Валерия МЕЩЕРЯКОВА
обозреватель BIS Journal

ОТ ХАОСА К ПОРЯДКУ

РЫНОК АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как известно, вопрос проведения аудита состояния информационной безопасности в финансовых организациях приобрёл актуальность с появлением ГОСТ 57580 и связанных с ним Положений Банка России. Сегодня требования о проведении аудита ИБ распространяются на примерно 420 кредитных (банки и НКО) и 170 крупных некредитных финансовых организаций. Среди них страховые, пенсионные фонды, профессиональные участники рынка ценных бумаг. И в ближайшее время эти цифры только вырастут. Рынок вырисовывается достаточно широкий. И, увы, представители аудиторского сообщества констатируют, что сегодня он недостаточно проработан и нуждается в грамотных инициативах и уверенных практических шагах регулятора, поднадзорных организаций и профессиональных аудиторов.

ТЕКУЩЕЕ СОСТОЯНИЕ РЫНКА АУДИТА ИБ. МОРЕ ПОДРЯДЧИКОВ И... МОРЕ ПРОБЛЕМ

На текущий момент единственным требованием для компании, которая может выполнять внешний аудит, является наличие лицензии ФСТЭК на ТЗКИ с определённым видом деятельности. Таких организаций насчитывается более двух тысяч, но необходимо учитывать, что при получении лицензии на ТЗКИ к ним предъявляются требования, никак не предполагающие знания и опыт работы в специфической финансовой отрасли, а именно знание процессов ФО и регуляторики ИБ ФО. По факту на рынке сейчас существуют не более 20–30 аудиторских компаний, которые имеют релевантный опыт и знания. Однако как финансовые организации могут найти «сильных» аудиторов с положительной репутацией? Реестра таких организаций нет, как нет и методики оценки релевантности опыта и знаний и разработанных официальных требований к профессиональным аудиторам по ИБ. Кроме того, всё ещё нет системы их обучения, профессиональной подготовки и подтверждения квалификации. Единственный ресурс на сегодня — это реестр аудиторов, прошедших обучение по ГОСТ в Академии информационных систем. Он размещён на сайте Ассоциации АБИСС и включает как информацию о внутренних специалистах финансовых организаций, так и данные о сотрудниках компаний-аудиторов. Таким образом, ситуация на рынке аудита ИБ финансовых организаций сейчас такова, что не имеющие релевантного опыта специалисты выполняют аудит низкого качества, результатам которого не может доверять ни финансовая организация, ни Банк России. Назрела необходимость в формировании доверенной системы аудита информационной безопасности финансовых организаций. И эту сложнейшую задачу возможно решить только при постоянном трёхстороннем взаимодействии регулятора, финансовых организаций и аудиторов.

КАК ЖЕ СЕГОДНЯ ФИНАНСОВЫЕ ОРГАНИЗАЦИИ ВЫБИРАЮТ АУДИТОРА?

Эксперты рынка аудита ИБ свидетельствуют, что часть поднадзорных Банку России организаций, которым показано проведение внешнего аудита, не проводят аудит в принципе. Распространены случаи, когда сотрудник банка самостоятельно

КОММЕНТАРИЙ АБИСС

Евгений ЦАРЁВ
RTM Group, эксперт АБИСС

Учитывая несформированность рынка и отсутствие критериев качества, в подавляющем числе конкурсов и запросов коммерческих предложений на проведение аудита контракт достаётся компании, которая предлагает самую низкую цену.

Антон СВИНЦИЦКИЙ,
ДиалогНаука, эксперт АБИСС

Аудиторы должны не только обладать знаниями нормативной базы, используемой при проведении оценки соответствия, но также должны подтвердить и поддерживать свою квалификацию и знания как процессов аудита, так и применяемых технологий защиты информации.

