ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

г. Москва

ОБ УСТАНОВЛЕНИИ ОБЯЗАТЕЛЬНЫХ ДЛЯ КРЕДИТНЫХ ОРГАНИЗАЦИЙ, ИНОСТРАННЫХ БАНКОВ, ОСУЩЕСТВЛЯЮЩИХ ДЕЯТЕЛЬНОСТЬ НА ТЕРРИТОРИИ РОССИЙСКОЙ ФЕДЕРАЦИИ ЧЕРЕЗ СВОИ ФИЛИАЛЫ, ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ В ЦЕЛЯХ ПРОТИВОДЕЙСТВИЯ ОСУЩЕСТВЛЕНИЮ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ БЕЗ СОГЛАСИЯ КЛИЕНТА

На основании статьи 57.4 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» настоящее Положение устанавливает обязательные для кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы, требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента.

1. Требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента применяются для обеспечения защиты

информации, подготавливаемой, обрабатываемой и хранимой в автоматизированных системах, входящих в состав объектов информационной инфраструктуры и используемых для осуществления банковских операций, связанных с осуществлением перевода денежных средств (далее соответственно - автоматизированные системы, защищаемая информация, осуществление банковских операций):

информации, содержащейся в документах, составленных при осуществлении банковских операций в электронном виде (далее - электронные сообщения), формируемых работниками кредитных организаций, иностранных банков, осуществляющих деятельность на территории Российской Федерации через свои филиалы (далее соответственно – филиалы иностранных банков, работники) и (или) клиентами кредитных организаций, филиалов иностранных банков (далее - клиенты), в том числе сведений, указанных в статье 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности» (далее – Федеральный закон «О банках и банковской деятельности»);

информации, необходимой для авторизации клиентов при совершении действий в целях осуществления банковских операций и удостоверения права клиентов распоряжаться денежными средствами;

информации об осуществленных банковских операциях;

информации, связанной с приемом к исполнению и исполнением распоряжений пользователя платформы цифрового рубля;

ключевой информации средств криптографической защиты информации (далее - СКЗИ), в том числе средств электронной подписи, используемой при осуществлении банковских операций (далее - криптографические ключи).

В случае если защищаемая информация содержит персональные данные, кредитные организации, филиалы иностранных банков должны применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее - Федеральный закон

«О персональных данных»).

2. Требования к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, включают в себя:

требования к обеспечению защиты информации при осуществлении банковской деятельности, применяемые в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечиваются кредитной организацией, филиалом иностранного банка для осуществления банковских операций (далее - объекты информационной инфраструктуры);

требования к обеспечению защиты информации при осуществлении банковской деятельности, применяемые в отношении прикладного программного обеспечения автоматизированных систем и приложений;

требования к обеспечению защиты информации при осуществлении банковской деятельности, применяемые в отношении технологии обработки защищаемой информации;

иные требования к обеспечению защиты информации при осуществлении банковской деятельности в соответствии с пунктами 6 - 9 настоящего Положения.

Кредитные организации, филиалы иностранных банков должны осуществлять деятельность по планированию, реализации, контролю и совершенствованию мер и мероприятий, направленных на реализацию требований, установленных абзацами третьим и четвертым настоящего пункта.

3. Кредитные организации, филиалы иностранных банков должны обеспечивать выполнение следующих требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, применяемых в отношении объектов информационной инфраструктуры.

3.1. Кредитные организации, филиалы иностранных банков должны обеспечить реализацию следующих уровней защиты информации для объектов информационной инфраструктуры, используемых для обработки, передачи, хранения защищаемой информации в целях осуществления банковских операций, определенных национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст[1] (далее – ГОСТ Р 57580.1-2017).

Системно значимые кредитные организации, кредитные организации, выполняющие функции оператора услуг платежной инфраструктуры системно значимых платежных систем, кредитные организации, значимые на рынке платежных услуг, должны реализовывать усиленный уровень защиты информации.

Кредитные организации, не относящиеся к кредитным организациям, указанным в абзаце втором настоящего подпункта, должны реализовывать стандартный уровень защиты информации.

Кредитные организации, 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 втором настоящего подпункта.

Филиалы иностранных банков должны реализовывать минимальный уровень защиты информации.

Филиалы иностранных банков должны реализовывать стандартный уровень защиты информации.

---

[1] М., ФГУП Стандартинформ, 2017.

В случае если в отношении объектов информационной инфраструктуры кредитной организации, совмещающей деятельность с деятельностью некредитной финансовой организации, оператора услуг информационного обмена, оператора услуг платежной инфраструктуры, оператора электронных платформ, и филиала иностранного банка действуют требования, установленные на основании статьи 76.4-1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (далее – Федеральный закон «О Центральном банке Российской Федерации (Банке России)»), части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – Федеральный закон «О национальной платежной системе»), и такая кредитная организация, филиал иностранного банка применяют один контур безопасности в соответствии с пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017 для реализации разных уровней защиты информации, тогда кредитная организация и филиал иностранного банка обязаны реализовать наиболее высокий уровень защиты информации.

