ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«25» июля 2022 г. г. Москва № 802-П

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 71124
от "25" ноября 2022 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»[1], части пятой статьи 5 Федерального закона от 2 декабря 1990 года № 395-I «О банках и банковской деятельности» (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ)[2] и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 24 июня 2022 года № ПСД-44) 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, являющиеся участниками обмена в соответствии с абзацем вторым пункта 3.10 Положения Банка России от 24 сентября 2020 года № 732-П «О платежной системе Банка России»[3]

---

[1] Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 27, ст. 3538.
[2] Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2017, № 31, ст. 4761.
[3] Зарегистрировано Минюстом России 10 ноября 2020 года, регистрационный № 60810, с изменениями, внесенными Указаниями Банка России от 25 марта 2021 года № 5756-У (зарегистрировано Минюстом России

(далее – Положение Банка России № 732-П) и кредитными организациями (их филиалами) (далее – участники обмена), являющиеся международными финансовыми организациями, 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 СБП), 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, установленные настоящим Положением, должны выполняться участниками обмена, ОПКЦ СБП и ОУИО СБП наряду с требованиями 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»[1] (далее – Федеральный закон от 27 июня 2011 года № 161-ФЗ).

2. Требования к защите информации распространяются на автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование (далее при совместном упоминании – объекты информационной инфраструктуры), применяемые для формирования (подготовки), обработки, передачи и хранения защищаемой информации, указанной в пунктах 2.2, 4.2 и 6.4 Положения Банка России от 4 июня 2020 года № 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

---

26 мая 2021 года, регистрационный № 63632), от 23 декабря 2021 года № 6030-У (зарегистрировано Минюстом России 14 марта 2022 года, регистрационный № 67709), от 4 апреля 2022 года № 6115-У (зарегистрировано Минюстом России 6 апреля 2022 года, регистрационный № 68096).

[1] Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423.

переводов денежных средств»[1] (далее – Положение Банка России № 719-П), в том числе информационных сообщений, содержащих реквизиты и иную информацию, необходимую для последующего формирования электронного сообщения, содержащего распоряжение в электронном виде (далее – информационные сообщения), на этапах формирования (подготовки), обработки, передачи и хранения информационных сообщений при осуществлении переводов денежных средств при трансграничном переводе денежных средств с использованием сервиса быстрых платежей (далее – ТПСБП).

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 (отдельного) сегмента (группы сегментов) вычислительных сетей участники ССНП должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация стандартного уровня (уровня 2) защиты информации, предусмотренного пунктом 6.7 раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.1- 2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии

[1] Зарегистрировано Минюстом России 23 сентября 2020 года, регистрационный № 59991.

от 8 августа 2017 года № 822-ст[1] и введенного в действие 1 января 2018 года (далее – ГОСТ Р 57580.1-2017).

4. Участники обмена, международные финансовые организации при осуществлении переводов денежных средств с использованием сервиса быстрых платежей (далее при совместном упоминании – 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 (отдельного) сегмента (группы сегментов) вычислительных сетей участники СБП должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация стандартного уровня (уровня 2) защиты информации, предусмотренного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

5. ОПКЦ СБП 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 (отдельного) сегмента (группы сегментов) вычислительных сетей ОПКЦ СБП должен применять меры защиты информации, посредством выполнения которых обеспечивается реализация усиленного уровня (уровня 1) защиты информации, предусмотренного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

6. ОУИО СБП должен размещать объекты информационной инфраструктуры, используемые при предоставлении услуг информационного обмена участникам СБП, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей.

---

[1] М., ФГУП «Стандартинформ», 2017.

Для объектов информационной инфраструктуры в пределах выделенного (отдельного) сегмента (группы сегментов) вычислительных сетей ОУИО СБП должен применять меры защиты информации, посредством выполнения которых обеспечивается реализация стандартного уровня (уровня 2) защиты информации, предусмотренного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017.

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

7.1. Участники ССНП, участники СБП, ОПКЦ СБП и ОУИО СБП должны разработать и утвердить внутренние документы, регламентирующие выполнение следующих процессов (направлений) защиты информации в рамках процессов (направлений) защиты информации, предусмотренных подпунктом 7.1.1 пункта 7.1 раздела 7 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 СБП и ОУИО СБП должны определить во внутренних документах:

технологии подготовки, обработки, передачи и хранения электронных сообщений, содержащих распоряжения о переводе денежных средств 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;

сведения о лице или лицах, допущенных к работе со СКЗИ;

сведения о лице или лицах, ответственных за обеспечение функционирования и безопасности СКЗИ (ответственных пользователей СКЗИ);

сведения о лице или лицах, обладающих правами по управлению криптографическими ключами, в том числе ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей.

