ГОСТ Р 57580.1-2017[1], как и любой другой стандарт на территории Российской Федерации, не является обязательным для применения. Однако Банком России выпущены нормативные акты[2], устанавливающие необходимость применения ГОСТ Р 57580.1-2017. В статье подробно описаны процесс подготовки к оценке соответствия, состав подсистем защиты информации, которые должны быть реализованы в банке, этапы реализации мероприятий по защите информации, схема оценки соответствия.

Подготовка и проведение внешней оценки соответствия требованиям ГОСТ Р 57580.1-2017

Антон СВИНЦИЦКИЙ,
АО «ДиалогНаука», директор по консалтингу

С появлением в 2017 г. первого Национального стандарта серии «Безопасность финансовых (банковских) операций» — ГОСТ Р 57580.1-2017 — начался новый этап развития стандартизации для кредитных и некредитных финансовых организаций.

Основываясь на риск-ориентированном подходе, описанном еще в конце 90-х годов в документах серии BS 7799, и продолжая начатую в комплексе документов Банка России адаптацию этого подхода к специфике российской банковской системы, ГОСТ Р 57580.1-2017 формализует подход к построению системы организации и управления защитой информации на базе следующих принципов:

— определение области действия путем идентификации и учета объектов информатизации;

— выбор мер защиты информации исходя из значимости организации, объемов банковских операций и видов деятельности;

[1] Национальный стандарт серии «Безопасность финансовых (банковских) операций» ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер».

[2] Положения Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России» (далее – Положение № 672-П), от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» (далее – Положение № 683-П), от 17.04.2019 № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (далее – Положение № 684-П).

Антон СВИНЦИЦКИЙ

— адаптация выбранных мер с учетом технической возможности и экономической целесообразности их реализации (соответствие риск-аппетиту);

— обеспечение полноты и качества реализуемых мер посредством контроля и оценки их эффективности, в том числе путем проведения периодических независимых аудитов (оценок соответствия);

— постоянное совершенствование мер защиты информации.

Банк России в Положениях № 672-П, № 683-П и № 684-П установил необходимость применения ГОСТ Р 57580.1-2017 и определил:

— область применения;

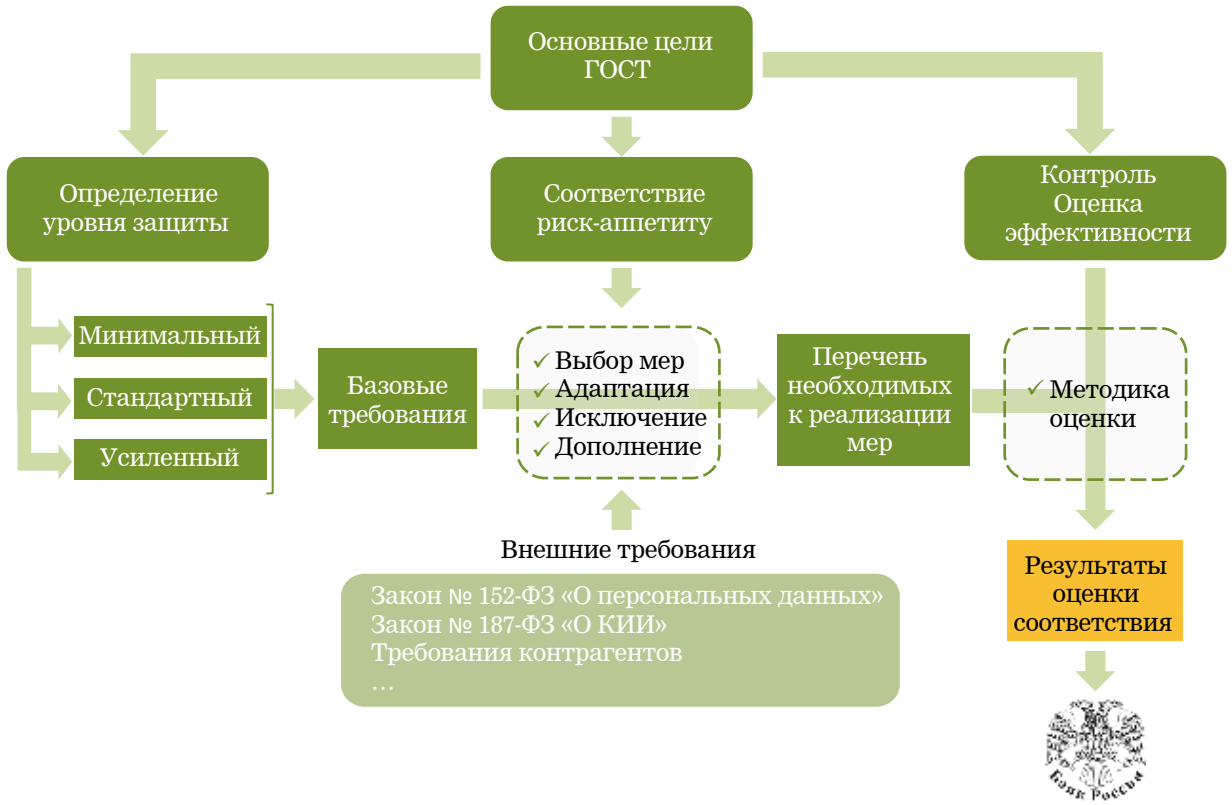
— критерии выбора уровня защиты;

