестирование защищённости автоматизированных систем предприятия (тест на проникновение, penetration test) – внешний взгляд на созданную систему.

Эти подходы имеют ряд достоинств и недостатков, которые приведены в таблице 1.

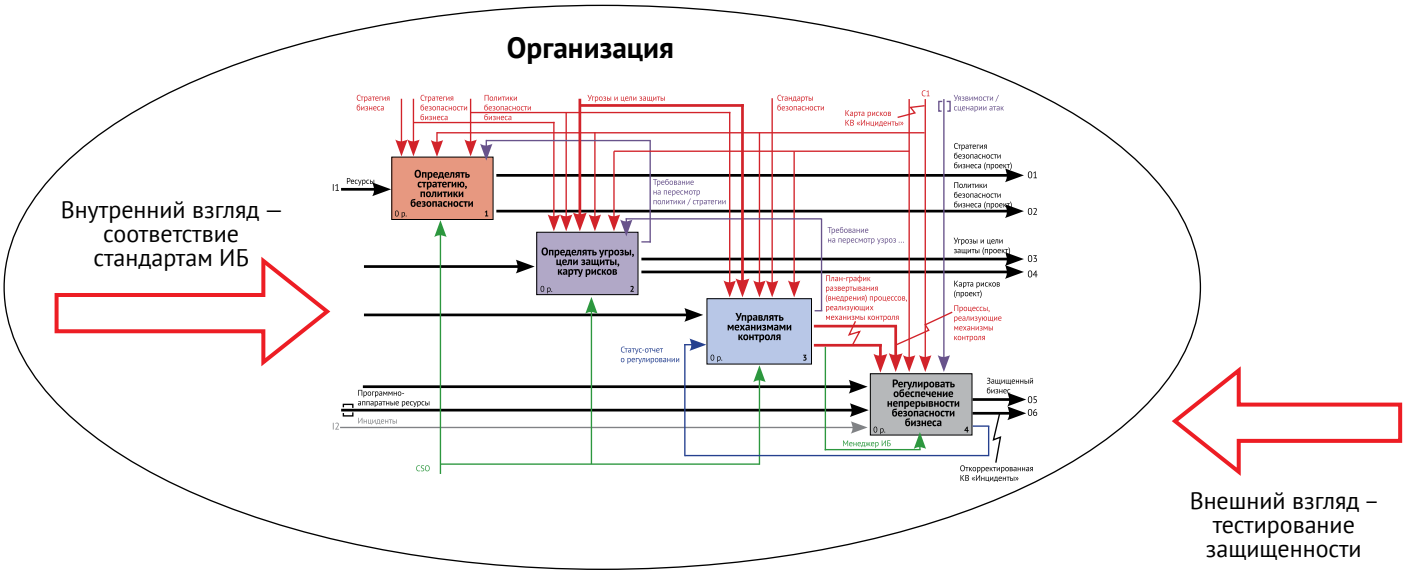


Рис. 5. Внутренний и внешний взгляды на систему обеспечения непрерывности бизнеса.

Внешний взгляд	Внутренний взгляд
Плюсы	
• Выявление просчётов при реализации положений и принципов стандартов ИБ • Определение реальных уязвимостей и успешных сценариев атак • Разработка рекомендаций для практического повышения защищённости	• Выявление соответствия ИБ предприятия лучшим практикам, отражённым в стандартах • Увеличение доверия со стороны инвестиционных, страховых и юридических компаний
Минусы	
• Высокая стоимость тестирования • Необходимость привлечения экспертов высокого уровня • Невозможно выявить все принципы организации процессов и систем ИБ предприятия	• Ограниченность прогнозирования сценариев атак • Невозможно выявить все просчёты при реализации требований стандартов на предприятии

Таблица 1.
Сильные и слабые стороны современных подходов тестирования защищённости.