готовит отчёт и подписывает его у дружественного лицензиата «за три копейки». Иногда не подписываются даже фиктивный договор и акты на работы по аудиту (по таким проектам не проходят оплаты). Часть поднадзорных организаций проводят аудит формально, оплачивая компании-аудитору символические 50–100 тысяч рублей, но только на бумаге. Отчёт же готовится силами самих сотрудников банка и лишь подписывается у лицензиата. По оценкам экспертов, не менее 30% кредитных организаций «проводили» аудиты по описанной модели.

Отдельная проблема — демпинг на рынке аудита ИБ. Учитывая несформированность рынка и отсутствие критериев качества, в подавляющем числе конкурсов и запросов коммерческих предложений на проведение аудита контракт достаётся компании, которая предлагает самую низкую цену. Экспертам известны примеры конкурсов как открытых, так и закрытых (без проведения торгов на площадке), по которым цена аудита по ГОСТ 57580 составляла 100–300 тысяч рублей без НДС для небольших организаций, 400–800 тысяч рублей для средних и 800–1200 тысяч рублей для крупных. Проведение качественного аудита при такой цене невозможно. Не так давно Ассоциация АБИСС провела анонимный опрос десяти компаний-аудиторов ИБ ФО о средней стоимости работ по проведению аудита ИБ для двух смоделированных банков — маленького с высоким уровнем зрелости ИБ и среднего с низким уровнем зрелости ИБ. Стоимость аудита по итогам опроса составила 1,2 млн рублей (10 недель работы аудиторов) и 3,4 млн рублей (16 недель работы аудиторов) соответственно. Разумеется, речь шла о качественном аудите с реальной оценкой соответствия требованиям и сбором всех необходимых свидетельств.

КАЧЕСТВО АУДИТОВ. ОБРАЗОВАНИЕ, ОПЫТ И КВАЛИФИКАЦИОННЫЕ ТРЕБОВАНИЯ

К сожалению, некоторые требования новых положений Банка России по защите информации и требования ГОСТ Р 57580.1–2017 написаны слишком обобщённо, что часто не позволяет двум независимым друг от друга аудиторам одинаково трактовать эти требования и использовать единый подход к оценке соответствия. Увы, разовым повышением квалификации эта проблема не решается. Необходимо планомерно повышать степень информированности аудиторского сообщества о подходах к оценке и видении Банка России в части результатов таких проверок. И делать это необходимо на регулярной основе на базе анализа со стороны

Ситуация на рынке аудита ИБ финансовых организаций сейчас такова, что не имеющие релевантного опыта специалисты выполняют аудит низкого качества, результатам которого не может доверять ни финансовая организация, ни Банк России

Банка России результатов оценок соответствия, отчётных документов аудиторов и предположений кредитно-финансовых организаций.

Аудиторы должны не только обладать знаниями нормативной базы, используемой при проведении оценки соответствия, но также должны подтвердить и поддерживать свою квалификацию и знания как процессов аудита, так и применяемых технологий защиты информации (в том числе применяемых ИТ-технологий, используемых для реализации технологических процессов). Сейчас же требования к квалификации и знаниям аудиторов не предъявляются.

ЕДИНАЯ БАЗА ЗНАНИЙ ПРОФЕССИОНАЛОВ АУДИТА ИБ

Эксперты полагают, что создавать систему доверенного аудита ИБ без детализации обобщённых формулировок и ведения единой базы знаний невозможно. Причём наполнять и использовать эту базу должны как внутренние специалисты по ИБ финансовых организаций, так и представители аудиторского сообщества при участии представителей Банка России, ответственных за методологию и надзор, в том числе по результатам анализа отчётных документов аудиторов и предложений кредитно-финансовых организаций. Единая база знаний может стать ещё одним шагом к созданию доверенной инфраструктуры аудита. С подобной инициативой выступила недавно Ассоциация АБИСС, подчеркнув готовность запустить базу знаний на своей платформе.