— периодичность и форму проведения оценки соответствия.

Ссылки на необходимость применения ГОСТ для разных сегментов корпоративной сети банка представлены в табл. 1.

Рисунок

Цели ГОСТ Р 57580.1-2017



Подготовка и проведение внешней оценки соответствия требованиям ГОСТ Р 57580.1-2017

Таблица 1

Применение ГОСТ для разных сегментов корпоративной сети банка

№	Контур безопасности	Нормативный документ	Уровень защиты информации	Критерий	Срок вступления в силу	Периодичность оценки соответствия
1	ЕБС. Технологический участок сбора биометрических ПДн	Пункт 5 Приложения 3 к Приказу Минкомсвязи России от 25.06.2018 № 321[1]. Пункт 2.1.2 Методических рекомендаций Банка России от 14.02.2019 № 4-МР[2]	2	Все кредитные организации	Вступило в силу	Ежегодно в соответствии с Приказом № 321. Методические рекомендации № 4-МР периодичность не устанавливают
2	ЕБС. Технологический участок обработки собранных биометрических персональных данных физических лиц с целью передачи в ЕБС	Пункт 5 Приложения 3 к Приказу № 321	2	Все кредитные организации	Вступило в силу	Ежегодно
3		Пункт 2.3.2 Методических рекомендаций № 4-МР	2	Все кредитные организации	Вступило в силу	Не установлено
4		Пункт 2.3.3 Методических рекомендаций № 4-МР	1	Системно значимые кредитные организации	Вступило в силу	Не установлено
5	Участок осуществления переводов денежных средств с использованием ССНП[3]	Пункт 3 Положения № 672-П	2	Все кредитные организации	Вступает в силу 01.07.2021. Не ниже 4-го уровня к 01.01.2023	1 раз в 2 года
6	Участок осуществления переводов денежных средств с использованием СБП[4]	Пункт 4 Положения № 672-П	2	Все кредитные организации	Вступает в силу 01.07.2021. Не ниже 4-го уровня к 01.01.2023	1 раз в 2 года
7	Автоматизированные системы и объекты среды обработки защищаемой информации (информации	Пункт 3.1 Положения № 683-П	2	Все кредитные организации	Вступает в силу 01.01.2021. Не ниже 3-го уровня к 01.01.2021.	1 раз в 2 года

[1] «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» (далее — Приказ № 321).

[2] Методические рекомендации по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее — Методические рекомендации № 4-МР).

[3] Сервисы срочного и несрочного перевода.

[4] Система быстрых платежей.