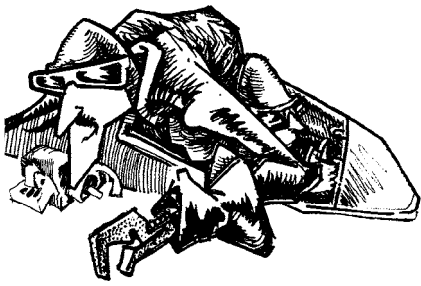
Внутренний взгляд – проверка бизнеса на соответствие требованиям стандартов ИБ

На сегодняшний день в мировой практике построения систем защиты ИБ бизнеса используется ряд стандартов. Наиболее популярными являются:

- стандарты серии ISO/IEC 27xxx;
- стандарт безопасности данных индустрии платежных карт PCI DSS;
- серия рекомендаций NIST SP 800.

Характеристика стандартов серии ISO/IEC 27xxx была приведена во второй статье цикла[6]. Дадим краткую характеристику двум другим стандартам.

Стандарт PCI DSS (Payment Card Industry Data Security Standard) исторически стал первым набором требований к обеспечению безопасности платежей. Он разработан сообществом международных платежных систем Visa, MasterCard, American Express, JCB и Discover, создавшим для его развития регулирующий орган – Совет PCI SSC[7].



Объектом применения этого стандарта является каждая организация, хранящая, обрабатывающая или передающая в своих информационных системах номера платежных карт, выпущенных под брендом любой из вышеуказанных международных платежных систем. Его требования распространяются на обычные и интернет-магазины, банки, платежные шлюзы, процессинговые центры и прочие сопутствующие структуры. Все организации, так или иначе вовлеченные в процесс обработки платежной транзакции, согласно идеологии регулятора делятся на две категории – торгово-сервисные организации (merchants) и поставщики услуг (service providers). К первым относятся все, кто продает товары или услуги и принимает в оплату от покупателей банковские карты: магазины, рестораны, отели, автозаправочные станции, парковки. Ко вторым – все те, кто обеспечивает процесс оплаты: банки, платежные шлюзы, сами международные платежные системы, хостинг-провайдеры и проч.

Серия рекомендаций NIST SP 800[8] содержит детальные разъяснения в области информационной безопасности по следующим направлениям:

- управление информационной безопасностью;
- технические вопросы обеспечения информационной безопасности;
- криптографическая защита информации.

Подход по тестированию защищённости с точки зрения внутреннего взгляда предполагает реализацию в организации одного из указанных стандартов информационной безопасности и последующую оценку защищенности, заключающуюся в определении соответствия систем и процессов предприятия требованиям стандарта.

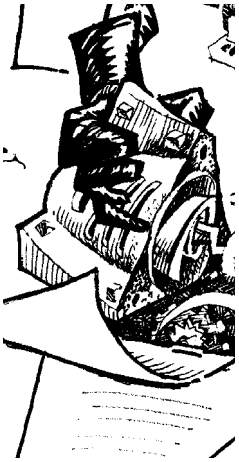
На российском рынке услуг ИБ имеются следующие предложения по определению уровня информационной защищённости предприятия:

- оценка соответствия системы управления информационной безопасностью стандарту ISO 27001:2005;

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

[7] PCI Security Standards Council. www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

[8] US National Institute of Standards and Technology (NIST) Special Publications 800 Series. http://csrc.nist.gov/publications/nistpubs/.



- оценка соответствия информационной безопасности организации банковской системы Стандарту Банка России (СТО БР ИББС);
- оценка соответствия автоматизированных систем организации внутренним нормативным требованиям компании по безопасности;
- аттестация автоматизированных систем и средств вычислительной техники по классу защиты в соответствии с РД ФСТЭК РФ;
- оценка соответствия платёжной системы стандарту PCI DSS.

Внешний взгляд – тестирование защищённости бизнеса

Этот подход предполагает оценку защищённости с точки зрения внешнего по отношению к предприятию злоумышленника, применение методик и техник для выявления и проверки угроз информационной безопасности организации. Данный подход требует наличия большого объёма экспертных знаний и техник в областях, связанных с преодолением систем и процессов защиты информации (безопасность ИТ-инфраструктуры, безопасность интернет-технологий, социальная инженерия, конкурентная разведка и т.д.), а также выполнения большого объема работы, связанного с пунктуальной проверкой систем, процессов и возможных сценариев атак. Помимо этого, внешняя оценка защищенности предприятия занимает длительное время и имеет высокую стоимость.