3.2. Кредитные организации, филиалы иностранных банков должны обеспечить ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

4. Кредитные организации, филиалы иностранных банков должны обеспечивать выполнение следующих требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений.

4.1. Кредитные организации, филиалы иностранных банков должны обеспечить использование для осуществления банковских операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых кредитной организацией, филиалом иностранного банка клиентам для совершения действий в целях

осуществления банковских операций, а также программного обеспечения, обрабатывающего защищаемую информацию на участках, используемых для приема электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю (далее – сертификация) или оценку соответствия по требованиям к оценочному уровню доверия (далее - ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст [2] (далее – проведение оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения).

В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего подпункта, кредитные организации, филиалы иностранных банков должны самостоятельно определять необходимость сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

4.2. По решению кредитной организации, филиала иностранного банка оценка соответствия программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения проводится самостоятельно или с привлечением организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации для проведения работ и услуг, предусмотренных подпунктами

[2] М., ФГУП Стандартинформ, 2014.

«б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 (далее - проверяющая организация).

4.3. В случае принятия кредитной организацией решения о необходимости проведения сертификации программного обеспечения автоматизированных систем и приложений кредитные организации, являющиеся системно значимыми кредитными организациями, кредитными организациями, значимыми на рынке платежных услуг (в отношении программного обеспечения автоматизированных систем и приложений, указанных в пункте 1.2 Положения Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств»[3]), должны обеспечить сертификацию программного обеспечения автоматизированных систем и приложений не ниже 4 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76[4] (далее - приказ ФСТЭК России № 76).

Кредитные организации, филиалы иностранных банков, принявшие решение о необходимости проведения сертификации программного обеспечения автоматизированных систем и приложений и не указанные в абзаце первом настоящего подпункта, должны обеспечить сертификацию программного обеспечения автоматизированных систем и приложений не ниже 5 уровня доверия в соответствии с приказом ФСТЭК России № 76.

Кредитные организации, которые должны обеспечивать сертификацию программного обеспечения автоматизированных систем и приложений

---

[3] Зарегистрировано Министерством юстиции Российской Федерации 6 декабря 2023 года № 76286.

[4] Зарегистрирован Министерством юстиции Российской Федерации 11 сентября 2020 года № 59772.

не ниже 5 уровня доверия в соответствии с приказом ФСТЭК России № 76, ставшие кредитными организациями, которые должны обеспечивать сертификацию программного обеспечения автоматизированных систем и приложений не ниже 4 уровня доверия в соответствии с приказом ФСТЭК России № 76, должны обеспечить сертификацию программного обеспечения автоматизированных систем и приложений не ниже 4 уровня доверия в соответствии с приказом ФСТЭК России № 76 не позднее восемнадцати месяцев после того, как стали кредитными организациями, указанными в абзаце первом настоящего подпункта.

4.4. Кредитные организации, филиалы иностранных банков должны обеспечивать проведение оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения при каждом внесении изменений в исходный текст программного обеспечения и приложений, реализующий технологию обработки защищаемой информации в соответствии с пунктом 5.2 настоящего Положения.

5. Кредитные организации, филиалы иностранных банков должны обеспечивать выполнение следующих требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, применяемых в отношении технологии обработки защищаемой информации.

5.1. Кредитные организации, филиалы иностранных банков должны обеспечить целостность электронных сообщений.

В целях обеспечения целостности электронных сообщений кредитные организации и филиалы иностранных банков должны обеспечивать реализацию мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

При использовании усиленной электронной подписи в целях обеспечения

целостности электронных сообщений кредитные организации, филиалы иностранных банков должны обеспечить использование усиленной электронной подписи, созданной с использованием средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

При осуществлении операций с цифровыми рублями в целях обеспечения целостности электронных сообщений кредитные организации должны обеспечить применение усиленной неквалифицированной электронной подписи и СКЗИ, через использование которых реализуются двухсторонняя аутентификация и шифрование информации на прикладном уровне и на уровне представления в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель», принятого постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78 и введенного в действие 1 января 2000 года (далее – ГОСТ Р ИСО/МЭК 7498-1-99), в соответствии с требованиями нормативного акта Банка России, принятого на основании статьи 82.10 Федерального закона «О Центральном банке Российской Федерации (Банке России)», пункта 7 части 1, части 3 статьи 30.7 Федерального закона «О национальной платежной системе».

