RTM GROUP

Что делать Банкам по информационной безопасности в 2022 году

rtmtech.ru

СОДЕРЖАНИЕ

Краткий обзор положения № 719-П

Положение Банка России от 04.06.2020 N 719-П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств" (Зарегистрировано в Минюсте России 23.09.2020 N 59991)

Аудит по ГОСТ необходимо проводить **раз в два года**, по ОУД 4 и технологическим мерам **необходимо постоянное соответствие**.

Оценка соответствия должна быть достигнута к 01.01.2022 г.

Краткий обзор положения 683-П

Положение Банка России от 17 апреля 2019 г. 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»

Аудит по ГОСТ необходимо проводить раз в два года, по ОУД 4 и технологическим мерам необходимо постоянное соответствие.

Оценка соответствия не ниже 0,85 должна быть достигнута к 01.01.2023 г.

Краткий обзор положения 747-П

Положение Банка России от 23 декабря 2020 г. № 747-П «О требованиях к защите информации в платежной системе Банка России»

Аудит по ГОСТ необходимо проводить раз в два года.

Аудит ЕБС (приказ №321 Минкомсвязи)

Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. N 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»

Аудит по ГОСТ необходимо проводит раз в год.

Тестирование на проникновение и анализ уязвимостей (пентест)

Проводить тестирование на проникновение необходимо в соответствии с Положениями Банка России: 683-П, 719-П.

Пентест необходимо проводить ежегодно.

Краткий обзор Анализ уязвимостей и оценка соответствия ПО (ОУД 4)

Проведение анализа уязвимостей в 683-П

Проведение оценки соответствия – в 719-П.

Анализ проводится при каждой смене версии ПО.

Краткий обзор положения 716-П

Положение Банка России от 8 апреля 2020 г. № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

ЦБ РФ данным положением установил требования к системе управления операционным риском в кредитной организации и банковской группе. Приведен классификатор событий. Уточнены способы управления.

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

Краткий обзор независимой оценки SWIFT

Все пользователи SWIFT на ежегодной основе обязаны проводить **самоаттестацию/независимую внешнюю оценку** на предмет соответствия требованиям Программы безопасности пользователей SWIFT Customer Security Program, а также обеспечить выполнение всех обязательных элементов контроля безопасности, предусмотренных Концепцией обеспечения безопасности пользователей SWIFT (SWIFT Customer Security Controls Framework) **в срок до 31 декабря каждого года.**

Разбор сроков исполнения

Согласно 683-П:

Проведение оценки соответствия **не реже одного раза в два года**, с привлечением лицензиатов ФСТЭК (п.9).

С 1 января 2023

- Не ниже четвертого
- Числовая оценка < 0,85

Когда нужно соответствовать определенному уровню защиты?

747-П

- Оценка соответствия не реже **одного раза в два года** (п.20)
- Уровень соответствия **не ниже четвертого** (п.20) с **1 января 2023 года** (> 0,85)
- **ССНП, СБП** должны применять меры защиты информации, реализующие **стандартный** уровень (уровень 2) защиты информации.

Приказ 321

- Оценка соответствия проводится **ежегодно** с привлечением **сторонних организаций**, имеющих лицензию ФСТЭК (п.9.2 Приложения 1).
- Должны использоваться информационные технологии и технические средства, соответствующие **стандартному** уровню защиты информации (п.5 Приложения 3).
- Необходимый уровень соответствия **не указан**.

Когда нужно соответствовать определенному уровню защиты?

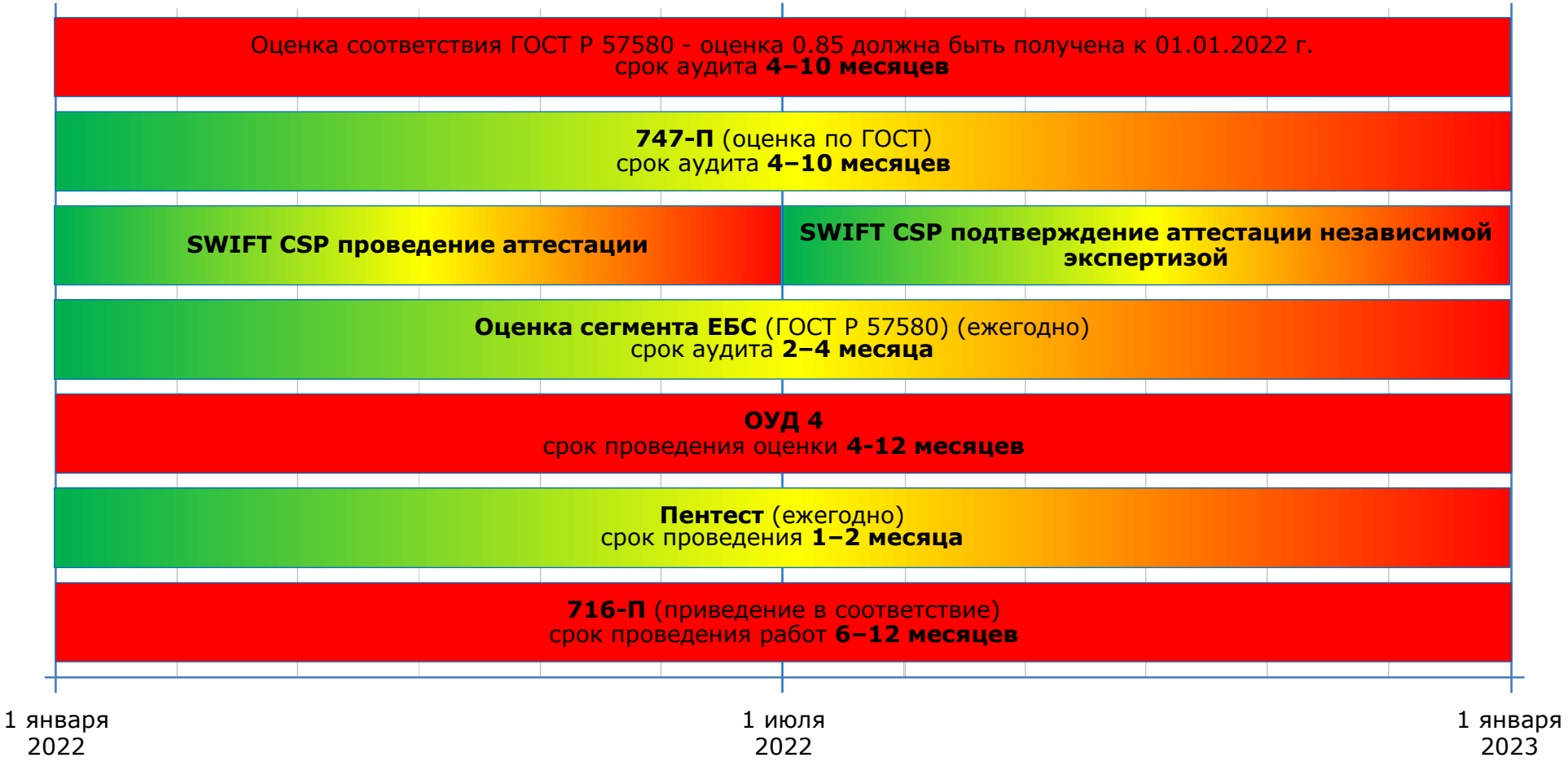
Согласно 719-П:

