ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«20» апреля 2021 г. № 757-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 63880
от "15" июня 2021 г.

Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций

Настоящее Положение на основании статьи 76^{4-1} 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) устанавливает обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью первой статьи 76^{1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2020, № 31, ст. 5018), в целях противодействия осуществлению незаконных финансовых операций.

Глава 1. **Общие требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков**

в целях противодействия осуществлению незаконных финансовых операций

1.1. Некредитные финансовые организации в целях противодействия осуществлению незаконных финансовых операций при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью первой статьи 76^1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», должны осуществлять защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в автоматизированных системах, используемых некредитными финансовыми организациями (далее соответственно – автоматизированные системы, защищаемая информация, защита информации):

информации, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками некредитных финансовых организаций и (или) клиентами некредитных финансовых организаций (далее – электронные сообщения);

информации, необходимой некредитным финансовым организациям для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;

информации об осуществленных некредитными финансовыми организациями и их клиентами финансовых операциях;

ключевой информации средств криптографической защиты информации, используемой некредитными финансовыми организациями и их клиентами при осуществлении финансовых операций (далее – криптографические ключи).

В случае если защищаемая информация содержит персональные данные, некредитные финансовые 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; 2021, № 1, ст. 54) (далее – Федеральный закон «О персональных данных»).

1.2. Обеспечение защиты информации с помощью средств криптографической защиты информации (далее – СКЗИ) некредитные финансовые организации должны осуществлять в соответствии с технической документацией на СКЗИ, а также следующими федеральными законами и нормативными правовыми актами Российской Федерации:

Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2021, № 9, ст. 1467) (далее – Федеральный закон «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);

приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», 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.

1.3. 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 некредитные финансовые организации должны проводить указанную оценку в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности.

В случае если некредитная финансовая организация применяет СКЗИ российского производства, СКЗИ должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

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.

1.4. Некредитные финансовые организации должны осуществлять защиту информации в отношении эксплуатируемых автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее при совместном упоминании – объекты информационной инфраструктуры) в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта Российской Федерации»

(М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017). ГОСТ Р 57580.1-2017 должен применяться по результатам определения некредитной финансовой организацией реализуемого в течение календарного года уровня защиты информации, предусмотренного ГОСТ Р 57580.1-2017 (далее – уровень защиты информации), с соблюдением следующих требований.

1.4.1. Определение уровня защиты информации должно осуществляться некредитной финансовой организацией ежегодно не позднее десятого рабочего дня календарного года определения уровня защиты информации (далее – дата определения уровня защиты информации).

1.4.2. Требования ГОСТ Р 57580.1-2017, соответствующие усиленному уровню защиты информации, должны соблюдать следующие некредитные финансовые организации (далее – некредитные финансовые организации, реализующие усиленный уровень защиты информации):

центральные контрагенты;

центральный депозитарий;

регистраторы финансовых транзакций.

1.4.3. Требования ГОСТ Р 57580.1-2017, соответствующие стандартному уровню защиты информации, должны соблюдать следующие некредитные финансовые организации (далее – некредитные финансовые организации, реализующие стандартный уровень защиты информации):

специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, размер активов которых, обслуживаемых по договорам об оказании услуг специализированного депозитария, составляет более одного триллиона рублей;

клиринговые организации;

организаторы торговли;

страховые организации, стоимость активов которых в течение последних шести календарных месяцев подряд по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, превышала двадцать миллиардов рублей;

негосударственные пенсионные фонды, осуществляющие деятельность по обязательному пенсионному страхованию;

негосударственные пенсионные фонды, осуществляющие деятельность по негосударственному пенсионному обеспечению, размер средств пенсионных резервов которых в течение последних шести календарных месяцев подряд по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, превышал десять миллиардов рублей;

репозитарии, не являющиеся регистраторами финансовых транзакций;