В настоящее время среди стандартов и методик, рассматривающих процесс тестирования защищённости с точки зрения внешнего заказчика, можно выделить следующие:

- **OSSTMM (Open Source Security Testing Methodology Manual).** Методика разработана ассоциацией ISECOM и предлагает комплексный подход к тестированию защищённости на основе практических методов преодоления систем защиты;
- **Стандарт PTES (Penetration Testing Execution Standard)**. В нем сообществом экспертов в области ИБ сделана попытка составить всеобъемлющий каталог сценариев атак и методов преодоления систем защиты;
- **Методология OWASP (Open Web Application Security Project).** Проект OWASP аккумулирует знания по обеспечению защиты Web-приложений. Проект является открытым и содержит лучшие практики тестирования на проникновение с использованием Web-приложений.

Из рассмотренных методик наиболее полно охватывает процесс тестирования защищённости методика OSSTMM и мы рекомендуем ее в качестве методологической базы

На рынке услуг ИБ в России представлены следующие предложения:

- тестирование на проникновение;
- тестирование защищённости в соответствии с методикой OSSTMM.

На современном этапе развития методик и стандартов информационной безопасности назрела необходимость:

- использовать системный подход в процессе обеспечения информационной безопасности предприятия, что предполагает объединение методик с разных взглядов для повышения качества ИБ и улучшения процесса управления непрерывностью безопасности бизнеса;
- разработать методику, позволяющую выполнять тестирование защищённости с регулируемым уровнем затрат и адаптивным подходом к выбору объектов и сложностью тестирования.

Требования к процессу верификации безопасности бизнеса

При верификации безопасности владельца бизнеса, как правило, интересуют следующие вопросы:

- Что представляет собой результат верификации бизнеса?
- Как он связан с реальной безопасностью организации?

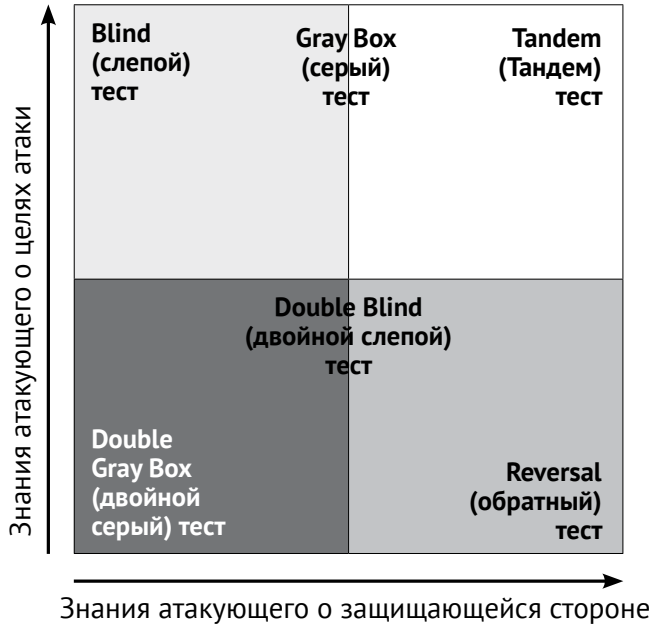
- Каким образом следует интегрировать результаты верификации безопасности непосредственно в процесс регулирования ИБ?
- Как сравнить два результата верификации бизнеса, выполненные разными проектными командами или в разное время?
- Не является ли процесс тестирования защищённости бизнеса на самом деле процессом тестирования проектных команд, которые занимаются тестированием защищённости?
- Можно ли доверять положительному результату верификации бизнеса?
- Не упущены ли тестировщиками какие-либо важные составляющие, критически влияющие на информационную безопасность организации?

