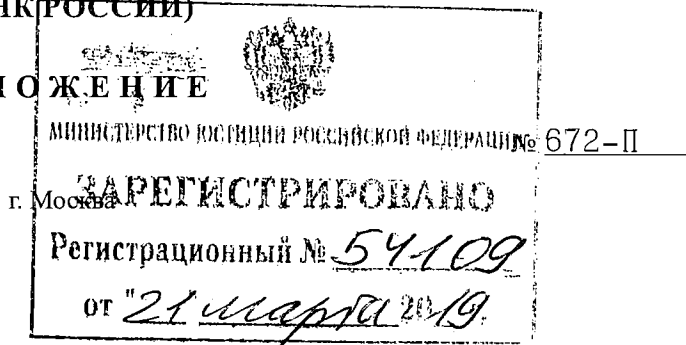




**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)**

ПОЛОЖЕНИЕ

« 9 » января 2019 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; 2012, № 53, ст. 7592; 2013, № 27, ст. 3477; № 30, ст. 4084; № 52, ст. 6968; 2014, № 19, ст. 2315, ст. 2317; № 43, ст. 5803; 2015, № 1, ст. 8, ст. 14; 2016, № 27, ст. 4221, ст. 4223; 2017, № 15, ст. 2134; № 18, ст. 2665; № 30, ст. 4456; 2018, № 27, ст. 3950, ст. 3952; № 32, ст. 5115, № 49, ст. 7524) (далее – Федеральный закон от 27 июня 2011 года № 161-ФЗ), решения Совета директоров Банка России (протокол заседания Совета директоров Банка России от 21 декабря 2018 года № 39) и в соответствии с требованиями 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), 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 участники платежной системы Банка России, являющиеся кредитными организациями (их филиалами), имеющие доступ к услугам по переводу денежных средств с использованием распоряжений в электронном виде, предусмотренный пунктом 3.7 Положения Банка России от 6 июля 2017 года № 595-П «О платежной системе Банка России», зарегистрированного Министерством юстиции Российской Федерации 6 октября 2017 года № 48458, 5 декабря 2018 года № 52892 (далее – Положение Банка России от 6 июля 2017 года № 595-П), 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 – участники обмена).

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 (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. 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) 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.

6. Документы участников ССНП, участников СБП и ОПКЦ, определяющие порядок обеспечения защиты информации при осуществлении переводов денежных средств (далее – документы), должны определять состав и порядок применения организационных мер защиты информации и состав и порядок использования технических средств защиты информации.

6.1. Документы должны приниматься 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.

6.2. Документы должны содержать информацию, определяющую:

технологии подготовки, обработки, передачи и хранения электронных сообщений 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. 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 (Положение ПКЗ-2005), 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.

8. Участники СБП должны обеспечить регистрацию информации, указанной в подпункте 2.6.3 пункта 2.6 Положения Банка России от 9 июня 2012 года № 382-П и связанной с действиями клиентов участников СБП, в целях информирования Банка России обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиентов в соответствии с главой 1 Указания 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 (далее – Указание Банка России от 8 октября 2018 года № 4926-У).

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.

11. Участники ССНП, участники СБП и ОПКЦ должны обеспечивать хранение входящих и исходящих электронных сообщений, подписанных электронной подписью, не менее пяти лет.

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

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

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

Криптографические ключи, 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 27 июня 2011 года № 161-ФЗ.

Криптографические ключи, 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 (далее – договор об оказании услуг между участником СБП и ОПКЦ).

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

14.1. Участники СБП должны обеспечивать удостоверение электронной подписью электронных сообщений при их передаче между участниками СБП и клиентами участников СБП.

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

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

шифрованием электронных сообщений на прикладном уровне в соответствии с эталонной моделью взаимосвязи открытых систем, определенной в ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель», утвержденным 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 при осуществлении регулирования в соответствии с пунктом «ш» статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности» (Собрание законодательства Российской Федерации, 1995, № 15, ст. 1269; 2000, № 1, ст. 9; № 46, ст. 4537; 2002, № 19, ст. 1794; № 30, ст. 3033; 2003, № 2, ст. 156; № 27, ст. 2700; 2004, № 35, ст. 3607; 2005, № 10, ст. 763; 2006, № 17, ст. 1779; № 31, ст. 3452; 2007, № 28, ст. 3348; № 31, ст. 4008; № 50, ст. 6241; 2008, № 52, ст. 6235; 2010, № 31, ст. 4207; № 42, ст. 5297; 2011, № 1, ст. 32; № 29, ст. 4282; 2011, № 30, ст. 4589; № 50, ст. 7366; 2013, № 19, ст. 2324; № 27, ст. 3477; № 48, ст. 6165; № 51, ст. 6689; 2014, № 19, ст. 2335; № 26, ст. 3365; № 26, ст. 3384; № 52, ст. 7557; 2016, № 1, ст. 88; № 27, ст. 4160, ст. 4238; № 28, ст. 4558; 2017, № 1, ст. 46; № 25, ст. 3596; 2018, № 11, ст. 1591) (далее – требования, установленные федеральным органом исполнительной власти в области обеспечения безопасности);

применением 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.