7.3. Участники СБП, ОПКЦ СБП и ОУИО СБП должны определить во внутренних документах состав и правила применения технологических мер защиты информации, используемых для контроля целостности и подтверждения подлинности электронных сообщений и информационных сообщений (при их наличии), при осуществлении перевода денежных средств с использованием сервиса быстрых платежей на этапах формирования (подготовки), обработки, передачи и хранения электронных сообщений и информационных сообщений (при их наличии).

Участники СБП, ОПКЦ СБП и ОУИО СБП должны применять технологические меры защиты информации, используемые для контроля целостности и подтверждения подлинности электронных сообщений и информационных сообщений на этапах их формирования (подготовки), обработки, передачи и хранения (при их наличии).

8. Защита информации участниками ССНП, участниками СБП, ОПКЦ СБП и ОУИО СБП с помощью СКЗИ должна обеспечиваться в соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66[1], и технической документацией на СКЗИ.

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

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.

11. Участники ССНП, участники СБП, ОПКЦ СБП и ОУИО СБП должны хранить входящие и исходящие электронные сообщения, подписанные электронной подписью, и средства, обеспечивающие проверку электронной подписи, не менее пяти лет с даты подписания электронных сообщений.

12. При обмене электронными сообщениями между Банком России и ОПКЦ СБП, Банком России и участниками ССНП должна применяться электронная подпись, сертификаты ключа проверки которой выданы Банком России участникам ССНП и ОПКЦ СБП, в соответствии с частью 2 статьи 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи»[2].

---

[1] Зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382, с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года № 173 (зарегистрирован Минюстом России 25 мая 2010 года, регистрационный № 17350).

[2] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794.

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

При обмене электронными сообщениями между ОПКЦ СБП, участниками СБП и ОУИО СБП должна применяться электронная подпись, сертификат ключа проверки которой выдан ОПКЦ СБП участнику СБП, в том числе при обмене электронными сообщениями между ОПКЦ СБП 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 аппаратных модулях безопасности информационной инфраструктуры ОУИО СБП, 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»[1] (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 проверки электронной подписи.

При обмене электронными сообщениями между ОПКЦ СБП и ОУИО СБП криптографические ключи участника СБП, предназначенные для подписания исходящих электронных сообщений и (или) расшифрования

---

[1] Собрание законодательства Российской Федерации, 1995, № 15, ст. 1269; 2003, № 27, ст. 2700.

на прикладном уровне входящих электронных сообщений, хранение и использование которых осуществляются в информационной инфраструктуре ОУИО СБП, изготавливаются участником СБП в аппаратных модулях безопасности самостоятельно. Для получения сертификата ключа проверки электронной подписи участник СБП обращается в ОПКЦ СБП самостоятельно.

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

Криптографические ключи ОПКЦ СБП, используемые при обмене электронными сообщениями между Банком России и ОПКЦ СБП, должны изготавливаться ОПКЦ СБП.

Криптографические ключи участника СБП, используемые при обмене электронными сообщениями между ОПКЦ СБП и участником СБП, должны изготавливаться участником СБП.

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

14.1. Участники СБП должны удостоверять электронной подписью электронные сообщения при их передаче клиентами участника СБП.

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

использования усиленной электронной подписи для контроля целостности и подтверждения подлинности электронных сообщений, состав которых определен договором об оказании операционных услуг, услуг платежного клиринга при осуществлении перевода денежных средств с использованием сервиса быстрых платежей, заключенным между участником СБП и ОПКЦ СБП в соответствии с частью 1 статьи 17, частью 1 статьи 18

Федерального закона от 27 июня 2011 года № 161-ФЗ[1] (далее – договор об оказании услуг между участником СБП и ОПКЦ СБП);

шифрования электронных сообщений на прикладном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 государственного стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель», принятого постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78[2] и введенного в действие 1 января 2000 года (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, посредством использования которых реализуется двухсторонняя аутентификация и шифрование информации на уровне представления или ниже, в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

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

Участники СБП должны реализовать технологии подготовки, обработки и передачи электронных сообщений и защищаемой информации, обеспечивающие проверку соответствия (сверку) реквизитов исходящих в адрес ОПКЦ СБП электронных сообщений с реквизитами соответствующих

---

[1] Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872.
[2] М., ИПК «Издательство стандартов», 1999.

им входящих электронных сообщений клиентов участников СБП и реквизитами электронных сообщений, 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 с использованием объектов информационной инфраструктуры участника ССНП в соответствии с пунктом 1 приложения к настоящему Положению, в котором установлены 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 СБП в соответствии с частью пятой статьи 5 Федерального закона от 2 декабря 1990 года № 395-I «О банках и банковской деятельности» (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ);

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, указанного в Альбоме электронных сообщений, ведение которого осуществляется Банком России в соответствии с абзацами вторым, третьим и подпунктом 5.2.1 пункта 5.2 Положения Банка России № 732-П;

шифрования электронных сообщений на прикладном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 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, предусмотренной пунктом 1.7 раздела 1 ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

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

обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ СБП в соответствии с пунктом 2 приложения к настоящему Положению;

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, предусмотренной пунктом 1.7 раздела 1 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, предусмотренной пунктом 1.7 раздела 1 ГОСТ Р ИСО/МЭК 7498-1-99, прошедших процедуру оценки соответствия

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

15. Значение показателя, характеризующего уровень переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием сервиса быстрых платежей, формируемого на ежеквартальной основе, в результате применения участниками СБП мер защиты информации не должно превышать 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 с использованием сервиса быстрых платежей 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 СБП должны обеспечивать выполнение следующих требований:

16.1. Участник СБП – банк плательщика должен осуществлять:

выявление операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, установленным Банком России в соответствии с частью 5^1 статьи 8 Федерального закона

от 27 июня 2011 года № 161-ФЗ[1] (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 соответствии с 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 СБП в формате и порядке, установленных договором об оказании услуг между участником СБП и ОПКЦ СБП, 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 СБП в формате и порядке, установленных договором об оказании услуг между участником СБП и ОПКЦ СБП, – в случае невыявления признаков осуществления перевода денежных средств без согласия клиента.

16.2. 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 СБП в формате и порядке, установленных договором об оказании услуг между участником СБП и ОПКЦ СБП.

16.3. ОПКЦ СБП должен осуществлять:

---

[1] Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2018, № 27, ст. 3950.

выявление операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основании моделей оценки риска операций по переводу денежных средств (далее – модели оценки риска операций Банка России), установленных в соответствии с 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[1] (далее – договор о взаимодействии между Банком России и ОПКЦ СБП), 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, в соответствии с договором об оказании услуг между участником СБП и ОПКЦ СБП;

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 СБП;

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 СБП;

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

---

[1] Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872.

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 СБП 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.

16.4. 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 СБП, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента участник СБП, ОПКЦ СБП 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 или клиентах косвенного участника, имеющего доступ к трансграничному переводу денежных средств с использованием СБП в соответствии с абзацем восьмым пункта 3.3 Положения Банка России № 732-П (далее – косвенный участник с доступом к ТПСБП), из формирующихся распоряжений клиента участника СБП о переводе денежных средств (далее – переборы идентификаторов), при осуществлении переводов денежных средств с использованием сервиса быстрых платежей осуществляет блокировку идентификатора клиента участника СБП, используемого для осуществления переборов идентификаторов, и незамедлительно уведомляет Банк России и ОПКЦ СБП о его блокировке;

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

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

при получении участником СБП – банком плательщика уведомления о блокировке идентификатора от ОПКЦ СБП 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 абзацем девятым пункта 5.1 Положения Банка России № 719-П;

участник СБП направляет уведомление о блокировке идентификатора клиента косвенного участника с доступом к ТПСБП косвенному участнику с доступом к ТПСБП и доводит до ОПКЦ СБП информацию о результатах проведенной проверки косвенным участником с доступом к ТПСБП в соответствии с договором об оказании услуг между участником СБП и ОПКЦ СБП;

ОПКЦ СБП осуществляет разблокировку идентификатора клиента участника СБП, клиента косвенного участника с доступом к ТПСБП в соответствии с договором об оказании услуг между участником СБП и ОПКЦ СБП.

17. При получении Банком России уведомления о блокировке идентификатора клиента участника СБП, клиента косвенного участника с доступом к ТПСБП от участника СБП или ОПКЦ СБП Банк России осуществляет информирование о переборах идентификаторов на стороне участников СБП или на стороне косвенного участника с доступом к ТПСБП

и об идентификаторе клиента участника СБП или косвенного участника с доступом к ТПСБП, применяемом для осуществления переборов идентификаторов клиентов участника СБП, путем направления уведомления участникам СБП и ОПКЦ СБП.

18. Для целей анализа обеспечения в платежной системе Банка России защиты информации при осуществлении переводов денежных средств участники ССНП, участники СБП и ОПКЦ СБП должны направлять информацию в соответствии с требованиями, установленными:

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»[1];

Указанием Банка России от 12 января 2022 года № 6060-У «О формах и методиках составления, порядке и сроках представления операторами услуг платежной инфраструктуры, операторами по переводу денежных средств отчетности по обеспечению защиты информации при осуществлении переводов денежных средств»[2];

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

---

[1] Зарегистрировано Минюстом России 14 июня 2012 года, регистрационный № 24573, с изменениями, внесенными Указаниями Банка России от 21 июня 2013 года № 3024-У (зарегистрировано Минюстом России 24 июля 2013 года, регистрационный № 29142), от 30 марта 2018 года № 4753-У (зарегистрировано Минюстом России 1 июня 2018 года, регистрационный № 51248).

