Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

Ксения ЗАСЕЦКАЯ
старший консультант отдела
консалтинга АО «ДиалогНаука»

НОВЫЙ ВЕКТОР

В РАЗВИТИИ РЕГУЛЯТОРНЫХ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

С момента выхода первой редакции Стандарта СТО БР ИББС-1.0 прошло 16 лет. За это время Банком России совместно со специалистами в области защиты информации проведена огромная работа по стандартизации требований по информационной безопасности для финансовых организаций. Но «рекомендательный» статус СТО БР ИББС не позволял создать единую, измеряемую и применимую ко всем финансовым организациям методологическую основу для реализуемых систем обеспечения информационной безопасности.

Подходы, заложенные как в СТО БР ИББС-1.0, так и в методику оценки соответствия СТО БР ИББС-1.2, не позволяли для финансовых организаций разного «масштаба» проводить сбалансированную политику в области защиты информации по нескольким основным причинам:

- *слишком большая обобщённость требований* — большинство требований имело формулировку «должны быть документально определены и утверждены руководством, должны выполняться и контролироваться процедуры…», позволяющую организациям самостоятельно выбирать глубину реализации с целью получения «положительной» оценки соответствия в ущерб качеству реализации и соответствию актуальным угрозам безопасности информации;
- *отсутствие градации* требований в зависимости от уровня значимости организации для финансового рынка в целом (нельзя подводить все организации под одни требования, которые могут быть легко реализованы в инфраструктуре крупных участников рынка, но невыполнимы с экономической точки зрения в маленьких организациях);
- СТО БР ИББС ориентирован в первую очередь на кредитные организации.

Двигаясь от СТО БР ИББС с добровольной областью применения (выбираемой кредитной организацией самостоятельно) к текущим Положениям Банка России с насколько это возможно в официальных документах формализованной областью применения (Положения 382-П, 672-П, 683-П и 684-П) появилась необходимость создания единой методологической основы к формализации требований к защите информации. Такой основой стали первые документы из серии Национальных стандартов ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (требования) и ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценка соответствия».

Вчитываясь в положения Национального стандарта ГОСТ Р 57580.1–2017, мы видим преемственность:

- необходимость построения сбалансированной, основанной на оценке рисков и моделировании угроз безопасности информации, экономически обоснованной системы обеспечения информационной безопасности;
- восприятие системы обеспечения информационной безопасности не как единожды созданного и статичного продукта, а как динамической системы, представляющей собой совокупность процессов обеспечения информационной безопасности и процессов управления информационной безопасности (цикл Plan — Do — Check — Act).

Однако, как и написано в Положениях Банка России, переводящих Национальный стандарт в область обязательных к применению документов, ГОСТ Р 57580.1 должен использоваться как базовый набор мер, необходимых к реализации на уровне ИТ-инфраструктуры финансовых организации, а требования к мерам защиты информации на уровне технологических процессов определяются соответствующими нормативными документами Банка России.

Банк России даёт возможность финансовым организациям делать выбор мер защиты информации, основываясь на формализованных в нормативных документах критериях, проводить их адаптацию и уточнение (с учётом особенностей ИТ-инфраструктуры и результатов моделирования угроз), а также предоставляет возможность применения компенсирующих мер (экономическая целесообразность). При этом Банк России уходит от «самооценок» в сторону внешних независимых аудитов.

Такой подход должен позволить получать повторяемые результаты, как один из критериев независимости аудита, и отслеживать состояние информационной безопасности финансовых организаций по единой методологии.

Изменился и подход к формированию базовых требований:

- градация требований исходя из выбранного уровня защиты информации: «минимальный», «стандартный» или «усиленный»;
- переход от общих требований «должно быть определено, выполняться и контролироваться» к детальным требованиям по основным процессам защиты информации;
- определение уровня реализации требований (организационные меры или технологические) и смещение в сторону необходимости технической реализации, особенно в контурах безопасности соответствующих усиленному уровню;
- расширение перечня требований, которые должны быть реализованы на уровне автоматизированных систем;
- применение PDCA-модели к каждому процессу защиты информации, а не к финансовой организации в целом;
- отсутствие дублирования требований, описанных в соответствующих документах других регуляторов, например, в ГОСТ Р 57580.1 отсутствуют требования к процессам применения средств криптографической защиты информации.

В ГОСТ 57580.1 *отсутствуют требования о необходимости обязательного* применения сертифицированных средств защиты информации, однако дана отсылка к результатам моделирования угроз (по аналогии с Приказом ФСТЭК России от 18 февраля 2013 г. № 21 и Постановлением Правительства Российской Федерации от 01.11.2012 № 1119):

Необходимо обеспечить применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определённых в модели угроз и нарушителей безопасности информации финансовой организации.

Методика оценки соответствия определена положениями ГОСТ Р 57580.2–2018, однако описание самого процесса проведения аудита информационной безопасности лучше раскрыто в документе СТО БР ИББС-1.1–2007 года. Данный подход может использоваться как при проведении оценки соответствия требованиям Положения 382-П, так и при проведении оценки соответствия требованиям ГОСТ Р 57580.1.

Ключевые отличия от подхода, применяемого в Положении Банка России 382-П:

- отсутствуют корректирующие коэффициенты, возникающие при невыполнении установленных требований;
- использование среднего арифметического как основного метода вычисления оценок по направлениям;
- введение «штрафов» за выявленные нарушения.

Единственное, на что стоит обратить внимание финансовым организациям — в разных нормативных документах определена разная периодичность оценки:

- для сегмента сбора и обработки биометрических персональных данных — 1 раз в год в соответствии с Приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 25.06.2018 г. № 321);
- для других контуров безопасности в соответствии с требованиями Банка России, например, в соответствии с Положением Банка России 683-П — 1 раз в два года.

* * *

Рассматривая развитие нормативной базы по защите информации на территории Российской Федерации в первую очередь обращаешь внимание, что растёт не только количество необходимых к реализации мер, но и увеличивается глубина проработки этих требований по отдельным направлениям, регулятор реагирует на изменяющиеся тренды и актуальные угрозы информационной безопасности. Поэтому стандартизация требований для организаций финансового рынка это логичное и прогнозируемое направление развития. Однако без должной поддержки и вовлечённости руководства и всех подразделений компаний, без корректного отношения компаний к аудиторам и выполнения аудиторами взятых на себя обязательств, таких, как соблюдение «аудиторской этики», обеспечение достоверности и независимости результатов аудитов, все попытки Банка России через регулирование донести до финансовых организаций актуальность текущих проблем информационной безопасности всё равно останутся «бумажной безопасностью».