**Условия по защите информации**

**Глава 1. Общие положения**

1. Клиент для участия в обмене электронными сообщениями
(далее – ЭС) в платежной системе Банка России или Пользователь для участия в обмене финансовыми сообщениями (далее – ФС) в системе передачи финансовых сообщений Банка России (далее – СПФС) выполняет требования по защите информации в соответствии с настоящими Условиями.
2. Настоящие Условия применяются для целей договора, заключаемого Банком России с Клиентом (Пользователем)
и предусматривающего участие в обмене ЭС в платежной системе
Банка России (ФС в СПФС) (далее – Договор).
3. Термины, используемые в настоящих Условиях, понимаются
в значениях, определенных Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон
№ 161-ФЗ), установленных правилами платежной системы Банка России.
4. Кроме того, в настоящих Условиях используются следующие термины и сокращения:

администратор информационной безопасности (далее – АИБ) – лицо, назначенное Клиентом (Пользователем) и выполняющее обязанности
по администрированию средств защиты и механизмов защиты, реализующих требования по обеспечению информационной безопасности;

администратор ключевой системы (далее – АКС) – лицо, назначенное владельцем криптографического ключа ответственным за управление криптографическими ключами, в том числе за формирование криптографических ключей и обеспечение безопасности криптографических ключей;

владелец ключа электронной подписи, ключа шифрования (владелец криптографического ключа) – Банк России, Клиент, Пользователь
или косвенный участник платежной системы Банка России, являющийся клиентом участника обмена – Клиента (далее – косвенный участник Клиента);

инцидент – нарушение требований к обеспечению защиты информации при обмене ЭС или ФС, в том числе нарушение, которое привело или может привести к осуществлению переводов денежных средств без согласия клиента или к неоказанию услуг по переводу денежных средств;

клиент косвенного участника с доступом к ТПСБП – лицо, заключившее с косвенным участником, имеющим доступ к услугам по трансграничному переводу денежных средств с использованием сервиса быстрых платежей платежной системы Банка России (далее – ТПСБП), договор, предусматривающий оказание услуг по переводу денежных средств;

клиент участника СБП, имеющего доступ к ТПСБП – лицо, заключившее договор с участником СБП, имеющим доступ к ТПСБП, предусматривающий оказание услуг по переводу денежных средств;

ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи с использованием средств криптографической защиты информации;

ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи
и предназначенная для проверки подлинности электронной подписи;

ключ шифрования – уникальная последовательность символов, используемая при зашифровании и расшифровании ЭС и ФС;

ключевая информация – специальным образом организованная совокупность криптографических ключей, предназначенная
для осуществления криптографической защиты информации,
а также сертификаты, список аннулированных сертификатов, справочники сертификатов и упакованные данные;

ключевой носитель – отчуждаемый машинный носитель информации, содержащий криптографический ключ;

криптографический ключ – ключ электронной подписи и (или) ключ шифрования;

компрометация криптографического ключа – событие, определяемое владельцем криптографического ключа как ознакомление неуполномоченным лицом (лицами) с его криптографическим ключом;

косвенный участник Клиента – организация, соответствующая критериям, определенным для косвенных участников Клиента платежной системы Банка России нормативным актом Банка России на основании части 9 статьи 20 Федерального закона № 161-ФЗ;

косвенный участник Клиента с доступом к ТПСБП – иностранный банк (иностранная кредитная организация), иностранный центральный (национальный) банк, которому доступ к ТПСБП предоставляется
через участника СБП с доступом к ТПСБП – кредитную организацию
(ее филиал), международную финансовую организацию, клиентом которой
он является, в соответствии с договором счета, заключенным указанным участником СБП с Банком России.

объекты информационной инфраструктуры – автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, эксплуатация и использование которых обеспечиваются Клиентом (Пользователем) для участия в обмене ЭС и ФС;

пользователь ключа электронной подписи, ключа шифрования
(далее – пользователь криптографического ключа) – лицо, назначенное владельцем криптографического ключа и уполномоченное им использовать криптографический ключ от имени владельца криптографического ключа;

регистрационная карточка сертификата ключа проверки электронной подписи (далее – регистрационная карточка сертификата ключа) – документ, содержащий распечатку сертификата ключа проверки электронной подписи (включая распечатку в шестнадцатеричной системе счисления ключа проверки электронной подписи, наименование и иные реквизиты, идентифицирующие владельца ключа электронной подписи, подпись руководителя (лица, его замещающего) владельца ключа электронной подписи или лица из числа работников владельца ключа электронной подписи, уполномоченного на подписание регистрационной карточки сертификата ключа от имени владельца ключа электронной подписи, а также оттиск печати (при ее наличии);

регистрационный центр – подразделение Банка России, выполняющее функции регистрации и сертификации ключей электронной подписи, а также управления ключами проверки электронной подписи Клиента, косвенного участника Клиента, Пользователя и ключами шифрования, применяемыми при обмене ЭС и ФС;

СБП – сервис быстрых платежей платежной системы Банка России;

сертификат ключа проверки электронной подписи – документ
в электронном виде, выданный регистрационным центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа;

средства криптографической защиты информации (далее – СКЗИ) – аппаратные и (или) программные средства, обеспечивающие создание
и проверку электронной подписи, создание ключей электронной подписи,
а также реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при обмене ЭС
по каналам связи либо с использованием отчуждаемых машинных носителей информации;

уполномоченное лицо[[1]](#footnote-2) – лицо, уполномоченное на подписание от имени Клиента, косвенного участника Клиента, Пользователя регистрационных карточек сертификатов ключей проверки электронной подписи, запросов
на выпуск сертификатов ключей проверки электронной подписи, а также
на направление и (или) подписание обращений (заявлений) о приостановлении (отмене приостановления) обмена ЭС или о приостановлении (возобновлении) оказания услуг по передаче ФС в случае выявления инцидента, связанного
с несоблюдением Клиентом, Пользователем требований к защите информации, который привел или может привести к осуществлению перевода денежных средств без согласия клиента;

электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1. Сведения о реализованных мерах и средствах защиты информации, в том числе сведения о ключевой информации, а также сведения, передаваемые Банком России и Клиентом, косвенным участником Клиента, Пользователем друг другу в ходе исполнения настоящих Условий, не подлежат передаче третьим лицам, за исключением случаев, установленных законодательством Российской Федерации или договором, заключенным Банком России, Клиентом, косвенным участником Клиента, Пользователем и третьим лицом.
2. Сведения, содержащиеся в ЭС Клиента (ФС Пользователя),
и в ЭС, направленных Клиенту (ФС, направленных Пользователю) в ходе исполнения настоящих Условий, не подлежат передаче Банком России третьим лицам, за исключением случаев, установленных законодательством Российской Федерации и Договором.
3. При обмене в электронном виде сведениями о реализованных мерах и средствах защиты информации, а также материалами работы согласительной комиссии, созданной в соответствии с приложением 5
к настоящим Условиям, применяются организационные и технические меры защиты информации, в том числе предназначенные для предотвращения несанкционированного доступа к содержанию защищаемой информации
при передаче по открытым каналам связи, а также с использованием информационно-телекоммуникационной сети «Интернет».
4. Клиент должен выполнять и обеспечивать выполнение косвенным участником Клиента требований, определенных настоящими Условиями,
при обмене ЭС, осуществлять эксплуатацию и функционирование автоматизированного рабочего места обмена ЭС с платежной системой
Банка России и (или) автоматизированного рабочего места обмена ФС
(далее – АРМ обмена) в соответствии с требованиями эксплуатационной документации на АРМ обмена, полученной в соответствии с Условиями передачи программного обеспечения Клиенту Банка России.
5. Банк России вправе проверять выполнение Клиентом, косвенным участником Клиента, Пользователем требований к защите информации
на соответствие сведениям, изложенным в акте о готовности Клиента к обмену
ЭС с Банком России и (или) акте о готовности Пользователя к обмену ФС
с использованием СПФС.
6. Банк России уведомляет Клиента (Пользователя)
о приостановлении (возобновлении) обмена ЭС (ФС)
с использованием технической инфраструктуры (автоматизированной системы) Банка России.

В случае технической невозможности направления информации
с использованием технической инфраструктуры (автоматизированной системы) Банка России информация направляется с использованием резервных способов взаимодействия.

Информация о технической инфраструктуре (автоматизированной системе) Банка России, а также о резервных способах взаимодействия участников информационного обмена с Банком России размещается
на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» по адресу https://www.cbr.ru/information\_security/fincert/[[2]](#footnote-3).

**Глава 2. Меры по защите информации при осуществлении переводов денежных средств в платежной системе Банка России**

* 1. Клиенты, являющиеся кредитными организациями
	(их филиалами), имеющие доступ к услугам по переводу денежных средств
	с использованием распоряжений в электронном виде (за исключением централизованных филиалов) обеспечивают выполнение требований подпунктов 2.3.4 – 2.3.6 пункта 2.3 и приложения 6 к настоящим Условиям.
	2. Клиенты, являющиеся участниками СБП с доступом к ТПСБП, обеспечивают включение в договор с косвенными участниками с доступом
	к ТПСБП следующих требований к защите информации.

2.2.1. Косвенные участники с доступом к ТПСБП обеспечивают выполнение требований к защите информации в соответствии с требованиями законодательства иностранного государства по вопросам защиты информации и иных правовых актов, принятых в соответствии с ним.

2.2.2. В целях противодействия осуществлению переводов денежных средств без согласия клиента с использованием ТПСБП и обеспечения защиты информации при осуществлении переводов денежных средств
с использованием ТПСБП косвенный участник с доступом к ТПСБП осуществляет 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 ЭС участнику СБП, имеющему доступ к ТПСБП.

В рамках реализации мер по выявлению и устранению причин
и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участника СБП, имеющего доступ
к ТПСБП, и (или) его клиентов, а также предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента, косвенный участник с доступом к ТПСБП осуществляет:

выявление информации о компьютерных атаках, проводимых
с использованием идентификаторов клиента косвенного участника с доступом к ТПСБП, направленных на получение информации о клиентах участника СБП, имеющего доступ к ТПСБП, из формирующихся распоряжений
о переводе денежных средств клиента косвенного участника с доступом
к ТПСБП (далее – переборы идентификаторов клиентов);

блокировку идентификатора клиента косвенного участника с доступом к ТПСБП, используемого для осуществления переборов идентификаторов клиентов участника СБП, имеющего доступ к ТПСБП;

уведомление участника СБП, имеющего доступ к ТПСБП, о блокировке идентификатора клиента косвенного участника с доступом к ТПСБП;

проверку информации о переборах идентификаторов клиентов участника СБП, имеющего доступ к ТПСБП, в том числе при получении уведомления о блокировке идентификатора клиента косвенного участника
с доступом к ТПСБП;

доведение до участника СБП, имеющего доступ к ТПСБП, информации о результатах проведенной проверки.

