

ИБ: Что делать банкам в 2021

В 2021 году банки столкнутся с необходимостью выполнять множество Положений от ЦБ (683-П, ОУД4, пентест, ЕБС, 382-П, SWIFT, 672-П, 719-П, 716-П).
На что нужно обратить особое внимание?



СОДЕРЖАНИЕ

01	Положение № 683-П
02	Анализ уязвимостей программного обеспечения по ОУД4
03	Тестирование на проникновение (Пентест)
04	Оценка соответствия ЕБС (приказ №321 Минкомсвязи)
05	Положение № 382-П
06	Независимая оценка SWIFT
07	Положение № 672-П
08	Положение № 719-П
09	Положение № 716-П
10	Сроки выполнений

Положение № 683-П

до 01.01.2021 – оценка по ГОСТ 57580

В состав требований 683-П входит (п.3) реализация уровня защиты информации в соответствии с ГОСТ 57580.1-2017. В соответствии с п. 9.2 необходимо обеспечить уровень соответствия ГОСТ не ниже второго (оценка 0.7) с 01.01.2021 г. Оценка (п.9) *«должна осуществляться с привлечением сторонних организаций, имеющих лицензию ФСТЭК на ТЗКИ»*. ГОСТ 57580.2-2018 предусматривает формат только внешней оценки соответствия. **Таким образом, до 01 января 2021 нужно было провести внешнюю оценку по ГОСТ Р 57580.2-2018*.**

* При этом ДИБ ЦБ в формате письменного ответа АБР представил два письма (от 22.05.2020 №56-1-11/265 и от 30.11.2020 №56-1-11/601), с различными сроками проведения оценки. Однако требуемый уровень не изменился к определенному сроку. Более того, в письме условием выполнения требований является достижение требуемого уровня соответствия в период с 2021 года по 2023 года, и не ограничивается количество проведения оценок соответствия проверяющей организацией (имеющей соответствующие лицензии ФСТЭК на ТЗКИ).

Анализ уязвимостей программного обеспечения по ОУД4

01.01.2020 – Положение 683-П

В соответствии с п. 4.1 683-П «*банки должны обеспечить использование прикладного ПО автоматизированных систем и приложений ... в отношении которых проведен анализ уязвимостей по ОУД4*».

01.01.2020 – Положение 382-П

Согласно п. 2.5.5_1. 382-П «... *обеспечить: использование для осуществления денежных переводов прикладного ПО автоматизированных систем и приложений ... которых проведен анализ уязвимостей по ОУД4*». Оба требования вступили в силу 01.01.2020 г. Отдельными письмами ЦБ дана отсрочка до середины 2021 года. Хочется напомнить, что положение 382-П все-таки еще действует.

01.01.2022 – Положение 719-П

В соответствии с Положением Банка России № 719-П ОПДС, БПА, ОУИО, ОУПИ, при осуществлении переводов денежных средств, должны обеспечивать использование прикладного ПО автоматизированных систем и приложений прошедших оценку соответствия не ниже чем ОУД 4 с 01.01.2022 г.

Тестирование на проникновение (пентест)

Положения 382-П и 683-П

Пункты 2.5.5_1. 382-П и п. 3.2. 683-П требуют «обеспечить **ежегодное** тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры».

Пункт 2.5.5_1 вступил в силу 01.07.2018

Поэтому рекомендуется ежегодный отсчёт именно от этой даты.

Очередная дата пентеста – 30.06.2021 г.



Оценка соответствия ЕБС (приказ №321 Минкомсвязи)

Приказ Минкомсвязи РФ от 25.06.2018 № 321,
Приложение 3, п. 5

Согласно п.5 Приложения 3 к приказу Минкомсвязи РФ от 25.06.2018 № 321, *«при обработке, сборе и хранении параметров биометрических ПДн в целях идентификации должны использовать информационные технологии и технические средства, соответствующие 2-му уровню защиты информации (стандартному), установленному ГОСТ Р 57580.1-2017».*

Приказ Минкомсвязи РФ от 25.06.2018 № 321,
Приложение 1, п. 9.2

В свою очередь п. 9.2. Приложения 1 к приказу требует **«ежегодное** проведение оценки соответствия требований по защите информации с привлечением сторонних организаций, имеющих лицензию ФСТЭК на ТЗКИ».

Требование подкреплено положениями Методических рекомендаций Банка России от 14.02.2019 № 4-МР.

Положение № 382-П

Никто не отменял 382-П

Оно является действующим с установленным сроками отчетности и, согласно пункту 2.15., необходимо проведение один раз в два года внешней оценки с привлечением организаций, имеющих лицензию ФСТЭК на ТЗКИ.

Перестает положение действовать только с 01.01.2022

Соответственно, невыполнение данного положения, в связи с последующей его отменой, не является уважительной причиной не проводить оценку соответствия. За невыполнение данного положения и не предоставление своевременной отчетности регулятор обязан применить санкции.

Независимая оценка SWIFT

В соответствии с CSCF 2021:

Начиная с середины 2021 года пользователям необходимо будет подтвердить свою аттестацию по CSCF v2021 независимой внутренней или внешней оценкой.

до 30.06.2021 – аттестация

Таким образом, до 30 июня 2021 года участникам необходимо провести аттестацию по CSCF v2021.

с 01.07.2021 по 31.12.2021 – подтверждение

В период с 1 июля 2021 года по 31 декабря 2021 года сделать независимую оценку – подтвердить пройденную аттестацию. Требования к организациям проводящим независимую оценку компанией SWIFT не установлено.