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

формированием электронных сообщений и контролем 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; 1998, № 31, ст. 3829; 1999, № 28, ст. 3459, ст. 3469; 2001, № 26, ст. 2586; № 33, ст. 3424; 2002, № 12, ст. 1093; 2003, № 27, ст. 2700; № 50, ст. 4855; № 52, ст. 5033, ст. 5037; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 1, ст. 18, ст. 45; № 30, ст. 3117; 2006, № 6, ст. 636; № 19, ст. 2061; № 31, ст. 3439; № 52, ст. 5497; 2007, № 1, ст. 9; № 22, ст. 2563; № 31, ст. 4011; № 41, ст. 4845; № 45, ст. 5425; № 50, ст. 6238; 2008, № 10, ст. 895; 2009, № 1, ст. 23; № 9, ст. 1043; № 18, ст. 2153; № 23, ст. 2776; № 30, ст. 3739; № 48, ст. 5731; № 52, ст. 6428; 2010, № 8, ст. 775; № 27, ст. 3432; № 30, ст. 4012; № 31, ст. 4193; № 47, ст. 6028; 2011, № 7, ст. 905; № 27, ст. 3873, ст. 3880; № 29, ст. 4291; № 48, ст. 6730; № 49, ст. 7069; № 50, ст. 7351; 2012, № 27, ст. 3588; № 31, ст. 4333; № 50, ст. 6954; № 53, ст. 7605, ст. 7607; 2013, № 11, ст. 1076; № 19, ст. 2317, ст. 2329; № 26, ст. 3207; № 27, ст. 3438, ст. 3477; № 30, ст. 4084; № 40, ст. 5036; № 49, ст. 6336; № 51, ст. 6683, ст. 6699; 2014, № 6, ст. 563; № 19, ст. 2311; № 26, ст. 3379, ст. 3395; № 30, ст. 4219; № 40, ст. 5317, ст. 5320; № 45, ст. 6144, ст. 6154; № 49, ст. 6912; № 52, ст. 7543; 2015, № 1, ст. 37; № 17, ст. 2473; № 27, ст. 3947, ст. 3950; № 29, ст. 4355, ст. 4357, ст. 4385; № 51, ст. 7243; 2016, № 1, ст. 23; № 15, ст. 2050; № 26, ст. 3860; № 27, ст. 4294, ст. 4295; 2017, № 14, ст. 2000; № 18, ст. 2661, ст. 2669; № 25, ст. 3596; № 30, ст. 4456; № 31, ст. 4754, ст. 4761, ст. 4830; 2018, № 1, ст. 66; № 18, ст. 2560, ст. 2576; № 22, ст. 3043; № 24, ст. 3400; № 27, ст. 3950; № 31, ст. 4852; № 32, ст. 5100, ст. 5115; № 49, ст. 7524; № 53, ст. 8440) (далее – Правила материально-технического обеспечения);

использованием 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;

применением третьего варианта защиты, предусмотренного Альбомом унифицированных форматов электронных банковских сообщений, размещенном на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет», который ведется Банком России в соответствии с пунктом 5.2 Положения Банка России от 6 июля 2017 года № 595-П;

шифрованием 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;

применением 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:

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

использованием 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;

шифрованием 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;

применением 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, а также ограничений по параметрам операций по осуществлению переводов денежных средств, устанавливаемых в соответствии с подпунктом 2.8.3 пункта 2.8 Положения Банка России от 9 июня 2012 года № 382-П, должно обеспечивать значение показателя, характеризующего уровень переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием сервиса быстрых платежей, 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. ОПКЦ при предоставлении операционных услуг и услуг

платежного клиринга должен обеспечивать реализацию мероприятий по достижению показателя доступности сервиса быстрых платежей не ниже 99,9 процента с учетом времени проведения плановых работ по поддержке работоспособности автоматизированных систем, обеспечивающих функционирование сервиса быстрых платежей, и не ниже 99,99 процента без учета плановых работ.