* 1. Клиенты, не указанные в пунктах 2.1, 2.2 настоящих Условий,
	в части требований к защите информации при обмене ЭС обеспечивают выполнение следующих требований.
		1. Клиенты должны размещать объекты информационной инфраструктуры, используемые при обмене ЭС, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей. Размещение
		в сегментах (группах сегментов) вычислительных сетей, в которых расположены объекты информационной инфраструктуры, используемые
		при обмене ЭС, иных объектов информационной инфраструктуры
		не допускается.

АРМ обмена должно быть реализовано в выделенном (отдельном) сегменте (группах сегментов) вычислительных сетей с использованием отдельного рабочего места.

Контур формирования ЭС и контур контроля реквизитов ЭС
в информационной инфраструктуре Клиента должны быть реализованы
с привлечением отдельных работников для выполнения функций операторов, администраторов и администраторов информационной безопасности
в каждом из контуров.

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей Клиенты должны применять меры защиты информации, реализующие минимальный уровень (уровень 3) 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 08.08.2017 № 822-ст
«Об утверждении национального стандарта Российской Федерации»
(М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017).

* + 1. Документы Клиентов, определяющие порядок обеспечения защиты информации при обмене ЭС (далее – документы), должны определять состав и порядок применения организационных мер защиты информации, состав и порядок использования технических средств защиты информации.

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;

защита среды виртуализации;

защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

Документы должны содержать информацию, определяющую:

технологии подготовки, обработки, передачи и хранения ЭС
и защищаемой информации на объектах информационной инфраструктуры;

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

план действий, направленных на обеспечение непрерывности
и (или) восстановление деятельности, связанной с обменом ЭС;

лиц, допущенных к работе с СКЗИ, – пользователей криптографических ключей, АИБ, АКС;

уполномоченных лиц.

* + 1. Клиенты при обмене ЭС в платежной системе Банка России
		с использованием СКЗИ должны обеспечивать выполнение требований, указанных в приложении 6 к настоящим Условиям.
		2. Передача и прием ЭС осуществляются Клиентом
		с использованием автоматизированного рабочего места обмена ЭС
		с платежной системой Банка России. Автоматизированное рабочее место обмена должно быть реализовано с использованием программного комплекса, предоставляемого Банком России в соответствии с Условиями передачи программного обеспечения Клиенту Банка России, размещенными
		на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» по адресу https://[www.cbr.ru/development/mcirabis/](http://www.cbr.ru/development/mcirabis/).
		3. Клиенты должны обеспечивать хранение входящих и исходящих ЭС, подписанных электронной подписью, не менее пяти лет.
		4. При обмене ЭС при переводе денежных средств в рамках платежной системы Банка России Клиентом должна применяться электронная подпись, сертификат ключа проверки которой выдан Банком России.

Банк России и Клиент признают, что:

внесение изменений в ЭС после формирования электронной подписи дает отрицательный результат проверки подлинности электронной подписи;

формирование подлинной электронной подписи возможно только
при использовании ключа электронной подписи владельца.

* + 1. Клиенты при обмене ЭС между Клиентом и Банком России должны руководствоваться Условиями управления криптографическими ключами, указанными в приложении 3 к настоящим Условиям.
		2. Организационные меры и (или) технические средства защиты информации, используемые при обмене ЭС, применяются с учетом следующих требований.

Клиенты должны обеспечивать защиту ЭС, подлежащих передаче (направлению) в платежную систему Банка России:

формированием ЭС и контролем реквизитов ЭС в информационной инфраструктуре Клиента в соответствии с приложением 7 к настоящим Условиям, а также использованием двух усиленных электронных подписей для контроля целостности и подтверждения подлинности ЭС;

применением третьего варианта защиты, предусмотренного Альбомом электронных сообщений, размещенным на официальном сайте Банка России
в информационно-телекоммуникационной сети «Интернет» по адресу https://www.cbr.ru/development/Formats/ (далее – Альбом ЭС);

шифрованием ЭС 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;

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[[3]](#footnote-4).

* + 1. Клиенты должны информировать Банк России об инцидентах.

Информация об инцидентах должна направляться с использованием технической инфраструктуры (автоматизированной системы) Банка России.

В случае технической невозможности направления информации
об инцидентах с использованием технической инфраструктуры (автоматизированной системы) Банка России информация должна направляться с использованием резервных способов взаимодействия[[4]](#footnote-5).

Клиенты должны информировать Банк России с использованием технической инфраструктуры (автоматизированной системы) Банка России
в случае перехода на обмен ЭС с использованием отчуждаемых машинных носителей информации при невозможности осуществлять обмен ЭС
по каналам связи.

Клиенты должны информировать Банк России с использованием технической инфраструктуры (автоматизированной системы) Банка России
в случае перехода на обмен документами на бумажном носителе
при невозможности осуществлять обмен ЭС по каналам связи
и на отчуждаемых машинных носителях информации.

При возобновлении возможности направления информации
об инцидентах с использованием технической инфраструктуры (автоматизированной системы) Банка России Клиент должен повторно направить информацию с использованием технической инфраструктуры (автоматизированной системы) Банка России.

Информация о технической инфраструктуре (автоматизированной системе) Банка России, а также о резервных способах взаимодействия участников информационного обмена с Банком России размещается
на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» по адресу https://www.cbr.ru/information\_security/fincert/.

* 1. В случае выявления инцидента Клиент вправе направить
	в Банк России обращение о приостановлении обмена ЭС в порядке, указанном
	в приложении 4 к настоящим Условиям.
	2. Выполнение требований к защите информации подтверждается документами Клиента, в том числе содержащими информацию о проведении контроля за выполнением указанных требований, а также о датах проведения и результатах контроля. Документы Клиента подписываются руководителем Клиента либо уполномоченным лицом и представляются по запросу
	Банка России[[5]](#footnote-6) при проведении проверки выполнения требований к защите информации.

Клиент предоставляет возможность Банку России проводить проверки выполнения требований к защите информации, указанных в акте о готовности Клиента к обмену ЭС с Банком России, в том числе в подразделении Клиента.

Клиент обязан устранять нарушения требований к защите информации, выявленные при проверке, в сроки, установленные в акте проверки
Банка России.

Клиент обязан оформлять результаты устранения нарушений требований актом об устранении в письменном виде, направлять данный акт не позднее третьего рабочего дня после срока, установленного Банком России для устранения выявленных нарушений, одним из указанных ниже способов, доступных Клиенту (в случае если способ направления не указан в акте проверки):

с использованием личного кабинета;

через систему межведомственного электронного документооборота (далее – система МЭДО);

письмом на бумажном носителе, подписанным руководителем Клиента либо уполномоченным лицом (при отсутствии возможности направления способами, указанными выше).

До начала обмена ЭС Клиент представляет в подразделение
Банка России, обслуживающее счет Клиента, акт о готовности Клиента
к обмену ЭС с Банком России, форма которого приведена в приложении 1
к настоящим Условиям, одним из указанных ниже способов, доступных Клиенту (в случае если способ направления не определен в Договоре):

с использованием личного кабинета;

через систему МЭДО;

письмом на бумажном носителе, подписанным руководителем Клиента либо уполномоченным лицом (при отсутствии возможности направления способами, указанными выше).

В случае внесения каких-либо изменений, в том числе в состав ответственных лиц, указанных в приложениях к акту о готовности Клиента
к обмену ЭС с Банком России, Клиент обязан представить в подразделение Банка России, обслуживающее счет Клиента, актуальную информацию
не позднее следующего рабочего дня после внесения изменений одним
из указанных ниже способов, доступных Клиенту (в случае если способ направления не определен в Договоре):

с использованием личного кабинета;

через систему МЭДО;

письмом на бумажном носителе, подписанным руководителем Клиента либо уполномоченным лицом (при отсутствии возможности направления способами, указанными выше).

* 1. Клиент обеспечивает контроль выполнения косвенными участниками Клиента требований к защите информации, указанных
	в подпунктах 2.3.1 – 2.3.8 пункта 2.3 настоящих Условий.
	2. Клиент должен обеспечить получение подтверждения
	от косвенного участника с доступом к ТПСБП о выполнении требований
	к защите информации, указанных в пункте 2.2 настоящих Условий.
	3. Косвенные участники Клиента до начала обмена ЭС сообщают Клиенту о готовности к обмену ЭС с Банком России.

Клиент обеспечивает контроль выполнения косвенными участниками Клиента требований к защите информации и информирует Банк России
о готовности косвенного участника к обмену ЭС с Банком России
с использованием федеральной почтовой связи или личного кабинета.

* 1. Клиент должен обеспечить получение Клиентом от косвенного участника Клиента информации о нарушениях требований к обеспечению защиты информации при обмене ЭС, в том числе которые привели или могут привести к осуществлению переводов денежных средств без согласия клиента или к неоказанию услуг по переводу денежных средств.

При поступлении указанной информации от косвенных участников Клиента Клиент должен информировать Банк России в соответствии
с требованиями подпункта 2.3.9 пункта 2.3 настоящих Условий.

**Глава 3. Меры по защите информации при оказании услуг по передаче ФС с использованием СПФС**

* 1. Пользователи в части требований по защите информации
	при обмене ФС обеспечивают выполнение следующих требований.
		1. Пользователи должны размещать объекты информационной инфраструктуры, используемые при обмене ФС, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей. Размещение
		в сегментах (группах сегментов) вычислительных сетей, в которых расположены объекты информационной инфраструктуры, используемые при обмене ФС, иных объектов информационной инфраструктуры не допускается.

АРМ обмена должно быть реализовано в выделенном (отдельном) сегменте (группах сегментов) вычислительных сетей с использованием отдельного рабочего места.

Контур формирования ФС и контур контроля реквизитов ФС
в информационной инфраструктуре Пользователя должны быть реализованы с привлечением отдельных работников для выполнения функций операторов, администраторов и администраторов информационной безопасности
в каждом из контуров[[6]](#footnote-7).

Для объектов информационной инфраструктуры в пределах выделенного сегмента (группы сегментов) вычислительных сетей Пользователи должны применять меры защиты информации, реализующие уровни защиты информации, определенные ГОСТ Р 57580.1-2017.

