Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

БЕЗОПАСНОСТЬ ФИНАНСОВ

СТАНДАРТ ГОСТ Р 57580.1–2017 — ПЕРВЫЙ В НОВОЙ ЭКОСИСТЕМЕ РЕГУЛИРОВАНИЯ ИБ В КОМПАНИЯХ, ПОДОТЧЁТНЫХ ЦЕНТРОБАНКУ

В августе 2017 года Ростехрегулирование утвердило национальный стандарт ГОСТ Р 57580.1–2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер». На данный момент национальный стандарт является рекомендательным, но в нём содержится, например, такое положение: «настоящий стандарт применяется путём включения нормативных ссылок на него в нормативных актах Банка России и (или) прямого использования устанавливаемых требований во внутренних документах финансовых организаций, а также в договорах». Банком России разработаны и опубликованы проекты положений, устанавливающих обязанность кредитных и некредитных финансовых организаций выполнять требования ГОСТ Р 57580.1–2017, начиная с 2021 года. Более того, ссылки на необходимость выполнения требований данного стандарта установлены в приказе Министерства цифрового развития, связи и массовых коммуникаций РФ для информационных технологий и технических средств, использующихся при обработке, включая сбор и хранение параметров биометрических персональных данных в целях идентификации (Приказ от 25.06.2018 г. № 321).

«...И ВОТ ОПЯТЬ»

Исторически Банк России разрабатывает собственные рекомендательные стандарты серии БР ИББС начиная с 2004 года, включающие в себя как базовые документы, содержащие требования к реализации системы обеспечения информационной безопасности и описание порядка проведения оценки соответствия (в том числе методику оценки соответствия), так и рекомендации по реализации отдельных процессов управления и обеспечения ИБ, таких как оценка рисков ИБ, менеджмент инцидентов ИБ, обеспечение ИБ на стадиях жизненного цикла автоматизированных банковских систем и другие. Область применения СТО БР ИББС определялась организацией банковской системы самостоятельно.

С выходом Положения Банка России 382-П были формализованы требования по обеспечению информационной безопасности при осуществлении переводов денежных средств, которые учитывали специфичные процессы и используемые информационные технологии: информационные системы дистанционного банковского обслуживания (в том числе использование мобильных приложений), терминальные устройства дистанционного банковского обслуживания (банкоматы и платёжные терминалы). При этом общие требования к основным процессам обеспечения информационной безопасности в большей степени дублируют положения СТО БР ИББС.

ГОСТ 57580.1–2017 является логичным продолжением многолетней работы Банка России в области стандартизации вопросов обеспечения информационной безопасности, так как в область его «потенциального» действия входят не только банки, но и другие финансовые организации (микрофинансовые организации, бюро кредитных историй, страховые компании и другие).

ОСНОВНЫЕ ПОЛОЖЕНИЯ

Стандарт ГОСТ Р 57580.1–2017 разработан совместно Центробанком и НПФ «КРИСТАЛЛ» (является одним из разработчиков документов Банка России в области стандартизации СТО БР ИББС) и внесён на рассмотрение в Ростехрегулирование техническим комитетом 122 (ТК-122)»Стандарты финансовых операций».

Положения стандарта могут использоваться кредитными и некредитными финансовыми организациями, а также субъектами национальной платёжной системы для достижения следующих целей защиты информации:

- определение требований к составу и содержанию организационных и технических мер защиты информации;
- соответствие состава и содержания мер защиты информации актуальным угрозам безопасности информации и уровню принятого организацией операционного риска (риск-аппетиту);
- обеспечение эффективного контроля состояния защиты информации на основе стандартизованного подхода.

Определение требований к составу и содержанию организационных и технических мер защиты информации осуществляется на основании выбранного уровня защиты. Стандартом установлены три уровня защиты: минимальный (третий), стандартный (второй) и усиленный (первый). Причём в финансовой организации могут быть выделены несколько контуров безопасности, каждый из которых может защищаться по своему уровню.

В соответствии с опубликованным *проектом* Положения Банка России «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности» установлены следующие критерии определения необходимого уровня защиты:

- 1-й уровень защиты (усиленный) — для системно значимых кредитных организаций, выполняющих функции оператора услуг платёжной инфраструктуры значимых платёжных систем, кредитных организаций, значимых на рынке платёжных услуг, при осуществлении более 3 млн банковских операций (среднедневной показатель);
- 2-й уровень защиты (стандартный) — для всех остальных кредитных организаций.

Значение 3 млн единиц операций соответствует критерию отнесения объектов критической информационной инфраструктуры Банка к значимым.

Соответствие состава и содержания мер защиты информации актуальным угрозам безопасности информации и уровню принятого организацией операционного риска (риск-аппетиту) должно достигаться путем адаптации, исключения и дополнения базового набора мер по результатам моделирования угроз безопасности информации и оценки рисков с учётом особенностей информационной инфраструктуры и реализуемых бизнес-процессов и/или технологических процессов, связанных с предоставлением финансовых, банковских услуг, а также услуг по осуществлению переводов денежных средств организации.