5.2. Кредитные организации, филиалы иностранных банков должны обеспечивать регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации, указанной в абзацах втором - пятом пункта 1 настоящего Положения, при совершении следующих действий (далее - технологические участки):

идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления банковских операций, в том числе

идентификация клиентов при создании сертификатов ключей проверки электронных подписей и выдаче таких сертификатов клиентам в соответствии с требованиями пункта 1 части 1 статьи 13 Федерального закона от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее - Федеральный закон «Об электронной подписи») в целях осуществления операций с цифровыми рублями;

формирование (подготовка), передача и прием электронных сообщений;

удостоверение права клиентов распоряжаться денежными средствами;

осуществление банковской операции, учет результатов ее осуществления;

хранение электронных сообщений и информации об осуществленных банковских операциях.

5.2.1. Технология обработки защищаемой информации, применяемая на всех технологических участках, указанных в настоящем пункте, должна обеспечивать целостность и достоверность защищаемой информации.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце втором подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать идентификацию устройств клиентов при осуществлении банковских операций с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций, филиалов иностранных банков.

В случае если банковская операция осуществляется с использованием мобильной версии приложения, кредитные организации в рамках реализуемой ими системы управления рисками должны обеспечить проверку использования клиентом - физическим лицом абонентского номера подвижной радиотелефонной связи в случае его использования во взаимоотношениях с кредитной организацией и использовать полученные сведения при анализе характера, параметров и объема совершаемых их клиентами операций (осуществляемой клиентами деятельности).

При использовании мобильной версии приложения кредитная организация, филиал иностранного банка должны обеспечивать контроль

изменения идентификационного модуля, предусмотренного подпунктом 3.2 пункта 3 статьи 2 Федерального закона от 7 июля 2003 года № 126-ФЗ «О связи», который используется в устройстве клиента, идентифицированном в соответствии с абзацем вторым настоящего пункта (далее – идентификационный модуль устройства клиента).

В случае выявления факта изменения идентификационного модуля устройства клиента кредитная организация, филиал иностранного банка не вправе осуществлять аутентификацию и авторизацию клиента с использованием абонентского номера подвижной радиотелефонной связи клиента или с использованием информационных систем третьих лиц, обеспечивающих аутентификацию и авторизацию физических лиц, доступ к которым может быть получен с использованием указанного абонентского номера подвижной радиотелефонной связи, до момента подтверждения принадлежности клиенту абонентского номера подвижной радиотелефонной связи способом, отличным от указанных в настоящем абзаце.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце третьем подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать:

двойной контроль посредством осуществления проверки правильности формирования (подготовки) электронных сообщений;

входной контроль посредством осуществления проверки правильности заполнения полей электронного сообщения и прав владельца электронной подписи;

контроль дублирования электронного сообщения (в случае если проведение такой процедуры дополнительно установлено кредитной организацией, филиалом иностранного банка с учетом положений пункта 2.2 Положения Банка России от 29 июня 2021 года № 762-П «О правилах осуществления перевода денежных средств»[5]);

---

[5] Зарегистрировано Министерством юстиции Российской Федерации 25 августа 2021 года № 64765 (с изменениями, внесенными Указанием Банка России от 25 марта 2022 года

структурный контроль электронных сообщений;

защиту при передаче по каналам связи защищаемой информации.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце четвертом подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать:

подписание клиентом электронных сообщений способом, указанным в подпункте 5.1 настоящего пункта;

получение от клиента подтверждения совершаемой банковской операции.

Технология обработки защищаемой информации, применяемая на технологическом участке, указанном в абзаце пятом подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать:

проверку соответствия (сверку) выходных электронных сообщений с соответствующими входными электронными сообщениями;

проверку соответствия (сверку) результатов осуществления банковских операций с информацией, содержащейся в электронных сообщениях;

направление клиентам уведомлений об осуществлении банковских операций в случае, когда такое уведомление предусмотрено законодательством Российской Федерации или договором.

Кредитные организации, филиалы иностранных банков должны реализовывать механизмы подтверждения использования клиентом адреса электронной почты в случае его использования во взаимоотношениях с кредитной организацией, филиалом иностранного банка, на который кредитной организацией, филиалом иностранного банка направляются уведомления о совершаемых банковских операциях, справки (выписки) по совершенным банковским операциям.

В случае использования единой системы идентификации и аутентификации, определенной в соответствии с пунктом 5 статьи 2

№ 6104-У, зарегистрированным Министерством юстиции Российской Федерации 25 апреля 2022 года № 68320, Указанием Банка России от 3 августа 2023 года № 6497-У, зарегистрированным Министерством юстиции Российской Федерации 10 августа 2023 года № 74717).

Федерального закона от 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее - единая система идентификации и аутентификации), кредитные организации, филиалы иностранных банков должны соблюдать требования к обеспечению защиты информации в соответствии с Техническими требованиями к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия, утвержденными приказом Министерства связи и массовых коммуникаций Российской Федерации от 23 июня 2015 года № 210 [6] , а также требования технической и эксплуатационной документации по подключению к единой системе идентификации и аутентификации.

5.2.2. Кредитные организации, филиалы иностранных банков должны обеспечивать регистрацию результатов выполнения действий, связанных с осуществлением доступа к защищаемой информации, на всех технологических участках, указанных в подпункте 5.2 настоящего пункта, которая включает регистрацию действий работников, а также регистрацию действий клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения.

