# Доверие по ГОСТу

*Текст*
**ВАДИМ ФЕРЕНЕЦ,**
ОБОЗРЕВАТЕЛЬ **«Б.О»**

Система добровольной сертификации независимых ИБ-аудиторов вкупе с развитием серии стандартов ГОСТ 57580 уже оказывает значительное воздействие на рынок услуг в сфере кибербезопасности за счет саморегулирования отрасли

Разработка и запуск Системы добровольной сертификации (СДС), разработанной АБИСС (Ассоциацией пользователей стандартов по информационной безопасности в финансовом секторе РФ), безусловно, являются важным шагом к установлению в нашей стране доверия между всеми участниками финансового рынка: кредитно-финансовыми организациями, Банком России, поставщиками услуг для финорганизаций и компаниями, оказывающими услуги по независимой оценке соответствия в сфере ИБ.

**Повысить качество услуг**

Что стало предпосылками создания системы сертификации ИБ-аудиторов? На одном из вебинаров, проведенном АБИСС, **Анастасия Харыбина,** пред-

седатель Ассоциации, поделилась подробностями. По ее словам, в начале 2020 года в ходе Уральского форума по кибербезопасности в финансовой сфере было принято решение о создании открытой рабочей группы по разработке системы сертификации ИБ-аудиторов с участием Банка России и АБИСС. Само наличие обязательного внешнего независимого ИБ-аудита было прописано в принятых в 2017 году ГОСТах 57580.1 и 57580.2.

Проблема заключалась в том, что к исполнителям, которые могли оказывать услуги по оценке соответствия в рамках аудита, применялось и до сих пор применяется требование о наличии лицензии на деятельность по технической защите конфиденциальной информации (ТЗКИ) от Федеральной службы по техническому и экспортному контролю (ФСТЭК). Лицензиатов ТЗКИ на сегодняшний день около 3 тыс., при этом компетенции большинства из них напрямую с проведением аудитов информационной безопасности и комплаенс-аудитов в финансовой сфере не связаны. Не секрет, что появились случаи формального или некачественного предоставления ими услуг по заниженным тарифам, что ограничивает возможности развития серьезных компаний.

Этот факт и обусловил необходимость создания прозрачной системы, в рамках которой все участники процесса могли бы доверять результатам внешней оценки соответствия требованиям ИБ к финансовым организациям. Это в идеале позволит регулятору со временем перейти к дистанционному контролю, что снизит нагрузку и на банки, и на аудиторов. При этом результаты аудита должны быть интегрированы в регулярную контрольно-надзорную деятельность со стороны регулятора. Сейчас этого, к сожалению, практически не делается. Дополнительно Банк России мог бы гораздо лучше понимать структуру и уровень зрелости рынка банковского аудита для масштабирования опыта на иных своих поднадзорных.

Что может дать новая система финансовым организациям? Помимо списка надежных поставщиков услуг, они должны получить инструмент решения спорных вопросов при повышении уровня собственной безопасности.

Сами же профессиональные ИБ-аудиторы заинтересованы в формировании здорового конкурентного рынка с наличием механизма подтверждения качества оказываемых услуг. Только это позволит им развивать компетенции и повышать уровень экспертизы, а также публично отвечать за результаты своей работы и получать подтверждение качества своих услуг от третьей независимой стороны.

**Два компонента решения**

По данным председателя АБИСС, создание прозрачной инфраструктуры ИБ-аудита идет по двум трекам.

***Во-первых,*** экспертами АБИСС были разработаны требования для оказания услуг по оценке соответствия. Они легли в основу Стандарта по оценке соответствия (СТО) АБИСС и проекта ГОСТ 57580.X, который успешно прошел первое обсуждение в Техническом комитете по стандартизации № 122 (ТК-122). На текущий момент все предложенные правки проработаны, а сам документ находится в Департаменте информационной безопасности Банка России.

В АБИСС рассчитывают, что в текущем году проект Стандарта будет зарегистрирован в «Росстандарте», после чего вступит в силу и станет обязательным к применению на основании положения Банка России. Необходимо отметить, что Стандарт содержит требования общего вида, которые будут распространяться на оценку соответствия не только по ГОСТ Р 57580.1-2, но и по ГОСТ Р 57580.4-5. Что касается Системы добровольной сертификации АБИСС — это первая в России система подтверждения качества и безопасности услуг в ИБ-сфере, в том числе услуг по оценке соответствия требованиям Банка России по информационной безопасности.

***Во-вторых,*** специалистами АБИСС была зарегистрирована в «Росстандарте» СДС компаний по информационной безопасности, что стало значимым шагом, так как подобных прецедентов в сфере ИБ-услуг ранее не существовало. Запущена процедура сертификации организаций, а появление первых сертифицированных компаний ожидается во втором квартале 2026 года. Таким образом, к моменту введения ГОСТ 57580.X должен появиться необходимый минимум сертифицированных организаций.

Кроме того, в качестве отдельного направления разработан и зарегистрирован в «Росстандарте» механизм сертификации специалистов и аудиторов (физических лиц), и уже принят первый экзамен.