брокеры, дилеры, управляющие, депозитарии и регистраторы, определившие хотя бы по одному из показателей деятельности, указанных в графе 2 приложения к Положению Банка России от 27 июля 2015 года № 481-П «О лицензионных требованиях и условиях осуществления профессиональной деятельности на рынке ценных бумаг, ограничениях на совмещение отдельных видов профессиональной деятельности на рынке ценных бумаг, а также о порядке и сроках представления в Банк России отчетов о прекращении обязательств, связанных с осуществлением профессиональной деятельности на рынке ценных бумаг, в случае аннулирования лицензии профессионального участника рынка ценных бумаг», зарегистрированному Министерством юстиции Российской Федерации 25 августа 2015 года № 38673, 29 июля 2016 года № 43030, 20 октября 2017 года № 48630, 22 января 2019 года № 53485, 26 января 2021 года № 62231 (далее – Положение Банка России № 481-П), в качестве годового диапазона квартальный диапазон, указанный в графе 5 приложения к Положению Банка России № 481-П, по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации;

брокеры, дилеры, управляющие, депозитарии и регистраторы, указанные в абзаце десятом подпункта 2.1.11 пункта 2.1 Положения Банка России № 481-П;

операторы инвестиционной платформы, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате

определения уровня защиты информации, осуществляли оказание услуг более чем ста тысячам лиц, с которыми заключены договоры об оказании услуг по привлечению инвестиций и (или) договоры об оказании услуг по содействию в инвестировании;

операторы финансовой платформы, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли оказание услуг более чем ста тысячам лиц, с которыми заключены договоры об оказании услуг оператора финансовой платформы;

операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, осуществлявшие в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, оказание услуг более чем двадцати пяти тысячам лиц, с которыми заключены договоры об оказании услуг оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов;

операторы обмена цифровых финансовых активов, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли оказание услуг более чем двадцати пяти тысячам лиц, с которыми заключены договоры об оказании услуг оператора обмена цифровых финансовых активов.

1.4.4. Требования ГОСТ Р 57580.1-2017, соответствующие минимальному уровню защиты информации, должны соблюдать следующие некредитные финансовые организации (далее – некредитные финансовые организации, реализующие минимальный уровень защиты информации):

специализированные депозитарии инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, не указанные в подпункте 1.4.3 настоящего пункта;

брокеры, дилеры, управляющие, депозитарии и регистраторы, не указанные в подпункте 1.4.3 настоящего пункта;

управляющие компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов;

форекс-дилеры;

операторы финансовой платформы, не указанные в подпункте 1.4.3 настоящего пункта;

операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, не указанные в подпункте 1.4.3 настоящего пункта;

операторы обмена цифровых финансовых активов, не указанные в подпункте 1.4.3 настоящего пункта;

страховые организации, не указанные в подпункте 1.4.3 настоящего пункта;

общества взаимного страхования;

страховые брокеры;

лица, указанные в абзаце третьем пункта 5 статьи 6^1 Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации» (Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации, 1993, № 2, ст. 56; Собрание законодательства Российской Федерации, 1998, № 1, ст. 4; 2020, № 30, ст. 4738).

1.4.5. Некредитные финансовые организации, реализующие усиленный уровень защиты информации, и некредитные финансовые организации, реализующие стандартный уровень защиты информации (далее при совместном упоминании – некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации), должны осуществлять ежегодное тестирование объектов информационной инфраструктуры на предмет проникновений и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

В случае выявления уязвимостей информационной безопасности объектов информационной инфраструктуры некредитные финансовые

организации, реализующие усиленный и стандартный уровни защиты информации, должны устранять выявленные уязвимости в порядке и сроки, установленные в разрабатываемых такими некредитными финансовыми организациями документах, регламентирующих процедуры нейтрализации угроз безопасности информации.

1.5. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать проведение оценки соответствия определенного ими уровня защиты информации (далее – оценка соответствия уровня защиты информации) с соблюдением следующих требований.

