

Изменения в Положение Банка России № 683-П. Разбор, сроки выполнения и последствия нарушения

СОДЕРЖАНИЕ

- 01** **Основные** изменения

- 02** **Что** необходимо сделать в первую очередь

- 03** **Разбор** сроков исполнения

- 04** **Последствия** неисполнения

01. Основные изменения

Указание Банка России от 18.02.2022 N 6071-У

"О внесении изменений в Положение Банка России от 17 апреля 2019 года N 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".

(Зарегистрировано в Минюсте России 20.06.2022 N 68919)

01. Основные изменения: ОУД 4 и сертификация

П. 4.1.

Было	Стало
Сертификация ПО на отсутствие НДВ или анализ уязвимостей по ОУД4	Сертификация ПО по 76 приказу ФСТЭК или оценка соответствия по ОУД4
К анализу по ОУД4 привлекать лицензиатов ФСТЭК	При выборе сертификации – 4 уровень для значимых банков и 5 для иных
	Оценка соответствия самостоятельно или привлечение лицензиатов ФСТЭК

01. Основные изменения: электронные сообщения

П. 5.1.

Было	Стало
Подписание способом, позволяющим обеспечить целостность	Обеспечить целостность
	Использование УКЭП, УНЭП, СКЗИ с имитозащитой*
	Случаи неприменения УКЭП, УНЭП, СКЗИ с имитозащитой*

* **Имитозащита** – защита целостности сообщения. Реализуется с помощью добавления к сообщению дополнительного кода, имитовставки, MAC, зависящей от содержания сообщения и секретного элемента, известного только отправителю и получателю (ключа).

01. Основные изменения: технология обработки защищаемой информации

П. 5.2.1

Было	Стало
Подтверждение совершенной операции.	Идентификация устройств клиентов
	Проверка абонентского номера
	Подтверждение совершаемой операции
	Подтверждение адреса электронной почты.

01. Основные изменения: ограничения по параметрам операций

п. 7

Было	Стало
<i>Вариант без изменений</i>	Добавлен П. 7.1 «Ограничения по параметрам операции»

Похожее требование встречалось в Положении Банка России № 382-П.

01. Основные изменения: требования к управлению инцидентами

П. 8

Было	Стало
Регистрация инцидентов.	Значения инцидентов в п.7.3 Положения 716-П
	Фиксация инцидентов в базе событий
	Информирование регулятора о принятых мерах по реагированию
	Информирование о сайтах в сети «Интернет»
	Предоставлять сведения регулятору через АС ЦБ РФ

01. Основные изменения: КИИ

П. 10

Было	Стало
<i>Вариант без изменений</i>	При обеспечении безопасности ПО, СВТ, Положение применяется наряду с требованиями 187-ФЗ

02. Что необходимо сделать в первую очередь

- **GAP**-анализ;
- **Внесение изменений** во внутренние документы всех уровней;
- **Закупка и внедрение** соответствующих требованиям технических решений/услуг;
- **Оценка** соответствия ОУД4;
- **Аудит** по 683-П;
- **Оценка** соответствия ГОСТ 57580.



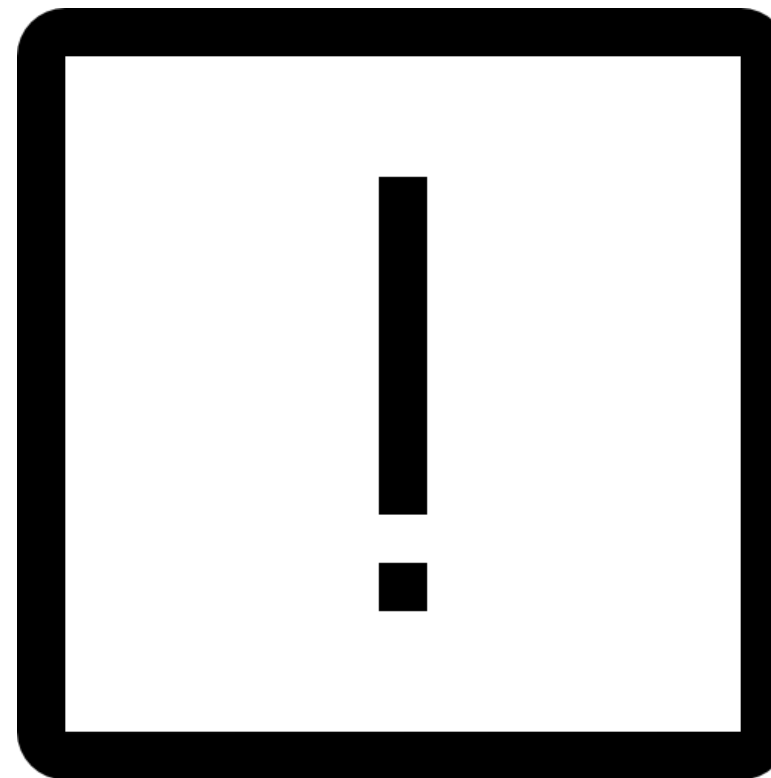
03. Разбор сроков исполнения

- **Указание Банка России от 18.02.2022 N 6071-У** (протокол заседания Совета директоров Банка России от 11 октября 2021 года N ПСД-24) вступает в силу с 1 октября 2022 года.

**Необходимо внести все изменения
до 1 октября 2022 года.**

04. Последствия неисполнения

- 1** Штрафные санкции со стороны регулятора
- 2** Рост риска несанкционированных списаний
- 3** Рост риска возникновения уязвимостей



ГОТОВЫ ОТВЕТИТЬ НА ВАШИ ВОПРОСЫ!

Музалевский Федор Александрович

Кандидат физико-математических наук;
Ведущий судебный эксперт;
Директор технического департамента **RTM Group**.

Кобец Дмитрий Андреевич

Эксперт в сфере информационной безопасности;
Заместитель директора технического департамента
RTM Group.



+7 (495) 197-64-95



info@rtmtech.ru



<https://rtmtech.ru>



rtm.group



t.me/kurilka_ib