

ЧТО ДЕЛАТЬ?	КОГДА?	КАК ЧАСТО?	КТО ВЫПОЛНЯЕТ?
<b>683-П</b>			
Провести тестирование на проникновение	С 01.06.2019	Ежегодно	Все кредитные организации с привлечением лицензиатов ФСТЭК России по технической защите конфиденциальной информации (далее – ТЗКИ)
Обеспечить подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление электронного сообщения уполномоченным на это лицом	С 01.06.2019	Постоянно	Все кредитные организации
Обеспечить регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации на технологических участках	С 01.06.2019	Постоянно	Все кредитные организации
Обеспечить формирование и доведение до клиентов рекомендаций по защите информации (ЗИ)	С 01.06.2019	Постоянно	Все кредитные организации
Осуществить классификацию, регистрацию инцидентов ИБ и информировать о них Банк России	С 01.06.2019	Постоянно	Все кредитные организации
Использовать сертифицированное ПО или ПО, в отношении которого проведен анализ уязвимостей к оценочному уровню доверия не ниже ОУД 4	С 01.01.2020	–	Все кредитные организации с привлечением лицензиатов ФСТЭК России по ТЗКИ
Реализовать усиленный уровень ЗИ	С 01.01.2021	Постоянно	Значимые кредитные организации <sup>1</sup>
Реализовать стандартный уровень защиты	С 01.01.2021	Постоянно	Кредитные организации, не отнесенные к значимым
Провести оценку уровня соответствия требованиям к соответствующему уровню ЗИ, реализованного по ГОСТ Р 57580.1	С 01.01.2021	Не реже одного раза в два года	Все кредитные организации с привлечением лицензиатов ФСТЭК по ТЗКИ
Обеспечить уровень соответствия не ниже третьего по ГОСТ Р 57580.2	С 01.01.2021	Постоянно до 01.01.2023	Все кредитные организации
Обеспечить уровень соответствия не ниже четвертого по ГОСТ Р 57580.2	С 01.01.2023	Постоянно	Все кредитные организации
<b>684-П</b>			
Обеспечить подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить составление уполномоченным на это лицом	С 01.06.2019	Постоянно	Значимые некредитные финансовые организации <sup>2</sup>
Обеспечить регламентацию, реализацию, контроль (мониторинг) технологии безопасной обработки защищаемой информации	С 01.06.2019	Постоянно	Значимые некредитные финансовые организации
Обеспечить формирование и доведение до клиентов рекомендаций по ЗИ	С 01.06.2019	Постоянно	Все некредитные финансовые организации
Осуществить классификацию, регистрацию инцидентов ИБ и информировать о них Банк России	С 01.06.2019	Постоянно	Значимые некредитные финансовые организации
Использовать сертифицированное ПО или ПО, в отношении которого проведен анализ уязвимостей к оценочному уровню доверия не ниже ОУД 4	С 01.01.2020	–	Значимые некредитные финансовые организации самостоятельно или с привлечением лицензиатов ФСТЭК России по ТЗКИ
Определить применимый к организации уровень защиты информации, предусмотренный ГОСТ Р 57580.1	С 01.01.2021	Ежегодно <sup>3</sup>	Все некредитные финансовые организации
Провести тестирование на проникновение	С 01.01.2021	Не установлено	Значимые некредитные финансовые организации
Провести оценку уровня соответствия требованиям к соответствующему уровню защиты, реализованного по ГОСТ Р 57580.1	С 01.01.2021	Не реже одного раза в год	Некредитные финансовые организации, реализующие усиленный уровень защиты с привлечением лицензиатов ФСТЭК России по ТЗКИ
		Не реже одного раза в 3 года	Некредитные финансовые организации, реализующие стандартный уровень защиты с привлечением лицензиатов ФСТЭК России по ТЗКИ
Обеспечить уровень соответствия не ниже третьего по ГОСТ Р 57580.2	С 01.01.2022	Постоянно до 30.06.2023	Значимые некредитные финансовые организации

<sup>1</sup> Значимые кредитные организации – системно значимые кредитные организации; кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем; кредитные организации, значимые на рынке платежных услуг

<sup>2</sup> Значимые некредитные финансовые организации – организации, реализующие усиленный или стандартный уровень защиты

<sup>3</sup> Не позднее первого рабочего дня календарного года определения уровня защиты информации