[2] Зарегистрировано Минюстом России 15 марта 2022 года, регистрационный № 67755.

платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента»[1].

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, предусмотренным пунктом 33 статьи 3 Федерального закона от 27 июня 2011 года № 161-ФЗ[2].

19. 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 неисполненные, до получения от участника ССНП обращения об отмене приостановления обмена электронными сообщениями.

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

19.1. 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 –

---

[1] Зарегистрировано Минюстом России 12 декабря 2018 года, регистрационный № 52988, с изменениями, внесенными Указанием Банка России от 30 марта 2021 года № 5760-У (зарегистрировано Минюстом России 13 мая 2021 года, регистрационный № 63403).

[2] Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423.

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.

19.2. 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 в информационно-телекоммуникационной сети «Интернет».

19.3. 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, с указанием в том числе фамилий, имен, отчеств (последних – при наличии), наименований должностей, номеров телефонов, при наличии – номеров факсимильного аппарата, адресов электронной почты.

19.4. 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 в информационно-телекоммуникационной сети «Интернет».

Не позднее одного рабочего дня после дня направления в соответствии с абзацем первым настоящего подпункта копии обращения участник ССНП должен направить оригинал обращения на бумажном носителе по адресу, указанному на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет».

19.5. 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, направленной в Банк России в соответствии с подпунктом 19.3 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.

20. Для оценки участниками ССНП, участниками СБП, ОПКЦ СБП 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 раздела 6 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[1] и введенного в действие 1 сентября 2018 года (далее – ГОСТ Р 57580.2-2018);

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

Участники ССНП, участники СБП, ОПКЦ СБП 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, предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

21. Контроль за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств Банк России осуществляет в отношении участников обмена и ОПКЦ СБП в соответствии с главой 7 Положения Банка России № 719-П.

22. 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.

Абзац третий пункта 18 и абзац пятый пункта 20 настоящего Положения вступают в силу с 1 января 2023 года.

Абзац второй пункта 18 настоящего Положения действует по 31 декабря 2022 года.

---

[1] М., ФГУП «Стандартинформ», 2018.

23. Со дня вступления в силу настоящего Положения признать утратившим силу Положение Банка России от 23 декабря 2020 года № 747-П «О требованиях к защите информации в платежной системе Банка России»[1].

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

[1] Зарегистрировано Минюстом России 3 февраля 2021 года, регистрационный № 62365.

Приложение
к Положению Банка России
от 25 июля 2022 года № 802-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 обмена при осуществлении переводов денежных средств в платежной системе Банка России с использованием сервиса срочного перевода и сервиса несрочного перевода, а также правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре операционного центра, платежного клирингового центра другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей

Глава 1. Формирование электронных сообщений и контроль реквизитов электронных сообщений в информационной инфраструктуре участника обмена при осуществлении переводов денежных средств в платежной системе Банка России с использованием сервиса срочного перевода и сервиса несрочного перевода

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

1.2. Участник ССНП должен разместить объекты информационной инфраструктуры контура формирования электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП 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. Участник ССНП в контуре формирования электронных сообщений на основе первичного документа в бумажной или электронной форме или входящего электронного сообщения должен обеспечить:

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. Участник ССНП в контуре контроля реквизитов электронных сообщений должен обеспечить:

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.

Глава 2. Обработка электронных сообщений и контроль реквизитов электронных сообщений в информационной инфраструктуре операционного центра, платежного клирингового центра другой платежной системы при предоставлении операционных услуг и услуг платежного клиринга при переводе денежных средств с использованием сервиса быстрых платежей

2.1. ОПКЦ СБП должен реализовать контур обработки электронных сообщений и контур контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ СБП с использованием разных рабочих мест, разных криптографических ключей и с привлечением отдельных работников для каждого из контуров.

2.2. ОПКЦ СБП должен разместить объекты информационной инфраструктуры контура обработки электронных сообщений и контура контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ СБП 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 СБП.

2.3. ОПКЦ СБП должен направлять электронные сообщения 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. ОПКЦ СБП в контуре контроля реквизитов электронных сообщений должен обеспечить:

контроль входящего электронного сообщения;

проверку электронной подписи входящего электронного сообщения;

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

контроль на предмет отсутствия дублирования входящих электронных сообщений;

помещение входящих электронных сообщений в эталонную базу входящих электронных сообщений (далее – ЭБВЭС) 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 СБП.

2.5. ОПКЦ СБП в контуре обработки электронных сообщений должен обеспечить:

контроль входящего электронного сообщения;

проверку электронной подписи входящего электронного сообщения;

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

обработку 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. ОПКЦ СБП в контуре контроля реквизитов электронных сообщений должен обеспечить:

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

проверку 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 предмет отсутствия 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).