Согласно п.2.4, п. 3.7, п. 4.5, п. 6.8 – необходимо обеспечить 4-ый уровень соответствия (0.85) со дня вступления положения в силу (01.01.2022 г). Оценка соответствия защиты информации должна осуществляться **с привлечением сторонних организаций,** имеющих лицензию ФСТЭК (п.1.1).

Соответствовать с 1 января 2022

- Не ниже четвертого
- Числовая оценка < 0,85

Сроки исполнения положений



Поддержка банков в спорах по хищениям денежных средств

- **Экспертиза ДБО** на предмет соблюдения требований законодательства;
- **Анализ обстоятельств** хищения на предмет нарушения условий договора с клиентом;
- **Консультирование** и представительство в судах.

Краткий обзор федерального закона № 152-ФЗ

Федеральный закон N 152-ФЗ "О персональных данных«

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

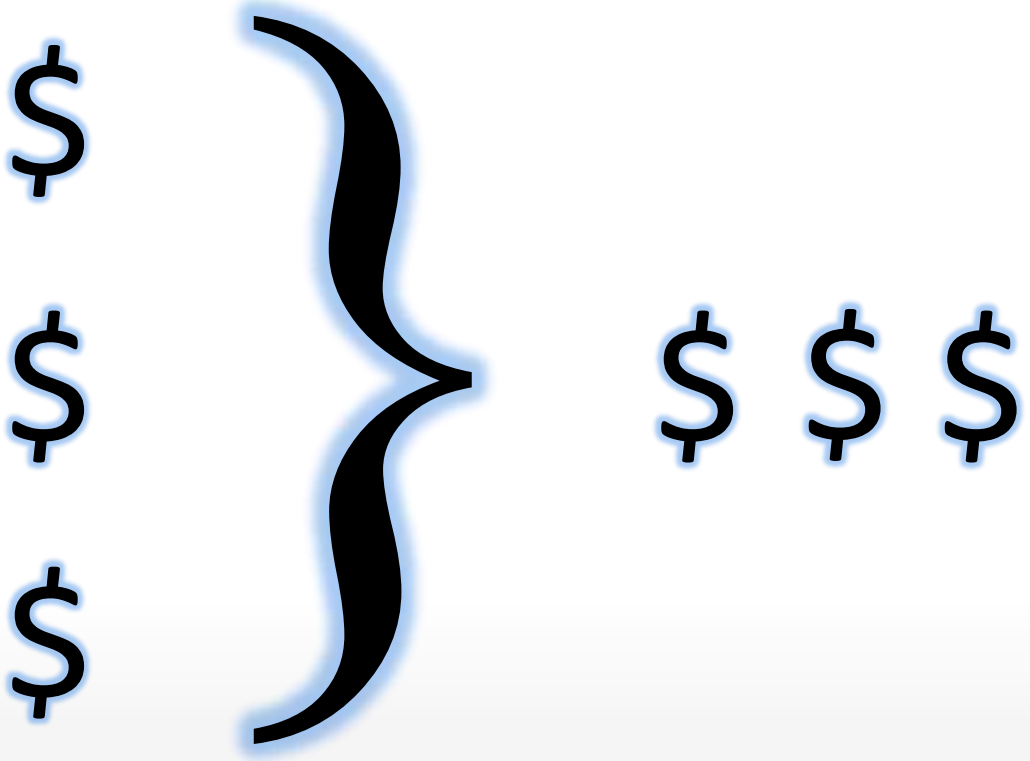
Аудит проводится на соответствие требованиям законодательства.

Рекомендации по оптимизации бюджета
Как выполнить все требования ЦБ и уменьшить на это затраты денежных средств

683-П

747-П

719-П



Рекомендации по оптимизации бюджета
Как выполнить все требования ЦБ и уменьшить на это затраты денежных средств

683-П

+

747-П

=

719-П

$ $ $ } $

Одним аудитом – можно!
Письмо ЦБ № 56-1-11/265 от 22.05.2020 г.

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