ОТВЕТСТВЕННОСТЬ АУДИТОРОВ. ОТСУТСТВИЕ КРИТЕРИЕВ КАЧЕСТВА РАБОТЫ АУДИТОРОВ

Говоря об ответственности аудиторов ИБ за результаты проверок, можно смело утверждать: сейчас качество их работы невозможно оценить в принципе. Проблема заключается в отсутствии установленных объективных критериев качества работы аудиторов. И даже профессионалы, за плечами которых десятки проектов по ГОСТ 57580, могут по-разному оценивать

одни и те же свидетельства и давать различные оценки. Причём невозможно однозначно утверждать, что один из них абсолютно прав, а второй полностью неправ. Причина таких разночтений обусловлена большой вариативностью трактовок мер и отдельных положений ГОСТ.

Действительно, оценивать качество аудита ИБ необходимо, но сначала нужно сформулировать критерии качества — рекомендации и разъяснения регулирующего органа. Для этого необходимо разработать три механизма:

1) базу знаний с разъяснениями по спорным моментам аудитов;

2) систему периодического обучения всех практикующих аудиторов;

3) систему, при которой по факту аудиты будут проводить только прошедшие специальное обучение специалисты, которые периодически повышают свою квалификацию и реально работают на проектах по аудиту.

СОЗДАНИЕ ЕДИНОЙ ИНФРАСТРУКТУРЫ АУДИТА

По мнению экспертов, решением проблемы качества аудита ИБ финансовой отрасли может стать система добровольной сертификации аудиторов, где объектом сертификации будет методика работы аудиторов. При этом инфраструктура будет описывать взаимодействие Банка России, финансовых организаций, компаний-аудиторов и учебных центров. (Анастасия Харыбина, директор по развитию AKTIV.CONSULTING, президент АБИСС)

Основные моменты концепции:

- Создание единой методики проведения аудита ИБ финансовых организаций с использованием упомянутой выше наработанной базы знаний, пользуясь которой будут работать как аудиторы, так и представители надзора и которая будет доступна внутренним специалистам финансовых организаций.
- Разработка требований к квалификации аудиторов, а также требования к компаниям-аудиторам.
- Создание методики оценки качества проведённых аудитов через выборочную проверку, а также определение последствий для компаний-аудиторов в случае ненадлежащего уровня качества.
- Разработка обучающих курсов для аудиторов и определение критериев аттестации и переаттестации.

В Ассоциации АБИСС создана рабочая группа, которая при взаимодействии с ДИБ Банка России прорабатывает данные вопросы.

ИЩЕМ ВЫГОДЫ ДЛЯ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ И РЕГУЛЯТОРА ОТ КАЧЕСТВЕННОГО АУДИТА

На прошедшей в конце марта в рамках конференции РусКрипто'2021 секции Ассоциации АБИСС по аудиту ИБ для финансовых организаций с участием представителей ДИБ Банка России спикеры говорили о реальных выгодах, которые получат регулятор, аудиторы и поднадзорные организации от создания системы доверенного аудита и повышения его качества. Профит для Банка России — реальная оценка уровня выполнения требований по ИБ, которая, в частности, влияет на риск-профиль финансовой организации и уровень резервирования средств, а также переход от бумажной безопасности к реальной. Профит для финансовых организаций — понятные критерии квалификации аудиторов, доверие к результатам аудита, на основе которых можно выстраивать программу развития ИБ. Профит для компаний-аудиторов — конкурентный рынок, на котором можно оказывать качественные услуги, при этом оставаясь коммерчески заинтересованными в этой деятельности. Очевидно, что весомые выгоды от упорядочения рынка аудита ИБ для всех его участников значительно ускорят процесс создания доверенной инфраструктуры.

КОММЕНТАРИЙ АБИСС

Евгений БЕЗГОДОВ
Deiteriy, эксперт АБИСС

Оценивать качество аудита ИБ необходимо, но сначала нужно сформулировать критерии качества — рекомендации и разъяснения регулирующего органа.

Анастасия ХАРЫБИНА
директор по развитию AKTIV.CONSULTING, президент АБИСС

Решением проблемы качества аудита ИБ финансовой отрасли может стать система добровольной сертификации аудиторов, где объектом сертификации будет методика работы аудиторов. При этом инфраструктура будет описывать взаимодействие Банка России, финансовых организаций, компаний-аудиторов и учебных центров.