1.5.1. Оценка соответствия уровня защиты информации должна осуществляться некредитными финансовыми организациями 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 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).

1.5.2. Оценка соответствия уровня защиты информации должна осуществляться некредитными финансовыми организациями с привлечением проверяющих организаций в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2018) (далее – ГОСТ Р 57580.2-2018).

1.5.3. Оценка соответствия уровня защиты информации некредитными финансовыми организациями, реализующими усиленный уровень защиты информации, должна осуществляться не реже одного раза в год, некредитными финансовыми организациями, реализующими стандартный уровень защиты информации, – не реже одного раза в три года.

1.6. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать хранение отчета, составленного проверяющей организацией по результатам оценки соответствия уровня защиты информации, в течение не менее чем пяти лет с даты его выдачи проверяющей организацией.

1.7. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить уровень соответствия не ниже третьего уровня соответствия, предусмотренного подпунктом «г» пункта 6.9 ГОСТ Р 57580.2-2018.

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить уровень соответствия не ниже четвертого уровня соответствия, предусмотренного подпунктом «д» пункта 6.9 ГОСТ Р 57580.2-2018.

1.8. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование для осуществления финансовых операций прикладного программного обеспечения автоматизированных систем и приложений, распространяемых некредитными финансовыми организациями своим клиентам для совершения действий в целях осуществления финансовых операций, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме 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 «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014) (далее – ГОСТ Р ИСО/МЭК 15408-3-2013) (далее – оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений).

Некредитные финансовые организации, не реализующие усиленный и стандартный уровни защиты информации, должны самостоятельно определять необходимость сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений.

В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего пункта, некредитные финансовые организации должны самостоятельно определять необходимость сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений.

По решению некредитной финансовой организации оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением проверяющей организации.

Некредитные финансовые организации, реализующие усиленный уровень защиты информации, в случае сертификации прикладного программного обеспечения автоматизированных систем и приложений должны обеспечить их сертификацию не ниже 4 уровня доверия в соответствии с Требованиями по безопасности информации,

устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными 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).

Некредитные финансовые организации, реализующие стандартный уровень защиты информации, в случае сертификации прикладного программного обеспечения автоматизированных систем и приложений должны обеспечить их сертификацию не ниже 5 уровня доверия в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом ФСТЭК России № 76.

1.9. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, 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 некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, 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 некредитными финансовыми организациями, реализующими усиленный и стандартный уровни защиты информации, 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 «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794).

1.10. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать регламентацию, реализацию, контроль (мониторинг) технологии безопасной обработки защищаемой информации, указанной в абзацах втором – четвертом пункта 1.1 настоящего Положения: при идентификации, аутентификации и авторизации своих клиентов в целях осуществления финансовых операций; при формировании (подготовке), передаче и приеме электронных сообщений; при удостоверении права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом; при осуществлении финансовой операции, учете результатов ее осуществления (при наличии учета); при хранении электронных сообщений и информации об осуществленных финансовых операциях (далее при совместном упоминании – технологические

участки) на основе анализа рисков с соблюдением следующих требований.

1.10.1. Технология обработки защищаемой информации, применяемая на технологических участках, должна обеспечивать целостность и неизменность защищаемой информации.

1.10.2. Технология обработки защищаемой информации, применяемая при идентификации, аутентификации и авторизации клиентов некредитных финансовых организаций в целях осуществления финансовых операций, должна обеспечивать выполнение следующих мероприятий:

в случае использования единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, – реализацию установленных приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», зарегистрированным Министерством юстиции Российской Федерации 14 мая 2013 года № 28375, 25 апреля 2017 года № 46487, 8 июля 2020 года № 58877, 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, технических и организационных мер в целях

нейтрализации угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации;

в случае использования единой системы идентификации и аутентификации – соблюдение требований к обеспечению защиты информации в соответствии 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 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия», зарегистрированным Министерством юстиции Российской Федерации 25 августа 2015 года № 38668, 2 июня 2017 года № 46934.