Пользователи, являющиеся системно значимыми кредитными организациями, кредитными организациями, выполняющими функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитными организациями, являющимися значимыми на рынке платежных услуг, должны реализовывать усиленный уровень (уровень 1) защиты информации.

Пользователи, являющиеся кредитными организациями,
не относящимися к кредитным организациям, указанным в абзаце пятом настоящего подпункта, должны реализовывать стандартный уровень
(уровень 2) защиты информации.

Пользователи, являющиеся кредитными организациями, которые должны реализовывать стандартный уровень защиты информации, ставшие кредитными организациями, которые должны реализовывать усиленный уровень защиты информации, должны обеспечить реализацию усиленного уровня защиты информации не позднее восемнадцати месяцев после того,
как стали кредитными организациями, указанными в абзаце пятом настоящего подпункта.

Пользователи, не являющиеся кредитными организациями, должны реализовывать минимальный уровень (уровень 3) защиты информации.

* + 1. Документы Пользователей, определяющие порядок обеспечения защиты информации при обмене ФС (далее –документы), должны определять состав и порядок применения организационных мер защиты информации,
		а также состав и порядок использования технических средств защиты информации.

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;

защита среды виртуализации;

защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

Документы должны содержать информацию, определяющую:

технологии подготовки, обработки, передачи и хранения ФС
и защищаемой информации на объектах информационной инфраструктуры;

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

план действий, направленных на обеспечение непрерывности
и (или) восстановление деятельности, связанной с обменом ФС;

лиц, допущенных к работе с СКЗИ, – пользователей криптографических ключей, АИБ, АКС;

уполномоченных лиц.

* + 1. Защита информации Пользователями с помощью СКЗИ
		при обмене ФС должна обеспечиваться в соответствии с требованиями, указанными в приложении 6 к настоящим Условиям.
		2. Передача и прием ФС Пользователя осуществляются
		с использованием автоматизированного рабочего места клиента Банка России – пользователя СПФС.

Автоматизированное рабочее место обмена ФС должно быть реализовано с помощью программного обеспечения, предоставляемого Банком России, – программного комплекса «Автоматизированное рабочее место клиента Банка России – пользователя системы передачи финансовых сообщений».

* + 1. Пользователи должны обеспечивать хранение входящих
		и исходящих ФС, подписанных электронной подписью, не менее пяти лет.
		2. При обмене ФС между Пользователем и Банком России должна применяться электронная подпись, сертификат ключа проверки которой выдан Банком России.

Банк России и Пользователь признают, что:

внесение изменений в ФС после формирования электронной подписи дает отрицательный результат проверки подлинности электронной подписи;

формирование подлинной электронной подписи возможно только
при использовании ключа электронной подписи владельца.

* + 1. Криптографические ключи, используемые при обмене ФС между Пользователем и Банком России, должны изготавливаться Пользователем
		в соответствии с Условиями управления криптографическими ключами, указанными в приложении 3 к настоящим Условиям.
		2. Пользователи должны обеспечивать защиту ФС при их направлении в СПФС посредством:

формирования ФС и контроля реквизитов ФС в соответствии
с приложением 8 к настоящим Условиям;

применения первого варианта защиты, предусмотренного Альбомом ЭС;

шифрования ФС 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[[7]](#footnote-8).

* 1. Пользователи должны информировать Банк России о нарушениях требований к обеспечению защиты информации при обмене ФС.

Информация об инцидентах должна направляться с использованием технической инфраструктуры (автоматизированной системы) Банка России.

В случае технической невозможности направления информации
об инцидентах с использованием технической инфраструктуры (автоматизированной системы) Банка России информация должна направляться с использованием резервных способов взаимодействия.

При возобновлении возможности направления информации
об инцидентах с использованием технической инфраструктуры (автоматизированной системы) Банка России Пользователь должен повторно направить информацию с использованием технической инфраструктуры (автоматизированной системы) Банка России.

Информация о технической инфраструктуре (автоматизированной системе) Банка России, а также о резервных способах взаимодействия участников информационного обмена с Банком России размещается
на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» по адресу https://www.cbr.ru/information\_security/fincert/.

* 1. В случае выявления Пользователем несоблюдения им требований к защите информации приостановление оказания услуг по передаче ФС Пользователю осуществляется путем приостановления обмена через СПФС
	на основании заявления Пользователя о приостановлении оказания услуг
	по передаче ФС, содержащего сведения о несоблюдении Пользователем требований к защите информации, направленного в порядке, указанном
	в приложении 4 к настоящим Условиям.
	2. Выполнение требований к защите информации при обмене ФС подтверждается документами Пользователя, в том числе содержащими информацию о проведении контроля за выполнением указанных требований, а также о датах проведения и результатах контроля. Документы Пользователя подписываются руководителем Пользователя либо уполномоченным лицом
	и представляются по запросу Банка России[[8]](#footnote-9) при проведении проверки выполнения требований к защите информации.

Пользователь предоставляет возможность Банку России проводить проверки выполнения требований к защите информации, указанных в акте
о готовности Пользователя к обмену ФС с использованием СПФС, в том числе в подразделении Пользователя.

Пользователь обязан устранять нарушения требований к защите информации, выявленные при проверке, в сроки, установленные в акте проверки Банка России.

Пользователь обязан оформлять результаты устранения нарушений требований актом об устранении в письменном виде, направлять данный
акт не позднее третьего рабочего дня после срока, установленного
Банком России для устранения выявленных нарушений, одним из указанных ниже способов, доступных Пользователю (в случае если способ направления
не указан в акте проверки):

с использованием личного кабинета;

через систему МЭДО;

письмом на бумажном носителе, подписанным руководителем Пользователя либо уполномоченным лицом (при отсутствии возможности направления способами, указанными выше).

До начала обмена ФС Пользователь представляет в подразделение
Банка России, в котором заключен Договор с Пользователем,
акт о готовности Пользователя к обмену ФС с использованием СПФС, форма которого приведена в приложении 2 к настоящим Условиям одним
из указанных ниже способов, доступных Пользователю (в случае если способ направления не определен в Договоре):

с использованием личного кабинета;

через систему МЭДО;

письмом на бумажном носителе, подписанным руководителем Пользователя либо уполномоченным лицом (при отсутствии возможности направления способами, указанными выше).

В случае внесения каких-либо изменений, в том числе в состав ответственных лиц, указанных в приложениях к акту о готовности Пользователя к обмену ФС с использованием СПФС, Пользователь обязан представить в подразделение Банка России, в котором заключен Договор
с Пользователем, актуальную информацию не позднее следующего рабочего дня после внесения изменений одним из указанных ниже способов, доступных Пользователю (в случае если способ направления не определен в Договоре):

с использованием личного кабинета;

через систему МЭДО;

письмом на бумажном носителе, подписанным руководителем Пользователя либо уполномоченным лицом (при отсутствии возможности направления способами, указанными выше).

Приложение 1

к Условиям по защите информации

УТВЕРЖДАЮ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(личная подпись, Ф.И.О. руководителя (лица, его замещающего или должностного лица, заключившего Договор от имени Клиента)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование Клиента)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

АКТ

о готовности Клиента \_\_\_\_\_\_\_\_\_ (указывается наименование Клиента)
к обмену ЭС с Банком России

от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ г.

Настоящий акт составлен по результатам проверки готовности к обмену ЭС с использованием \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[[9]](#footnote-10).

Комиссия[[10]](#footnote-11) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указывается наименование Клиента), созданная на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указывается наименование, дата и номер распорядительного документа Клиента), в составе:

|  |  |  |
| --- | --- | --- |
|  | Руководитель Комиссии |  |
|  | Члены Комиссии: | (наименование должности, инициалы, фамилия) |
|  |  | (наименование должности, инициалы, фамилия) |
|  |  | (наименование должности, инициалы, фамилия) |
|  |  | (наименование должности, инициалы, фамилия) |

провела проверку готовности к обмену ЭС с Банком России.

Комиссия установила следующее:

1. Выполняются следующие меры в части защиты информации, указанные в Условиях по защите информации:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

2.  Информация о реализации мер в части защиты информации, указанных в подпунктах 2.3.1, 2.3.2 пункта 2.3 Условий по защите информации:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указываются конкретные меры в части защиты информации и планируемые сроки их реализации).

3. Выполняются следующие меры в части защиты информации:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Меры в части защиты информации** | **Перечень документов и описаний, отражающих реализацию правил материально-технического обеспечения формирования ЭС и контроля реквизитов ЭС, для участника ССНП** |
| 3.1. | Контур формирования ЭС и контур контроля реквизитов ЭС 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.АРМ обмена реализовано в выделенном (отдельном) сегменте (группах сегментов) вычислительных сетей с использованием отдельного рабочего места. | Участник ССНП направляет всю необходимую информацию[[11]](#footnote-12), подтверждающую выполнение указанных мер в части защиты информации, в соответствии с приложением 5 к настоящему Акту, в том числе:* название владельца и идентификаторы ключей ЭП с указанием их принадлежности к контуру формирования ЭС или контуру контроля реквизитов ЭС;
* сведения об АРМ, на которых осуществляется обработка защищаемой информации: сетевое имя, IP-адрес (при наличии – выделенный пул IP-адресов), MAC-адрес, соответствующий указанному IP-адресу, принадлежность к контуру формирования ЭС или контуру контроля реквизитов ЭС;
* реквизиты организационно-распорядительных документов участника о назначении операторов АРМ контура формирования ЭС, АРМ контура контроля реквизитов ЭС;
* реквизиты организационно-распорядительных документов участника о назначении администраторов АРМ контура формирования ЭС, АРМ контура контроля реквизитов ЭС;
* реквизиты организационно-распорядительных документов участника о назначении администраторов информационной безопасности АРМ контура формирования ЭС, АРМ контура контроля реквизитов ЭС.
 |
| 3.2. | Объекты информационной инфраструктуры контура формирования ЭС и контура контроля реквизитов ЭС 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. | Участник ССНП направляет всю необходимую информацию[[12]](#footnote-13), подтверждающую выполнение указанных в Условиях по защите информации мер в части защиты информации, в том числе:* описание способа информационного взаимодействия между объектами информационной инфраструктуры (сегментами вычислительных сетей) контура формирования ЭС и контура контроля реквизитов ЭС (автоматизированная система учета операций, АРМ контура контроля ЭС, АРМ контура формирования ЭС, АРМ обмена с Банком России, иное);
* реквизиты оформленного, согласованного со службой информационной безопасности и утвержденного руководством участника документа, описывающего способ и порядок допустимого информационного взаимодействия между сегментами вычислительных сетей, содержащими объекты информационной инфраструктуры контура формирования ЭС и контура контроля реквизитов ЭС, включая установленные правила фильтрации сетевого трафика (списки контроля доступа) между контуром формирования ЭС и контуром контроля реквизитов ЭС с указанием разрешенных протоколов сетевого, транспортного и прикладного уровней, а также между указанными контурами и иными сегментами локальной вычислительной сети, в том числе явно определяющие способы и правила взаимодействия с внешними сетями (описание данных взаимодействий должно содержать обоснование их необходимости);
* схему информационного взаимодействия на прикладном уровне между объектами информационной инфраструктуры, предназначенными для формирования, контроля и отправки платежных сообщений по технологическим каналам в Банк России;
* логическую схему сети с разделением на VLAN, указанием диапазона IP-адресов, масок подсетей, а также телекоммуникационного оборудования, используемого для сегментации сети в части размещения объектов информационной инфраструктуры контура формирования ЭС и контура контроля реквизитов ЭС в информационной инфраструктуре участника;
* сведения об оборудовании, используемом для сегментации сети в целях размещения объектов информационной инфраструктуры контура формирования ЭС и контура контроля реквизитов ЭС в информационной инфраструктуре участника (тип, производитель, модель, серийный номер, инвентарный номер);

