В 2024–2025 годах в области защиты информации и операционной надежности финансовых организаций произошли существенные изменения. Были актуализированы положения Банка России, приняты новые методические рекомендации и разработаны проекты национальных стандартов серии ГОСТ Р 57580, направленные на унификацию требований и повышение уровня защищенности. Разберем ключевые изменения и их возможное влияние на практику оценки соответствия и обеспечения информационной безопасности.

# Изменения регулирования в области защиты информации: Банк России обновляет нормативную базу

**Антон СВИНЦИЦКИЙ**,
*АО «ДиалогНаука», директор по консалтингу*

## Первое направление — изменения в нормативных документах Банка России по защите информации

### Изменения в Положении № 851-П

Положение № 851-П[1], пришедшее на смену Положению № 683-П[2], существенно пересмотрено. Основные изменения касаются:

— формализации обязательной реализации цикла PDCA (планирование – реализация – контроль – совершенствование) для мер защиты информации, реализуемых на технологических участках реализации банковских операций;

— закрепления необходимости защиты банковской тайны;

— уточнения требования к сертификации или повторной оценке ПО (ОУД4) при изменении исходного кода прикладного ПО автоматизированных систем и приложений;

[1] Положение Банка России от 30.01.2025 № 851-П «Об установлении обязательных для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

[2] Положение Банка России 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».

# Изменения регулирования в области защиты информации: Банк России обновляет нормативную базу

— обязательного использования сертифицированных средств электронной подписи и средств удостоверяющего центра при применении усиленной неквалифицированной электронной подписи для обеспечения целостности электронных сообщений;

— необходимости контроля за изменением идентификационного модуля клиентских устройств (к такому модулю может относиться, например, SIM-карта);

— уточнения требований по регистрации и хранению информации о действиях клиентов;

— введения требований по взаимодействию с несовершеннолетними пользователями банковских услуг (уведомление родителей несовершеннолетних о выданных картах и об операциях, которые дети совершают с их использованием).

Эти меры направлены на формализацию технических требований и снижение неоднозначности в трактовке положений при проверках.

## Изменения в Положении № 821-П (проект)

Банк России подготовил проект изменений в Положение № 821-П[1]. Ключевые изменения направлены на гармонизацию с требованиями Положения № 851-П, в том числе включены следующие планируемые к принятию требования:

— включение филиалов иностранных банков в перечень субъектов регулирования в соответствии с положениями Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе». Определены минимальный и стандартный уровни защиты с коэффициентами соответствия (не ниже 0,71 и 0,86 соответственно), срок перехода на стандартный уровень — с 2027 г.;

— реализация в отношении отдельных мер Положения № 821-П процессов цикла PDCA. По сути, тот же подход, что и в Методических рекомендациях Банка России № 3-МР (от 06.03.2025), однако количество мер значительно расширено.

К другим ключевым изменениям можно отнести следующие:

1. Детализированы требования к составу регистрируемых событий при осуществлении клиентами действий в АС:

— дата и время начала и окончания соединения сессии на транспортном уровне при авторизации устройства, с которого осуществлен доступ к системам дистанционного банковского обслуживания;

[1] Положение Банка России от 17.08.2023 № 821-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».

Антон СВИНЦИЦКИЙ

— идентификационная информация устройства (IP и порт) клиента и (или) сетевого оборудования;

— идентификационная информация автоматизированных систем (систем дистанционного банковского обслуживания), в том числе IP-адрес и порт;

— географическое местоположение устройства клиента.

2. Уточнены требования в части оценки соответствия прикладного ПО автоматизированных систем и приложения:

— вводится необходимость проведения сертификации или оценки соответствия по требованиям к оценочному уровню доверия (ОУД) не ниже чем ОУД4, предусмотренного ГОСТ Р ИСО/МЭК 15408-3-2013, при внесении изменений в исходный код (по аналогии с Положением № 851-П);

В проекте изменений в Положение № 821-П вводится необходимость проведения сертификации или оценки соответствия по требованиям к оценочному уровню доверия (ОУД) не ниже чем ОУД4, предусмотренного ГОСТ Р ИСО/МЭК 15408-3-2013, при внесении изменений в исходный код (по аналогии с Положением № 851-П).

— появляется право не проводить сертификацию ПО или оценку по ОУД4 в случае, если организация пройдет сертификацию ФСТЭК России своих процессов разработки в соответствии с ГОСТ 56939-2024 (за исключением ПО с СКЗИ) (данное положение вступает в силу с 01.10.2027).

3. Детализированы требования к защите информации при осуществлении переводов денежных средств с использованием биометрических персональных данных (ПДн):

— технологические участки были логично изменены: в них включены операции с использованием биометрических ПДн;

— информация, связанная с идентификацией и (или) аутентификацией с использованием биометрических ПДн, отнесена к защищаемой информации;

— требования по сертификации ПО (или проведению оценки по уровню ОУД4) теперь распространяются и на приложения, используемые для приема/передачи идентификатора электронного средства платежа, применяемого для расчетов с использованием биометрических ПДн;

— для защиты информации об идентификаторе электронного средства платежа, применяемого для расчетов с использованием биометрических ПДн, необходимо использовать СКЗИ КС1.