1.10.3. Технология обработки защищаемой информации, применяемая при формировании (подготовке), передаче и приеме электронных сообщений, должна обеспечивать выполнение следующих мероприятий:

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;

структурный контроль электронных сообщений;

защиту, в том числе криптографическую, защищаемой информации при ее передаче по каналам связи.

1.10.4. Технология обработки защищаемой информации, применяемая при удостоверении права клиентов некредитных финансовых организаций распоряжаться денежными средствами, ценными бумагами или иным имуществом, должна обеспечивать выполнение следующих мероприятий:

получение электронных сообщений клиента, подписанных им способом, указанным в пункте 1.9 настоящего Положения;

получение от клиента подтверждения совершаемой финансовой операции.

1.10.5. Технология обработки защищаемой информации, применяемая при осуществлении финансовой операции, учете результатов ее осуществления (при наличии учета), должна обеспечивать выполнение следующих мероприятий:

проверку соответствия (сверку) выходных электронных сообщений соответствующим входным электронным сообщениям;

проверку соответствия (сверку) результатов осуществления финансовых операций информации, содержащейся в электронных сообщениях;

направление клиентам некредитных финансовых организаций уведомлений об осуществлении финансовых операций в случае, когда такое уведомление предусмотрено законодательством Российской Федерации, регулирующим деятельность некредитных финансовых организаций, или договором.

Некредитные финансовые организации должны реализовывать механизмы подтверждения принадлежности клиенту адреса электронной почты, на который некредитной финансовой организацией направляются уведомления о совершаемых финансовых операциях, в том числе при предоставлении клиентам справок (выписок) по финансовым операциям.

1.11. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать регистрацию результатов выполнения действий, связанных с осуществлением доступа к защищаемой информации, на всех технологических участках, включая регистрацию действий своих работников и клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения, с соблюдением следующих требований.

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны регистрировать

следующую информацию о действиях своих работников и клиентов, выполняемых с использованием автоматизированных систем, программного обеспечения:

в отношении работника – дату (день, месяц, год) и время (часы, минуты, секунды) осуществления финансовой операции, в отношении клиента – совершение действий в целях осуществления финансовой операции;

присвоенный работнику (клиенту) идентификатор, позволяющий идентифицировать работника (клиента) в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

в отношении работника – результат осуществления финансовой операции, в отношении клиента – совершение действий в целях осуществления финансовой операции;

информацию, используемую для идентификации устройства, с применением которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления финансовых операций: сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора) работника (клиента), международный идентификатор абонента-клиента (индивидуальный номер абонента-клиента – физического лица), международный идентификатор пользовательского оборудования (оконечного оборудования) клиента – физического лица, номер телефона и (или) иной идентификатор устройства клиента.

1.12. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать:

хранение информации, указанной в абзацах втором и четвертом пункта 1.1 настоящего Положения, информации о регистрации данных, указанных в пункте 1.11 настоящего Положения, и информации об инцидентах, связанных с обеспечением защиты информации при осуществлении деятельности в сфере финансовых рынков (далее – инциденты защиты информации);

целостность и доступность информации, указанной в абзаце втором настоящего пункта, в течение не менее чем пяти лет с даты ее формирования некредитной финансовой организацией (даты поступления в некредитную финансовую организацию), а в случае, если законодательством Российской Федерации, регулирующим деятельность некредитных финансовых организаций, установлен иной срок, – в течение этого срока.

1.13. Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны обеспечивать доведение до своих клиентов рекомендаций по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код), в целях противодействия незаконным финансовым операциям.

Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны обеспечивать доведение до своих клиентов:

информации о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;

информации о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

1.14. Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны в соответствии со своими внутренними документами осуществлять регистрацию инцидентов защиты информации, а также представлять сведения о выявленных инцидентах защиты информации должностному лицу

(отдельному структурному подразделению), ответственному за управление рисками, при наличии такого должностного лица (отдельного структурного подразделения) при соблюдении следующих требований.

1.14.1. К инцидентам защиты информации некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны относить события, которые привели или по их оценке могут привести к осуществлению финансовых операций без согласия (волеизъявления) клиента некредитной финансовой организации, неоказанию услуг, связанных с осуществлением финансовых операций, в том числе события, включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на своем официальном сайте в сети «Интернет».

1.14.2. По каждому инциденту защиты информации некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны осуществлять регистрацию:

защищаемой информации на технологических участках, на которых произошел несанкционированный доступ к защищаемой информации;

результата реагирования на инцидент защиты информации, в том числе совершенных действий по возврату денежных средств, ценных бумаг или иного имущества клиента некредитной финансовой организации.

1.15. Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны информировать Банк России:

о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на своем официальном сайте в сети «Интернет», а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный некредитной финансовой организацией или Банком России

инцидент защиты информации;

о принадлежащих некредитной финансовой организации и (или) администрируемых в ее интересах сайтах в сети «Интернет», которые используются некредитной финансовой организацией для осуществления деятельности в сфере финансовых рынков;

о планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети «Интернет», в отношении инцидентов защиты информации не позднее одного рабочего дня до дня проведения мероприятия.

Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны предоставлять в Банк России сведения, указанные в абзацах втором – четвертом настоящего пункта, с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае технической невозможности взаимодействия некредитных финансовых организаций с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны предоставлять в Банк России сведения с использованием резервного способа взаимодействия. Информация о технической инфраструктуре (автоматизированной системе) Банка России, резервном способе взаимодействия, форме и сроках направления сведений размещается на официальном сайте Банка России в сети «Интернет».

Глава 2. **Особенности обеспечения защиты информации при осуществлении деятельности оператора финансовой платформы, регистратора финансовых транзакций**

2.1. Оператор финансовой платформы, регистратор финансовых транзакций дополнительно к информации, указанной в пункте 1.1 настоящего

Положения, должны осуществлять защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в используемых ими автоматизированных системах:

информации, обрабатываемой оператором финансовой платформы при совершении финансовых сделок с использованием финансовой платформы;

информации, обрабатываемой регистратором финансовых транзакций при осуществлении репозитарной деятельности в отношении финансовых сделок;

информации, содержащейся в электронных сообщениях, составляемых участниками финансовой платформы, оператором финансовой платформы и регистратором финансовых транзакций при заключении и исполнении финансовых сделок с использованием финансовой платформы, в том числе содержащейся в электронных сообщениях – указаниях потребителей финансовых услуг;

информации о размещенных с использованием финансовой платформы банковских вкладах и об операциях с денежными средствами по ним, информации о совершении иных финансовых сделок и об операциях по ним, предоставленной оператором финансовой платформы регистратору финансовых транзакций;

электронных сообщений, которые содержат распоряжения оператора финансовой платформы в кредитную организацию о совершении операций по специальному счету на основании указания потребителя финансовых услуг.

2.2. Оператор финансовой платформы, регистратор финансовых транзакций в дополнение к установленным пунктом 1.10 настоящего Положения требованиям к технологии обработки защищаемой информации должны обеспечивать выполнение следующих требований.

2.2.1. Технология обработки защищаемой информации, применяемая оператором финансовой платформы, регистратором финансовых транзакций, на всех технологических участках должна обеспечивать целостность и неизменность защищаемой информации, в том числе путем:

применения механизмов и (или) протоколов формирования и обмена электронными сообщениями, обеспечивающих защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе аутентификации входных электронных сообщений;

взаимной (двухсторонней) аутентификации участников обмена электронными сообщениями средствами вычислительной техники оператора финансовой платформы, потребителей финансовых услуг и финансовых организаций или эмитентов, регистраторов финансовых транзакций;

восстановления защищаемой информации в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