сведения об оборудовании, используемом для фильтрации сетевого трафика (тип, производитель, модель/версия, серийный номер, инвентарный номер). |
| 3.3. | В контуре формирования ЭС на основе первичного документа в бумажной или электронной форме или входящего ЭС должны осуществляться:формирование исходящего ЭС, предназначенного для направления в платежную систему Банка России;контроль реквизитов исходящего ЭС, предназначенного для направления в платежную систему Банка России;подписание исходящего ЭС, предназначенного для направления в платежную систему Банка России, электронной подписью, применяемой в контуре формирования ЭС, при положительном результате контроля реквизитов, указанного в [абзаце третьем](#Par157) настоящего подпункта;направление исходящего ЭС, предназначенного для направления в платежную систему Банка России, в контур контроля реквизитов ЭС. | Участник ССНП направляет всю необходимую информацию[[13]](#footnote-14), подтверждающую выполнение указанных мер в части защиты информации, в том числе:* реквизиты документа, согласованного со службой информационной безопасности, описывающего информационное взаимодействие и технологический процесс, в том числе реализацию указанных процедур и мер в части защиты информации;
* технологическую схему и описание технологического процесса формирования ЭС на основе первичного документа, контроля первичного документа и отправки по технологическим каналам в Банк России на каждом этапе, в том числе:
	+ описание этапа формирования исходящего ЭС;
	+ описание этапа контроля реквизитов исходящего ЭС в контуре формирования ЭС с указанием основных контролируемых полей и способов контроля;
	+ описание этапа подписания исходящего ЭС в контуре формирования ЭС с описанием механизма разграничения доступа при выполнении операций,
	+ описание этапа направления исходящего ЭС в контур контроля реквизитов ЭС;
	+ описание этапа контроля реквизитов исходящего ЭС в контуре контроля реквизитов ЭС с указанием основных контролируемых полей и способа контроля;
	+ указание источника эталонной информации для сравнения и способа взаимодействия,
	+ описание этапа контроля на отсутствие дублирования исходящих ЭС с указанием основных контролируемых полей и способа контроля;
	+ описание этапа подписания исходящего ЭС, предназначенного для направления в платежную систему Банка России, электронной подписью, применяемой в контуре контроля реквизитов ЭС, с описанием механизма разграничения доступа при выполнении операций;
	+ описание процедуры (порядок, ответственные) шифрования исходящего ЭС;
	+ описание процедуры (порядок, ответственные) установления защищенного соединения с ТШ КБР (vpn) и отправки готовых (подписанных и зашифрованных) ЭС.
 |
| 3.4. | В контуре контроля реквизитов ЭС должны осуществляться:контроль реквизитов исходящего ЭС, предназначенного для направления в платежную систему Банка России, на соответствие реквизитам первичного документа в бумажной или электронной форме или входящего ЭС;контроль на отсутствие дублирования исходящих ЭС;подписание исходящего ЭС, предназначенного для направления в платежную систему Банка России, электронной подписью, применяемой в контуре контроля реквизитов ЭС, при положительном результате контроля реквизитов, указанного в [абзаце втором](#Par161) настоящего подпункта. |

4. АРМ обмена эксплуатируется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указываются полное наименование, адрес подразделения Клиента, номера телефонов, фамилии, имена, отчества (при наличии) руководителей подразделения Клиента, ответственных
за эксплуатацию АРМ обмена, выполнение требований к защите информации).

5. СКЗИ эксплуатируется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(указываются полное наименование, адрес подразделения Клиента, номера телефонов, фамилии, имена, отчества (при наличии) ответственных за эксплуатацию СКЗИ, выполнение требований
к защите информации).

6. АС Клиента эксплуатируется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указываются полное наименование, адрес подразделения Клиента, номера телефонов, фамилии, имена, отчества
(при наличии) ответственных за эксплуатацию АС, выполнение требований к защите информации).

7. Информация о лицах, уполномоченных на направление в Банк России и подписание обращений о приостановлении (возобновлении) обмена ЭС при переводе денежных средств в рамках платежной системы Банка России
в случае несоблюдения участником обмена требований к защите информации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(указывается информация в соответствии с пунктом 4 приложения 4 Условий по защите информации).

Заключение

Комиссия считает, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 (указывается наименование Клиента)

готов к осуществлению обмена ЭС при переводе денежных средств в рамках платежной системы Банка России с использованием \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[[14]](#footnote-15).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Руководитель Комиссии |  |  |  |
|  | Члены Комиссии: | (инициалы, фамилия) |  | (подпись, дата) |
|  |  | (инициалы, фамилия) |  | (подпись, дата) |
|  |  | (инициалы, фамилия) |  | (подпись, дата) |
|  |  | (инициалы, фамилия) |  | (подпись, дата) |

Приложения:

1. Акт о готовности АРМ обмена к обмену ЭС[[15]](#footnote-16) (составляется в произвольной форме, акт утверждается руководителем Клиента (лицом, его замещающим) или должностным лицом, заключившим Договор от имени Клиента).

2. Организационно-распорядительный документ участника
о назначении администраторов АРМ контура формирования ЭС, АРМ контура контроля реквизитов ЭС и АРМ обмена (с указанием фамилии, инициалов, занимаемой должности, номера телефона).

3. Организационно-распорядительный документ участника
о назначении администраторов информационной безопасности АРМ контура формирования ЭС, АРМ контура контроля реквизитов ЭС и АРМ обмена
(с указанием фамилии, инициалов, занимаемой должности, номера телефона).

4. Организационно-распорядительный документ участника
о назначении операторов АРМ контура формирования ЭС, АРМ контура контроля реквизитов ЭС и АРМ обмена, а также лиц допущенных к работе
с СКЗИ, АКС и документы о предоставлении полномочий уполномоченным лицам[[16]](#footnote-17) (составляется в произвольной форме с указанием фамилии, инициалов, занимаемой должности, номеров телефонов, перечня филиалов (в том числе централизованных)/ перечня централизованных ТОФК[[17]](#footnote-18), от имени которых работает данный пользователь (данные пользователи)

5. Документы, отражающие (поясняющие) реализацию правил материально-технического обеспечения формирования ЭС и контроля реквизитов ЭС для участника ССНП, в том числе описание информационного взаимодействия и технологического процесса, а также иные документы, указанные в пункте 3 приложения 1 к Условиям по защите информации
(в соответствии с приложением к Положению Банка России от 25.07.2022 № 802-П «О требованиях к защите информации в платежной системе Банка России).

6. Сведения об информационной инфраструктуре, предназначенной для формирования, контроля и направления ЭС в ПС БР (по форме приложения
к настоящему приложению).

7. Распорядительный документ Клиента о проведении проверки готовности к обмену ЭС с Банком России.

Приложение

к Приложению 1

к Условиям по защите информации

Сведения об информационной инфраструктуре, предназначенной
для формирования, контроля и направления ЭС в ПС БР

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Доменное имя | IP-адрес, маска подсети, VLAN | MAC-адрес | Установленное ПО |
| АРМ обмена[[18]](#footnote-19) |   |  |  |  |
| АРМ контура формирования |  |  |  |  |
| АРМ контура контроля |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Технологический участок  | Роль | ФИО (основной/ замещающий) | Идентификатор ключа электронной подписи | Реквизиты документа о назначении  |
| АРМ обмена | *Оператор АРМ* |  |  |  |
| *Администратор АРМ* |  |  |  |
| *Администратор информационной безопасности автоматизированного рабочего места (далее - АИБ АРМ)* |  |  |  |
| Контур формирования | *Оператор АРМ* |  |  |  |
| *Администратор АРМ* |  |  |  |
| *АИБ АРМ* |  |  |  |
| Контур контроля | *Оператор АРМ* |  |  |  |
| *Администратор АРМ* |  |  |  |
| *АИБ АРМ* |  |  |  |

Приложение 2

к Условиям по защите информации

УТВЕРЖДАЮ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(личная подпись, Ф.И.О. руководителя (лица, его замещающего), или должностного лица, заключившего Договор от имени Пользователя)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(наименование Пользователя)

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г.

АКТ

о готовности Пользователя \_\_\_\_\_\_\_\_\_ (указывается наименование Пользователя)
к обмену ФС с использованием СПФС

от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ г.

Настоящий акт составлен по результатам проверки готовности к обмену ФС с использованием \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[[19]](#footnote-20).

Комиссия[[20]](#footnote-21) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указывается наименование Пользователя), созданная на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указывается наименование, дата и номер распорядительного документа Пользователя), в составе:

|  |  |  |
| --- | --- | --- |
|  | Руководитель Комиссии |  |
|  | Члены Комиссии: | (наименование должности, инициалы, фамилия) |
|  |  | (наименование должности, инициалы, фамилия) |
|  |  | (наименование должности, инициалы, фамилия) |
|  |  | (наименование должности, инициалы, фамилия) |

провела проверку готовности к обмену ФС с Банком России.

Комиссия установила следующее:

1. Информация о реализации мер в части защиты информации, указанных в подпункте 3.1.1 пункта 3.1 Условий по защите информации:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(указываются конкретные меры в части защиты информации и планируемые сроки их реализации).

1. Выполняются следующие меры в части защиты информации:

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Содержание требований по защите информации** | **Перечень документов и описаний, отражающих реализацию правил материально-технического обеспечения формирования ФС для Пользователя СПФС** |
| 1. | Объекты информационной инфраструктуры, используемые при осуществлении передачи ФС через СПФС, размещены в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей, отличных от сегментов (групп сегментов) вычислительных сетей, где размещены объекты информационной инфраструктуры, используемые при осуществлении передачи ЭС в ПС БР. |  |
| 2. | Для объектов информационной инфраструктуры в пределах указанного сегмента (группы сегментов) вычислительных сетей Пользователь реализует меры защиты информации по следующим направлениям: |  |
| 2.1. | обеспечение защиты информации при управлении доступом; |  |
| 2.2. | обеспечение защиты вычислительных сетей; |  |
| 2.3. | контроль целостности и защищенности информационной инфраструктуры; |  |
| 2.4. | защита от вредоносного кода; |  |
| 2.5. | предотвращение утечек информации; |  |
| 2.6. | управление инцидентами защиты информации; |  |
| 2.7. | защита среды виртуализации. |  |
| 3. | Пользователем разработаны документы, определяющие: |  |
| 3.1. | порядок обеспечения защиты информации при передаче ФС, включающий описание: |  |
| 3.1.1. | технологии подготовки, обработки, передачи и хранения ФС и защищаемой информации на объектах информационной инфраструктуры участника обмена СПФС; |  |
| 3.1.2. | состав и порядок применения технологических мер защиты информации, применяемых для контроля целостности и подтверждения подлинности ФС на этапах их подготовки, приема, ввода, обработки и передачи, в том числе порядок применения СКЗИ и управления ключевой информацией СКЗИ; |  |
| 3.1.3. | обеспечение защиты информации с помощью СКЗИ пользователем осуществляется в соответствии с технической документацией на СКЗИ; |  |
| 3.1.4. | логическую схему сети с разделением на VLAN, указанием диапазона IP-адресов, масок подсетей, а также телекоммуникационного оборудования, используемого для сегментации сети в части размещения объектов информационной инфраструктуры используемой при осуществлении передачи ФС. |  |
| 4. | Пользователь обеспечивает назначение лиц: |  |
| 4.1. | допущенных к работе с СКЗИ; |  |
| 4.2. | ответственных за обеспечение функционирования и безопасности СКЗИ (ответственный пользователь СКЗИ); |  |
| 4.3. | обладающих правами по управлению криптографическими ключами, в том числе ответственных за формирование криптографических ключей и обеспечение безопасности криптографических ключей |  |
| 5. | Пользователь обеспечивает регистрацию действий своих работников, обладающих правами по формированию ФС. |  |
| 6. | Пользователь обеспечивает ведение архива входящих и исходящих ФС, подписанных электронной подписью, со сроком их хранения не менее пяти лет. |  |
| 7. | В случае реализации подписания ФС в информационной инфраструктуре (автоматизированной системе) Пользователя обеспечена защита ФС при их передаче в Банк России посредством формирования ФС и контроля реквизитов ФС в информационной инфраструктуре с учетом следующего: |  |
| 7.1. | Контур формирования ФС и контур контроля реквизитов ФС в информационной инфраструктуре Пользователя реализованы с использованием разных рабочих мест и с привлечением отдельных работников для каждого из контуров. |  |
| 7.2. | Объекты информационной инфраструктуры контура формирования ФС и контура контроля реквизитов ФС в информационной инфраструктуре Пользователя размещены в разных сегментах вычислительных сетей, в том числе реализованных с использованием технологии виртуализации. Способ допустимого информационного взаимодействия между указанными сегментами вычислительных сетей оформлен документально. |  |
| 7.3. | В контуре формирования ФС на основе первичного документа в бумажной или электронной форме, или входящего ФС осуществляется:формирование исходящего ФС, предназначенного для направления в СПФС;контроль реквизитов исходящего ФС, предназначенного для направления в СПФС;подписание исходящего ФС, предназначенного для направления в СПФС, электронной подписью, применяемой в контуре формирования ФС, при положительном результате контроля реквизитов;направление исходящего ФС, предназначенного для направления в СПФС Банка России, в контур контроля реквизитов ФС. |  |
| 7.4. | В контуре контроля реквизитов ФС осуществляется:контроль реквизитов исходящего ФС на соответствие реквизитам первичного документа в бумажной или электронной форме, или входящего ФС;контроль на отсутствие дублирования исходящих ФС;передача исходящего ФС, при положительном результате контроля реквизитов, на автоматизированное рабочее место обмена ФС. |  |
| 7.5. | На АРМ обмена ФС получение исходящего ФС осуществляется с последующим:шифрованием ФС 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 |  |

3. АРМ обмена эксплуатируется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указываются полное наименование, адрес подразделения Пользователя, номера телефонов, фамилии, имена, отчества (при наличии) руководителей подразделения Пользователя, ответственных за эксплуатацию АРМ обмена, выполнение требований к защите информации).

4. СКЗИ эксплуатируется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(указываются полное наименование, адрес подразделения Пользователя, номера телефонов, фамилии, имена, отчества (при наличии) ответственных за эксплуатацию СКЗИ, выполнение требований к защите информации).

5. АС Пользователя эксплуатируется \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (указываются полное наименование, адрес подразделения Пользователя, номера телефонов, фамилии, имена, отчества (при наличии) ответственных за эксплуатацию АС, выполнение требований к защите информации).

6. Информация о лицах, уполномоченных на направление в Банк России и подписание обращений о приостановлении (возобновлении) обмена ФС при оказании услуг по передаче ФС в случае несоблюдения участником обмена требований к защите информации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
(указывается информация в соответствии с пунктом 4 приложения 4 Условий по защите информации).

Заключение

Комиссия считает, что \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
 (указывается наименование Пользователя)

готов к осуществлению обмена ФС через СПФС с использованием \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[[21]](#footnote-22).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Руководитель Комиссии |  |  |  |
|  | Члены Комиссии: | (инициалы, фамилия) |  | (подпись, дата) |
|  |  | (инициалы, фамилия) |  | (подпись, дата) |
|  |  | (инициалы, фамилия) |  | (подпись, дата) |
|  |  | (инициалы, фамилия) |  | (подпись, дата) |

Приложения[[22]](#footnote-23):

1. Акт о готовности АРМ обмена к обмену ФС[[23]](#footnote-24) (составляется в произвольной форме, акт утверждается руководителем Пользователя (лицом, его замещающим) или должностным лицом, заключившим Договор от имени Пользователя).

2. Организационно-распорядительный документ участника
о назначении администраторов АРМ обмена (с указанием фамилии, инициалов, занимаемой должности, номера телефона).

3. Организационно-распорядительный документ участника
о назначении администраторов информационной безопасности АРМ обмена
(с указанием фамилии, инициалов, занимаемой должности, номера телефона).

4. Организационно-распорядительный документ участника
о назначении операторов АРМ обмена, а также лиц, допущенных к работе
с СКЗИ, АКС и документы о предоставлении полномочий уполномоченным лицам[[24]](#footnote-25) (составляется в свободной форме с указанием фамилии, инициалов, занимаемой должности, номеров телефонов, перечня филиалов (в том числе централизованных) /перечня централизованных ТОФК[[25]](#footnote-26), от имени которых работает данный Пользователь (данные Пользователи).

5. Документы, отражающие (поясняющие) реализацию правил материально-технического обеспечения формирования ФС для участника обмена СПФС, указанные в пункте 2 приложения 2 к Условиям по защите информации.

6. Сведения об информационной инфраструктуре, предназначенной для формирования, контроля и направления ФС (по форме приложения к настоящему приложению).

7. Распорядительный документ Пользователя о проведении проверки готовности к обмену ФС с Банком России.

Приложение

к Приложению 2

к Условиям по защите информации

Сведения об информационной инфраструктуре, предназначенной
для формирования, контроля и направления ФС через СПФС

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Доменное имя | IP-адрес, маска подсети, VLAN | MAC-адрес | Установленное ПО |
| АРМ обмена[[26]](#footnote-27) |   |  |  |  |
| АРМ контура формирования[[27]](#footnote-28) |  |  |  |  |
| АРМ контура контроля |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Технологический участок  | Роль | ФИО (основной/ замещающий) | Идентификатор ключа электронной подписи | Реквизиты документа о назначении  |
| АРМ обмена | *Оператор АРМ* |  |  |  |
| *Администратор АРМ* |  |  |  |
| *АИБ АРМ* |  |  |  |
| Контур формирования | *Оператор АРМ* |  |  |  |
| *Администратор АРМ* |  |  |  |
| *АИБ АРМ* |  |  |  |
| Контур контроля | *Оператор АРМ* |  |  |  |
| *Администратор АРМ* |  |  |  |
| *АИБ АРМ* |  |  |  |

Приложение 3

к Условиям по защите информации

Условия управления криптографическими ключами

1. Условия управления криптографическими ключами
(далее – Условия) выполняются Клиентом (косвенным участником Клиента, Пользователем) при управлении ключами электронной подписи и ключами шифрования, применяемыми при обмене ЭС при переводе денежных средств в рамках платежной системы Банка России или при обмене ФС.
2. Клиент (косвенный участник Клиента, Пользователь) может иметь несколько криптографических ключей, а также при необходимости резервные криптографические ключи.
3. Криптографические ключи Клиент (косвенный участник Клиента, Пользователь) изготавливает самостоятельно на учтенных ключевых носителях с использованием средств, входящих в комплект поставки СКЗИ.

Допускается генерация Клиентом (косвенным участником Клиента, Пользователем) криптографических ключей в регистрационном центре,
для чего Банк России предоставляет Клиенту (косвенному участнику Клиента, Пользователю) рабочее место для генерации криптографических ключей, оборудованное СКЗИ (при этом согласие Клиента (косвенного участника Клиента, Пользователя) на изготовление криптографических ключей
на технических средствах Банка России должно быть документально зафиксировано и оформляться при каждом изготовлении криптографических ключей).

Для самостоятельного изготовления криптографических ключей Клиент (косвенный участник Клиента, Пользователь) получает в регистрационном центре данные, необходимые для заполнения полей сертификата криптографического ключа.

1. Взаимодействие Банка России с Клиентом (Пользователем)
в части управления ключами осуществляется АКС Банка России.

Клиент (Пользователь) не позднее одного месяца до срока окончания действия криптографического ключа должен инициировать проведение
его плановой смены, в случае необходимости инициировать проведение внеплановой смены криптографического ключа. Криптографические ключи
с истекшим сроком действия не используются. Взаимодействие
с Банком России по вопросам управления ключами со стороны Клиента (Пользователя) осуществляется АКС Клиента (Пользователя).
Для обеспечения бесперебойной работы по управлению криптографическими ключами рекомендуется назначать не менее двух АКС Клиента (Пользователя).

1. Клиент обеспечивает сохранность своих криптографических ключей и обеспечение косвенным участником Клиента сохранности
его криптографических ключей.

Пользователь обеспечивает сохранность своих криптографических ключей.

1. Организационно-техническая информация, необходимая
для взаимодействия Банка России и Клиента (косвенного участника Клиента, Пользователя), доводится в Регламенте взаимодействия Банка России
и Клиента (косвенного участника Клиента, Пользователя) при управлении криптографическими ключами (далее – Регламент), предоставляемом Клиенту (косвенному участнику Клиента, Пользователю) подразделением Банка России, в лице которого Банк России заключил Договор.

Клиент (Пользователь) обязуется соблюдать положения, приведенные
в Регламенте. Клиент включает в договор с косвенным участником Клиента условие о выполнении косвенным участником Клиента Регламента.

1. Регламент содержит следующее.
	1. Порядок получения данных, необходимых для заполнения полей сертификата криптографического ключа.
	2. Порядок изготовления и сертификации криптографических ключей.
	3. Порядок изготовления регистрационной карточки сертификата ключа на бумажном носителе.
	4. Порядок плановой и внеплановой смены криптографических ключей.
	5. Порядок действий в случае компрометации криптографических ключей.
	6. Порядок действий с криптографическими ключами в случае доступа (подозрении на доступ) к ним неуполномоченных лиц, а также
	в случае прекращения полномочий работников по доступу к указанным ключам.
	7. Порядок уничтожения криптографических ключей.
	8. Порядок взаимодействия АКС Клиента (Пользователя) и АКС Банка России по вопросам управления ключевой системой.
	9. Наименование регистрационного центра.
2. Особенности управления криптографическими ключами косвенного участника Клиента.

Клиенту при формировании договора, заключаемого между Клиентом
и косвенным участником Клиента, в части управления криптографическими ключами косвенного участника Клиента следует руководствоваться настоящими Условиями, в том числе следующим.

* 1. Клиент доводит до косвенного участника Клиента настоящие Условия и Регламент.
	2. Косвенный участник Клиента назначает АКС и доводит
	эту информацию до Клиента.
	3. Клиент передает информацию об АКС косвенного участника Клиента в регистрационный центр для возможности получения АКС косвенного участника Клиента в регистрационном центре данных, необходимых для заполнения полей сертификата криптографического ключа.
	4. АКС косвенного участника Клиента самостоятельно получает данные, необходимые для заполнения полей сертификата криптографического ключа в регистрационном центре.
	5. Генерация криптографических ключей косвенного участника Клиента осуществляется либо самостоятельно АКС косвенного участника Клиента на технических средствах косвенного участника Клиента, технических средствах Клиента, технических средствах Банка России, либо АКС Клиента на технических средствах Клиента в присутствии АКС косвенного участника Клиента. Доступ к криптографическим ключам косвенного участника Клиента со стороны АКС Клиента должен быть исключен.
	6. Дальнейшее взаимодействие по управлению криптографическими ключами косвенного участника Клиента осуществляется между АКС косвенного участника Клиента и АКС Клиента с последующим взаимодействием АКС Клиента с АКС Банка России и производится
	в соответствии с Регламентом.
1. Регистрационная карточка сертификата ключа изготавливается
в двух экземплярах и содержит:

наименование владельца ключа электронной подписи;

наименование используемого СКЗИ и стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи;

информацию, идентифицирующую ключ электронной подписи (идентификатор[[28]](#footnote-29) и (или) номер ключа электронной подписи[[29]](#footnote-30), идентификатор и (или) номер серии);

информацию о назначении ключа электронной подписи (область применения);

уникальный номер сертификата ключа проверки электронной подписи;

распечатку ключа проверки электронной подписи в шестнадцатеричной системе счисления;

даты начала и окончания действия ключа электронной подписи;

даты начала и окончания действия ключа проверки электронной подписи;

фамилию и инициалы, должность и подпись руководителя
(или замещающего его лица) владельца ключа электронной подписи
или уполномоченного на подписание от его имени регистрационных карточек сертификатов ключей, заверенные оттиском печати владельца ключа электронной подписи (при ее наличии);

фамилию и инициалы, подпись АКС Банка России.

Регистрационная карточка сертификата ключа косвенного участника Клиента дополнительно заверяется собственноручной подписью руководителя (лица, его замещающего, или уполномоченного лица) Клиента, а также печатью Клиента (при ее наличии).

Регистрационная карточка сертификата ключа может распечатываться на одном листе или нескольких страницах. При распечатке регистрационной карточки на нескольких страницах каждая страница должна содержать подпись руководителя (или замещающего его лица) владельца ключа электронной подписи или уполномоченного на подписание от имени Клиента (Пользователя) регистрационных карточек сертификатов ключей Клиента (Пользователя), заверенную оттиском печати владельца ключа электронной подписи (при ее наличии).

Один экземпляр регистрационной карточки сертификата ключа
на бумажном носителе хранится в регистрационном центре,
другой – у владельца ключа. Ключ электронной подписи считается зарегистрированным со дня передачи в регистрационный центр надлежащим образом заверенного экземпляра регистрационной карточки сертификата ключа на бумажном носителе.

Порядок ввода в действие ключей электронной подписи и ключей шифрования определяется Регламентом.

1. При компрометации или подозрении на компрометацию криптографического ключа использование скомпрометированного ключа должно быть прекращено. Пользователь ключа в соответствии с внутренним регламентом обязан немедленно проинформировать о факте компрометации/подозрении на компрометацию АКС, АИБ и Руководителя Клиента (Пользователя). В случае принятия Клиентом (Пользователем) решения о компрометации криптографического ключа Клиент (Пользователь) должен уведомить регистрационный центр о необходимости аннулирования сертификата скомпрометированного ключа и проведении его внеплановой смены.

По факту компрометации криптографического ключа владелец ключа организовывает служебное расследование, результаты которого оформляются актом. Клиент (Пользователь) обязан направить письмо с приложенным экземпляром указанного акта Клиента (Пользователя) или косвенного участника Клиента в регистрационный центр не позднее трех рабочих дней
со дня окончания расследования.

1. В случае увольнения или прекращения полномочий работника
по доступу к криптографическому ключу заблаговременно, в сроки, установленные Регламентом, должна быть проведена замена криптографического ключа, к которому указанный работник имел единоличный доступ.
2. Уничтожение криптографических ключей на ключевых носителях проводится комиссией, состоящей из представителей Клиента (Пользователя), с составлением акта (для косвенного участника Клиента в комиссию включаются также представители косвенного участника Клиента).

Приложение 4

к Условиям по защите информации

Порядок направления обращений о приостановлении (возобновлении) обмена ЭС или заявлений о приостановлении (возобновлении) обмена ФС
в случае выявления инцидента, связанного с несоблюдением Клиентом (Пользователем) требований к защите информации

1. В случае выявления инцидента, связанного с несоблюдением требований к защите информации, Клиент (Пользователь) вправе направить
в Банк России обращение о приостановлении обмена ЭС в платежной системе Банка России или заявление о приостановлении оказания услуг по передаче ФС.

По результатам устранения причин инцидента Клиент (Пользователь) должен направлять обращение о возобновлении обмена ЭС (заявление
о возобновлении оказания услуг по передаче ФС), при получении которого Банк России снимает ранее введенное ограничение для возобновления обмена ЭС (оказания услуг по передаче ФС) с Клиентом (Пользователем).

1. Обращения о приостановлении обмена ЭС (заявления
о приостановлении оказания услуг по передаче ФС) в случае выявления инцидента, связанного с несоблюдением требований к защите информации,
и обращения о возобновлении обмена ЭС (заявления о возобновлении оказания услуг по передаче ФС) (далее при совместном упоминании – обращения (заявления) должны направляться с использованием технической инфраструктуры (автоматизированной системы) Банка России.

В случае технической невозможности направления обращения (заявления) с использованием технической инфраструктуры (автоматизированной системы) Банка России обращение (заявление) должно направляться с использованием резервных способов взаимодействия.

При возобновлении возможности направления обращений (заявлений)
с использованием технической инфраструктуры (автоматизированной системы) Банка России Клиент (Пользователь) должен повторно направить обращение (заявление) с использованием технической инфраструктуры (автоматизированной системы) Банка России.

1. Информация о технической инфраструктуре (автоматизированной системе) Банка России, а также о резервных способах взаимодействия Клиента (Пользователя) с Банком России, с помощью которого направляются обращения (заявления), размещается на официальном сайте Банка России
в информационно-телекоммуникационной сети «Интернет» по адресу https://www.cbr.ru/information\_security/fincert/.
2. В целях направления обращений (заявлений) Клиент (Пользователь) должен обеспечить назначение должностных лиц, уполномоченных на направление и (или) подписание обращений (заявлений), и направление в Банк России письма, содержащего информацию
об уполномоченных лицах, не позднее следующего дня после дня
их назначения или изменения.

Указанное письмо составляется по форме, размещенной на сайте
Банка России в информационно-телекоммуникационной сети «Интернет»
по адресу https://www.cbr.ru/information\_security/fincert/, и направляется
в Банк России (Департамент информационной безопасности) не позднее рабочего дня, следующего за днем их назначения или изменения,
с использованием одного из указанных ниже способов (в случае если способ направления не определен в Договоре):

с использованием личного кабинета;

через систему МЭДО;

письмом на бумажном носителе, подписанным руководителем Клиента (Пользователя) либо уполномоченным лицом (при отсутствии возможности направления способами, указанными выше).

5. Не позднее одного рабочего дня после дня направления обращения (заявления) Клиент (Пользователь) должен направить оригинал обращения
о приостановлении обмена ЭС (заявления о приостановлении оказания услуг по передаче ФС) или о возобновлении обмена ЭС (заявления о возобновлении оказания услуг по передаче ФС), оформленного в письменном виде, подписанного уполномоченным лицом и заверенного печатью Клиента (Пользователя) (при ее наличии), в Банк России с использованием одного
из указанных ниже способов (в случае если способ направления не определен в Договоре):

с использованием личного кабинета;

через систему МЭДО;

письмом на бумажном носителе, подписанным руководителем Клиента (Пользователя) либо уполномоченным лицом) (при отсутствии возможности направления способами, указанными выше).

6. Формы обращения о приостановлении обмена ЭС (заявления
о приостановлении оказания услуг по передаче ФС) и обращения
о возобновлении обмена ЭС (заявления о возобновлении оказания услуг
по передаче ФС), направляемых в письменном виде, а также с использованием технической инфраструктуры (автоматизированной системы) Банка России или с использованием резервных способов, размещены на официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет»
по адресу https://www.cbr.ru/information\_security/fincert/.

Приложение 5

к Условиям по защите информации

Урегулирование споров и разногласий при обмене ЭС (ФС)

1. Споры и разногласия при обмене ЭС (ФС), возникающие вследствие неисполнения или ненадлежащего исполнения Клиентом (Пользователем) или Банком России обязательств по Договору, неотъемлемой частью которого являются настоящие Условия, или в связи с ним, разрешаются путем переговоров, создания согласительной комиссии,
а в случае невозможности разрешения существующих разногласий рассматриваются в судебном порядке в соответствии с законодательством Российской Федерации.
2. Для урегулирования разногласий при обмене ЭС (ФС), установления фактических обстоятельств, послуживших основанием
для их возникновения, а также для проверки подлинности и контроля целостности ЭС (ФС) Банком России совместно с Клиентом (Пользователем) создается согласительная комиссия (далее – комиссия).
3. При возникновении разногласий в связи с обменом ЭС (ФС) заявляющая разногласие Сторона (Клиент (Пользователь) либо Банк России)
(далее – Сторона-инициатор) направляет другой Стороне (Клиенту (Пользователю) либо Банку России) заявление о разногласиях, подписанное уполномоченным должностным лицом, с изложением причин разногласий
и предложением создать комиссию.

В заявлении указываются:

наименование Стороны-инициатора;

тип и описание претензии;

фамилии, инициалы и занимаемые должности представителей Стороны-инициатора, которые будут участвовать в работе комиссии;

место, время и дату сбора комиссии (не позднее семи рабочих дней
со дня отправления заявления).

До подачи заявления Сторона-инициатор обязана убедиться
в целостности своего программного обеспечения, неизменности используемой ключевой информации, а также отсутствии нарушения целостности информационной инфраструктуры и несанкционированных действий
со стороны персонала, обслуживающего АРМ обмена.

1. В состав комиссии включается равное количество представителей каждой Стороны, но не более пяти человек, включая представителей службы безопасности и юридической службы (при их наличии).

Члены комиссии от каждой Стороны назначаются приказом либо иным распорядительным актом соответствующей Стороны.

В случае необходимости привлечения независимых специалистов,
не представляющих какую-либо из Сторон и имеющих официально подтвержденную квалификацию, данные специалисты включаются в состав комиссии по письменному соглашению Сторон сверх квоты представителей Сторон, определяемой в соответствии с абзацем первым настоящего пункта.

Порядок оплаты работы независимых специалистов в комиссии определяется по соглашению Сторон.

1. Комиссия создается на срок до 10 рабочих дней. В случае необходимости срок работы комиссии по согласованию Сторон может быть продлен до 30 рабочих дней.
2. Стороны обязуются оказывать содействие в работе комиссии
и не допускать отказа от представления необходимых документов, за исключением случаев, предусмотренных законодательством Российской Федерации.
3. Стороны обязуются предоставить комиссии возможность ознакомления с условиями и порядком работы своих программных
и аппаратных средств, используемых для обмена ЭС (ФС) (АРМ обмена).
4. Клиент (Пользователь) обязуется предоставлять членам комиссии доступ в помещение, где размещается АРМ обмена, для проведения проверок соблюдения Клиентом (Пользователем) настоящих Условий.
5. Работа комиссии проходит в два этапа.
	1. Первый этап – подготовительный.
		1. Комиссия устанавливает ПО СКЗИ, предоставленное
		Банком России, на СВТ с системным ПО, удовлетворяющим требованиям эксплуатационной документации на СКЗИ. Установленное ПО СКЗИ принимается для работы Комиссии.
		2. По запросу Комиссии ей передаются: необходимые сертификаты ключей Банка России и сертификат Клиента (Пользователя)
		с соответствующими регистрационными карточками, справочник сертификатов ключей с АРМ обмена Клиента (Пользователя), актуальный
		на момент обработки оспариваемого ЭС (ФС), и другие материалы.

Комиссия сравнивает сертификаты ключа Банка России и Клиента (Пользователя) с соответствующими регистрационными карточками.
При положительном результате сравнения сертификаты ключей используются в работе комиссии.

* 1. Второй этап – проверка и анализ спорных ЭС (ФС).
		1. Комиссией рассматриваются разногласия следующих типов:

Сторона-отправитель утверждает, что не направляла ЭС (ФС),
а Сторона-получатель утверждает, что ЭС (ФС) было получено;

Сторона-получатель утверждает, что не получала ЭС (ФС), а Сторона-отправитель утверждает, что ЭС (ФС) было направлено.

* + 1. Разрешение разногласий первого типа осуществляется
		в следующем порядке.

Сторона-получатель представляет ЭС (ФС), оспариваемое Стороной-отправителем.

Комиссия осуществляет проверку электронной подписи Стороны-отправителя с помощью принятого комиссией к использованию ПО СКЗИ.

На основе положительного результата проверки электронной подписи
в ЭС (ФС) комиссия подтверждает факт направления Стороной-отправителем ЭС (ФС) Стороне-получателю.

Если Сторона-отправитель настаивает на том, что данное ЭС (ФС)
она не отправляла, комиссия может дополнительно сделать вывод
о возможной компрометации ключа электронной подписи Стороны-отправителя.

На основе отрицательного результата проверки электронной подписи Стороны-отправителя по оспариваемому ЭС (ФС) комиссия подтверждает факт, что Сторона-отправитель не направляла ЭС (ФС) Стороне-получателю.

* + 1. Разрешение разногласий второго типа осуществляется
		в следующем порядке.

Сторона-отправитель представляет ЭС (ФС), полученное от Стороны-получателя, о результатах проверки электронной подписи в ЭС (ФС) Стороны-отправителя (независимо от того, с каким результатом (положительным или отрицательным) завершена проверка), что свидетельствует о получении ЭС (ФС) Стороной-получателем.

Комиссия осуществляет проверку электронной подписи в ЭС (ФС), предоставленном Стороной-отправителем, с помощью принятого комиссией
к использованию ПО СКЗИ.

На основе положительного результата проверки электронной подписи
в ЭС (ФС), представленном Стороной-отправителем, комиссия подтверждает факт того, что Сторона-получатель получила ЭС (ФС).

На основе отрицательного результата проверки электронной подписи
в ЭС (ФС), представленном Стороной-отправителем, или в случае непредставления ЭС (ФС) Стороной-отправителем комиссия подтверждает факт того, что Сторона-получатель не получала ЭС (ФС).

Комиссия не принимает к рассмотрению претензии по ЭС (ФС),
для которых Альбомом ЭС не предусмотрено получение подтверждения
о получении ЭС (ФС) от Стороны-получателя, снабженного электронной подписью Стороны-получателя.

1. По итогам работы комиссии составляется акт, содержащий:

описание фактических обстоятельств, послуживших основанием
для возникновения разногласий;

описание работ, проведенных членами комиссии;

вывод по результатам работы комиссии по оспариваемому ЭС (ФС),
в том числе о причинах возникновения инцидента, и его обоснование;

рекомендации по предотвращению возникновения инцидентов.

Акт составляется в двух экземплярах, подписывается всеми членами комиссии. Каждой из Сторон комиссия направляет по одному экземпляру акта для принятия итогового согласованного решения. Члены комиссии,
не согласные с мнением большинства, вправе изложить особое мнение, которое прикладывается к акту.

1. Если в течение двух рабочих дней на предложение Стороны-инициатора о создании комиссии ответ другой Стороны не был получен
или был получен отказ от участия в работе комиссии, или другая Сторона препятствовала работе комиссии, Сторона-инициатор вправе составить акт
в одностороннем порядке с указанием причины его составления. В акте приводится информация, указанная в пункте 10 настоящего приложения. Акт составляется в двух экземплярах, подписывается уполномоченными должностными лицами Стороны-инициатора. Один экземпляр акта направляется другой Стороне.
2. Акт комиссии является основанием для принятия Сторонами окончательного решения, которое должно быть подписано Сторонами не позднее 10 (десяти) рабочих дней после дня окончания работы комиссии.

Приложение 6

к Условиям по защите информации

Требования к использованию СКЗИ

1. Защита информации Клиентами (косвенными участниками Клиента, Пользователями) 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 09.02.2005 № 66
«Об утверждении Положения о разработке, производстве, реализации
и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», зарегистрированным Министерством юстиции Российской Федерации 03.03.2005 № 6382, 25.05.2010 № 17350,
и технической документацией на СКЗИ.
2. Для подписания электронных сообщений и обеспечения шифрования на прикладном уровне используются следующие СКЗИ: программный комплекс «Сигнатура-клиент» или программный комплекс «Сигнатура-клиент L», система криптографической защиты информации автоматизированных систем Банка России «Янтарь» или программный комплекс «Система криптографической защиты информации автоматизированных систем Банка России «Янтарь L». При подключении
к криптографической сети Транспортного шлюза Банка России для обмена платежными и финансовыми сообщениями используется специальное программное обеспечение (далее – ПО) СКЗИ «Клиент криптографического сервера доступа «DiSec-W» (СКЗИ DiSec-W), предназначенное
для организации защищенных VPN-туннелей, и ПО СКЗИ «Модуль генерации ключей МГК-3», предназначенное для генерации ключевой информации, используемой ПО СКЗИ DiSec-W.
3. Установка и настройка СКЗИ на АРМ обмена выполняются Клиентами (косвенными участниками Клиента, Пользователями) с учетом требований, изложенных в эксплуатационной документации на СКЗИ.
При каждом запуске АРМ обмена должен быть обеспечен контроль целостности установленного программного обеспечения СКЗИ.
4. Определяется порядок учета, хранения и использования ключевых носителей (ключевых идентификаторов Touch Memory, ключевых Smart-карт и других носителей ключевой информации), который должен полностью исключать возможность неконтролируемого доступа к ним.
5. Полномочия лиц, имеющих доступ к криптографическим ключам, должны быть определены распорядительным документом, подписанным руководителем (лицом, его замещающим) Клиента (косвенного участника Клиента, Пользователя) или должностным лицом, заключившим Договор
от имени Клиента (Пользователя).
6. Для хранения ключевых носителей с криптографическими ключами должны использоваться надежные металлические шкафы (сейфы). Хранение ключевых носителей допускается в одном металлическом шкафу (сейфе) с другими документами в отдельной упаковке, исключающей неконтролируемый доступ к ключевым носителям.
7. В течение рабочего дня вне времени составления, передачи
и приема ЭС или ФС, а также по окончании рабочего дня носители ключевой информации с криптографическими ключами помещаются в металлические шкафы (сейфы).
8. Не допускается:

снимать несанкционированные копии с носителей ключевой информации, оставлять ключевые носители без присмотра, в том числе
в считывателе АРМ обмена;

знакомить с содержанием носителей ключевой информации лиц,
к ней не допущенных, а также передавать им носители ключевой информации;

выводить криптографические ключи на устройство отображения (дисплей, монитор) электронно-вычислительной машины (ЭВМ)
или устройство печати (принтер);

устанавливать носители с криптографическими ключами
в считывающее устройство АРМ обмена, программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие ЭВМ;

записывать на носители ключевой информации постороннюю информацию.