5.2.3. Регистрации подлежат данные о действиях работников, выполняемых с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) осуществления банковской операции;

---

[6] зарегистрирован Министерством юстиции Российской Федерации 25 августа 2015 года, № 38668 (с изменениями, внесенными приказом Министерства связи и массовых коммуникаций Российской Федерации от 22 февраля 2017 года № 71, зарегистрированным Министерством юстиции Российской Федерации 2 июня 2017 года, регистрационный № 46934).

присвоенный работнику идентификатор, позволяющий установить работника в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат осуществления банковской операции (успешная или неуспешная);

идентификационная информация, используемая для адресации устройства, с использованием которого и в отношении которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора).

5.2.4. Регистрации подлежат данные о действиях клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) совершения действий клиентом в целях осуществления банковской операции;

присвоенный клиенту идентификатор, позволяющий установить клиента в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат совершения клиентом действия в целях осуществления банковской операции (успешная или неуспешная);

идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора), международный идентификатор абонента (индивидуальный номер абонента клиента - физического лица), международный идентификатор пользовательского оборудования (оконечного оборудования) клиента - физического лица, номер телефона и (или) иной идентификатор устройства).

Регистрации подлежат данные о действиях клиентов, выполняемых на технологическом участке идентификации, аутентификации и авторизации

клиентов при совершении действий в целях осуществления банковских операций с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) начала соединения и окончания соединения сессии транспортного уровня в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 государственного стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99, при авторизации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций;

идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (сетевой адрес и транспортный адрес (порт) компьютера и (или) коммуникационного устройства (маршрутизатора), предусмотренные разделом 11 государственного стандарта Российской Федерации ГОСТ Р ИСО 7498-3-97 «Информационная технология. Взаимосвязь открытых систем базовая эталонная модель. Часть 3. Присвоение имен и адресация», принятого постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 19 августа 1997 года № 286[7] и введенного в действие 1 июля 1998 года (далее - ГОСТ Р ИСО 7498-3-97);

идентификационная информация, используемая для адресации автоматизированной системы, программного обеспечения, к которым осуществлен доступ с целью осуществления банковских операций (сетевой адрес и транспортный адрес (порт) автоматизированной системы, используемой кредитной организацией, филиалом иностранного банка предусмотренные разделом 11 ГОСТ Р ИСО 7498-3-97);

---

[7] М., ИПК «Издательство стандартов», 1997.

геолокация устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления банковских операций (при наличии).

5.2.5. Кредитные организации, филиалы иностранных банков должны обеспечивать хранение:

информации, указанной в абзацах втором, четвертом пункта 1 настоящего Положения;

информации, указанной в подпунктах 5.2.3 и 5.2.4 настоящего пункта, пункте 8 настоящего Положения.

Кредитные организации, филиалы иностранных банков должны обеспечивать целостность и доступность информации, указанной в настоящем подпункте, не менее пяти лет начиная с даты ее формирования (поступления).

5.2.6. При направлении информации, необходимой для авторизации клиентов при совершении действий в целях осуществления банковских операций и удостоверения права клиентов распоряжаться денежными средствами, кредитные организации, филиалы иностранных банков должны убедиться в том, что за совершением банковской операции обращается то физическое лицо либо тот представитель, которые были идентифицированы в порядке, предусмотренном Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

5.3. Кредитные организации, филиалы иностранных банков должны подтвердить составление электронных сообщений уполномоченным на это лицом.

Кредитные организации, филиалы иностранных банков в целях подтверждения составления электронных сообщений уполномоченным на это лицом должны:

обеспечить использование электронной подписи в соответствии с Федеральным законом «Об электронной подписи»;

осуществлять признание электронных сообщений, подписанных

электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, в соответствии со статьей 6 Федерального закона «Об электронной подписи».

При использовании усиленной электронной подписи в целях подтверждения составления электронных сообщений уполномоченным на это лицом кредитные организации, филиалы иностранных банков должны обеспечить использование усиленной электронной подписи, созданной с использованием средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

6. Обеспечение защиты информации с помощью СКЗИ при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, осуществляется в соответствии с Федеральным законом «Об электронной подписи», Федеральным законом «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 [8] (далее - Положение ПКЗ-2005), приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 [9] и технической документацией на СКЗИ.

В случае наличия в технической документации на СКЗИ требований

---

[8] Зарегистрирован Министерством юстиции Российской Федерации 3 марта 2005 года № 6382 (с изменениями, внесенными приказом Федеральной службы безопасности Российской Федерации от 12 апреля 2010 года № 173, зарегистрированным Министерством юстиции Российской Федерации 25 мая 2010 года № 17350).

9 зарегистрирован Министерством юстиции Российской Федерации 18 августа 2014 года № 33620.