Антон СВИНЦИЦКИЙ

Окончание табл. 1

№	Контур безопасности	Нормативный документ	Уровень защиты информации	Критерий	Срок вступления в силу	Периодичность оценки соответствия
	о переводах денежных средств)				Не ниже 4-го уровня к 01.01.2023	
8			1	Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг	Вступает в силу 01.01.2021. Не ниже 3-го уровня к 01.01.2021. Не ниже 4-го уровня к 01.01.2023	1 раз в 2 года
9	Автоматизированные системы и объекты среды обработки защищаемой информации (защищаемая информация в соответствии с п. 1 Положения № 684-П)	Пункт 5.2 Положения № 684-П	1	Центральные контрагенты, центральный депозитарий	Вступает в силу 01.01.2021. Не ниже 3-го уровня к 01.01.2022. Не ниже 4-го уровня к 01.01.2023	1 раз в год
10		Пункт 5.3 Положения № 684-П	2	Соответствующие критериям, описанным в п. 5.3 Положения № 684-П	Вступает в силу 01.01.2021. Не ниже 3-го уровня к 01.01.2022. Не ниже 4-го уровня к 01.07.2023	1 раз в 3 года
11		Пункт 5 Положения № 684-П	3	Остальные	Вступает в силу 01.01.2021	Не установлено

Идентификация объектов информатизации

Подготовка к внешней оценке соответствия (как и к внутренней самооценке/аудиту) должна начинаться с корректного определения и описания области применения ГОСТ Р 57580.1-2017, а именно с *«идентификации и учета объектов информатизации»*.

Подготовка и проведение внешней оценки соответствия требованиям ГОСТ Р 57580.1-2017

Область применения ГОСТ Р 57580.1-2017 устанавливается следующими нормативными документами:

1) Приказом № 321;
2) Положением № 672-П;
3) Положением № 683-П;
4) Методическими рекомендациями № 4-МР;
5) Положением № 684-П (для некредитных финансовых организаций).

ГОСТ Р 57580.1-2017 уточняет, что объект информатизации — это совокупность объектов и ресурсов доступа, необходимость учета которых предусмотрена не только общими положениями ГОСТ, но и конкретными мерами защиты информации, проверяемыми при оценке соответствия (например, базовым составом мер по организации учета и контроля состава ресурсов и объектов доступа, мерами ИУ.1–ИУ.3).

Определение контуров безопасности

Следующим шагом в документационной подготовке к оценке соответствия является определение контуров безопасности (совокупности объектов информатизации с единой степенью критичности, в отношении которых должен применяться единый перечень мер защиты информации).

В кредитной организации можно выделить следующие контуры безопасности (в случае необходимости реализовать одинаковый уровень защиты или в случае выбора мер по наивысшему из применимых уровней защиты их можно объединить):

— совокупность объектов информатизации, реализующих операции по переводу денежных средств;

— контур платежной системы Банка России (сервисы срочного и несрочного перевода и сервис быстрых платежей);

— совокупность объектов информатизации на участке сбора и обработки биометрических персональных данных;

— совокупность объектов информатизации, реализующих иные банковские операции (в соответствии со ст. 5 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»).

Для большинства финансовых организаций в соответствии с табл. 1 можно выделить один контур безопасности, в котором надо реализовать 2-й (стандартный) уровень защиты.

Для большинства кредитных организаций в соответствии с нормативными документами Банка России и Минкомсвязи России можно выделить один контур безопасности, в котором надо реализовать 2-й (стандартный) уровень защиты.

Выбор мер защиты информации

ГОСТ Р 57580.1-2017 вводит новый термин «выбор мер защиты информации», который раньше не применялся в нормативных документах Банка России (в отличие от документов ФСТЭК России, где необхо-

Антон СВИНЦИЦКИЙ

димость выбора мер защиты информации определена в том числе Приказом ФСТЭК России от 18.02.2013 № 21).

Выбор мер — это процесс, результаты которого должны быть документированы. Более того, рекомендуется документировать не только результаты выбора мер защиты, но и результаты их адаптации, исключения и дополнения. Форму документирования банк может выбрать самостоятельно, однако рекомендуется, чтобы она включала:

— название базовой меры;

— способ реализации (реализация путем применения организационной или технической меры защиты информации);

— результат адаптации/исключения/использования компенсирующей меры;

— уровень реализации (для документов — название документа, для технической реализации — уровень информационной инфраструктуры: аппаратный уровень, сетевой уровень, уровень операционных систем и т.п.).

Рекомендуется документировать не только результаты выбора мер защиты, но и результаты их адаптации, исключения и дополнения.

Разработка и доработка внутренних документов

Следующим этапом подготовки к оценке соответствия являются разработка/доработка внутренних документов и реализация технических мер защиты информации на соответствующем уровне информационной инфраструктуры (в т.ч. при помощи дополнительных наложенных средств защиты информации).

Разрабатываемые документы должны:

— содержать детальное описание организационных мер защиты информации, соответствующих уровню защиты;

— соответствовать требованиям к планированию деятельности, требованиям к системе организации и управления защитой информации, описанным в разделе 8.1 ГОСТ Р 57580.1-2017 (контроли ПЗИ.1–ПЗИ.3);

— быть утверждены в финансовой организации.

Разработку нормативной документации по вопросам защиты информации рекомендуется вести с учетом положений, отраженных в РС БР ИББС-2.0-2007 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0».

Применение технических мер защиты информации должно сопровождаться описанием порядка их реализации с обязательным указанием:

— правил размещения технических мер защиты информации в информационной инфраструктуре;

Подготовка и проведение внешней оценки соответствия требованиям ГОСТ Р 57580.1-2017

— руководств по применению технических мер защиты информации (включающих руководства по эксплуатации, контролю эксплуатации и использованию по назначению технических мер защиты информации);

— состава ролей и прав субъектов доступа, необходимых, чтобы обеспечить применение технических мер защиты информации (включающего эксплуатацию, контроль эксплуатации и использование по назначению мер защиты информации);

— параметров настроек технических мер защиты информации и информационной инфраструктуры, предназначенных для размещения технических мер защиты информации (при необходимости).

Названные положения могут быть отражены в документах, разрабатываемых при проектировании подсистем защиты информации или объектов информатизации, а также во внутренних документах, определяющих порядок реализации соответствующего процесса защиты информации.

Например, правила межсетевых экранов могут быть отражены в документе «Частная политика обеспечения информационной безопасности корпоративной сети».

Разработку нормативной документации по вопросам защиты информации рекомендуется вести с учетом положений, отраженных в РС БР ИББС-2.0-2007.

Подсистемы защиты информации

Анализируя требования ГОСТ Р 57580.1-2017, можно выделить базовый состав подсистем защиты информации, которые должны быть реализованы в банке для стандартного уровня защиты (табл. 2). В каждом конкретном случае набор подсистем должен выбираться исходя из результатов адаптации мер защиты информации и особенностей ИТ-инфраструктуры финансовой организации.

Таблица 2

Базовый состав подсистем защиты информации

№	Процесс	Подсистемы
1	Обеспечение защиты информации при управлении доступом	Подсистема многофакторной аутентификации администраторов. Подсистема защиты от несанкционированного доступа
2	Обеспечение защиты вычислительных сетей	Подсистема межсетевого экранирования. Подсистема обнаружения вторжений и выявления аномальной сетевой активности. Подсистема криптографической защиты информации при ее передаче по незащищенным каналам связи
3	Контроль целостности и защищенности информационной инфраструктуры	Подсистема анализа защищенности (в т.ч. контроль и анализ настроек прикладного программного обеспечения, операционных систем)

Антон СВИНЦИЦКИЙ

Окончание табл. 2

№	Процесс	Подсистемы
4	Защита от вредоносного кода	Подсистема эшелонированной мультивендорной антивирусной защиты (использование средств защиты от вредоносного кода различных производителей, как минимум для АРМ пользователей, серверного оборудования и межсетевого трафика)
5	Предотвращение утечек информации	Подсистема защиты информации от утечек (контроль как минимум следующих каналов: почтового трафика, веб-трафика, печати, съемных носителей информации)
6	Управление инцидентами защиты информации	Подсистема централизованного управления событиями информационной безопасности (хранение информации о событиях не менее трех лет и обеспечение возможности выполнять нормализацию, фильтрацию, агрегацию и классификацию данных регистрации событий защиты информации)
7	Защита среды виртуализации	Подсистема защиты сред виртуализации
8	Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств	Подсистема защищенного удаленного доступа

Применение PDCA-модели в защите информации

Все мероприятия по защите информации (как организационные, так и технические) в соответствии с ГОСТ Р 57580.1-2017 должны реализовываться по циклической PDCA-модели (модели Деминга–Шухарта Plan–Do–Check–Act).

На этапе «Реализация» (Do) должны обеспечиваться:

— применение мер защиты информации;

— определение ролей, связанных с применением мер защиты информации (например, во внутренних нормативных документах);

— назначение ответственных лиц (например, в форме приказов о назначении на роль);

— обучение работников, назначенных на соответствующие роли;

— повышение осведомленности работников в области защиты информации.

На этапе «Контроль» (Check) должны обеспечиваться:

— контроль области применения процесса (соответствие области объектам информатизации, идентифицированным на начальном этапе реализации мер);

— контроль корректности эксплуатации технических мер защиты информации;

— контроль полноты реализации мер защиты информации;

Подготовка и проведение внешней оценки соответствия требованиям ГОСТ Р 57580.1-2017

— проверка знаний работников в части применения мер защиты информации.

На этапе «Совершенствование» (Act) должно обеспечиваться принятие решений о необходимости совершенствования процессов управления и обеспечения информационной безопасности:

— по результатам анализа и расследования инцидентов;

— при обнаружении недостатков в рамках контроля системы защиты информации;

— при изменении целевых показателей допустимого остаточного операционного риска (риск-аппетита), связанного с обеспечением безопасности информации;

— при изменении базовой модели нарушителя и угроз безопасности;

— при изменении требований законодательства, требований регуляторов, партнеров, контрагентов.

Для получения положительных результатов при оценке соответствия результаты выполнения задач по защите информации на этапах контроля и совершенствования должны быть документированы.

Все мероприятия по защите информации (как организационные, так и технические) в соответствии с ГОСТ Р 57580.1-2017 должны реализовываться по циклической PDCA-модели.

Методика оценки соответствия

Нормативные документы Банка России устанавливают необходимость периодической оценки соответствия требованиям ГОСТ Р 57580.1-2017 с привлечением независимой аудиторской компании — лицензиата ФСТЭК России.

Оценка соответствия должна проводиться в соответствии с методикой, описанной в Национальном стандарте ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» (далее — Методика, ГОСТ Р 57580.2-2018).

Методикой установлены шесть качественных уровней, которые используются для оценки полноты реализации восьми основных процессов защиты информации. Более того, нормативными документами Банка России (Положениями № 672-П, № 683-П, № 684-П) установлены минимальные значения и сроки их достижения:

1) контур платежной системы Банка России (сервис срочного и несрочного перевода и сервис быстрых платежей): уровень соответствия не ниже четвертого с 1 января 2023 г.;

2) совокупность объектов информатизации, реализующих банковские операции (в соответствии со ст. 5 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности»):

Антон СВИНЦИЦКИЙ

— уровень соответствия не ниже третьего с 1 января 2021 г.;
— уровень соответствия не ниже четвертого с 1 января 2023 г.;

3) для некредитных финансовых организаций, подпадающих под действие Положения № 684-П:

— уровень соответствия не ниже третьего с 1 января 2022 г.;
— уровень соответствия не ниже четвертого с 1 июля 2023 г.

Оценка соответствия проводится по следующей схеме.

1. Определяется область оценки соответствия

Область оценки соответствия должна совпадать с областью применения ГОСТ Р 57580.1-2017. На основе предоставленной проверяемой организацией информации об области действия, о включенных объектах информатизации и местах их расположения проверяющая организация делает выборку, в рамках которой будет проводиться оценка соответствия.

Информация считается достоверной только в том случае, если она получена непосредственно в момент выполнения проверяемых процедур или функционирования процессов.

2. Формируется перечень неоцениваемых показателей

Перечень включает в себя:

— показатели, связанные с неиспользуемыми информационными технологиями (например, беспроводные сети);

— показатели, реализация которых не является необходимой для нейтрализации актуальных угроз безопасности, определенных в модели угроз и нарушителей.

3. Проводится документационная проверка

Цель проверки — оценить документационное обеспечение защиты информации и сформировать план оценки соответствия на месте. Обычно в плане отражаются:

— направление оценки;
— перечень ключевых тем;
— вовлеченные лица со стороны проверяемой организации;
— вовлеченные лица со стороны проверяющей организации;
— проверяемые объекты информатизации.

4. Проводится оценка соответствия на месте

Цель оценки — сформировать аудиторское суждение о состоянии процессов защиты информации. При оценке могут использоваться следующие формы сбора информации и свидетельств выполнения (реализации) мер:

Подготовка и проведение внешней оценки соответствия требованиям ГОСТ Р 57580.1-2017

— экспертная оценка устных высказываний сотрудников проверяемой организации в процессе опросов (интервьюирования);

— наблюдение членов проверяющей группы за процессами системы защиты информации и за деятельностью работников проверяемой организации в области оценки соответствия;

— оценка параметров конфигураций и настроек технических объектов информатизации и средств защиты информации;

— применение дополнительных технических методов анализа (анализ электронных журналов регистрации, анализ фактических настроек, анализ уязвимостей, тестирование на проникновение и т.п.).

Информация считается достоверной только в том случае, если она получена непосредственно в момент выполнения проверяемых процедур или функционирования процессов.

Если выборка не позволяет сделать однозначные суждения о выполнении и (или) невыполнении требований по защите информации, аудиторская организация должна расширить выборку.

5. Разрабатывается отчет по итогам проверки

Состав информации в отчете должен соответствовать требованиям Методики. В отчет должны быть включены оценки, характеризующие выбор банком организационных и технических мер защиты информации, применение организационных и технических мер на этапах жизненного цикла автоматизированных систем и характеризующие полноту реализации организационных и технических мер (всего 667 показателей).

Ключевые отличия Методики в части расчета этих показателей в сравнении с методикой оценки, определенной Положением № 382-П:

— большинство показателей оцениваются как 1 (мера выбрана) или 0 (мера не выбрана);

— отсутствуют корректирующие коэффициенты, снижающие оценку при значительном количестве невыполненных требований по защите информации.

Итоговая оценка формируется независимо для каждого процесса (а их всего 8) как сумма значений по направлениям с весовыми коэффициентами:

— оценка процесса защиты информации, связанная с выбором мер защиты информации (весовой коэффициент 0,5);

— оценка процесса защиты информации, характеризующая планирование процесса системы (весовой коэффициент 0,1);

— оценка процесса защиты информации, характеризующая реализацию процесса системы (весовой коэффициент 0,2);

Антон СВИНЦИЦКИЙ

— оценка процесса защиты информации, характеризующая планирование процесса системы (весовой коэффициент 0,125);

— оценка процесса защиты информации, характеризующая планирование процесса системы (весовой коэффициент 0,075).

Ключевым отличием в методике расчета итоговой оценки соответствия является необходимость корректировать оценку с учетом выявленных нарушений (значительных несоответствий). За каждое нарушение итоговая оценка снижается на 0,01. Такими нарушениями могут быть, например, следующие:

— в любой из систем, попадающих в область оценки соответствия, есть незаблокированные учетные записи уволенных работников;

— логический доступ осуществляется под коллективными неперсонифицированными учетными записями;

— отсутствует сетевая изоляция внутренних вычислительных сетей и интернета и (или) беспроводных сетей;

— используется нелицензионное программное обеспечение;

— не применяются средства защиты от воздействия вредоносного кода;

— и др.

Отчет о результатах оценки соответствия должен иметь сквозную нумерацию страниц, регистрационный номер, должен быть прошит нитью, не имеющей разрывов, и скреплен печатью проверяющей организации с указанием количества листов в заверительной надписи, подписанной руководителем проверяющей группы (по факту это несколько томов).

Проверяемая организация должна хранить отчет не менее пяти лет.

Введя новые понятия и сделав акцент на ключевые меры защиты информации для финансовых организаций разных размеров и степени критичности для банковской системы, ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2-2018 стали базовыми документами, на которых будут строиться отраслевые требования к созданию и оценке соответствия систем защиты информации. Для большинства банков данные изменения будут скорее техническими, так как необходимость выполнять требования по защите информации и проходить оценку соответствия для них не является чем-то новым.