Результаты верификации безопасности бизнеса должны быть понятны заказчику и измеримы, чтобы он получил ответы на все эти вопросы. К сожалению, на сегодняшний день не существует простых способов верификации безопасности бизнеса. Большая часть организаций работает по собственным методикам и внутренним стандартам. Ответы на поставленные вопросы могут быть получены в рамках разработанной модели, описывающей процесс верификации информационной безопасности бизнеса – составной части процессов управления непрерывностью безопасности бизнеса. Функциональная модель (как это будет показано ниже) использует оба из рассмотренных подходов.

Приведенный в статье анализ преимуществ и недостатков вышеуказанных подходов позволяет сформулировать требования к процессу верификации безопасности бизнеса:

- использование подходов тестирования защищённости с точки зрения внутреннего и внешнего взглядов;
- непрерывность и периодичность тестирования, получение на конечном этапе ясного результата, пригодного для практического улучшения процесса управления ИБ организации;
- выполнение тестирования должно основываться на широкой базе техник и практик преодоления систем и процессов информационной безопасности;
- методика, использующаяся в процессе верификации безопасности бизнеса, должна предусматривать в качестве одного из своих результатов возможность переоценки рисков ИБ организации, связанных с нарушением информационной безопасности;
- результаты тестирования должны позволять экспертам концентрировать внимание на выявленных проблемных областях для выработки контрмер;
- методика, используемая в процессе верификации безопасности, должна предлагать подход для построения метрик ИБ исследуемых объектов.

Рис. 6.
Категории тестов в методике OSSTMM.



При построении процесса тестирования защищённости в рамках функциональной модели для выполнения разработанных выше требований к тестированию защищённости в качестве методологической базы (в силу практической направленности) взята методика OSSTMM. Из всех рассмотренных методик OSSTMM наиболее полно охватывает процесс тестирования защищённости и включает следующий набор тестов[9] (рис. 6):

1. Blind (слепой) тест – учения;
2. Double Blind (двойной слепой) тест – тест на проникновение;
3. Gray Box (серый) тест – самопроверка;
4. Double Gray Box (двойной серый) тест – «белый ящик»;
5. Tandem (тандем) тест – отладка внедрённых контрмер;
6. Reversal (обратный) тест – стресс-тест.

[9] В настоящее время авторами готовятся следующие статьи, посвященные методике OSSTMM: «Введение в Open Source Security Testing Methodology Manual» и «Ключевые понятия Open Source Security Testing Methodology Manual».

В таблице 2 для каждого из указанных тестов приведены начальные условия выполнения тестов и задачи, которые ставятся при тестировании. Классы безопасности и каналы воздействия в методах OSSTMM приведены в таблице 3. Методика OSSTMM предоставляет инструментарий для построения метрик информационной безопасности, которые позволяют получать измеримые результаты оценки информационной безопасности организации. В качестве справочника по сценариям атак и методикам преодоления систем защиты в предлагаемой модели верификации ИБ взят стандарт PTES.

[10] См. таблицу 3.

Таблица 2.
Начальные условия выполнения тестов и задачи, которые ставятся при выполнении тестирования.