к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований, такая оценка должна проводиться в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности.

6.1. В случае если кредитная организация, филиал иностранного банка применяют СКЗИ российского производства, то СКЗИ должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

6.2. Криптографические ключи должны изготавливаться клиентом (самостоятельно) и (или) кредитной организацией.

6.3. Безопасность процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

7. Кредитные организации, филиалы иностранных банков должны обеспечивать формирование для клиентов рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код) в целях противодействия осуществлению переводов денежных средств без согласия клиента.

Кредитные организации, филиалы иностранных банков должны обеспечивать доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления банковских операций лицами, не обладающими правом их осуществления, и мерах по их снижению:

мерах по предотвращению несанкционированного доступа к защищаемой

информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом совершались действия в целях осуществления банковской операции;

мерах по контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления банковской операции, и своевременному обнаружению воздействия вредоносного кода.

7.1. В целях противодействия осуществлению переводов денежных средств без согласия клиента кредитные организации в случаях, предусмотренных договорами с клиентами, содержащими условия указанного в части 1 статьи 9 Федерального закона «О национальной платежной системе» договора об использовании электронного средства платежа (далее – договор об использовании электронного средства платежа), на основании их заявлений устанавливают в отношении операций, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций через информационно-телекоммуникационную сеть «Интернет», ограничения на осуществление операций клиентами либо ограничения максимальной суммы одной операции и (или) операций за определенный период времени. Ограничения по операциям могут быть установлены как на все операции клиентов, так и в разрезе видов (типов) операций.

7.2. Кредитные организации в рамках реализуемой ими системы управления рисками или на основании сведений, полученных от операторов услуг платежной инфраструктуры, и в порядке, предусмотренном договором об использовании электронного средства платежа, устанавливают ограничения по параметрам (на сумму одной операции, общую сумму, период времени) операций по приему наличных денежных средств с использованием преобразованных данных платежной карты (токенизированная (цифровая) платежная карта), посредством банкоматов или иных технических устройств.

7.3. Системно значимые кредитные организации, кредитные организации, значимые на рынке платежных услуг, должны обеспечить

возможность использования программ для электронных вычислительных машин, применяемых клиентами с использованием пользовательского оборудования (оконечного оборудования), имеющего в своем составе идентификационный модуль, для получения услуг банка, или посредством других способов дистанционного доступа к банковскому счету клиента, для приема в соответствии со статьей 30.1 Федерального закона «О банках и банковской деятельности» заявлений клиентов – физических лиц о каждом случае совершения операций без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием, а также обеспечить возможности формирования на основании указанного заявления справки (выписки) о каждой указанной выше операции, содержащей информацию, указанную в приложении 2, не позднее 18 месяцев после дня признания кредитной организации системно значимой, значимой на рынке платежных услуг.

Кредитные организации должны обеспечить возможность приема заявлений клиентов – физических лиц о каждом случае заключения договоров потребительского кредита (займа) и осуществления операций с использованием кредитных (заемных) денежных средств под влиянием обмана или при злоупотреблении доверием в порядке, установленном статьей 30.1 Федерального закона «О банках и банковской деятельности».

Кредитные организации должны обеспечить возможность приема заявлений физических лиц о случаях зачисления наличных денежных средств на банковские счета третьих лиц с применением токенизированных (цифровых) платежных карт посредством банкоматов или иных технических устройств, осуществленного под влиянием обмана или при злоупотреблении доверием в порядке, установленном статьей 30.1 Федерального закона «О банках и банковской деятельности».

Кредитные организации должны регистрировать заявления, указанные в абзацах первом - третьем подпункта 7.3 настоящего пункта, с указанием даты регистрации и регистрационного номера заявления, а также обеспечить

хранение заявлений в соответствии со сроками, установленными статьей 30.1 Федерального закона «О банках и банковской деятельности».

7.4. Кредитные организации в порядке, предусмотренном договором об использовании электронного средства платежа, должны уведомлять законных представителей (родителей, усыновителей или попечителя) несовершеннолетнего в возрасте от четырнадцати до восемнадцати лет об открытии несовершеннолетними в возрасте от четырнадцати до восемнадцати лет электронного средства платежа, о совершаемых несовершеннолетними в возрасте от четырнадцати до восемнадцати лет операциях с использованием электронного средства платежа на основании пункта 2 статьи 857 Гражданского кодекса Российской Федерации.

7.5. Кредитные организации должны осуществлять проверку наличия письменного согласия законных представителей (родителей, усыновителей или попечителя) несовершеннолетнего в возрасте от четырнадцати до восемнадцати лет, полученного в соответствии с пунктом 1 статьи 26 Гражданского кодекса Российской Федерации, при заключении с несовершеннолетними в возрасте от четырнадцати до восемнадцати лет договора потребительского кредита (займа), указанного в части первой статьи 3 Федерального закона от 21 декабря 2013 года № 353-ФЗ «О потребительском кредите (займе)».

