ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«23» декабря 2020 г. № 747-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 62305
от 03 февраля 2021 г.

О требованиях к защите информации в платежной системе Банка России

Настоящее Положение на основании пункта 19 части 1 и части 9 статьи 20 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 18 декабря 2020 года № ПСД-30) устанавливает требования к защите информации в платежной системе Банка России.

1. Требования к защите информации в платежной системе Банка России (далее – требования к защите информации) должны выполнять прямые участники платежной системы Банка России, имеющие доступ к услугам по переводу денежных средств с использованием распоряжений о переводе денежных средств (далее – распоряжения) в электронном виде, предусмотренные абзацем вторым пункта 3.10 Положения Банка России от 24 сентября 2020 года № 732-П «О платежной системе Банка России», зарегистрированного Министерством юстиции Российской Федерации 10 ноября 2020 года № 60810 (далее – Положение Банка России от 24 сентября 2020 года № 732-П), являющиеся кредитными организациями (их филиалами)

(далее – участники обмена), а также операционный центр, платежный клиринговый центр другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей (далее – ОПКЦ), оператор услуг информационного обмена при предоставлении участникам обмена услуг информационного обмена при осуществлении переводов денежных средств с использованием сервиса быстрых платежей (далее – ОУИО СБП).

Требования к защите информации должны выполняться участниками обмена, ОПКЦ и ОУИО СБП с учетом требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленными в соответствии с частью 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) (далее – Федеральный закон от 27 июня 2011 года № 161-ФЗ).

2. Требования к защите информации, установленные настоящим Положением, распространяются на автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, применяемые для обработки защищаемой информации, перечисленной в пункте 2.1 Положения Банка России от 9 июня 2012 года № 382-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», зарегистрированного Министерством юстиции Российской Федерации 14 июня 2012 года № 24575, 1 июля 2013 года № 28930, 10 сентября 2014 года № 34017, 22 июня 2018 года № 51411 (далее – Положение Банка России от 9 июня 2012 года № 382-П) (далее при совместном упоминании – объекты информационной инфраструктуры).

3. Участники обмена при осуществлении переводов денежных средств

в платежной системе Банка России (далее – осуществление переводов денежных средств) с использованием сервиса срочного перевода и сервиса несрочного перевода (далее – участники ССНП) должны размещать объекты информационной инфраструктуры, используемые при осуществлении переводов денежных средств с использованием сервиса срочного перевода и сервиса несрочного перевода, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей участники ССНП должны применять меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определенный национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017).

4. Участники обмена при осуществлении переводов денежных средств с использованием сервиса быстрых платежей (далее – участники СБП) должны размещать объекты информационной инфраструктуры, используемые при осуществлении переводов денежных средств с использованием сервиса быстрых платежей, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей участники СБП должны применять меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определенный ГОСТ Р 57580.1-2017.

5. ОУИО СБП должен размещать объекты информационной

инфраструктуры в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей ОУИО СБП должен применять меры защиты информации, реализующие стандартный уровень (уровень 2) защиты информации, определенный ГОСТ Р 57580.1-2017.

6. ОПКЦ должен размещать объекты информационной инфраструктуры, используемые при предоставлении операционных услуг и услуг платежного клиринга участникам СБП, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) ОПКЦ должен применять меры защиты информации, реализующие усиленный уровень (уровень 1) защиты информации, определенный ГОСТ Р 57580.1-2017.

7. Участники ССНП, участники СБП, ОПКЦ и ОУИО СБП во внутренних документах должны определять состав и порядок применения организационных мер защиты информации и состав и порядок использования технических средств защиты информации.

7.1. Участники ССНП, участники СБП, ОПКЦ и ОУИО СБП должны принимать внутренние документы в рамках следующих процессов (направлений) защиты информации, определенных ГОСТ Р 57580.1-2017:

обеспечение защиты информации при управлении доступом;

обеспечение защиты вычислительных сетей;

контроль целостности и защищенности информационной инфраструктуры;

защита от вредоносного кода;

предотвращение утечек информации;

управление инцидентами защиты информации;

защита среды виртуализации;

защита информации при осуществлении удаленного логического

доступа с использованием мобильных (переносных) устройств.