применения при взаимодействии между оператором финансовой платформы и регистратором финансовых транзакций, а также между оператором финансовой платформы и кредитными организациями СКЗИ, имеющих сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

2.2.2. Технология обработки защищаемой информации, применяемая оператором финансовой платформы при идентификации, аутентификации и авторизации в соответствии с подпунктом 1.10.2 пункта 1.10 настоящего Положения, должна распространяться на идентификацию потребителей финансовых услуг в соответствии с Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (Собрание законодательства Российской Федерации, 2001, № 33, ст. 3418; 2021, № 1, ст. 75) и аутентификацию участников финансовой платформы при заключении и исполнении финансовых сделок.

2.3. Оператор финансовой платформы, регистратор финансовых транзакций должны обеспечивать подписание электронных сообщений, в том

числе договоров между оператором финансовой платформы и потребителем финансовых услуг, соглашений об электронном документообороте между оператором финансовой платформы, потребителем финансовых услуг и финансовой организацией или эмитентом, а также иных документов, необходимых для обеспечения их взаимодействия при заключении и исполнении финансовых сделок с использованием финансовой платформы, способом, позволяющим обеспечить целостность подписываемых документов и подтвердить их составление уполномоченным на это лицом, в соответствии с требованиями пункта 1.9 настоящего Положения.

Глава 3. Особенности обеспечения защиты информации при осуществлении деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператора обмена цифровых финансовых активов

3.1. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов дополнительно к информации, указанной в пункте 1.1 настоящего Положения, должны осуществлять защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в используемых ими автоматизированных системах:

информации, обрабатываемой оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, на основании которой осуществляются выпуск и обращение цифровых финансовых активов, в том числе информации, содержащейся в электронных сообщениях – указаниях о внесении или изменении записи о цифровых финансовых активах в информационной системе, в которой осуществляется выпуск цифровых финансовых активов, по указанию лиц или в силу действия, совершенного в

рамках сделки, указанных в части 2 статьи 4 Федерального закона от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (Собрание законодательства Российской Федерации, 2020, № 31, ст. 5018) (далее – Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»);

информации, обрабатываемой оператором обмена цифровых финансовых активов, на основании которой обеспечивается заключение сделок с цифровыми финансовыми активами;

информации, обрабатываемой оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, обо всех совершенных сделках с цифровыми финансовыми активами, выпущенными в информационной системе, оператором которой он является, а также об участниках таких сделок;

информации, обрабатываемой оператором обмена цифровых финансовых активов при обеспечении заключения сделок с цифровыми финансовыми активами, обо всех совершенных сделках с цифровыми финансовыми активами, а также об участниках таких сделок.

3.2. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов в дополнение к установленным пунктом 1.10 настоящего Положения требованиям к технологии обработки защищаемой информации в рамках выпуска и обращения цифровых финансовых активов должны обеспечивать выполнение следующих мероприятий:

использование многофакторной аутентификации лиц, выпускающих цифровые финансовые активы, обладателей цифровых финансовых активов, оператора обмена цифровых финансовых активов при осуществлении доступа к информационной системе, в которой осуществляется выпуск цифровых

финансовых активов, в том числе реализованной с использованием СКЗИ;

защиту, в том числе криптографическую, защищаемой информации при ее хранении и передаче в информационной системе, в которой осуществляется выпуск цифровых финансовых активов;

применение организационных и технических мер, обеспечивающих обработку инцидентов защиты информации, связанных с несанкционированным доступом к криптографическим ключам при их формировании, использовании и хранении, в том числе в соответствии с требованиями технической документации на СКЗИ;

взаимную аутентификацию узлов информационной системы, участвующих в обмене защищаемой информацией;

реализацию системы управления жизненным циклом сделки, предусмотренной частью 2 статьи 4 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», и реализацию ее типовых функций в виде стандартных библиотек с целью управления рисками и уязвимостями, связанными с исполнением указанной сделки;

применение организационных и технических мер, направленных на обработку риска использования уязвимостей программной среды исполнения сделки, предусмотренной частью 2 статьи 4 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»;

реализацию системы мониторинга инцидентов защиты информации и регламентацию мер по реакции на инциденты защиты информации;

реализацию системы мониторинга исполнения сделок, предусмотренных частью 2 статьи 4 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».

3.3. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов в дополнение к установленным в пунктах 1.10 и 3.2 настоящего Положения требованиям к технологии обработки защищаемой информации в рамках выпуска и обращения цифровых финансовых активов в информационной системе на основе распределенного реестра должны обеспечивать выполнение следующих мероприятий:

анализ трафика сетевого взаимодействия между узлами информационной системы на основе распределенного реестра с целью обеспечения непрерывности внесения (изменения) записей в информационную систему на основе распределенного реестра, обеспечения блокировки потенциально опасных записей в информационную систему на основе распределенного реестра, способных привести к изменению последовательности записей в информационной системе, обеспечения анализа и контроля алгоритма (алгоритмов), обеспечивающего тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр, направленных на обеспечение невозможности реализации компьютерных атак, в том числе со стороны узлов информационной системы, путем управления указанными алгоритмами;

обеспечение защиты защищаемой информации между узлами информационной системы на основе распределенного реестра СКЗИ, реализующих в том числе функцию имитозащиты информации с аутентификацией отправителя информации;

использование узлами информационной системы безопасной топологии коммуникационных сетей, программного кода и протоколов с учетом актуальных угроз безопасности и применяемых информационных технологий, в том числе реализацию системы защиты от атак, направленных на отказ в обслуживании, с возможностью фильтрации передаваемых данных,

хранение узлами информационной системы доверенных сетевых адресов и реализацию механизма проверки некорректных узлов информационной системы.

Глава 4. **Заключительные положения**

4.1. В случае если некредитная финансовая организация на дату определения уровня защиты информации определила более высокий уровень защиты информации по сравнению с реализуемым ею уровнем защиты информации, такая некредитная финансовая организация должна обеспечить выполнение предусмотренных настоящим Положением требований к более высокому уровню защиты информации не позднее девяти месяцев с даты определения уровня защиты информации.

4.2. В случае совмещения некредитной финансовой организацией видов деятельности в сфере финансовых рынков, осуществление которых обусловливает необходимость реализации одновременно двух уровней защиты информации, такая некредитная финансовая организация должна обеспечить соблюдение требований, предъявляемых к более высокому уровню защиты информации, при условии, что при совмещении деятельности она использует единые объекты информационной инфраструктуры.

4.3. Действие настоящего Положения 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).

При обеспечении безопасности автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация и использование которых обеспечиваются при осуществлении финансовых операций

некредитными финансовыми организациями и которые являются 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».

Действие настоящего Положения не распространяется на лиц, осуществляющих актуарную деятельность.

4.4. Настоящее Положение в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 4 декабря 2020 года № ПСД-29) 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 четвертый подпункта 1.4.2, абзацы одиннадцатый – четырнадцатый подпункта 1.4.3 пункта 1.4, главы 2 и 3, за исключением абзаца четвертого пункта 3.3, настоящего Положения вступают в силу с 1 января 2022 года.

Подпункт 1.4.4 пункта 1.4 настоящего Положения вступает в силу с 1 июля 2022 года.

Абзац первый пункта 1.7 настоящего Положения вступает в силу с 1 января 2022 года и действует по 30 июня 2023 года включительно.

Абзац второй пункта 1.7 настоящего Положения вступает в силу с 1 июля 2023 года.

Абзац четвертый пункта 3.3 настоящего Положения вступает в силу с 1 января 2024 года.

4.5. Со дня вступления в силу настоящего Положения признать утратившим силу Положение Банка России от 17 апреля 2019 года № 684-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия

осуществлению незаконных финансовых операций», зарегистрированное Министерством юстиции Российской Федерации 16 мая 2019 года № 54634.

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