8. Кредитные организации, филиалы иностранных банков к инцидентам защиты информации в значении, установленном в пункте 7.3 Положения Банка России от 8 апреля 2020 года № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе»[10] (далее соответственно - Положение Банка России от 8 апреля 2020 года № 716-П, инцидент защиты информации), должны относить события, которые привели или могут привести к осуществлению банковских операций

[10] Зарегистрировано Министерством юстиции Российской Федерации 3 июня 2020 года № 58577 (с изменениями, внесенными Указанием Банка России от 25 марта 2022 года № 6103-У, зарегистрированным Министерством юстиции Российской Федерации 30 августа 2022 года № 69846).

без согласия клиента, неоказанию услуг, связанных с осуществлением банковских операций, в том числе включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на официальном сайте Банка России в сети «Интернет» (далее - перечень типов инцидентов).

Кредитные организации устанавливают во внутренних документах порядок фиксации инцидентов защиты информации в базе событий в соответствии с пунктами 7.3 и 7.5 Положения Банка России от 8 апреля 2020 года № 716-П и информационного обмена со службой управления рисками, создаваемой в соответствии с пунктом 3.6 Указания Банка России от 15 апреля 2015 года № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы»[11].

Филиалы иностранных банков устанавливают во внутренних документах порядок фиксации инцидентов защиты информации.

Кредитные организации, филиалы иностранных банков должны обеспечивать регистрацию инцидентов защиты информации.

По каждому инциденту защиты информации кредитные организации, филиалы иностранных банков должны обеспечивать регистрацию:

защищаемой информации, обрабатываемой на технологическом участке (участках), на котором (которых) произошел несанкционированный доступ к защищаемой информации;

---

[11] Зарегистрировано Министерством юстиции Российской Федерации 26 мая 2015 года № 37388 (с изменениями, внесенными Указанием Банка России от 3 декабря 2015 года, зарегистрированным Министерством юстиции Российской Федерации 28 декабря 2015 года № 40325, Указанием Банка России от 16 ноября 2017 года № 4606-У, зарегистрированным Министерством юстиции Российской Федерации 7 декабря 2017 года № 49156, Указанием Банка России от 27 июня 2018 года, зарегистрированным Министерством юстиции Российской Федерации 5 сентября 2018 года № 52084, Указанием Банка России от 8 апреля 2020 года № 5431-У, зарегистрированным Министерством юстиции Российской Федерации 3 июня 2020 года № 58576, Указанием Банка России от 10 января 2023 гожа № 6356-У, зарегистрированным Министерством юстиции Российской Федерации 14 июня 2023 года № 73833, Указанием Банка России от 6 октября 2023 года № 6569-У, зарегистрированным Министерством юстиции Российской Федерации 25 декабря 2023 года № 76594).

результата реагирования на инцидент защиты информации, в том числе действий по возврату денежных средств или электронных денежных средств.

Кредитные организации, филиалы иностранных банков должны осуществлять информирование Банка России, в том числе на основании запросов Банка России:

о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, принятых мерах и проведенных мероприятиях по реагированию на выявленные кредитной организацией, филиалом иностранного банка или Банком России инциденты защиты информации, включенные в перечень типов инцидентов, а также о планируемых мероприятиях по раскрытию информации об инцидентах защиты информации, включая размещение информации на официальных сайтах в сети «Интернет», выпуск пресс-релизов и проведение пресс-конференций не позднее одного рабочего дня до дня проведения мероприятия;

о сайтах в сети «Интернет», которые используются кредитной организацией, филиалом иностранного банка для осуществления банковской деятельности, принадлежащих кредитной организации, филиалом иностранного банка и (или) администрируемых в ее интересах.

Информация о рекомендуемой форме предоставления кредитными организациями, филиалами иностранных банков Банку России сведений размещается на официальном сайте Банка России в сети «Интернет».

Кредитные организации, филиалы иностранных банков должны предоставлять в Банк России сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае возникновения технической невозможности взаимодействия кредитных организаций, филиалов иностранных банков с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России кредитные организации, филиалы иностранных банков должны предоставлять в Банк России сведения с использованием резервного способа взаимодействия.

Информация о технической инфраструктуре (автоматизированной системе) Банка России, резервном способе взаимодействия размещается на официальном сайте Банка России в сети «Интернет».

Предоставление сведений, указанных в абзаце девятом пункта 8 настоящего Положения, кредитными организациями, филиалами иностранных банков в Банк России осуществляется в сроки, установленные приложением 1 к настоящему Положению.

9. Кредитные организации, филиалы иностранных банков должны обеспечить проведение оценки соответствия уровню защиты информации, установленному в подпункте 3.1 пункта 3 настоящего Положения (далее - оценка соответствия защиты информации) и оценки выполнения требований к мерам защиты информации в отношении технологии безопасной обработки защищаемой информации и прикладного программного обеспечения автоматизированных систем и приложений с соблюдением следующих требований:

9.1. Оценка соответствия защиты информации должна осуществляться в соответствии с национальным стандартом Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст[12] (далее - ГОСТ Р 57580.2-2018).

