Аудит и стандарты:
свой путь или заимствование западного опыта

Анна РЫЖЕНКОВА,
ведущий консультант-аналитик отдела консалтинга и аудита, АО «ЭЛВИС-ПЛЮС»

Кому доверить аудит?

Аудит в сфере информационной безопасности является очень популярной услугой. Аудит зачастую отправная точка для многих проектов – с его помощью мы можем определить реальное состояние дел и получить актуальные данные в интересующей нас области. Кроме того, аудит должен проводиться периодически для проверки общих тенденций, качества функционирования аудируемых процессов, статуса соответствия требованиям с учетом внешних и внутренних изменений в организации.

Причем направлений аудита может быть довольно много в зависимости от выбранных целей и критериев оценки: это могут быть, например, требования стандартов – как российских, так и международных. И не каждая организация обладает достаточным количеством сотрудников необходимой квалификации. Поэтому целесообразно обращаться к услугам специализированных компаний. Кроме того, взгляд со стороны часто весьма полезен: внешний аудитор беспристрастно смотрит на область аудита, а не проверяет результаты собственной работы.

Квалификация аудиторов может быть подтверждена специализированными органами. Например, на международном уровне для систем менеджмента, сертифицируемых на соответствие требованиям международных стандартов, это может быть Национальный Совет по аккредитации США – ANAB (American National Accreditation Board). Для стандарта безопасности данных платежных карт (PCI DSS) также существует реестр аккредитованных компаний, имеющих статус Qualified Security Assessors (QSA). В России для аттестации объектов информатизации – это наличие аттестата аккредитации органа по аттестации, т. е. аккредитация ФСТЭК России. Для такой популярной темы как защита персональных данных тоже существует своя аккредитация: на сайте Роскомнадзора размещен «Реестр граждан и организаций, привлекаемых в качестве экспертов и экспертных организаций в ходе проверок в области персональных данных». В банковской сфере есть Ассоциация пользователей стандартов по информационной безопасности «АБИСС», на сайте этой организации можно ознакомиться со списками организаций-аудиторов и организаций-консультантов, оказывающих услуги в области обеспечения информационной безопасности.

Среди индивидуальных сертификаций специалистов в России, как и во всем мире, в последнее время стали очень популярны такие международные сертификаты, как CISSP (Certified Information Systems Security Professional), CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager) и др.

Наличие подобных аккредитаций и сертификатов является своеобразной гарантией качества предоставляемых услуг. Аккредитованные компании и специалисты по крайней мере занимают активную позицию в профессиональном сообществе, готовы выполнять определенные условия и следовать установленным правилам для получения и поддержания своей аккредитации или сертификата, а также заботятся о своей репутации.

Итак, тут мы идем в ногу с общемировыми практиками, и помимо российских компаний, включенных в международные реестры, для локальных требований у нас тоже действуют перечни, среди которых можно выбрать надежного исполнителя для проведения работ по аудиту. В чем тогда разница в подходах?

Прежде всего, это особенности менталитета. Например, в восприятии процесса аудита. В международной практике аудитор – это друг и помощник, сторонний квалифицированный специалист, работа которого направлена на то, чтобы выявить узкие места и проблемные зоны, чтобы впоследствии найденные несоответствия были устранены, ошибки исправлены и в результате происходило постоянное совершенствование объектов аудита. То есть по идее рабочие процессы и системы должны демонстрироваться аудитору «как есть», чтобы какие-то важные моменты не были упущены.

В российских компаниях, если речь идет об аудите, выполняемом системным интегратором (например, в начале проекта по внедрению каких-либо подсистем безопасности), то он вполне может носить дружественный характер. При этом есть надежда получить

объективные данные и свидетельства, отражающие реальную ситуацию. Но даже здесь могут возникнуть проблемы. Во-первых, многие структурные подразделения (особенно те, что связаны с бухгалтерией и финансами) изначально к аудиту относятся весьма негативно, даже если это аудит не финансовый, т. е. при этом не проверяется профессиональная пригодность сотрудника, уровень знаний в его предметной области и т. п. Количество и качество получаемой аудитором информации может существенно варьироваться: некоторые сотрудники начинают вести себя как партизаны на допросе, другие, наоборот, предоставляют слишком много информации, которая к целям и задачам аудита никак не относится, третьи пытаются приукрасить картину. Если добавить к этому еще и возможную конфронтацию между подразделениями (например, между ИТ и ИБ), то можно представить, как сложно в итоге аудитору докопаться до сути и оценить текущую ситуацию.

