

ГОТОВНОСТЬ К ПРОВЕРКЕ БАНКА РОССИИ

чек-лист по ИТ и защите информации для МФО, КПК, ломбардов, брокеров и финтех-компаний
редакция от 23.09.2026, нормы сверены 23.09.2026

Положение 757-П обязывает выполнять требования ГОСТ Р 57580 по своему уровню защиты, а на усиленном и стандартном уровнях подтверждать это оценкой соответствия у лицензиата. МФО, КПК и ломбарды в перечни уровней пока не входят, для МФО минимальный уровень обязателен с 1 января 2027 года, для всех МФО с 2028 года. Разрывы обычно находят за месяц до проверки. Этот лист проходит за один день и показывает, где организация стоит сейчас. Каждая незакрытая строка получает цену и срок в карте разрывов.

0. Паспорт организации

Вид организации	
Уровень защиты по 757-П (усиленный, стандартный, минимальный или не установлен)	
Дата последней оценки соответствия и результат	
Проверки Банка России и предписания	

1. Описание защищаемого

- ☐ Перечень информационных систем составлен. Учётная система, сайт, личный кабинет, телефония, почта.
- ☐ Перечень защищаемой информации утверждён. Данные клиентов, операции, отчётность.
- ☐ Известно, где физически лежат данные и какие договоры с ИТ-поставщиками это закрывают.

2. Документы

- ☐ Политика информационной безопасности утверждена и совпадает с тем, как устроена работа.
- ☐ Ответственный за защиту информации назначен приказом.
- ☐ Политика обработки персональных данных опубликована, уведомление в Роскомнадзор подано, согласия собираются.
- ☐ Регламенты реагирования на инциденты и резервного копирования утверждены и знакомы сотрудникам.

3. Доступы

- ☐ Доступы поимённые, общих учётных записей нет, права выдаются по ролям с фиксацией.
- ☐ Уволенные отключаются в день увольнения. Проверено по последним трём.
- ☐ Администраторский доступ отделён от пользовательского, пароли в менеджере паролей, а не в чате.

4. Журналирование

- ☐ Действия в учётной системе оставляют след. Кто, что, когда.
- ☐ Входы в системы журналируются, журнал хранится не меньше срока по политике и защищён от правки задним числом.

5. Резервирование и восстановление

- ☐ Копии делаются автоматически по записанному расписанию и лежат отдельно от боевых систем.
- ☐ Восстановление проверено на практике, есть акт учений с фактическим временем.
- ☐ Целевое время восстановления и допустимая потеря данных записаны в плане восстановления.

6. Путь клиента и 115-ФЗ

- ☐ Проверка клиента по перечням встроена в путь заявки, а не держится в памяти сотрудника.
- ☐ Результат каждой проверки оставляет след в системе с датой и результатом.
- ☐ Правила внутреннего контроля актуальны, ответственный по ПОД/ФТ назначен.

7. Отчётность в Банк России

- ☐ Календарь форм и сроков ведётся, ответственный назначен.
- ☐ Формы собираются из систем автоматически, ручная сборка отмечена как разрыв.
- ☐ Понятно, кто готовит XBRL и чем проверяет, если формат предписан.

8. Инциденты

- ☐ Мониторинг доступности работает и оповещает живого человека.
- ☐ Известно, какие события требуют уведомления регулятора и в какой срок, шаблон уведомления заготовлен.
- ☐ Последний инцидент разобран письменно.

Итог

Блок	Готово	Частично	Нет	Первым закрыть
1. Описание				
2. Документы				
3. Доступы				
4. Журналирование				
5. Резервирование				
6. 115-ФЗ				
7. Отчётность				
8. Инциденты				

Оценку соответствия ГОСТ Р 57580 проводит организация с лицензией ФСТЭК, криптографию внедряют лицензиаты ФСБ. Этот лист готовит организацию к оценке и не заменяет её. Нормы: положение Банка России 757-П, ГОСТ Р 57580.1-2017 и 57580.2-2018, 115-ФЗ, 152-ФЗ.