Тесты	Начальные условия теста	Задачи теста
Blind (слепой) тест – учения	• **эксперт** не обладает какими-либо начальными знаниями об устройстве организации, механизмах и процессах защиты, активах и каналах взаимодействия[10] • **персонал защиты** заранее знает о тестах и обо всех его деталях	Обучение и отработка на практике действий по противостоянию известным атакам: • отработка согласованности и координации действий по противостоянию кибератакам; • проверка экспертного уровня тестировщиков, осуществляющих попытки внешнего и внутреннего проникновений.
Double Blind (двойной слепой) тест – тест на проникновение	• **эксперт** не обладает какими-либо начальными знаниями об устройстве организации, механизмах и процессах защиты, активах и каналах • **персонал защиты** не имеет никакой информации о границах тестов, тестируемых каналах взаимодействия или векторах атак	Практическая проверка готовности всех подразделений к защите от киберугроз: • отрабатывается согласованность и координация действий по противостоянию неизвестной кибератаке в условиях приближенных к реальным; • проверяются внедренные и используемые механизмы контроля, выявляются уязвимости и недочеты. Выявляются и применяются новые эффективные способы атакующих действий, уязвимостей и сценариев атак.
Gray Box (серый) тест – самопроверка	• **эксперт** обладает ограниченными знаниями об устройстве организации, механизмах и процесса защиты, активах, но обладает полным знанием каналов взаимодействия. Ширина и глубина тестов зависит от полноты информации, предоставленной команде тестирования • **персонал защиты** заранее знает о тестировании и обо всех его деталях	Проверка внедрённых и используемых механизмов контроля, выявление недочётов, уязвимостей и сценариев атак: • отрабатывается согласованность и координация действий по противостоянию известной кибератаке с большой глубиной и/или шириной границ тестирования; • выявляются недочёты в развёрнутых механизмах контроля. Повышается квалификация тестировщиков, выполняется их обучение, проверяется их квалификация.
Double Gray Box (двойной серый) тест – «белый ящик»	• **эксперт** обладает ограниченными знаниями об устройстве организации, механизмах и процесса защиты, активах, а также полным знанием каналов взаимодействия, которые будут использоваться для тестирования • **персонал защиты** заранее предупреждён о тестировании, времени его начала, длительности, но не обладает знаниями об используемых векторах атаки и каналах взаимодействия	Выполняется проверка: • готовности персонала защиты и всех механизмов контроля противостоять неизвестной атаке с большой глубиной и/или шириной границ тестирования, используя разработанные и внедренные механизмы контроля; • проверяется квалификация тестировщиков, выявляются недостатки в используемых механизмах контроля.
Tandem (тандем) тест – отладка	• **эксперт** выполняет тестирование с полными начальными знаниями об устройстве организации, механизмах и процесса защиты, активах и каналах взаимодействия, которые будут использоваться для тестирования • **персонал защиты** заранее предупреждён о тестировании, времени его начала, длительности и всех деталях атаки	Совместная отладка внедрённых контрмер. Тестирование выполняется для поиска просчётов и ошибок во внедрении и настройке механизмов контроля как для команды тестирования, так и для персонала защиты.
Reversal (обратный) тест – стресс-тест	• **эксперт** обладает полными начальными знаниями об устройстве организации, механизмах и процесса защиты, активах и каналах взаимодействия, которые будут использоваться для тестирования • **персонал защиты** работает в штатном режиме, не предупреждён о тестировании и не обладает информацией о деталях тестирования	Проверка готовности организации противостоять неизвестным атакам: • контрольная проверка всех механизмов защиты, их способность противостоять неизвестным атакам; • выявить работающие векторы атак, найти критические пути по преодолению механизмов защиты и недостатки в механизмах контроля.

№	Класс	Канал	Описание
1	Physical Security (PHYSEC)	Human (HUMSEC)	Канал воздействия представляет собой все элементы коммуникации с сотрудниками организации, при которых коммуникация осуществляется физически или психологически.
		Physical	Канал воздействия представляет собой всевозможные физические, не электронные, способы коммуникации с организацией. Ключевым признаком является необходимость ощутимых физических усилий для взаимодействия.
2	Spectrum Security (SPECSEC)	Wireless	Канал воздействия представляет собой все электронные сигналы и излучения электромагнитного спектра. Включает: • ELSEC – коммуникации по беспроводному каналу; • SIGSEC – управляющие излучения; • EMSEC – побочные излучения устройств и кабелей.
3	Communication Security (COMSEC)	Telecommunication	Канал представляет собой все виды взаимодействия с использованием цифровых и аналоговых видов сигналов по телефонным сетям, т.е. сетям, в которых для взаимодействия используется принцип коммутации.
		Data Networks	Представляет собой все виды взаимодействия с организацией, осуществляющиеся через сети с пакетной коммутацией.

Таблица 3.
Классы и каналы воздействия в методике OSSTMM.

Процесс верификации безопасности бизнеса в функциональной модели «Управлять непрерывностью безопасности бизнеса»

Как мы писали во второй статье цикла, верификация информационной безопасности бизнеса – составная часть подпроцесса «Регулировать обеспечение непрерывности безопасности бизнеса»[11]. Декомпозиция подпроцесса «Регулировать обеспечение непрерывности безопасности бизнеса»[12] показывает роль и место верификации безопасности бизнеса (блок 44 «Выполнить тестирование внешнего проникновения»). Эта процедура важна как для тестирования достигнутого уровня защищенности бизнеса (за счет развёртывания процессов, реализующих механизмы контроля (блок 42), а также постоянного выполнения процессов, реализующих механизмы контроля (блок 43)), так и постоянного обучения и тренажа персонала службы кибербезопасности. Инициатором начала процесса тестирования является менеджер безопасности, регулирующий обеспечение непрерывности безопасности бизнеса. При этом он руководствуется в первую очередь «Планом-графиком развёртывания (внедрения) процессов, реализующих механизмы контроля», стандартами «Процессов, реализующих механизмы контроля» и статус-отчетами экспертов (реализующих подпроцессы А42 и А43).

Декомпозиция блока «Выполнить тестирование внешнего проникновения» представлена на рис. 7. При чтении декомпозиции указанного блока необходимо руководствоваться моделью ролевого распределения участников процесса тестирования, приведенной ниже. Подпроцесс «Выполнить тестирование внешнего проникновения» будем рассматривать как мини-проект, требующий для своего выполнения как программно-аппаратные, так и человеческие ресурсы. При его декомпозиции будем выделять следующие подпроцессы (блоки):

1. управлять тестированием внешнего проникновения (А441);
2. подготовить сценарий внешнего проникновения, проект отчета (А442);
3. выполнить сценарий внешнего проникновения (А443);
4. собрать информацию, построить метрики (А444).

Получив задание на внешнее проникновение («Задание на внешнее воздействие»[13]С1), эксперт – руководитель команды тестирования вырабатывает управляющие решения (блок А441):

- формирует план-график тестирования и распределяет роли между выделенными на проект специалистами по тестированию («Ресурсы»)[14];
- формулирует поручение аналитику на подготовку сценария внешнего проникновения и вида используемого теста;
- рассматривает проект сценария и возвращает его на доработку (управляющая дуга

[11] Декомпозиция процесса «Управлять непрерывностью безопасности бизнеса» показана на рис. 3 в статье «Обеспечение непрерывности бизнеса. Часть 2. Функциональная модель «Управлять непрерывностью безопасности бизнеса». Information Management №3 2013.

[12] Декомпозиция подпроцесса «Регулировать обеспечение непрерывности безопасности бизнеса» представлена на рис. 4 в статье «Обеспечение непрерывности бизнеса. Часть 2. Функциональная модель «Управлять непрерывностью безопасности бизнеса». Information Management №3 2013.

[13] В зависимости от типа теста может содержать сведения о целевой системе, которая будет тестироваться (см. табл. 2).

[14] Описание ролей участников команды тестирования приведены в табл. 4.