7.2. Участники ССНП, участники СБП, ОПКЦ и ОУИО СБП должны определять во внутренних документах информацию, предусматривающую:

технологии подготовки, обработки, передачи и хранения сообщений, содержащих распоряжения в электронном виде (далее – электронные сообщения), и защищаемой информации на объектах информационной инфраструктуры;

состав и правила применения технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности электронных сообщений на этапах их формирования (подготовки), обработки, передачи и хранения, в том числе порядок применения средств криптографической защиты информации (далее – СКЗИ) и управления ключевой информацией СКЗИ;

план действий, направленных на обеспечение непрерывности и (или) восстановление деятельности, связанной с осуществлением переводов денежных средств;

лиц, допущенных к работе со СКЗИ;

лиц, ответственных за обеспечение функционирования и безопасности СКЗИ (ответственный пользователь СКЗИ);

лиц, обладающих правами по управлению криптографическими ключами, в том числе ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей.

7.3. ОПКЦ и ОУИО СБП должны определять во внутренних документах состав и правила применения технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности сообщений, содержащих реквизиты и иную информацию, необходимую для последующего формирования электронного сообщения, при осуществлении перевода денежных средств с использованием сервиса быстрых платежей (далее – информационные сообщения) на этапах формирования (подготовки), обработки, передачи и хранения информационных сообщений (при их

наличии).

ОПКЦ и ОУИО СБП должны обеспечивать применение технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности электронных сообщений и информационных сообщений (при их наличии) на этапах их формирования (подготовки), обработки, передачи и хранения.

8. Защита информации участниками ССНП, участниками СБП и ОПКЦ с помощью СКЗИ должна обеспечиваться в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года № 6382, 25 мая 2010 года № 17350, и технической документацией на СКЗИ.

9. Формирование и подписание электронных сообщений участника ССНП и ОПКЦ осуществляются в информационной инфраструктуре (автоматизированной системе) участника ССНП и ОПКЦ.

10. Передача и прием электронных сообщений участника ССНП осуществляются с использованием автоматизированного рабочего места обмена электронными сообщениями с платежной системой Банка России. Автоматизированное рабочее место обмена электронными сообщениями с платежной системой Банка России должно быть реализовано с использованием программного обеспечения Банка России и в соответствии с условиями по защите информации, выполнение которых предусмотрено договором, заключенным между Банком России и участником ССНП.

11. Участники ССНП, участники СБП, ОПКЦ и ОУИО СБП должны обеспечивать хранение входящих и исходящих электронных сообщений, подписанных электронной подписью, и средств, обеспечивающих проверку

электронной подписи, не менее пяти лет с даты подписания электронных сообщений.

12. При обмене электронными сообщениями между Банком России и ОПКЦ, Банком России и участниками ССНП должна применяться электронная подпись, сертификаты ключа проверки которой выданы Банком России участникам ССНП и ОПКЦ.

При обмене электронными сообщениями между ОПКЦ и участниками СБП должна применяться электронная подпись, сертификат ключа проверки которой выдан ОПКЦ участникам СБП.

При обмене электронными сообщениями между ОПКЦ, участниками СБП и ОУИО СБП должна применяться электронная подпись, сертификат ключа проверки которой выдан ОПКЦ участнику СБП, в том числе при обмене электронными сообщениями между ОПКЦ и ОУИО СБП, ОПКЦ и ОУИО СБП, оказывающим участнику СБП услуги по обеспечению подписания исходящих электронных сообщений и (или) зашифрования на прикладном уровне электронных сообщений, проверки электронной подписи во входящих электронных сообщениях и (или) расшифрования на прикладном уровне входящих электронных сообщений.