4. Утверждены/уточнены требования к отчетности в части реализованных мер защиты информации для субъектов национальной платежной системы:

— для операторов по переводу денежных средств — форма 0409071;

— для операторов услуг платежной инфраструктуры, являющихся кредитными организациями, — форма 0409071;

— для операторов услуг платежной инфраструктуры, не являющихся кредитными организациями, — форма 0403202;

# Изменения регулирования в области защиты информации: Банк России обновляет нормативную базу

— для операторов электронных платформ — форма 0420722.

Все требования (за исключением указанного выше) планируются к вступлению в силу с 01.10.2026.

## Второе направление – утверждение Банком России новых методических рекомендаций

1. «Методические рекомендации Банка России по расчету значений показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в целях составления отчетности об оценке выполнения требований к обеспечению защиты информации» (утв. Банком России 06.03.2025 № 3-МР).

Обновленные рекомендации исключают устаревшие ссылки (например, на Положение № 747-П[1]), интегрируют меры из Положения № 802-П[2], касающиеся Системы быстрых платежей, и требования по обеспечению безопасности цифрового рубля (требования устанавливаются Положением № 833-П[3]). Также сделаны незначительные редакционные уточнения формулировок.

2. «Методические рекомендации по управлению риском информационной безопасности и обеспечению операционной надежности» (утв. Банком России 21.03.2024 № 7-МР).

Рекомендации устанавливают подходы к управлению рисками реализации информационных угроз и обеспечению операционной надежности. Уточняется необходимость документирования и соблюдения процедур, связанных с выявлением и устранением уязвимостей и управлением инцидентами. Это первый шаг к внедрению полноценных подходов к обеспечению непрерывности бизнеса в рамках Национальных стандартов ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022.

3. «Методические рекомендации Банка России по проведению тестирования на проникновение и анализа уязвимостей информационной безопасности объектов информационной инфраструктуры организаций финансового рынка» (утв. Банком России 22.01.2025 № 2-МР).

Рекомендации описывают подход к определению области тестирования на проникновение и определению требований к таким услугам, в том числе при привлечении внешних поставщиков.

Методические рекомендации Банка России от 21.03.2024 № 7-МР устанавливают подходы к управлению рисками реализации информационных угроз и обеспечению операционной надежности. Это первый шаг к внедрению полноценных подходов к обеспечению непрерывности бизнеса в рамках ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022.

[1] Положение Банка России от 23.12.2020 № 747-П «О требованиях к защите информации в платежной системе Банка России».

[2] Положение Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России».

[3] Положение Банка России от 07.12.2023 № 833-П «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля».

Антон СВИНЦИЦКИЙ

## Третье направление — изменение существующих и разработка новых национальных стандартов серии ГОСТ Р 57580

### Проект изменений ГОСТ Р 57580.1 «Безопасность финансовых (банковских) операций. Базовый состав организационных и технических мер»

Проект предусматривает расширение области применения стандарта за пределы финансовых организаций. Изменены подходы к выбору и адаптации мер защиты с учетом актуальных угроз и особенностей ИТ-инфраструктуры. Ключевые изменения по каждому процессу защиты информации приведены в табл. 1.

Таблица 1

**Изменения в процессах защиты информации (проект изменений ГОСТ Р 57580.1)**

| | |
|---|---|
| Процесс 1 «Обеспечение защиты информации при управлении доступом» | Определены требования к управлению технологическими учетными записями (УЗ) и заданными по умолчанию УЗ.<br>Уточнены формулировки по контролю прав доступа и контролю действий пользователей.<br>Пароль пользователя — не менее 10 символов.<br>Использование менеджеров хранения паролей.<br>Добавлены требования к организации резервного копирования |
| Процесс 2 «Обеспечение защиты вычислительных сетей» | Уточнены требования к определению и контролю сетевого взаимодействия с сетью Интернет и использованию протоколов почтового обмена.<br>Уточнены требования к сегменту разработки и тестирования |
| Процесс 4 «Защита от вредоносного кода» | Уточнены формулировки использования антивирусного программного обеспечения (АВПО) на уровне виртуальной инфраструктуры.<br>Реализация работы АВПО в резидентном режиме на АРМ, серверах и виртуальной инфраструктуре |
| Процесс 5 «Предотвращение утечек информации» | Уточнены отдельные формулировки.<br>Определена необходимость контентного анализа при передаче графических файлов (сканов, фотографий) |
| Процесс 7 «Защита среды виртуализации» | Уточнено название процесса защиты информации «Защита сред виртуализации и контейнеризации».<br>Добавлены требования по защите операционных систем с системами контейнеризации и контейнеров.<br>Уточнены отдельные формулировки |
| Процесс 8 «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств» | Уточнено название процесса защиты информации «Защита информации при осуществлении удаленного доступа».<br>Уточнены формулировки по сегментированию.<br>Уточнены формулировки по требованиям к MDM-решениям[1].<br>Добавлено требование к шифрованию данных на устройствах, с которых осуществляется удаленный доступ |

[1] Mobile Device Management — управление мобильными устройствами.