Если же аудит проводится каким-то государственным органом (например, проверка Роскомнадзора в части защиты персональных данных) или международным органом по сертификации (например, в целях сертификации на соответствие ISO 27001), то с большой степенью вероятности в такой ситуации аудиторы видят тщательно подготовленную область аудита. Однако не все компании могут впоследствии обеспечить функционирование построенных процессов на заявленном уровне, а уж тем более их совершенствование. Если эти процессы были искусственно надстроены, а не адаптированы с учетом особенностей конкретной компании и интегрированы в ее оперативную и стратегическую деятельность, то довольно скоро они будут отвергнуты бизнесом, и очередной аудит это обязательно выявит.

Следовательно, цель пройти проверку не должна становиться стратегической для руководства компании, а является одной из задач, логическим следствием выполненной работы. Аудит при этом играет роль всего лишь одного из механизмов достижения поставленных бизнес-целей организации.

Импортозамещение методик и стандартов

С адаптацией и применением лучших международных практик, закрепленных в стандартах, в России также возникают сложности.

Статистика по срокам введения международных и идентичных им национальных стандартов по тематике управления информационной безопасностью

Международный стандарт [1]	Дата введения международного стандарта	Национальный стандарт	Дата введения национального стандарта	Примечание	Разница по времени разработки (отставание ГОСТ)
ISO/IEC 27000:2009 Information technology. Security techniques. Information security management systems. Overview and vocabulary	Июль 2009	ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология	Декабрь 2013	ISO/IEC 27000:2009 заменен на ISO/IEC 27000:2012	4 года 5 мес.
ISO/IEC 27000:2012 Information technology. Security techniques. Information security management systems. Overview and vocabulary	Январь 2013	Информация отсутствует	нет	На данный момент действует ГОСТ, идентичный предыдущей версии международного стандарта	Более 3 лет
ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements	Октябрь 2005	ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования	Февраль 2008	ISO/IEC 27001:2005 заменен на ISO/IEC 27001:2013.	2 года 4 мес.
ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements	Октябрь 2013	ГОСТ находится в разработке	нет	На данный момент действует ГОСТ, идентичный предыдущей версии международного стандарта	Более 3 лет
ISO/IEC 27002:2005 Information technology. Security techniques. Code of practice for information security management	Июнь 2005	ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности	Январь 2014	ISO/IEC 27002:2005 заменен на ISO/IEC 27002:2013	9 лет 6 мес.
ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls	Октябрь 2013	Информация отсутствует	нет	На данный момент действует ГОСТ, идентичный предыдущей версии международного стандарта	Более 3 лет

[1] Цветом выделены не действующие на данный момент международные стандарты, которые были заменены новыми версиями.

ГОСТы, идентичные международным стандартам, выходят существенно позже, при этом часто бывает так, что на международном уровне уже достаточно долго действует обновленная версия стандарта (или даже принципиально новый стандарт, который заменяет прежний), а новый ГОСТ еще не введен. В качестве примера можно посмотреть на статистику по вводу в действие основных и наиболее популярных международных стандартов из серии ISO 27000, посвященной системам управления информационной безопасностью, и идентичных им ГОСТ (см. табл.).

Как видно из таблицы, наиболее оперативно был разработан ГОСТ Р ИСО/МЭК 27001-2006. Он был принят «всего лишь» на два с небольшим года позже международной версии. И такой срок в современных динамичных условиях ведения бизнеса и глобальной интеграции – это очень долго. Как тут быть специалистам: придерживаться устаревших локальных версий стандартов или ориентироваться на актуальные международные варианты?

Однако есть более удачный пример отраслевого стандарта для финансово-кредитной сферы, которая исторически занимает лидирующие позиции в вопросах защиты информации, а именно – стандарт Банка России (СТО БР ИББС). Этот стандарт был разработан на основе ISO 27001, причем он более динамичен в сравнении с ГОСТ и в отличие от ISO 27001 пытается учитывать российские реалии (например, тематику защиты персональных данных в привязке к российским требованиям).

Идентичность текста стандартов в определенных моментах тоже весьма условна. Прежде всего это связано со сложностью перевода. Бывает, что какие-то положения международных стандартов трактуются в несколько ином ключе, а где-то используется прямая калька с английского языка, и в результате текст становится сложным для восприятия.

Конечно, ГОСТы носят рекомендательный характер и каждая компания вправе решать, применять их или нет, но такая путаница и расхождения в тексте и актуальных версиях стандартов дискредитируют их в профессиональной среде.

Наличие официального текста международного стандарта на русском языке должно облегчить работу и взаимопонимание как между российскими специалистами, так и при взаимодействии с иностранными коллегами. Безусловно, многие сейчас владеют английским, но при этом у каждого может быть как свой вариант перевода, так и трактовки положений стандарта. Эти разночтения как раз должны устраняться своевременным введением ГОСТов, идентичных международным стандартам.

Таким образом, отказываться от западных наработок в области методик и стандартизации не стоит – их нужно разумно заимствовать и использовать, адаптируя под наши условия. ■