Хранение и использование криптографических ключей участника СБП, предназначенных для подписания исходящих электронных сообщений и (или) расшифрования на прикладном уровне входящих электронных сообщений, должны осуществляться в информационной инфраструктуре ОУИО СБП в аппаратных модулях безопасности, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности» (Собрание законодательства Российской Федерации, 1995, № 15, ст. 1269; 2019, № 49, ст. 6963) (далее – требования, установленные федеральным органом исполнительной власти в области

обеспечения безопасности). Доступ к криптографическим ключам участника СБП должен быть обеспечен только для участника СБП как владельца сертификата ключа электронной подписи.

При обмене электронными сообщениями между ОПКЦ и ОУИО СБПкриптографические ключи участника СБП, предназначенные для подписания исходящих электронных сообщений и (или) расшифрования на прикладном уровне входящих электронных сообщений, хранение и использование которых осуществляется в информационной инфраструктуре ОУИО СБП, изготавливаются участником СБП в аппаратных модулях безопасности самостоятельно. Формирование и передача в ОПКЦ запроса на сертификат ключа проверки электронной подписи осуществляется самостоятельно участником СБП.

13. Криптографические ключи участника ССНП, используемые при обмене электронными сообщениями между Банком России и участником ССНП, должны изготавливаться участником ССНП.

Криптографические ключи ОПКЦ, используемые при обмене электронными сообщениями между Банком России и ОПКЦ, должны изготавливаться ОПКЦ, если иное не предусмотрено договором о взаимодействии, заключаемым между Банком России и оператором внешней платежной системы в соответствии с частью 37 статьи 15 Федерального закона от 27 июня 2011 года № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) (далее – договор о взаимодействии).

Криптографические ключи участника СБП, используемые при обмене электронными сообщениями между ОПКЦ и участником СБП, должны изготавливаться участником СБП, если иное не предусмотрено договором об оказании операционных услуг, услуг платежного клиринга при осуществлении перевода денежных средств с использованием сервиса быстрых платежей, заключенным между участником СБП и ОПКЦ в соответствии с частью 1 статьи 17, частью 1 статьи 18 Федерального закона от 27 июня 2011 года

№ 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2014, № 19, ст. 2317; 2018, № 49, ст. 7524) (далее – договор об оказании услуг между участником СБП и ОПКЦ).

14. Организационные меры и (или) технические средства защиты информации, используемые при обмене электронными сообщениями при осуществлении переводов денежных средств, применяются с учетом следующих требований.

14.1. Участники СБП должны обеспечивать удостоверение электронной подписью электронных сообщений при их передаче клиентам участника СБП.

14.2. Участники СБП и ОПКЦ должны обеспечивать защиту электронных сообщений при передаче между участниками СБП и ОПКЦ посредством:

использования усиленной электронной подписи для контроля целостности и подтверждения подлинности электронных сообщений, состав которых определен договором об оказании услуг между участником СБП и ОПКЦ;

шифрования электронных сообщений на прикладном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, определенной в государственном стандарте Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель», утвержденном постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78 (М., ИПК Издательство стандартов, 1999) (далее – ГОСТ Р ИСО/МЭК 7498-1-99), с использованием СКЗИ, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

применения средств защиты информации, реализующих двухстороннюю аутентификацию и шифрование информации на уровне представления или ниже, в соответствии с эталонной моделью взаимосвязи открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1-99, прошедших

процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

Участники СБП, ОПКЦ и ОУИО СБП должны обеспечивать защиту электронных сообщений при их передаче между ОПКЦ, участниками СБП и ОУИО СБП в соответствии с требованиями, установленными абзацами вторым – четвертым настоящего подпункта.

Участники СБП должны обеспечить реализацию технологии подготовки, обработки и передачи электронных сообщений и защищаемой информации, обеспечивающей проверку соответствия (сверку) реквизитов исходящих в адрес ОПКЦ электронных сообщений с реквизитами соответствующих им входящих электронных сообщений клиентов участников СБП и реквизитами электронных сообщений, содержащих распоряжения в электронном виде, на основе которых участником СБП осуществляются операции по списанию денежных средств со счетов клиентов.