**«Под капотом» СТО и СДС**

По словам авторов СТО, он описывает требования и к проверяющим организациям, и к их специалистам. Значительная часть документа посвящена требованиям к процессам проведения оценки соответствия и к процедурам формирования и написания отчета, для того чтобы уже сейчас аудиторы могли начинать работы, не дожидаясь вступления в силу ГОСТ 57580.X

Ассоциация предлагает прохождение сертификации по СТО АБИСС, требования которого полностью гармонизированы с проектом ГОСТа. Кроме того, СТО написан так, что подходит не только под требования серии стандартов ГОСТ 57580 в финансовой сфере, но и для любых оценок соответствия в других индустриях.

Эксперты обращают особое внимание на то, что происходит активное развитие серии ГОСТов 57580, в частности, в ТК № 122 во втором чтении были приняты согласованные правки их расширения в части методики оценки операционной надежности. Оценки соответствия по надежности также со временем станут обязательными, поэтому есть возможность подготовиться к этой

**Что может дать новая система финансовым организациям? Помимо списка надежных поставщиков услуг, они должны получить инструмент решения спорных вопросов при повышении уровня собственной безопасности**

процедуре в рамках СТО АБИСС, где уже учтены это и другие нормативные новшества.

СДС АБИСС — первая в России система подтверждения качества и безопасности услуг в сфере ИБ, в том числе услуг по оценке соответствия требованиям Банка России по информационной безопасности. В АБИСС полагают, что саморегуляция со стороны рынка не противоречит регулированию со стороны государства, а дополняет его.

Для специалистов предусмотрено подтверждение знаний по проведению оценки соответствия (ГОСТ.Х / СТО АБИСС), подтверждение знаний в соответствии с областью сертификации (ГОСТ 57580.1-2 и связанные с ним положения Банка России). Срок действия сертификата — три года.

Организациям при первичной сертификации необходимо учитывать два момента. Во-первых, требуется наличие сертифицированных в СДС АБИСС специалистов, соответствующих в том числе требованиям к руководителям проверяющей группы (РПГ). Во-вторых, изучается относительно небольшой набор внедренных процессов управления качеством, ресурсами, экспертизой, конфликтом интересов, а также конфиденциальностью.

В дальнейшем, после проведения первичной сертификации, для АБИСС ключевым становится ежегодный инспекционный контроль, в рамках которого оцениваются качество отчетов и их соответствие ГОСТ.Х / СТО АБИСС в рамках планового контроля или внеочередных проверок проведенных аудитов. Для этого случайным образом выбирается отчет, происходит его обезличивание, чтобы не было понятно, о какой именно финансовой организации в нем идет речь, после чего он передается для проверки в систему добровольной сертификации.

Эксперты признают, что идеальным сценарием было бы повторение и у нас процедур инспекционного контроля, предусмотренных в международном PCI Security Standards Council, в котором не требуется обезличивать отчеты. К сожалению, в силу особенностей нашего законодательства в области обеспечения конфиденциальности передача документа, где указано наименование проверяемой организации, невозможно.

### Первые итоги

Многие аудиторские компании волнует вопрос: как будет выстраиваться работа с финансовыми организациями в части согласования областей оценки, выборки, порядка урегулирования разногласий и предоставления свидетельств?

**Алексей Сторож,** ведущий консультант по ИБ AKTIV.CONSULTING, утверждает: «Область оценки определяется совместно с проверяемой организацией на старте проекта, однако может быть расширена в ходе проведения аудита при выявлении новых систем, обрабатывающих защищаемую информацию. Выборка же применяется в отношении типовых объектов из той самой области оценки непосредственно при запросе файлов свидетельств: скриншотов, выгрузок конфигураций, логов и т.п. Для сбора и учета всех видов свидетельств мы уже используем систему собственной разработки, которую в скором будущем планируем открыть для прямого заполнения представителями проверяемых организаций, что позволит наладить оперативную обратную связь с ответственными лицами внутри финансовых организаций, а также обеспечить прозрачность проведения оценки соответствия на всех ее этапах».

А насколько сложна процедура проведения внутреннего аудита на соответствие СТО АБИСС? Исполнительный директор компании «Дейтерий» **Евгений Безгодов** поделился опытом: «По большей части требования СТО АБИСС в том или ином виде присутствуют в нормативных документах международных регуляторов, включая Совет PCI SSC. Эти требования привычны для нас как для аудиторской компании со стажем более 15 лет и уже реализованы в наших документах и в повседневной работе. Исключение конфликтов интересов, обеспечение достаточными ресурсами, повышение компетентности и постоянное совершенствование навыков, внутренний и внешний контроль качества, защита клиентской информации — все это естественная жизнь аудиторской компании».

Из специфических требований СТО АБИСС эксперт отметил обучение и сертификацию специалистов по соответствующим программам. В компании «Дейтерий» на данный момент сертифицированы пять аудиторов.