Приложение 7

к Условиям по защите информации

Требования к формированию ЭС

и контролю реквизитов ЭС

1. Формирование ЭС и контроль реквизитов ЭС в информационной инфраструктуре Клиента должны осуществляться с учетом следующего.

1.1. Контур формирования ЭС и контур контроля реквизитов ЭС
в информационной инфраструктуре Клиента должны быть реализованы
с использованием разных рабочих мест, разных криптографических ключей
и с привлечением отдельных работников для каждого из контуров[[30]](#footnote-31).

1.2. Объекты информационной инфраструктуры контура формирования ЭС и контура контроля реквизитов ЭС в информационной инфраструктуре Клиента 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 Клиентов.

1.3. В контуре формирования ЭС на основе первичного документа
в бумажной или электронной форме, или входящего ЭС должны осуществляться:

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

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

подписание исходящего ЭС, предназначенного для направления
в платежную систему Банка России, электронной подписью, применяемой
в контуре формирования ЭС, при положительном результате контроля реквизитов, указанного в [абзаце третьем](http://scakonsultant.vip.cbr.ru/veda/static4018_00_50_402652/document_notes_inner.htm#p157) настоящего подпункта;

направление исходящего ЭС, предназначенного для направления
в платежную систему Банка России, в контур контроля реквизитов ЭС.

1.4. В контуре контроля реквизитов электронных сообщений должны осуществляться:

контроль реквизитов исходящего ЭС, 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 ЭС;

подписание исходящего ЭС, предназначенного для направления
в платежную систему Банка России, электронной подписью, применяемой
в контуре контроля реквизитов ЭС, при положительном результате контроля реквизитов, указанного в [абзаце втором](http://scakonsultant.vip.cbr.ru/veda/static4018_00_50_402652/document_notes_inner.htm#p161) настоящего подпункта.

Приложение 8

к Условиям по защите информации

Требования к формированию ФС

и контролю реквизитов ФС

1. В случае реализации подписания ФС в информационной инфраструктуре (автоматизированной системе) Пользователя Пользователи должны обеспечивать защиту ФС при их передаче в Банк России посредством формирования ФС и контроля реквизитов ФС в информационной инфраструктуре (автоматизированной системе) с учетом следующего:
	1. Контур формирования ФС и контур контроля реквизитов ФС
	в информационной инфраструктуре Пользователя должны быть реализованы с использованием разных рабочих мест и с привлечением отдельных работников для каждого из контуров.
	2. Объекты информационной инфраструктуры контура формирования ФС и контура контроля реквизитов ФС в информационной инфраструктуре Пользователя 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.
	3. В контуре формирования ФС на основе первичного документа
	в бумажной или электронной форме, или входящего ФС должны осуществляться:

формирование исходящего ФС, предназначенного для направления
в СПФС;

контроль реквизитов исходящего ФС, предназначенного
для направления в СПФС;

подписание исходящего ФС, предназначенного для направления
в СПФС, электронной подписью, применяемой в контуре формирования ФС, при положительном результате контроля реквизитов, предусмотренного предыдущим абзацем;

направление исходящего ФС, предназначенного для направления
в СПФС Банка России, в контур контроля реквизитов ФС.

* 1. В контуре контроля реквизитов ФС должны осуществляться:

контроль реквизитов исходящего ФС на соответствие реквизитам первичного документа в бумажной или электронной форме, или входящего ФС;

контроль на отсутствие дублирования исходящих ФС;

передача исходящего ФС при положительном результате контроля реквизитов, предусмотренного абзацем вторым настоящего подпункта,
на автоматизированное рабочее место обмена ФС.

1. Может осуществляться уполномочивание нескольких лиц. Копии документов о наделении соответствующими полномочиями предоставляются в Банк России. [↑](#footnote-ref-2)
2. Банк России может направлять информацию клиенту полевого учреждения Банка России через обслуживающее полевое учреждение Банка России. [↑](#footnote-ref-3)
3. Абзац 6 подпункта 2.3.8 пункта 2.3 настоящих Условий для клиентов полевых учреждений Банка России, которые не подключены к Транспортному шлюзу Банка России для обмена платежными и финансовыми сообщениями с Клиентами Банка России, и/или Клиентов Банка России, не являющихся кредитными организациями, вступает в силу с 01.01.2025. [↑](#footnote-ref-4)
4. Клиенты полевых учреждений Банка России могут направлять информацию в Банк России через обслуживающее полевое учреждение Банка России. [↑](#footnote-ref-5)
5. Способ представления информации указывается в запросе Банка России. [↑](#footnote-ref-6)
6. В случае реализации подписания ФС в информационной инфраструктуре (автоматизированной системе) Пользователя. [↑](#footnote-ref-7)
7. Абзац 6 подпункта 3.1.8 пункта 3.1 настоящих Условий для Пользователей, не являющихся кредитными организациями, вступает в силу с 01.01.2025. [↑](#footnote-ref-8)
8. Способ предоставления информации указывается в запросе Банка России. [↑](#footnote-ref-9)
9. Указывается наименование используемых АРМ обмена, СКЗИ. [↑](#footnote-ref-10)
10. Комиссия назначается соответствующим распорядительным документом Клиента, подписанным руководителем (лицом, его замещающим). [↑](#footnote-ref-11)
11. Все документы, подтверждающие выполнение указанных мер, представляются в виде электронного документа и скан-копий с утвержденного оригинала ). [↑](#footnote-ref-12)
12. Все документы, подтверждающие выполнение указанных мер, предоставляются в виде электронного документа и скан-копий с утвержденного оригинала (в составе приложения 5 к настоящему Акту). [↑](#footnote-ref-13)
13. Все документы, подтверждающие выполнение указанных мер, предоставляются в виде электронного документа и скан-копий с утвержденного оригинала (в составе приложения 5 к настоящему Акту). [↑](#footnote-ref-14)
14. Указывается наименование программных комплексов, используемых для АРМ обмена, наименование СКЗИ. [↑](#footnote-ref-15)
15. Акт содержит значения хеш-сумм модулей программного обеспечения СКЗИ, а также значение
хеш-суммы самой программы вычисления хеш-сумм. [↑](#footnote-ref-16)
16. Клиент обязан предоставлять в Банк России сведения о назначении и изменении состава лиц, указанных
в приложениях 2-4 к настоящему акту не позднее следующего рабочего дня после внесения изменений. [↑](#footnote-ref-17)
17. Перечень территориальных органов Федерального казначейства, которые осуществляют перевод денежных средств в платежной системе Банка России путем обмена ЭС через уполномоченный территориальный орган Федерального казначейства. Срок начала использования возможности централизованного обмена ЭС
для территориальных органов Федерального казначейства определяется правилами платежной системы
Банка России. [↑](#footnote-ref-18)
18. Клиенты должны размещать объекты информационной инфраструктуры, используемые при обмене ЭС,
в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей в соответствии
с подпунктом 2.3.1 пункта 2.3 Условий по защите информации. [↑](#footnote-ref-19)
19. Указывается наименование используемых АРМ обмена, СКЗИ. [↑](#footnote-ref-20)
20. Комиссия назначается соответствующим распорядительным документом Пользователя, подписанным руководителем (лицом, его замещающим). [↑](#footnote-ref-21)
21. Указывается наименование программных комплексов, используемых для АРМ обмена, наименование СКЗИ. [↑](#footnote-ref-22)
22. В случае реализации подписания ФС в информационной инфраструктуре (автоматизированной системе) Пользователя для приложений № 2-4 к настоящему акту также предоставляются сведения об АРМ контура формирования и АРМ контура контроля. [↑](#footnote-ref-23)
23. Акт содержит значения хеш-сумм модулей программного обеспечения СКЗИ, а также значение
хеш-суммы самой программы вычисления хеш-сумм. [↑](#footnote-ref-24)
24. Пользователь обязан предоставлять в Банк России сведения о назначении и изменении состава лиц, указанных в приложениях 2-4 к настоящему акту, не позднее следующего рабочего дня после внесения изменений. [↑](#footnote-ref-25)
25. Перечень территориальных органов Федерального казначейства, которые осуществляют перевод денежных средств в платежной системе Банка России путем обмена ЭС через уполномоченный территориальный орган Федерального казначейства. Срок начала использования возможности централизованного обмена ЭС
для территориальных органов Федерального казначейства определяется правилами платежной системы
Банка России. [↑](#footnote-ref-26)
26. Пользователи должны размещать объекты информационной инфраструктуры, используемые при обмене ФС, в выделенных (отдельных) сегментах (группах сегментов) вычислительных сетей в соответствии с подпунктом 3.1.1 пункта 3.1 Условий по защите информации. [↑](#footnote-ref-27)
27. Сведения о контуре формирования и контуре контроля заполняются в случае реализации подписания ФС в информационной инфраструктуре (автоматизированной системе) Пользователя в соответствии с Приложением 8 к Условиям по защите информации. [↑](#footnote-ref-28)
28. При наличии. [↑](#footnote-ref-29)
29. При наличии. [↑](#footnote-ref-30)
30. Для Клиентов, счета которых обслуживаются в полевом учреждении Банка России, не являющихся кредитными организациями и территориальными органами Федерального казначейства, не имеющих технической возможности выполнить требования подпункта 1.1 пункта 1 Приложения 7 к настоящим Условиям, по согласованию с Банком России, указанный подпункт вступает в силу с 01.01.2025. [↑](#footnote-ref-31)