14.3. Участники ССНП должны обеспечивать защиту электронных сообщений при их передаче в Банк России посредством:

формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП в соответствии с пунктом 1 Правил материально-технического обеспечения формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП, а также правил материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ, установленных приложением к настоящему Положению в соответствии с частью пятой статьи 5 Федерального закона «О банках и банковской деятельности» (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ) (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2019, № 30, ст. 4151) (далее – Правила материально-технического

обеспечения);

использования двух усиленных электронных подписей – электронной подписи, применяемой в контуре формирования электронных сообщений, и электронной подписи, применяемой в контуре контроля реквизитов электронных сообщений, – для контроля целостности и подтверждения подлинности электронных сообщений;

применения третьего варианта защиты, предусмотренного Альбомом электронных сообщений, размещенным на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее соответственно – сеть «Интернет», официальный сайт Банка России), который ведется Банком России в соответствии с пунктом 5.2 Положения Банка России от 24 сентября 2020 года № 732-П;

шифрования электронных сообщений на прикладном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1-99, с использованием СКЗИ, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

применения средств защиты информации, реализующих двухстороннюю аутентификацию и шифрование информации на уровне звена данных или сетевом уровне в соответствии с эталонной моделью взаимосвязи открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

14.4. ОПКЦ должен обеспечивать защиту электронных сообщений при их передаче в Банк России посредством:

обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ в соответствии с пунктом 2 Правил материально-технического обеспечения;

использования двух усиленных электронных подписей – электронной

подписи, применяемой в контуре обработки электронных сообщений, и электронной подписи, применяемой в контуре контроля реквизитов электронных сообщений, – для контроля целостности и подтверждения подлинности электронных сообщений;

шифрования электронных сообщений на прикладном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1-99, с использованием СКЗИ, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

применения средств защиты информации, реализующих двухстороннюю аутентификацию и шифрование информации на уровне звена данных или сетевом уровне в соответствии с эталонной моделью взаимосвязи открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

15. Применение участниками СБП мер защиты информации должно обеспечивать значение показателя, характеризующего уровень переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием сервиса быстрых платежей, формируемого на ежеквартальной основе, не более 0,005 процента.

Значение показателя, характеризующего уровень переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием сервиса быстрых платежей, должно рассчитываться как отношение суммы денежных средств, в отношении которых получены уведомления от клиентов участников СБП о списании денежных средств с их банковских счетов без их согласия за оцениваемый квартал, за исключением случаев, предусмотренных законодательством Российской Федерации, к общей сумме денежных средств, списанных с банковских счетов клиентов участников СБП посредством осуществления перевода денежных средств с использованием сервиса быстрых платежей.

16. В рамках реализации мер по противодействию осуществлению переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием сервиса быстрых платежей участник СБП, являющийся банком плательщика (далее – участник СБП – банк плательщика), участник СБП, являющийся банком получателя (далее – участник СБП – банк получателя), ОПКЦ, ОУИО СБП должны обеспечивать выполнение следующих требований.

Участник СБП – банк плательщика должен осуществлять:

выявление операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, установленным Банком России и размещенным на официальном сайте Банка России в соответствии с частью 5^1 статьи 8 Федерального закона от 27 июня 2011 года № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 27, ст. 3538) (далее – признаки осуществления переводов денежных средств без согласия клиента), в рамках реализуемой им системы управления рисками при осуществлении переводов денежных средств с использованием сервиса быстрых платежей;

приостановление в порядке, установленном частью 5^1 статьи 8 Федерального закона от 27 июня 2011 года № 161-ФЗ, исполнения распоряжения в рамках выявленной операции, соответствующей признакам осуществления переводов денежных средств без согласия клиента, с учетом информации об уровне риска операции без согласия клиента (далее – индикатор уровня риска операции), включенной в электронное сообщение, полученной от ОПКЦ в формате, установленном договором об оказании услуг между участником СБП и ОПКЦ, содержащей в том числе информацию об индикаторе уровня риска операции, сформированном участником СБП – банком получателя;

формирование индикатора уровня риска операции на основе оценки рисков операций в рамках реализуемой участником СБП – банком плательщика системы управления рисками и его направление в электронном

сообщении в ОПКЦ в формате, установленном договором об оказании услуг между участником СБП и ОПКЦ, – в случае невыявления признаков осуществления перевода денежных средств без согласия клиента.