# Изменения регулирования в области защиты информации: Банк России обновляет нормативную базу

## Проект изменений ГОСТ Р 57580.2 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия»

Ключевые положения:

— уточнено определение проверяющей организации;

— уточнены качественные уровни соответствия (от нулевого до пятого);

— уточнено понятие шкалы оценки выбора меры:

1 — мера выбрана (при предъявлении проверяющей организации свидетельств выбора в виде фактического применения);

0 — мера не выбрана (при отсутствии у проверяемой организации свидетельств выбора, состояния и срока применения и порядка применения выбранных мер, отсутствии технической возможности применения меры, необоснованном превышении сроков реализации применения меры либо невозможности обеспечить в организации условия, необходимые для применения меры);

— определен порядок обоснования применения компенсирующих мер;

— уточнены требования к содержанию отчета (в том числе определена возможность передачи в электронном виде с УКЭП);

— определены требования к срокам передачи отчетных материалов;

— уточнен перечень нарушений. Новые нарушения:

а) непроведение или некорректное проведение (без обоснования границ и модели нарушителя) тестирования на проникновение и анализа уязвимостей;

б) отсутствие реализации требований к безопасности удаленного доступа, мобильных (переносных) устройств;

в) выявление на момент проверки отсутствия фактов реализации выбранных (запланированных к реализации) мер защиты информации (для каждой установленной меры);

г) неустранение уязвимостей критичного и высокого уровня в установленные сроки;

— уточнен порядок формирования оценки для нескольких контуров безопасности.

## Проект ГОСТ Р 57580.х «Безопасность финансовых (банковских) операций. Требования к проверяющим организациям и руководящие указания по проведению оценки соответствия»

Проект национального стандарта направлен на определение единых требований к организациям, привлекаемым для проведения внешней

Антон СВИНЦИЦКИЙ

оценки соответствия, и использование единого подхода к такой оценке. Объект стандартизации: деятельность проверяющих организаций и процесс проведения оценки соответствия требованиям ГОСТ Р 57580.1 и иным (например, ГОСТ Р 57580.4). Устанавливаются требования, перечисленные в табл. 2.

Таблица 2

**Требования, установленные в проекте ГОСТ Р 57580.х**

| | |
|---|---|
| Требования к проверяющей организации | Отсутствие в реестрах недобросовестных поставщиков и банкротства.<br>Лицензия ТЗКИ.<br>Подтверждение участия в системе добровольной сертификации (СДС).<br>Наличие документированных политик.<br>Аттестованные в рамках СДС работники, привлекаемые к оценке соответствия.<br>Требования к привлечению соисполнителей |
| Требования к лицам, входящим в проверяющую группу | Требования к руководителям проверяющей группы: образование, подтверждение опыта работы, подтверждение квалификации по одному из национальных или международных стандартов в области информационной безопасности.<br>Требования к участникам проверяющей группы: образование, требования СДС (если установлены) |
| Требования к процессу оценки соответствия | 1. Планирование:<br>— область оценки;<br>— требования к заказчику (ресурсы, документы и т.д.);<br>— недопустимость установления целей (количественных или качественных).<br>2. Проведение:<br>— требование к выборке;<br>— обязательность включения областей, отданных на аутсорсинг (и предоставления соответствующих свидетельств);<br>— хранение свидетельств (сроки и порядок).<br>3. Требования к отчету, содержанию и срокам хранения |

## Проект ГОСТ Р 57580.5 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Методика оценки соответствия»

Проект стандарта определяет подходы к независимой оценке реализации мер по обеспечению операционной надежности. Ключевые особенности:

— методика оценки соответствия аналогична ГОСТ Р 57580.2-2018;

— требования к привлекаемым организациям: лицензия на техническую защиту конфиденциальной информации и компетенции персонала;

— формализованная проверка полноты реализации организационных и технических мер обеспечения операционной надежности.

Проект проходит обсуждение в ТК 122 и может стать основой для определения порядка оценки операционной надежности в кредитных

# Изменения регулирования в области защиты информации: Банк России обновляет нормативную базу

и некредитных организациях на основании требований Положений Банка России.

Итак, изменения в законодательстве и национальных стандартах в сфере защиты информации и операционной надежности отражают переход к более зрелому, унифицированному и прозрачному регулированию. Банкам предстоит адаптировать процессы под новые требования, усиливая контроль, прозрачность и документирование. При этом важно не только обеспечить формальное соответствие, но и интегрировать требования в практику управления рисками информационной безопасности, защиты информации и операционной надежности, не забывая учитывать особенности деятельности организации и их влияние на устойчивость всей финансовой системы Российской Федерации.