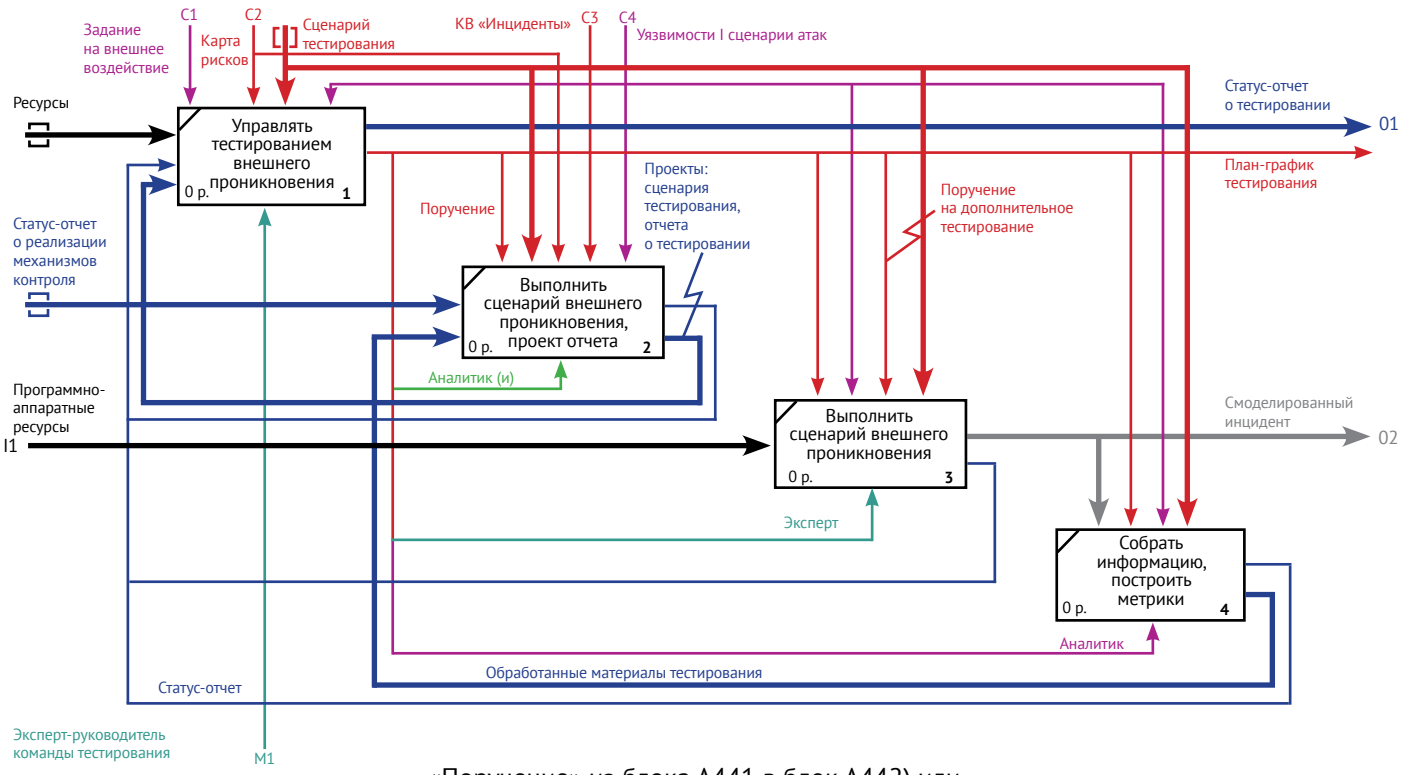


Рис. 7. Декомпозиция подпроцесса «Выполнить тестирование внешнего проникновения».

«Поручение» из блока А441 в блок А442) или

- направляет его на утверждение менеджеру безопасности, регулирующему обеспечение непрерывности безопасности бизнеса (составная часть статус-отчета о тестировании О1).

При выполнении поручения на разработку «Проекта сценария проникновения» (блок А442) аналитик (нижняя стрелка), входящий в команду тестирования[15], руководствуется следующими документами:

- статус-отчетами о реализации механизмов контроля (туннельная входная дуга), которые он получает от менеджера безопасности, регулирующего обеспечение непрерывности безопасности бизнеса;
- картой рисков (С2);
- базой данных «КВ Инциденты» (С3);
- уязвимостями/сценариями атак (С4)[16].

Результат выполнения поручения – «Проект сценария проникновения» (выходная дуга), направляется на рассмотрение эксперту – руководителю команды тестирования, как и информация о ходе разработки сценария проникновения (выходная дуга «Статус-отчёт»). Получив утверждённый «Сценарий тестирования» (туннельная дуга блока А441) и откорректировав (в случае необходимости) «План-график тестирования», он инициирует подпроцесс «Выполнить сценарий внешнего проникновения» (блок А443). Используя выделенные программно-аппаратные ресурсы (I1, блок А443), эксперт в соответствии с утверждённым сценарием и планом-графиком тестирования формирует «Смоделированный инцидент» (О2).