ЧТО ДЕЛАТЬ?	КОГДА?	КАК ЧАСТО?	КТО ВЫПОЛНЯЕТ?
Обеспечить уровень соответствия не ниже четвертого по ГОСТ Р 57580.2	С 01.07.2023	Постоянно	Значимые некредитные финансовые организации
<b>672-П</b>			
Разместить объекты информационной инфраструктуры в выделенных сегментах вычислительных сетей	С 06.04.2019	Постоянно	ОПКЦ <sup>4</sup>
Обеспечить усиленный уровень защиты информации в выделенных сегментах	С 06.04.2019	Постоянно	ОПКЦ
Разработать документацию, определяющую состав и порядок применения организационных мер защиты информации и использования технических средств защиты информации	С 06.04.2019	–	ОПКЦ и кредитные финансовые организации, являющиеся участниками ССНП и СБП <sup>5</sup>
Обеспечить регистрацию информации, связанной с действиями клиентов участников СБП	С 06.04.2019	Постоянно	Кредитные финансовые организации, являющиеся участниками СБП
Обеспечить защиту электронных сообщений при обмене ими между участниками взаимодействия	С 06.04.2019	Постоянно	ОПКЦ и кредитные финансовые организации, являющиеся участниками ССНП и СБП
Обеспечить хранение входящих и исходящих электронных сообщений, подписанных электронной подписью, не менее пяти лет	С 06.04.2019	Постоянно	ОПКЦ и кредитные финансовые организации, являющиеся участниками ССНП и СБП
Обеспечить реализацию мер по противодействию осуществлению переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием СБП	С 06.04.2019	Постоянно	ОПКЦ
Информировать Банк России о нарушениях требований к обеспечению защиты информации при осуществлении переводов денежных средств	С 06.04.2019	Постоянно	ОПКЦ и кредитные финансовые организации, являющиеся участниками ССНП и СБП
Предоставить отчетность по 2831-У в части анализа обеспечения в платежной системе Банка России защиты информации при осуществлении переводов денежных средств	С 06.04.2019	Ежемесячно не позднее 10 раб. дней, следующего за отчетным. По требованию Банка России	Кредитные финансовые организации, являющиеся участниками ССНП и СБП
Обеспечить формирование и контроль реквизитов электронных сообщений с учетом Правил <sup>7</sup>	С 06.04.2019	Постоянно	ОПКЦ и кредитные финансовые организации, являющиеся участниками ССНП и СБП
Размещать объекты информационной инфраструктуры в выделенных сегментах вычислительных сетей	с 01.07.2021	Постоянно	Кредитные финансовые организации, являющиеся участниками ССНП и СБП
Обеспечить стандартный уровень защиты информации в выделенных сегментах	с 01.07.2021	Постоянно	Кредитные финансовые организации, являющиеся участниками ССНП и СБП
Применить средстваЗИ, реализующие двухстороннюю аутентификацию и шифрование информации на уровне звена данных или сетевом уровне, прошедшие оценку соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности	с 01.07.2020	Постоянно	ОПК при передаче сообщений в Банк России
	с 01.07.2021	Постоянно	Кредитные финансовые организации, являющиеся участниками ССНП, при передаче сообщений в Банк России
	с 01.07.2021	Постоянно	ОПКЦ и кредитные финансовые организации, являющиеся участниками СБП, при передаче сообщений между участниками СБП и ОПКЦ
Провести оценку уровня соответствия требованиям к соответствующему уровнюЗИ, реализованного по ГОСТ Р 57580.1	с 01.07.2021	Не реже одного раза в два года. По требованию Банка России	ОПКЦ и кредитные финансовые организации, являющиеся участниками СБП, при передаче сообщений между участниками СБП и ОПКЦ
Обеспечить уровень соответствия не ниже четвертого по ГОСТ Р 57580.2	с 01.01.2023	Постоянно	ОПКЦ и кредитные финансовые организации, являющиеся участниками СБП, при передаче сообщений между участниками СБП и ОПКЦ

<sup>4</sup> Операционный центр, платежный клиринговый центр другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием СБП

<sup>5</sup> Сервис срочного перевода и сервис несрочного перевода

<sup>6</sup> Сервис быстрых платежей

<sup>7</sup> Приложение к 672-П «Правила материально-технического обеспечения формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП, а также правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ»