Банком России обозначены рекомендованные сроки внедрения стандартов ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022

Банком России опубликованы Методические рекомендации от 21.03.2024 № 7-МР, в которых изложены порядок и сроки внедрения финансовыми организациями ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022.

ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022, регламентирующие вопросы управления риском информационной безопасности и обеспечения операционной надёжности, введены в действие с 1 февраля 2023 года и до настоящего времени не были ни обязательными, ни рекомендованными к применению. Поднадзорные организации ожидали появления ссылок на новые стандарты при внесении изменений в соответствующие положения Банка России – № 716-П от 08.04.2020 по управлению операционным риском (и риском информационной безопасности как его подвидом), № 787-П от 12.01.2022 и № 779-П от 15.11.2021 по обеспечению операционной надежности.

Банк России внес ясность в вопрос о статусе новых стандартов. Стало понятно, каким финансовым организациям, какие меры стандартов и в какие сроки следует внедрять. И несмотря на то, что 7-МР рекомендует (а не обязывает), де-факто рекомендуемое Банком России является необходимым к исполнению.

Для понимания Методических рекомендаций обозначим, что ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022 устанавливают следующие уровни защиты, применительно к которым определяется состав мер, подлежащих реализации:

- усиленный/стандартный/минимальный в части управления риском информационной безопасности;
- усиленный/стандартный/минимальный в части обеспечения операционной надежности.

Относительно этих уровней защиты Банком России и рекомендовано финансовым организациям реализовывать требования к управлению риском информационной безопасности (ГОСТ Р 57580.3-2022) и обеспечению операционной надежности (ГОСТ Р 57580.4-2022).

Кредитным организациям

Кредитные организации обязаны в своей деятельности выполнять требования как к управлению риском информационной безопасности (глава 7 Положения № 716-П), так и к обеспечению операционной надежности (Положение № 787-П), поэтому им рекомендовано реализовывать меры обоих стандартов:

Тип кредитной организации	**Уровень защиты согласно ГОСТ Р 57580.3-2022**	**Уровень защиты согласно ГОСТ Р 57580.4-2022**	**Рекомендованный срок внедрения**	**Количество мер для внедрения**
Банк, размер активов которого составляет 500	Усиленный	Усиленный	до 31 декабря 2025 года	**222** по ГОСТ Р 57580.3-2022, **293** по

Тип кредитной организации	Уровень защиты согласно ГОСТ Р 57580.3-2022	Уровень защиты согласно ГОСТ Р 57580.4-2022	Рекомендованный срок внедрения	Количество мер для внедрения
миллиардов рублей и более				ГОСТ Р 57580.4-2022
Банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей	Усиленный	Стандартный	до 31 декабря 2026 года	**222** по ГОСТ Р 57580.3-2022, **275** по ГОСТ Р 57580.4-2022
Иные кредитные организации	Стандартный	Стандартный	до 31 декабря 2026 года	**210** по ГОСТ Р 57580.3-2022, **275** по ГОСТ Р 57580.4-2022

Некредитным финансовым организациям

Некредитные финансовые организации обязаны руководствоваться требованиями Положения № 779-П к обеспечению операционной надежности, поэтому 7-МР рекомендует им реализовывать только ГОСТ Р 57580.4-2022:

Тип некредитной организации	Уровень защиты согласно ГОСТ Р 57580.4-2022	Рекомендованный срок внедрения	Количество мер для внедрения
• Центральные контрагенты • Центральный депозитарий • Регистраторы финансовых транзакций	Усиленный	до 31 декабря 2026 года	**293**
Некредитные финансовые организации, указанные в подпункте 1.4.3 пункта 1.4 Положения № 757-П, в том числе: • Специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов. • Клиринговые организации • Организаторы торговли • Страховые организации	Стандартный	до 31 декабря 2026 года	**275**

Тип некредитной организации	Уровень защиты согласно ГОСТ Р 57580.4-2022	Рекомендованный срок внедрения	Количество мер для внедрения
• Негосударственные пенсионные фонды. • Репозитарии • Брокеры, дилеры, управляющие, депозитарии и регистраторы • Операторы инвестиционной платформы и операторы финансовой платформы			
Некредитные финансовые организации, указанные в подпункте 1.4.4 пункта 1.4 Положения № 757-П, в том числе: • Управляющие компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов • Форекс-дилеры • Общества взаимного страхования • Страховые брокеры • Иные, не указанные в подпункте 1.4.3 пункта 1.4 Положения № 757-П	Минимальный	до 31 декабря 2027 года	**190**

Как кредитным, так и некредитным финансовым организациям 7-МР рекомендуют разработать планы внедрения стандартов, предусматривающие выбор и применение необходимых для каждого уровня организационных и технических мер. Соответственно, планы должны укладываться в вышеуказанные сроки.

Что необходимо делать

Финансовым организациям предстоит большой объем работы. Проще будет тем, кто обстоятельно подошел к внедрению требований Положений 716-П и 787-П/779-П (какие-то меры будут уже реализованы), а также внимательно отнесся к составлению новой отчетности в Банк России – о показателях операционной надежности и применяемых организацией информационных технологиях (процесс «Идентификация критичной архитектуры» ГОСТ Р 57580.4-2022, требующий значительных ресурсов, будет во многом внедрен).

Для разработки планов внедрения стандартов необходимо будет не только изучить и понять их требования, но и провести аудит внутренних нормативных документов и процессов организации. Последующая реализация плана потребует командной скоординированной работы специалистов нескольких подразделений. А по итогам такой работы хорошей практикой будет провести повторный аудит на соответствие – чтобы убедиться, что необходимые меры внедрены, и внедрены так, как было запланировано.

Наши эксперты помогут и ответят на возникающие вопросы на любом этапе внедрения ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022 в вашей организации. Заполните форму обратной связи или позвоните по телефону для получения консультации. Менеджер свяжется с вами и вместе мы разработаем оптимальное решение для вашей компании.

ФБК обладает необходимым опытом и компетенциями для качественной подготовки организации к будущей проверке со стороны регулятора при минимальном вовлечении в работу ее специалистов. Для минимизации данного комплаенс-риска ФБК предлагает услугу «Консалтинг по выполнению требований ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022». В составе услуги:

1. предварительная оценка для выявления текущего уровня соответствия стандартам;
2. разработка рекомендаций для повышения уровня соответствия требованиям ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022;
3. разработка / доработка внутренней нормативной документации с учетом специфики организации и действующих в ней процессов.

Контакты для уточнения информации по требованиям ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022 и запроса коммерческих предложений:

Алексей Карпушкин
Руководитель практики аудиторских и консалтинговых услуг
в областях ИБ и ИТ
Aleksey.Karpushkin@fbk.ru

Михаил Манцуров
Руководитель направления аудиторских и консалтинговых услуг
в области ИБ
Mikhail.Mantsurov@fbk.ru