17. В рамках реализации мер по противодействию осуществлению переводов денежных средств без согласия клиента при осуществлении переводов денежных средств с использованием сервиса быстрых платежей ОПКЦ должен осуществлять:

выявление операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, установленным Банком России и размещенным на его официальном сайте в информационно-телекоммуникационной сети «Интернет» в соответствии с частью 5¹ статьи 8 Федерального закона от 27 июня 2011 года № 161-ФЗ (далее – признаки осуществления переводов денежных средств без согласия клиента), при осуществлении переводов денежных средств с использованием сервиса быстрых платежей, в том числе с использованием информации, получаемой от участников СБП;

приостановление процедуры приема к исполнению и исполнения распоряжений о переводе денежных средств в рамках выявленной операции, соответствующей признакам осуществления переводов денежных средств без согласия клиента, при осуществлении переводов денежных средств с использованием сервиса быстрых платежей;

немедленное уведомление участников СБП о выявлении операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, при осуществлении переводов денежных средств с использованием сервиса быстрых платежей;

продолжение процедур приема к исполнению и исполнения распоряжений о переводе денежных средств при получении дальнейших

электронных сообщений по приостанавливаемой операции от участника СБП в течение времени, установленного договором об оказании услуг между участником СБП и ОПКЦ;

прекращение процедур приема к исполнению и исполнения распоряжений о переводе денежных средств при неполучении дальнейших электронных сообщений по приостанавливаемой операции от участника СБП в течение времени, установленного договором об оказании услуг между участником СБП и ОПКЦ.

18. 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, в том числе которые 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 2.13¹ 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 (далее – Указание Банка России от 9 июня 2012 года № 2831-У);

Указанием Банка России от 8 октября 2018 года № 4926-У.

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 приостанавливать обмен электронными сообщениями и аннулировать электронные сообщения, ранее поступившие от участника ССНП, 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 снимает ранее введенное ограничение для возобновления 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 – 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-коммуникационной 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, в том числе фамилий, имен, отчеств (при наличии), наименований должностей, контактных 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 обращения участник ССНП должен направить оригинал обращения о приостановлении обмена электронными сообщениями или об отмене приостановления обмена электронными сообщениями на бумажном носителе по адресу, размещенному 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, указанной в подпункте 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, являющимися субъектами, на которых распространяются требования Положения Банка России от 9 июня 2012 года № 382-П, и ОПКЦ 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 3–5 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», 2017) (далее – ГОСТ Р 57580.2-2018);

оценка соответствия должна проводиться не реже одного раза в два года, а также по требованию Банка России.

Участники ССНП, участники СБП и ОПКЦ должны обеспечивать для объектов информационной инфраструктуры, размещенных в отдельных

выделенных сегментах (группах сегментов) вычислительных сетей, указанных в пунктах 3–5 настоящего Положения, уровень соответствия не ниже четвертого согласно ГОСТ Р 57580.2-2018.

21. Для анализа обеспечения в платежной системе Банка России защиты информации при осуществлении переводов денежных средств участники ССНП, участники СБП, являющиеся субъектами, на которых распространяются требования Указания Банка России от 9 июня 2012 года № 2831-У, и ОПКЦ должны предоставлять результаты оценки соответствия согласно требованиям к содержанию, форме и периодичности представления информации, установленным Указанием Банка России от 9 июня 2012 года № 2831-У.

22. 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.

23. 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 9 и 10 настоящего Положения вступают в силу с 28 июня 2019 года.

Абзац пятый подпункта 14.4 пункта 14 настоящего Положения вступает в силу с 1 июля 2020 года.

Пункты 3, 4, подпункт 6.1 пункта 6, абзац четвертый подпункта 14.2, абзац шестой подпункта 14.3 пункта 14, абзацы первый – четвертый пункта 20 настоящего Положения вступают в силу с 1 июля 2021 года.

Абзац пятый пункта 20 настоящего Положения вступает в силу с 1 января 2023 года.

Со дня вступления в силу настоящего Положения признать утратившим силу Положение Банка России от 24 августа 2016 года № 552-П «О требованиях к защите информации в платежной системе Банка России»,

зарегистрированное Министерством юстиции Российской Федерации
6 декабря 2016 года № 44582.

Председатель
Центрального банка
Российской Федерации

Э.С. Набиуллина

**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 с электронными сообщениями, находящимися в ЭБВЭС, на основании которых был сформировано исходящее электронное сообщение;

контроль на отсутствие дублирования исходящих электронных сообщений;

подписание исходящего электронного сообщения электронной подписью, применяемой в контуре контроля реквизитов электронных сообщений (не снимая электронную подпись, применяемую в контуре обработки).