Модельные инциденты фиксируются аналитиком в блоке «Собрать информацию, построить метрики» (А444). По завершении выполнения сценария проникновения обработанные результаты тестирования (выходная дуга блока А444) направляются в блок А442 для подготовки проекта отчета по выполненному проекту. Проект отчета (готовится в блоке А442) направляется на утверждение эксперту – руководителю команды тестирования. Понятно, что он может поручить выполнить дополнительное тестирование (дуга управления в блок А443) или в статус-отчете о тестировании (О1 блока А441) обосновать необходимость выполнения дополнительных тестов и запросить соответствующие ресурсы у менеджера безопасности, регулирующего обеспечение непрерывности безопасности бизнеса.

[15] Команда тестирования включает: аналитиков, экспертов по методам, технологиям и т. д. Распределение и описание ролей команды тестирования представлены в табл. 4.

[16] Требуемую информацию о выявленных уязвимостях команда тестирования может получить из публичных источников, например: http://cve.mitre.org/; http://nvd.nist.gov/; http://www.exploit-db.com/; http://www.osvdb.org/; http://1337day.com/; http://www.metasploit.com/ и др.

Модель ролевого распределения участников процесса тестирования

Тесты в функциональной модели – инструмент практической учёбы, проводимый подразделениями информационной безопасности во взаимодействии с другими структурными подразделениями организации. Они направлены на приобретение и закрепление навыков по противостоянию кибератакам, координации действий структурных единиц, а также на отработку различных тактических и стратегических сценариев потенциально возможного инцидента нарушения информационной безопасности организации. Тесты являются высшей формой подготовки и одновременно контрольной проверкой компетенций персонала. Роли участников процесса верификации информационной безопасности представлены в таблице 4. Мы полагаем, что большую часть тестов должны выполнять сотрудники организации. Вместе с тем, для проведения таких тестов как Double Blind, Double Gray рекомендуется регулярно привлекать сторонние компании.

Таблица 4.
Роли участников процесса верификации информационной безопасности.

	Роль	Выполняемые задачи
1	Эксперт – руководитель команды тестирования	• взаимодействовать с менеджером безопасности по уточнению задания на тестирование, а также по всем другим вопросам, связанным с тестированием внешнего проникновения • декомпозировать задание по тестированию на подзадачи • ставить задачи экспертам-тестировщикам и аналитикам • корректировать и согласовывать проекты сценариев внешнего проникновения • корректировать и согласовывать план-график тестирования • на основании результатов работы команды тестирования готовить статус-отчёты • осуществлять управление группой тестирования в целях соблюдения сроков и целей тестирования
2	Аналитик	• разрабатывать сценарии внешнего проникновения и векторы атак • взаимодействовать с руководителем группы тестирования по вопросам уточнения задания на тестирование • взаимодействовать с экспертами-тестировщиками по вопросам уточнения векторов атак • собирать информацию о результатах тестирования внешнего проникновения, в т.ч. на промежуточных этапах • на основании полученных результатов строить метрики устойчивости бизнеса к внешнему проникновению
3	Эксперт	• непосредственно выполнять атаки и сценарии внешнего проникновения • взаимодействовать с руководителем группы тестирования по всем вопросам тестирования, в первую очередь по задачам, границам и срокам тестирования • взаимодействовать с аналитиком по вопросам разработки сценариев атак, векторов атак и результатам тестов • взаимодействовать с другими экспертами-тестировщиками по вопросам тестирования на пограничных областях знаний, например: социальная инженерия и эксплуатация уязвимостей браузеров

Авторы отдают себе отчёт в том, что для реализации всех описанных процедур организация должна иметь соответствующие ресурсы, структуры, обученный и подготовленный персона и т.д. Однако организации находятся на различных этапах своего развития и на разных уровнях в обеспечении непрерывности безопасности бизнеса. В этой связи в следующей статье цикла будет предложена модель зрелости компании, которая даст возможность оценить текущую зрелость бизнеса в области ИБ и сформировать предложение по поэтапному повышению его зрелости.