Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

У К А З А Н И Е

«___» _____ 2021 г. №_____ -У

г. Москва

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»

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; 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 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, следующие изменения.

1.1. В подпункте 4.1 пункта 4:

а) 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»;

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

1.2. Подпункт 4.2 пункта 4 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 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 – проверяющая организация).».

1.3. Дополнить пункт 4 подпунктом 4.3 следующего содержания:

«4.3. В случае принятия решения кредитной организацией о необходимости проведения сертификации программного обеспечения автоматизированных систем и приложений кредитные организации,

являющиеся системно значимыми кредитными организациями, кредитными организациями, значимыми на рынке платежных услуг, 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 «Об утверждении Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», зарегистрированным Министерством юстиции Российской Федерации 11 сентября 2020 года № 59772 (далее – приказ ФСТЭК России № 76).

Кредитные организации, 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.».

1.4. Подпункт 5.1 пункта 5 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 иных СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

Указанные в абзаце втором настоящего пункта требования по реализации мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или иных 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 сегменты вычислительных сетей и указанные меры определены кредитными организациями как неактуальные 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»).».

1.5. Подпункт 5.2.1 пункта 5 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 мобильных (переносных) устройств вычислительной техники кредитные организации в рамках реализуемой ими системы управления рисками должны обеспечить проверку используемого клиентом – физическим лицом абонентского номера подвижной радиотелефонной связи на основе анализа 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:

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 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 принадлежности клиенту адреса электронной почты, на который кредитной организацией направляются уведомления о совершаемых банковских операциях, справки (выписки) по совершенным банковским операциям.».

1.6. Подпункт 5.2.3 пункта 5 изложить в следующей редакции:

«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;

код банковской операции;

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).»

1.7. Подпункт 5.2.4 пункта 5 изложить в следующей редакции:

«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;

код банковской операции;

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).»

1.8. Дополнить пунктом 7^1 следующего содержания:

«7^1. Кредитные организации на основании заявлений клиентов, переданных способами, определенными договорами кредитных организаций с клиентами, должны установить ограничения по осуществлению операций клиентами либо максимальную сумму перевода денежных средств за одну операцию и (или) за определенный период времени, осуществляемых с использованием удаленного доступа клиентов к объектам информационной инфраструктуры кредитных организаций.»

1.9. В пункте 8:

абзац второй изложить в следующей редакции:

«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, 3 июня 2020 года № 58576 (далее – Указание Банка России от 15 апреля 2015 года № 3624-У). Сведения об инцидентах защиты информации направляются в службу управления рисками в целях включения их в соответствии с пунктом 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, в аналитическую базу данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в значении, установленном в пункте 4.3 приложения 1 к Указанию Банка России от 15 апреля 2015 года № 3624-У, в порядке, установленном внутренними документами кредитной организации.»;

абзацы седьмой – десятый 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;

о сайтах в сети «Интернет», которые используются кредитной организацией для осуществления банковской деятельности, принадлежащих кредитной организации и (или) администрируемых в ее интересах, в том числе путем предоставления сведений в отчетности, предусмотренной нормативными актами Банка России;

о принятых мерах и проведенных мероприятиях по реагированию на выявленный кредитной организацией или Банком России инцидент защиты информации, включенный 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 форме и сроке предоставления кредитными организациями Банку России сведений размещается на официальном сайте Банка России в сети «Интернет» (иной срок может быть указан в запросе Банка России).

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».».

1.10. В пункте 9 слова «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)» заменить словами «проверяющих организаций».

1.11. Пункт 10 изложить в следующей редакции:

«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) (далее – Федеральный закон № 187-ФЗ).

При обеспечении безопасности автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечивается кредитными организациями, являющихся объектами критической информационной инфраструктуры Российской Федерации, настоящее Положение применяется наряду с требованиями Федерального закона № 187-ФЗ.».

2. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от _____2021 года № ___) вступает в силу с 1 апреля 2022 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