Кредитные организации, филиалы иностранных банков должны обеспечивать хранение отчета, подготовленного проверяющей организацией по результатам оценки соответствия защиты информации, не менее пяти лет начиная с даты его выдачи проверяющей организацией.

9.2. Кредитные организации должны обеспечивать уровень соответствия, не ниже четвертого предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018 в соответствии с ГОСТ Р 57580.2-2018.

---

[12] М., ФГУП «Стандартинформ», 2018.

Филиалы иностранных банков должны обеспечивать уровень соответствия, не ниже третьего предусмотренного подпунктом «г» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

Кредитные организации, филиалы иностранных банков должны обеспечивать уровень соответствия, не ниже четвертого предусмотренного подпунктом «д» пункта 6.9 раздела 6 ГОСТ Р 57580.2-2018.

9.3. Оценка соответствия защиты информации должна осуществляться с привлечением проверяющих организаций.

9.4. Оценка соответствия защиты информации и оценка выполнения требований к мерам защиты информации в отношении технологии безопасной обработки защищаемой информации и прикладного программного обеспечения автоматизированных систем и приложений кредитными организациями, филиалами иностранных банков должна осуществляться не реже одного раза в два года.

9.5. Кредитные организации при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении видов оценки соответствия, указанных в пунктах 4.3 и 5.3 порядка составления и представления отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации», установленного Указанием Банка России от 10.04.2023 № 6406-У «О формах, сроках, порядке составления и представления отчетности кредитных организаций (банковских групп) в Центральный банк Российской Федерации, а также о перечне информации о деятельности кредитных организаций (банковских групп)»[13].

---

[13] Зарегистрировано Министерством юстиции Российской Федерации 16 августа 2023 года № 74823 (с изменениями, внесенными Указанием Банка России от 8 декабря 2023 года

10. Настоящее Положение не распространяется на отношения, регулируемые Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

При обеспечении безопасности автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечиваются кредитными организациями, филиалами иностранных банков являющихся объектами критической информационной инфраструктуры Российской Федерации, настоящее Положение применяется наряду с требованиями Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

11. Настоящее Положение в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от _____ года № ___) вступает в силу по истечении 10 дней после дня его официального опубликования, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления их в силу.

Абзац третий пункта 5.1, абзацы седьмой – одиннадцатый подпункта 5.2.4 пункта 5.2, абзац пятый пункта 5.3, пункт 7.3 настоящего Положения вступают в силу с 1 октября 2025 года.

Абзац шестой пункта 3.1, абзац третий пункта 9.2 вступают в силу с 1 января 2027 года.

Абзац пятый пункта 3.1, абзацы первый, второй пункта 9.2 действуют по 31 декабря 2026 года.

12. Со дня вступления в силу настоящего Положения признать утратившим силу:

№ 6621-У, зарегистрированным Министерством юстиции Российской Федерации 22 января 2024 года № 76927, Указанием Банка России от 13 марта 2024 года, зарегистрированным Министерством юстиции Российской Федерации 29 мая 2024 года № 78345).

Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», зарегистрированное Министерством юстиции Российской Федерации 16 мая 2019 года № 54637;

Указание Банка России от 18 февраля 2022 года № 6071-У «О внесении изменений в Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», зарегистрированное в Министерством юстиции Российской Федерации 20 июня 2022 года № 68919;

Указание Банка России от 6 декабря .2023 № 6620-У «О внесении изменений в Положение Банка России от 17 апреля 2019 года N 683-П», зарегистрированное в Министерством юстиции Российской Федерации 22 декабря 2023 года № 76546.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение 1
к Положению Банка России
от __ ____ ____ года № ____
«Об установлении обязательных
для кредитных организаций, иностранных
банков, осуществляющих деятельность
на территории Российской Федерации
через свои филиалы, требований
к обеспечению защиты информации
при осуществлении банковской
деятельности в целях противодействия
осуществлению переводов денежных
средств без согласия клиента»

Сроки предоставления кредитными организациями, филиалами иностранных банков Банку России сведений о выявленных инцидентах защиты информации, о принятых мерах и проведенных мероприятиях по реагированию на выявленный инцидент защиты информации

Вид сведений	Срок предоставления
1	2
Сведения о выявлении инцидента защиты информации	В течение 3 часов с момента выявления инцидента защиты информации
Сведения о выявлении незаконного раскрытия банковской тайны и (или) защищаемой информации, указанной в пункте 1 настоящего Положения	
Сведения о результатах расследования инцидента защиты информации или незаконного раскрытия банковской тайны и (или) защищаемой информации, указанной в пункте 1 настоящего Положения	В течение 30 дней с момента направления в Банк России формы представления данных о выявлении инцидента защиты информации или незаконного раскрытия банковской тайны и (или) защищаемой информации, указанной в пункте 1 настоящего Положения
Сведения о компьютерных инцидентах (в соответствии с частью 5 статьи 2 Федерального закона от 26.07.2017 № 187-	В течение 3 часов с момента выявления компьютерного инцидента в случае его связи с функционированием значимого

ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»)	объекта критической информационной инфраструктуры. В течение 24 часов с момента выявления компьютерного инцидента во всех иных случаях

Приложение 2
к Положению Банка России
от __ _____ ___ года № ___
«Об установлении обязательных
для кредитных организаций, иностранных
банков, осуществляющих деятельность
на территории Российской Федерации
через свои филиалы, требований
к обеспечению защиты информации
при осуществлении банковской
деятельности в целях противодействия
осуществлению переводов денежных
средств без согласия клиента»

Перечень информации для формирования справки (выписки) о случаях совершения операций без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием,

1. Наименование кредитной организации;

2. Информация о заявителе (плательщике):

2.1. Фамилия, имя, отчество (при наличии), дата рождения, реквизиты документа удостоверяющего личность;

2.2. Информация об идентификаторах операции и (или) способе ее проведения:

2.2.1. Платежная карта:

2.2.1.1. Номер платежной карты;

2.2.1.2. Наименование кредитной организации, выпустившей платежную карту;

2.2.2. Банковский счет:

2.2.2.1. Банковский идентификационный код (далее - БИК) кредитной организации;

2.2.2.2. Номер банковского счета;

2.2.2.3. Наименование кредитной организации, в которой открыт банковский счет;

2.2.3. Электронное средства платежа (за исключением предоплаченных карт), использованное в системах (средствах) дистанционного обслуживания

в целях совершения операций с электронными денежными средствами (далее – электронный кошелек):

2.2.3.1. Номер электронного кошелька;

2.2.3.2. Наименование платежной системы;

2.2.4. Сервис быстрых платежей платежной системы Банка России:

2.2.4.1. БИК кредитной организации;

2.2.4.2. Абонентский номер подвижной радиотелефонной связи;

2.2.5. Банкомат или иное техническое устройство:

2.2.5.1. Наименование кредитной организации, обслуживающей банкомат или иное техническое устройство;

2.2.5.2. Номер банкомата или иного технического устройства;

2.2.5.3. Адрес нахождения банкомата или иного технического устройства;

3. Информация о получателе средств:

3.1. Наименование организации, идентификационный номер налогоплательщика (далее – ИНН) для юридического лица;

3.2. Информация об идентификаторах операции и (или) способе ее проведения:

3.2.1. Платежная карта;

3.2.1.1. Номер платежной карты (в формате, установленном правилами платежной системы, с учетом требований по защите номера платежной карты);

3.2.1.2. Наименование кредитной организации, выпустившей платежную карту;

3.2.2. Электронный кошелек;

3.2.2.1. Номер электронного кошелька;

3.2.2.2. Наименование платежной системы;

3.2.3. Сервис быстрых платежей платежной системы Банка России (в случае осуществления переводов денежных средств между физическими лицами):

3.2.3.1. Абонентский номер подвижной радиотелефонной связи;

3.2.4. Банковский счет:

3.2.4.1. БИК кредитной организации;

3.2.4.2. Номер банковского счета;

3.2.4.3. Наименование кредитной организации, в которой открыт банковский счет;

3.2.5. Сервис быстрых платежей платежной системы Банка России (в случае зачисления денежных средств на банковские счета получателя средств, являющегося торгово-сервисным предприятиям (далее – ТСП)):

3.2.5.1. Абонентский номер подвижной радиотелефонной связи;

3.2.5.2. ИНН ТСП;

3.2.5.3. Идентификатор ТСП;

3.2.5.4. БИК кредитной организации;

3.2.5.5. Номер банковского счета, открытого в кредитной организации.

3.2.5.6. Наименование банка-получателя денежных средств.

3.2.5.7. Номер операции в Сервисе быстрых платежей платежной системы Банка России.

3.2.6. Зачисление денежных средств на банковские счета получателя средств, являющегося ТСП;

3.2.6.1. банковский идентификационный номер (далее – БИН) участника платежной системы, обслуживающего получателя средств, являющегося ТСП;

3.2.6.2. ИНН ТСП;

3.2.6.3. Идентификатор ТСП;

3.2.6.4. БИК кредитной организации;

3.2.6.5. Номер банковского счета, открытого в кредитной организации.

3.2.6.6. Наименование банка-получателя денежных средств.

3.2.7. Банкомат или иное техническое устройство;

3.2.7.1. Наименование кредитной организации, обслуживающей банкомат или иное техническое устройство;

3.2.7.2. Номер банкомата или иного технического устройства;

3.2.7.3. Адрес нахождения банкомата;

4. Сумма операции;
5. Валюта операции;
6. Дата и время операции (с указанием часовой зоны (часового пояса)).