Участник СБП – банк получателя должен осуществлять формирование индикатора уровня риска операции в рамках реализуемой им системы управления рисками, применяемой для выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, и его направление в электронном сообщении в ОПКЦ в формате, установленном договором об оказании услуг между участником СБП и ОПКЦ.

ОПКЦ должен осуществлять:

выявление операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основании моделей оценки риска операций по переводу денежных средств, установленных Банком России (далее – модели оценки риска операций Банка России), индикаторов уровня риска операции при осуществлении переводов денежных средств с использованием сервиса быстрых платежей, полученных от участников СБП;

приостановление процедуры приема к исполнению, в том числе последующих процедур приема к исполнению и исполнения распоряжений в рамках выявленной операции, соответствующей признакам осуществления переводов денежных средств без согласия клиента, при осуществлении переводов денежных средств с использованием сервиса быстрых платежей в соответствии с договором об оказании услуг между участником СБП и ОПКЦ;

незамедлительное уведомление участников СБП о выявлении операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, в соответствии с договором об оказании услуг между участником СБП и ОПКЦ;

уведомление Банка России о выявлении операций, соответствующих

признакам осуществления переводов денежных средств без согласия клиента, в соответствии с договором о взаимодействии между Банком России и ОПКЦ;

формирование индикатора уровня риска операции на основе моделей оценки риска операций Банка России и направление участнику СБП – банку плательщика сформированных ОПКЦ и участником СБП – банком получателя индикаторов уровня риска операций в электронном сообщении в формате, установленном договором об оказании услуг между участником СБП и ОПКЦ, – в случае невыявления признаков осуществления перевода денежных средств без согласия клиента.

Процедура принятия решения о наличии признаков осуществления перевода денежных средств без согласия клиента участником СБП на основании индикатора уровня риска операции, поступившего в электронном сообщении от участника СБП, ОПКЦ при осуществлении операции по переводу денежных средств с использованием сервиса быстрых платежей, устанавливается участником СБП в рамках реализуемой им системы управления рисками в соответствии с частью 5^1 статьи 8 Федерального закона от 27 июня 2011 года № 161-ФЗ.

Формат, порядок заполнения и передачи электронного сообщения, содержащего индикаторы уровня риска операции, определяются в соответствии с договором об оказании услуг между участником СБП и ОПКЦ.

16.1. В рамках реализации мер по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участника СБП и (или) его клиентов, ОПКЦ, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента участник СБП, ОПКЦ должны обеспечить выполнение следующих требований.

Участник СБП – банк плательщика при выявлении информации о компьютерных атаках, проводимых с использованием идентификаторов клиентов участника СБП, направленных на получение информации о клиентах участника СБП из формирующихся распоряжений клиента участника СБП о

переводе денежных средств (далее – переборы идентификаторов клиентов участника СБП), при осуществлении переводов денежных средств с использованием сервиса быстрых платежей осуществляет блокировку идентификатора клиента участника СБП, используемого для осуществления переборов идентификаторов клиентов участника СБП, и незамедлительно уведомляет Банк России и ОПКЦ о его блокировке.

ОПКЦ осуществляет выявление переборов идентификаторов клиентов участника СБП на стороне участников СБП, блокировку идентификатора клиента участника СБП, используемого для осуществления переборов идентификаторов клиентов участника СБП, при каждом выявлении перебора идентификаторов клиентов участника СБП, в том числе при отсутствии уведомления участника СБП о блокировке, на срок, установленный договором об оказании услуг между участником СБП и ОПКЦ, и направление уведомлений участнику СБП и Банку России о блокировке идентификатора клиента участника СБП.

При получении участником СБП – банком плательщика уведомления о блокировке идентификатора клиента участника СБП при осуществлении переводов денежных средств с использованием сервиса быстрых платежей от ОПКЦ участник СБП обязан осуществлять проверку полученной информации в соответствии с договором между клиентом участника СБП и участником СБП, о результатах которой Банк России уведомляется в соответствии с пунктом 2.13[1] Положения Банка России от 9 июня 2012 года № 382-П.

Участник СБП принимает решение о разблокировке идентификатора клиента участника СБП по результатам проведенной проверки и доводит принятое им решение до ОПКЦ в соответствии с договором об оказании услуг между участником СБП и ОПКЦ.

ОПКЦ осуществляет разблокировку идентификатора клиента участника СБП в соответствии с договором об оказании услуг между участником СБП и ОПКЦ.

17. При получении Банком России уведомления о блокировке

идентификатора клиента участника СБП при осуществлении переводов денежных средств с использованием сервиса быстрых платежей от участника СБП или ОПКЦ Банк России осуществляет информирование о переборах идентификаторов клиентов участника СБП на стороне участников СБП и об идентификаторе клиента участника СБП, применяемом для осуществления переборов идентификаторов клиентов участника СБП, путем направления уведомления участникам СБП и ОПКЦ. Для целей анализа обеспечения в платежной системе Банка России защиты информации при осуществлении переводов денежных средств участники ССНП, участники СБП и ОПКЦ должны информировать Банк России о нарушениях требований к обеспечению защиты информации при осуществлении переводов денежных средств, которые в том числе привели или могут привести к осуществлению переводов денежных средств без согласия клиента или к неоказанию услуг по переводу денежных средств, в рамках реализации требований, установленных:

пунктом 2.13[1] Положения Банка России от 9 июня 2012 года № 382-П;

Указанием Банка России от 9 июня 2012 года № 2831-У «Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств», зарегистрированным Министерством юстиции Российской Федерации 14 июня 2012 года № 24573, 24 июля 2013 года № 29142, 1 июня 2018 года № 51248;

Указанием Банка России от 8 октября 2018 года № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о

порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента», зарегистрированным Министерством юстиции Российской Федерации 12 декабря 2018 года № 52988.

ОУИО СБП обязан информировать участника СБП о нарушениях требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе о тех, которые привели или могут привести к осуществлению переводов денежных средств без согласия клиента или к неоказанию услуг по переводу денежных средств, в соответствии с договором между участником СБП и ОУИО СБП.

18. В случае выявления инцидента, связанного с несоблюдением требований к защите информации, который привел или может привести к осуществлению перевода денежных средств без согласия участника ССНП, участник ССНП вправе направить в Банк России обращение о приостановлении обмена электронными сообщениями.

При получении обращения о приостановлении обмена электронными сообщениями Банк России должен приостановить обмен электронными сообщениями и аннулировать электронные сообщения, в том числе ранее поступившие от участника ССНП и не исполненные, до получения от участника ССНП обращения об отмене приостановления обмена электронными сообщениями.

По результатам устранения причин инцидента участник ССНП должен направлять обращение об отмене приостановления обмена электронными сообщениями, при получении которого Банк России отменяет ранее введенное приостановление обмена электронными сообщениями с участником ССНП.

18.1. Обращения о приостановлении обмена электронными сообщениями в случае выявления инцидента, связанного с несоблюдением требований к защите информации, и обращения об отмене приостановления обмена электронными сообщениями (далее при совместном упоминании –

обращения) должны направляться с использованием технической инфраструктуры (автоматизированной системы) Банка России.

В случае невозможности направления обращения с использованием технической инфраструктуры (автоматизированной системы) Банка России обращение должно направляться с использованием резервного способа взаимодействия.

При возобновлении возможности направления обращений с использованием технической инфраструктуры (автоматизированной системы) Банка России участник ССНП должен повторно направить обращение с использованием технической инфраструктуры (автоматизированной системы) Банка России.

18.2. Информация о технической инфраструктуре (автоматизированной системе) Банка России, а также о резервном способе взаимодействия участника ССНП с Банком России, с помощью которого направляются обращения, размещается на официальном сайте Банка России.

18.3. В целях направления обращений участник ССНП должен обеспечить назначение должностных лиц, уполномоченных на направление и (или) подписание обращений (далее – уполномоченное лицо), и направление в Банк России информации об уполномоченных лицах, в том числе фамилий, имен, отчеств (последние при наличии), наименований должностей, контактных номеров телефонов, при наличии – номеров факсимильного аппарата, адресов электронной почты.

18.4. Одновременно с направлением обращений участник ССНП должен направить копию обращения о приостановлении обмена электронными сообщениями или об отмене приостановления обмена электронными сообщениями, подписанного уполномоченным лицом и заверенного печатью участника ССНП, по факсимильной связи либо по электронной почте в соответствии с контактными данными, размещенными на официальном сайте Банка России.

Не позднее одного рабочего дня после дня направления обращения

участник ССНП должен направить оригинал обращения на бумажном носителе по адресу, размещенному на официальном сайте Банка России.

18.5. При получении обращений с использованием технической инфраструктуры (автоматизированной системы) Банка России Банк России должен обеспечивать контроль целостности и подтверждение подлинности содержащейся в них информации.

При получении обращений с использованием резервного способа взаимодействия Банк России должен обеспечивать проверку соответствия реквизитов обращений информации, указанной в подпункте 18.3 настоящего пункта.

В случае отрицательного результата контроля целостности и подтверждения подлинности обращений, проверки соответствия реквизитов обращений Банк России не должен принимать обращения к исполнению, о чем уведомляется участник ССНП.

Уведомление участника ССНП осуществляется с использованием технической инфраструктуры (автоматизированной системы) Банка России.

В случае невозможности уведомления участника ССНП с использованием технической инфраструктуры (автоматизированной системы) Банка России уведомление осуществляется с использованием резервного способа взаимодействия.

19. Для оценки участниками ССНП, участниками СБП, ОПКЦ и ОУИО СБП выполнения ими требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее – оценка соответствия) устанавливаются следующие требования:

оценка соответствия должна проводиться в пределах выделенных сегментов (группы сегментов) вычислительных сетей, указанных в пунктах 3–6 настоящего Положения;

оценка соответствия должна проводиться в соответствии с положениями национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации

финансовых организаций. Методика оценки соответствия», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2018) (далее – ГОСТ Р 57580.2-2018);

оценка соответствия должна проводиться не реже одного раза в два года.

Участники ССНП, участники СБП, ОПКЦ и ОУИО СБП должны обеспечивать для объектов информационной инфраструктуры, размещенных в отдельных выделенных сегментах (группах сегментов) вычислительных сетей, указанных в пунктах 3–6 настоящего Положения, уровень соответствия не ниже четвертого согласно ГОСТ Р 57580.2-2018.

20. Контроль за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств Банк России осуществляет в соответствии с главой 3 Положения Банка России от 9 июня 2012 года № 382-П.

21. Настоящее Положение вступает в силу по истечении 10 дней после дня его официального опубликования, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления их в силу.

Пункты 3, 4, подпункт 7.1 пункта 7, абзацы первый – четвертый пункта 19 настоящего Положения вступают в силу с 1 июля 2021 года.

Пункт 5, абзацы третий – пятый пункта 12 настоящего Положения вступают в силу с 1 января 2022 года.

Абзацы четвертый и пятый подпункта 14.2, абзац шестой подпункта 14.3 пункта 14 настоящего Положения вступают в силу с 1 июля 2022 года.

Абзац пятый пункта 19 настоящего Положения вступает в силу с 1 января 2023 года.

22. Со дня вступления в силу настоящего Положения признать утратившим силу Положение Банка России от 9 января 2019 года № 672-П «О требованиях к защите информации в платежной системе Банка России»,

зарегистрированное Министерством юстиции Российской Федерации 21 марта 2019 года № 54109.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Положению Банка России
от «23» декабря 2020 года № 747-П
«О требованиях к защите информации
в платежной системе Банка России»

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

1. Формирование электронных сообщений и контроль реквизитов электронных сообщений в информационной инфраструктуре участника ССНП должны осуществляться с учетом следующего.

1.1. Контур формирования электронных сообщений и контур контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП должны быть реализованы с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров.

1.2. Объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП должны быть размещены в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформляется документально и согласовывается со службой информационной безопасности участников ССНП.

