



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

У К А З А Н И Е

«18» мая 2019 г.

№ 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 защите информации при осуществлении
банковской деятельности в целях противодействия осуществлению
переводов денежных средств без согласия клиента»**

На основании статьи 57⁴ Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2018, № 27, ст. 3950):

1. Внести в Положение Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защите 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, следующие изменения:

1.1. В пункте 4:

в подпункте 4.1:

в абзаце первом слово «сообщений,» заменить словом «сообщений», слова «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» заменить словами «прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю или оценку соответствия»;

в абзаце втором слова «анализа уязвимостей и контроля отсутствия недекларированных возможностей» заменить словами «оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений»;

подпункт 4.2 изложить в следующей редакции:

«4.2. По решению кредитной организации оценка соответствия программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением организации, имеющей лицензию на осуществление деятельности по технической защите конфиденциальной информации для проведения 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 (Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049) (далее – проверяющая организация).»;

дополнить подпунктом 4.3 следующего содержания:

«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 4 июня 2020 года № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», зарегистрированного Министерством юстиции Российской Федерации 23 сентября 2020 года № 59991), 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, зарегистрированным Министерством юстиции Российской Федерации 11 сентября 2020 года № 59772 (далее – приказ ФСТЭК России № 76).

Кредитные организации, 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.».

1.2. В пункте 5:

подпункт 5.1 изложить в следующей редакции:

«5.1. Кредитные организации должны обеспечить целостность электронных сообщений и подтвердить их составление уполномоченным на это лицом.

В целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом кредитные организации должны обеспечивать реализацию мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

Указанные в абзаце втором настоящего подпункта требования по реализации мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения, не применяются в случае, если в целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом при передаче электронных сообщений используются выделенные контролируемые сегменты вычислительных сетей, доступ к которым нарушителем невозможен, и угрозы нарушения целостности электронных сообщений определены кредитными организациями как неактуальные, что обосновано в модели угроз и нарушителей безопасности информации.

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; 2019, № 52, ст. 7794) (далее – Федеральный закон «Об электронной подписи»).»;

подпункт 5.2.1 изложить в следующей редакции:

«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.

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).

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 с учетом положений пункта 2.2 Положения Банка России от 29 июня 2021 года № 762-П «О правилах осуществления перевода денежных средств», зарегистрированного Министерством юстиции Российской Федерации 25 августа 2021 года № 64765, 25 апреля 2022 года № 68320);

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 должны реализовывать механизмы подтверждения использования клиентом адреса электронной почты в случае его использования во взаимоотношениях с кредитной организацией, на который кредитной организацией направляются уведомления о совершаемых

банковских операциях, справки (выписки) по совершенным банковским операциям.».

1.3. Дополнить пунктом 7¹ следующего содержания:

«7¹. 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 от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872) договора 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 операций.».

1.4. В пункте 8:

в абзаце первом слова «, связанным с нарушениями требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств (далее – инциденты защиты информации)» заменить словами «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», зарегистрированного Министерством юстиции Российской Федерации 3 июня

2020 года № 58577 (далее соответственно – Положение Банка России от 8 апреля 2020 года № 716-П, инцидент защиты информации)»;

абзац второй изложить в следующей редакции:

«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», 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, 3 июня 2020 года № 58576.»;

абзацы седьмой – девятый изложить в следующей редакции:

«Кредитные организации 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 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 для осуществления банковской деятельности, принадлежащих кредитной организации и (или) администрируемых в ее интересах.»;

дополнить абзацем следующего содержания:

«Кредитные организации должны предоставлять в Банк России сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае возникновения технической невозможности взаимодействия кредитных организаций с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России кредитные организации 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»..».

1.5. Пункт 9 изложить в следующей редакции:

«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 проверяющих организаций.».

1.6. Пункт 10 дополнить абзацем следующего содержания:

«При обеспечении безопасности автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечиваются кредитными организациями, 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»..».

2. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 11 октября 2021 года № ПСД-24) вступает в силу с 1 октября 2022 года.

Председатель
Центрального банка
Российской Федерации

Э.С. Набиуллина

СОГЛАСОВАНО

Директор
Федеральной службы безопасности
Российской Федерации

А.В. Бортников

_____ 20 ____ г.

Директор
Федеральной службы по
техническому и экспортному
контролю

В.В. Селин

_____ 20 ____ г.