«Помимо этого терминология в нашей внутренней нормативной документации уточнена и приведена в соответствие терминологии СТО АБИСС. Обновлены некоторые формы внутренних и отчетных документов. Дополнены календарные планы и перечни регулярных процедур в части взаимодействия с СДС АБИСС», — добавил Евгений Безгодов.

На первый взгляд, довольно затруднительной выглядит перестройка внутренних процессов и систем управления качеством аудита, чтобы соответствовать новым требованиям сертификации организаций и ежегодного инспекционного контроля.

Однако **Александр Хонин,** директор Центра консалтинга компании Angara Security, уверен в обратном: «В Angara Security уже выстроены внутренние процессы и система управления качеством проектной деятельности. Поскольку проектная деятельность — основное направление нашей

работы, ничего сверхъестественного и нового в требованиях сертификации организаций для нас нет. Несомненно, потребуются точечные изменения, чтобы соответствовать всем установленным требованиям. Но в целом, можно констатировать, что большой перестройки не потребуется».

**Сергей Сугоняев,** руководитель проектов по ИБ AKTIV.CONSULTING, также не видит здесь серьезных проблем: «Процессы и система качества организации в процессе подготовки к сертификации в СДС АБИСС не подверглись серьезным изменениям, так как изначально были выстроены исходя из лучших российских практик с учетом опыта реализации многочисленных проектов по информационной безопасности. Утвержденная в организации "Политика по контролю качества" лишь устранила некоторые шероховатости процессов и подходов для полного соответствия требованиям СТО АБИСС. Политика распространяется на все этапы и процессы, связанные с проведением оценок соответствия, включая планирование, выполнение работ, подготовку отчетности и взаимодействие с проверяемыми организациями».

**Эксперты признают, что идеальным сценарием было бы повторение и у нас процедур инспекционного контроля, предусмотренных в международном PCI Security Standards Council, в котором не требуется обезличивать отчеты. К сожалению, в силу особенностей нашего законодательства в области обеспечения конфиденциальности передача документа, где указано наименование проверяемой организации, невозможно**

### Кадры решают все

«Какие шаги уже предприняты для подготовки специалистов к сертификации и экзаменам по СТО АБИСС и будущему ГОСТу? Как оценивается уровень готовности вашей команды?» — эти вопросы «Б.О» задал экспертам.

Сергей Сугоняев считает: «В нашей команде работают специалисты с большим опытом и подтвержденной квалификацией, поэтому каких-либо особенных шагов для подготовки не потребовалось. На данный момент некоторые сотрудники уже сдали экзамен по СТО АБИСС. Компания полностью готова к проведению работ в соответствии с новыми стандартами и уже подала заявку на сертификацию».

Александр Хонин добавил: «В настоящее время наши специалисты проходят добровольную сертификацию по информационной безопасности в СТО АБИСС. С учетом накопленного проектного опыта уровень подготовки экспертов позволяет сдать сертификационные экзамены. Кроме того, все наши сотрудники за плечами имеют не один выполненный проект, что также способствует успешной сдаче экзаменов. В части требований нового ГОСТа также больших трудностей не ожидается, так как мы активно и неоднократно участвовали в обсуждении его проектов».

### Плюсы и планы

Обобщая мнение экспертов о плюсах нововведений, можно утверждать — результаты оценки соответствия могут и должны быть использованы для принятия управленческих решений по развитию функции ИБ. Например, благодаря взаимодействию с СДС АБИСС появляется возможность получить разъяснения по разногласиям, а также сообщить системе о некачественной оценке соответствия. А взаимодействие участников с Банком России приводит к изменению состава подаваемой информации по результатам оценки соответствия (71-я форма).

Благодаря взаимодействию с СДС АБИСС появляется возможность получить разъяснения по разногласиям, а также сообщить системе о некачественной оценке соответствия.

Помимо этого необходимо выделить три явных эффекта.

*Во-первых,* СДС обеспечивает доверие к результатам оценок соответствия для регуляторов и самих финансовых организаций.

*Во-вторых,* с этого года сертифицированные организации будут проводить оценку в соответствии с новыми требованиями, что позволит проверяемым организациям постепенно внедрять новые подходы.

*В-третьих,* в этом году будет запущена разработка сертификации для услуг по оценке соответствия требованиям операционной надежности.

Кроме того, уже видны перспективы развития основных компонентов СДС и возможности для расширения спектра услуг. **Варвара Шубина,** руководитель направления маркетинга АБИСС, поделилась такой информацией: «В планах АБИСС — развитие системы добровольной сертификации по новым направлениям, включая блок обеспечения операционной надежности, согласно ГОСТ 57580.3, ГОСТ 57580.4 и ГОСТ 57580.5. Что касается того, какие компетенции и ресурсы потребуется развивать в первую очередь, то необходимо иметь в виду, что все инициативы, которые разрабатываются на базе АБИСС, носят некоммерческий характер, выдвигаются и воплощаются силами членов Ассоциации. В данном случае прежде всего необходимо желание кого-то из членов Ассоциации лидировать данные инициативы. Что касается компетенций, то их у членов АБИСС накоплено достаточно. Тем не менее всегда есть куда расти». Б.О