1.3. В контуре формирования электронных сообщений на основе первичного документа в бумажной или электронной форме или входящего

электронного сообщения должны осуществляться:

формирование исходящего электронного сообщения, предназначенного для направления в платежную систему Банка России;

контроль реквизитов исходящего электронного сообщения, предназначенного для направления в платежную систему Банка России;

подписание исходящего электронного сообщения, предназначенного для направления в платежную систему Банка России, электронной подписью, применяемой в контуре формирования электронных сообщений, при положительном результате контроля реквизитов, указанного в абзаце третьем настоящего подпункта;

направление исходящего электронного сообщения, предназначенного для направления в платежную систему Банка России, в контур контроля реквизитов электронных сообщений.

1.4. В контуре контроля реквизитов электронных сообщений должны осуществляться:

контроль реквизитов исходящего электронного сообщения, предназначенного для направления в платежную систему Банка России, на соответствие реквизитам первичного документа в бумажной или электронной форме или входящего электронного сообщения;

контроль на отсутствие дублирования исходящих электронных сообщений;

подписание исходящего электронного сообщения, предназначенного для направления в платежную систему Банка России, электронной подписью, применяемой в контуре контроля реквизитов электронных сообщений, при положительном результате контроля реквизитов, указанного в абзаце втором настоящего подпункта.

2. Обработка электронных сообщений и контроль реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ должны осуществляться с учетом следующего.

2.1. Контур обработки электронных сообщений и контур контроля

реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ должны быть реализованы с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров.

2.2. Объекты информационной инфраструктуры контура обработки электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ должны быть размещены в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформляется документально и согласовывается со службой информационной безопасности ОПКЦ.

2.3. Направление электронных сообщений должно осуществляться таким образом, чтобы все входящие электронные сообщения поступали в контур обработки электронных сообщений только из контура контроля реквизитов электронных сообщений, а все исходящие электронные сообщения из контура обработки электронных сообщений передавались только в контур контроля реквизитов электронных сообщений.

2.4. В контуре контроля реквизитов электронных сообщений должны осуществляться:

контроль входящего электронного сообщения.

проверка электронной подписи входящего электронного сообщения;

структурный и логический контроль входящего электронного сообщения, в том числе проверка соответствия реквизитов (данных) входящего электронного сообщения;

контроль на отсутствие дублирования входящих электронных сообщений;

помещение в эталонную базу входящих электронных сообщений (далее – ЭБВЭС) входящих электронных сообщений без снятия электронной подписи с целью осуществления контроля результатов обработки защищаемой информации в рамках процедуры выходного контроля.

Состав электронных сообщений, подлежащих помещению в ЭБВЭС, определяется договором об оказании услуг между участником СБП и ОПКЦ.

2.5. В контуре обработки электронных сообщений должны осуществляться:

контроль входящего электронного сообщения;

проверка электронной подписи входящего электронного сообщения;

структурный и логический контроль входящего электронного сообщения, в том числе проверка соответствия реквизитов (данных) входящего электронного сообщения;

обработка информации, содержащейся во входящем электронном сообщении, и формирование исходящего электронного сообщения;

подписание исходящего электронного сообщения электронной подписью, применяемой в контуре обработки электронных сообщений;

направление исходящего электронного сообщения, подписанного электронной подписью, применяемой в контуре обработки электронных сообщений, в контур контроля реквизитов электронных сообщений.

2.6. В контуре контроля реквизитов электронных сообщений должны осуществляться:

проверка в исходящем электронном сообщении электронной подписи, применяемой в контуре обработки электронных сообщений;

проверка электронной подписи в электронных сообщениях, находящихся в ЭБВЭС, на основании которых было сформировано исходящее электронное сообщение;

контроль значений реквизитов исходящего электронного сообщения со значениями реквизитов электронных сообщений, находящихся в ЭБВЭС, на основании которых было сформировано исходящее электронное сообщение;

контроль на отсутствие дублирования исходящих электронных сообщений;

подписание исходящего электронного сообщения электронной подписью, применяемой в контуре контроля реквизитов электронных сообщений (без снятия электронной подписи, применяемой в контуре обработки).