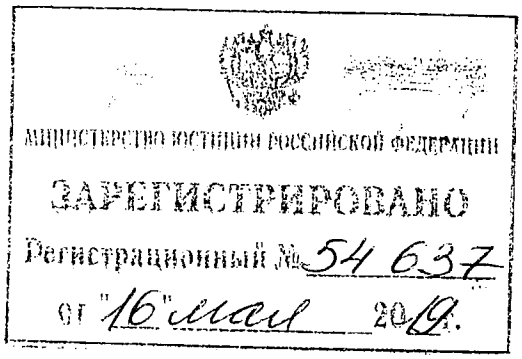
ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«17» апреля 2019 г. № 683-П

г. Москва



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

На основании статьи 57^4 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699; № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317; № 27, ст. 3634; № 30, ст. 4219; № 40, ст. 5318; № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, ст. 37; № 27, ст. 3958, ст. 4001; № 29,

ст. 4348, ст. 4357; № 41, ст. 5639; № 48, ст. 6699; 2016, № 1, ст. 23, ст. 46, ст. 50; № 26, ст. 3891; № 27, ст. 4225, ст. 4273, ст. 4295; 2017, № 1, ст. 46; № 14, ст. 1997; № 18, ст. 2661, ст. 2669; № 27, ст. 3950; № 30, ст. 4456; № 31, ст. 4830; № 50, ст. 7562; 2018, № 1, ст. 66; № 9, ст. 1286; № 11, ст. 1584, ст. 1588; № 18, ст. 2557; № 24, ст. 3400; № 27, ст. 3950; № 31, ст. 4852; № 32, ст. 5115; № 49, ст. 7524; № 53, ст. 8411, ст. 8440) настоящее Положение устанавливает обязательные для кредитных организаций 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 (далее – работники) и (или) клиентами кредитных организаций (далее – клиенты);

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;

ключевой информации средств криптографической защиты информации (далее – СКЗИ), используемой при осуществлении банковских операций

(далее – криптографические ключи).

В случае если защищаемая информация содержит персональные данные, кредитные организации 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» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, ст. 4196; № 49, ст. 6409; 2011, № 23, ст. 3263; № 31, ст. 4701; 2013, № 14, ст. 1651; № 30, ст. 4038; № 51, ст. 6683; 2014, № 23, ст. 2927; № 30, ст. 4217, ст. 4243; 2016, № 27, ст. 4164; 2017, № 9, ст. 1276; № 27, ст. 3945; № 31, ст. 4772; 2018, № 1, ст. 82) (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 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.

3. Кредитные организации 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 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 «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 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.

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

4. Кредитные организации 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 должны обеспечить использование для осуществления банковских операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых кредитной организацией 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»), сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, или в отношении которых проведен анализ уязвимостей 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 «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014).

В отношении прикладного программного обеспечения автоматизированных систем и приложений, не указанных в абзаце первом настоящего подпункта, кредитные организации должны самостоятельно определять необходимость сертификации или анализа уязвимостей и контроля отсутствия недекларированных возможностей.

4.2. Для проведения анализа уязвимостей в прикладном программном обеспечении автоматизированных систем и приложений кредитные организации должны привлекать организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «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 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049) (далее – постановление Правительства Российской Федерации № 79).

5. Кредитные организации 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 должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом.

Признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, должно осуществляться в соответствии со статьей 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ

«Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880; 2012, № 29, ст. 3988; 2013, № 14, ст. 1668; № 27, ст. 3463, ст. 3477; 2014, № 11, ст. 1098; № 26, ст. 3390; 2016, № 1, ст. 65; № 26 , ст. 3889) (далее – Федеральный закон «Об электронной подписи»).

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

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

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 третьем подпункта 5.2 настоящего пункта, дополнительно должна обеспечивать:

проверку правильности формирования (подготовки) электронных сообщений (двойной контроль);

проверку правильности заполнения полей электронного сообщения и прав владельца электронной подписи (входной контроль);

контроль дублирования электронного сообщения (в случае если проведение такой процедуры дополнительно установлено кредитной

организацией с учетом положений абзаца девятого пункта 2.1 Положения Банка России от 19 июня 2012 года № 383-П «О правилах осуществления перевода денежных средств», зарегистрированного Министерством юстиции Российской Федерации 22 июня 2012 года № 24667, 14 августа 2013 года № 29387, 19 мая 2014 года № 32323, 11 июня 2015 года № 37649, 27 января 2016 года № 40831, 31 июля 2017 года № 47578, 24 декабря 2018 года № 53109);

структурный контроль электронных сообщений;

защиту защищаемой информации при ее передаче по каналам связи.

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 совершенной 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.

5.2.2. Кредитные организации 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;

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).

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

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» (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257), 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, зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года № 6382, 25 мая 2010 года № 17350 (далее – Положение ПКЗ-2005), приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении Состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», зарегистрированным Министерством юстиции Российской Федерации 18 августа 2014 года № 33620, и технической документацией на СКЗИ.

В случае наличия в технической документации на СКЗИ требований 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 применяет 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 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 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.

8. Кредитные организации к инцидентам, связанным с нарушениями требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств (далее – инциденты защиты информации), должны относить события, которые привели или могут привести к осуществлению банковских операций 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 регистрации инцидентов защиты информации 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», зарегистрированного Министерством юстиции Российской Федерации 26 мая 2015 года № 37388, 28 декабря 2015 года № 40325, 7 декабря 2017 года № 49156, 5 сентября 2018 года

№ 52084. Сведения об инцидентах защиты информации направляются в службу управления рисками в целях включения их в аналитическую базу данных об убытках, понесенных вследствие реализации операционного риска, в порядке, установленном внутренними документами кредитной организации.

Кредитные организации должны обеспечивать регистрацию инцидентов защиты информации.

По каждому инциденту защиты информации кредитные организации должны обеспечивать регистрацию:

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

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

Кредитные организации должны осуществлять информирование Банка России:

о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов;

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.

Информация о рекомендуемых форме и сроке предоставления кредитными организациями Банку России сведений размещается на официальном сайте Банка России в сети «Интернет».

9. Кредитные организации должны обеспечить проведение оценки соответствия уровню защиты информации, установленному в подпункте 3.1 пункта 3 настоящего Положения (далее – оценка соответствия защиты информации), не реже одного раза в два года. Оценка соответствия защиты информации должна осуществляться с привлечением сторонних организаций, имеющих лицензию на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании

деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации № 79 (далее – проверяющая организация).

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 «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2018) (далее – ГОСТ Р 57580.2-2018).

Кредитные организации 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 обеспечить уровень соответствия не ниже третьего в соответствии с ГОСТ Р 57580.2-2018 с 1 января 2021 года.

Кредитные организации должны обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018 с 1 января 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» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736).

11. Настоящее Положение в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 21 декабря 2018 года № 39) 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.

Пункт 4 настоящего Положения вступает в силу с 1 января 2020 года.

Подпункт 3.1 пункта 3, пункт 9 настоящего Положения вступают в силу с 1 января 2021 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Согласовано

Директор
Федеральной службы безопасности
Российской Федерации А.В. Бортников

Директор
Федеральной службы по техническому
и экспортному контролю В.В. Селин