Однако рекомендуется учитывать требования регулятора и проводить внешнюю оценку имеющими лицензии ФСТЭК на ТЗКИ.

Положение № 672-П

с 01.07.2021 – оценка по ГОСТ 57580

С 1 июля 2021 года (п.20) необходимо проводить не реже одного раза в два года оценку СБП и ССНП по ГОСТ 57580, а так же по требованию Банка России.

к 01.01.2023 – уровень соответствия не ниже 4

А к 1 января 2023 года необходимо достичь уровня соответствия не ниже 4 согласно ГОСТ Р 57580.2-2018.



Положение № 719-П

01.01.2022 – оценка по ГОСТ 57580

п. 1.1 требует оценку по ГОСТ 57580, проводимую сторонним лицензиатом ФСТЭК. Согласно п.2.4, п. 3.7, п. 4.5, п. 6.8 – необходимо обеспечить 4-ый уровень соответствия (0.85) с момента вступления положения в силу (1 января 2022 г.). **Таким образом, до 01 января 2022 нужно провести внешнюю оценку по ГОСТ Р 57580.2-2018 и обеспечить 4 уровень соответствия.**



Положение № 716-П

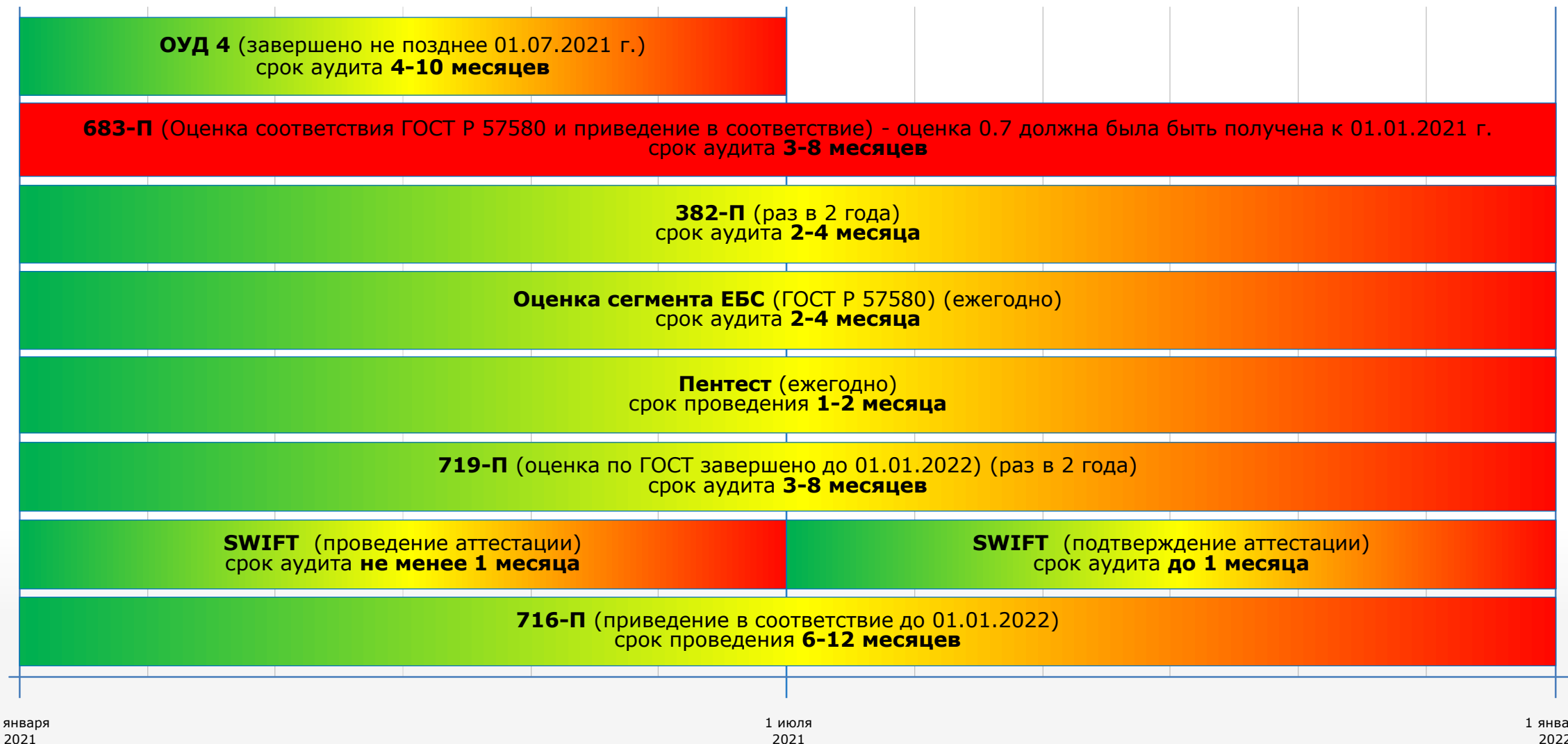
до 01.01.2022 – привести в соответствие

Вступил в силу 01 октября 2020 года.
Привести в соответствие систему управления рисками
необходимо до 01 января 2022 (п. 10.2).

Привлечение сторонней организации не требуется,
однако объем работы очень большой.



Сроки



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>



GroupRTM



rtm.group



@GroupRtm



rtm.group.Russia



t.me/kurilka_ib