ГОСТ Р 57580.1–2017 описывает следующие основные направления в рамках организации системы защиты информации Банка:

- обеспечение защиты информации при управлении доступом;
- обеспечение защиты вычислительных сетей;
- контроль целостности и защищённости информационной инфраструктуры;
- защита от вредоносного кода;
- предотвращение утечек информации;
- управление инцидентами защиты информации;
- защита среды виртуализации;
- защита информации при осуществлении удалённого логического доступа с использованием мобильных (переносных) устройств;
- защита информации на этапах жизненного цикла автоматизированных систем и приложений.

В рамках каждого направления определен перечень мер, необходимых к реализации как в виде организационных мероприятий по защите информации, так и путём применения специализированных средств защиты информации. Если мера защиты информации не может быть реализована, то необходимо рассмотреть возможность (а в отдельных случаях необходимость) применения компенсирующих мер, направленных на обработку рисков, связанных с реализацией тех же угроз безопасности (перечень рассматриваемых угроз должен учитывать положения базовой модели угроз и нарушителей безопасности информации, описанные в Приложении А к ГОСТ Р 57580.1–2017). При этом выбор компенсирующих мер должен быть формализован и закреплён во внутренних нормативных документах организации.

Также стоит обратить внимание, что часть мер, описанных в стандарте, дополняют друг друга и могут быть использованы как компенсирующие.

Обеспечение эффективного контроля состояния защиты информации на основе стандартизованного подхода должно достигаться путём реализации следующих мероприятий:

- осуществление мониторинга и контроля состояния защиты информации;
- проведение оценки эффективности реализованных мер;
- анализа и совершенствования системы защиты информации;
- проведения периодической независимой оценки выполнения установленных требований.

А СУДЬИ КТО?

Примерно через полгода после принятия ГОСТ Р 57580.1–2017 была принята методика оценки соответствия (ГОСТ Р 57580.2–2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»). Методика оценки соответствия содержит описание как процесса проведения оценки соответствия, так и требования к формированию отчётных материалов по результатам оценки.

Оценка выбора и реализации финансовой организацией организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1–2017 должна проводиться только независимой организацией

Оценка выбора и реализации финансовой организацией организационных и технических мер ЗИ в соответствии с требованиями ГОСТ Р 57580.1–2017 должна проводиться только независимой организацией: обладающей необходимой компетенцией (порядок оценки такой компетенции не определён) и лицензией на деятельность по технической защите конфиденциальной информации.

И если процесс оценки соответствия требованиям ГОСТ Р 57580.1–2017 не сильно отличается от процесса, описанного в документах стандарта Банка России СТО БР ИББС-1.1, то подход к оценке реализации мер защиты информации кардинально изменён:

1. Из методики убраны оценки, соответствующие состоянию «не в полной мере», «практически полностью», «что-то делается», позволявшие довольно расширенное толкование со стороны проверяющих: все меры, описанные в разделе 7 ГОС Р 57580.1–2017, оцениваются по следующей шкале:
   - 0 — мера не выбрана;
   - 1 — мера выбрана;
2. Процессы управления информационной безопасности (планирование, реализация, контроль и совершенствование) рассматриваются не в разрезе всей организации, а применительно к 8 основным процессам, описанным в разделе 7 ГОСТ Р 57580.1–2017.
3. Перечень мер защиты информации, подлежащих оценке, может быть скорректирован по результатам работ по их адаптации и/или применения компенсирующих мер, направленных на обработку рисков, связанных с реализацией тех же угроз безопасности.
4. Если в организации выделены несколько контуров безопасности, то оценка должна формироваться независимо для каждого контура с общей итоговой оценкой соответствий всей организации.

Другим нововведением, определяемым ГОСТ Р 57580.2–2018, являются детализированные требования к отчётным документам, формируемым по результатам оценки соответствия. К таким требованиям в том числе относятся:

- отчёт по результатам оценки соответствия защиты информации должен быть прошит и скреплён мастичной печатью проверяющей организации с указанием количества листов в заверительной надписи, подписанной руководителем проверяющей группы;
- для каждого электронного документа, файла данных, прилагаемых к отчёту по результатам оценки соответствия ЗИ, должны быть вычислены хэш-функции, реализованной в соответствии с ГОСТ Р 34.11–2012.

* * *

Выпущенные под контролем Банка России национальные стандарты ГОСТ Р 57580.1–2017 и ГОСТ Р 57580.2–2018 несколько нарушают традиции отраслевого стандарта СТО БР ИББС, тем не менее понятно, что это только первые документы в создаваемой экосистеме регулирования информационной безопасности в компаниях, которые подотчётны Центробанку. Аналогичный путь для банков, проделанный стандартом СТО БР ИББС, показывает, что со временем и ГОСТ Р 57580.1 также станет фактически обязательным, причем для значительно большего круга организаций, в частности, некредитных финансовых компаний. Поэтому для таких компаний логично рассмотреть возможность реализации данного стандарта уже сейчас. Пока конкретных сроков перевода требований ГОСТ в разряд обязательных официально не названо, в проектах Положений Банка России указан 2021 год.