Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

« » _____ 20__ г. № -П

г. Москва

П О Л О Ж Е Н И Е

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

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; 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 некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью 1 статьи 76^1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», 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. В целях противодействия осуществлению незаконных финансовых операций при осуществлении деятельности в сфере финансовых рынков, предусмотренной частью 1 статьи 76^1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)», некредитные финансовые организации, 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 (далее – СКЗИ), 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; 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»).

1.2. Некредитные финансовые организации должны обеспечивать доведение до своих клиентов рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного

функционирования средства вычислительной техники (далее – вредоносный код), в целях противодействия незаконным финансовым операциям.

Некредитные финансовые организации должны обеспечивать доведение до своих клиентов следующей информации:

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

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.

1.3. Обеспечение защиты информации с помощью 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; № 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»);

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.

1.4. 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 указанная оценка должна проводиться 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.

1.5. Защита информации в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых осуществляется некредитными финансовыми организациями (далее при совместном упоминании – объекты информационной инфраструктуры), должна осуществляться некредитной финансовой организацией 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» (М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017). Требования ГОСТ Р 57580.1-2017 должны применяться по результатам определения некредитной финансовой организацией применимого к ней в течение календарного года уровня защиты информации, предусмотренного ГОСТ Р 57580.1-2017 (далее соответственно – уровень защиты информации, определение уровня защиты информации), с соблюдением следующих требований.

1.5.1. 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).

1.5.2. Требования ГОСТ Р 57580.1-2017, соответствующие усиленному уровню защиты информации, должны соблюдать:

центральные контрагенты;

центральный депозитарий;

регистраторы финансовых транзакций, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли оказание услуг более

чем 2 миллионам лиц, с которыми заключены договоры об оказании услуг регистратора финансовых транзакций (далее – некредитные финансовые организации, реализующие усиленный уровень защиты информации).

1.5.3. 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 на обслуживании по договорам об оказании услуг специализированного депозитария у которых составляет более 1 000 млн. руб.;

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 20 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 10 миллиардов рублей;

репозитарии, не являющиеся регистраторами финансовых транзакций;

брокеры, дилеры, управляющие, депозитарии и регистраторы, определившие хотя бы по одному из показателей деятельности, установленных в графе 2 приложения к Положению Банка России от 27.07.2015 № 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» (далее – Положение № 481-П), в качестве годового диапазона квартальный диапазон, указанный в графе 5 приложения к Положению № 481-П, по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации;

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 15 тысяч лиц, с которыми заключены договоры об оказании услуг по привлечению инвестиций и (или) договоры об оказании услуг по содействию в инвестировании оператора инвестиционной платформы;

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 10 тысяч лиц, с которыми заключены договоры об оказании услуг оператора финансовой платформы;

регистраторы финансовых транзакций, которые в течение трех последних кварталов по состоянию на 31 декабря года, предшествующего дате определения уровня защиты информации, осуществляли оказание услуг менее чем 2 миллионам лиц, с которыми заключены договоры об оказании услуг регистратора финансовых транзакций;

операторы информационных систем, в которых осуществляется выпуск 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 15 тысяч 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 15 тысяч лиц, с которыми заключены договоры об оказании услуг оператора обмена цифровых финансовых активов.

1.5.4. 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):

брокеры, дилеры и управляющие, не достигающие указанных в подпункте 1.5.3 настоящего пункта показателей;

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

форекс-дилеры;

операторы финансовой платформы, не достигающие указанных в подпункте 1.5.3 настоящего пункта показателей;

страховые организации, не достигающие указанных в подпункте 1.5.3 настоящего пункта показателей;

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 делав Российской Федерации» (Российская газета, 1993, 12 января, № 6; Собрание законодательства Российской Федерации, 2020, № 30, ст. 4738).

1.5.5. 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.

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны устранять выявленные уязвимости информационной безопасности объектов информационной инфраструктуры в случае их выявления в порядке и сроки, установленные в документах, регламентирующих процедуры нейтрализации информационных угроз.

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

1.6.1. Оценка определенного уровня 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 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).

1.6.2. Оценка определенного уровня защиты информации должна осуществляться 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).

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

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

1.8. 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.

1.9. 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 некредитной финансовой организацией 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 указанные в абзаце первом настоящего пункта, 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, должны обеспечить сертификацию прикладного

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).

Некредитные финансовые организации, реализующие усиленный уровень защиты информации, должны обеспечить сертификацию прикладного программного обеспечения автоматизированных систем и приложений не ниже 5 уровня доверия в соответствии с приказом ФСТЭК России № 76.

1.10. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом.

В целях обеспечения контроля целостности электронных сообщений некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать подписание электронных сообщений усиленной электронной подписью или использовать иные аналоги собственноручной подписи, коды, пароли и другие средства с применением дополнительных организационных и технологических мер защиты информации в соответствии с настоящим Положением.

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».

1.11. 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, в рамках идентификации, аутентификации и авторизации своих клиентов при совершении действий в целях осуществления финансовых операций, формировании (подготовке), передаче и приеме электронных сообщений, удостоверении права клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом, осуществлении финансовой операции, учете результатов ее осуществления, хранении электронных сообщений и информации об осуществленных финансовых операциях (далее при совместном упоминании – технологические участки) на основе анализа рисков с соблюдением следующих требований.

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

1.11.2. Технология обработки защищаемой информации, применяемая при идентификации, аутентификации и авторизации клиентов некредитных финансовых организаций при совершении действий в целях осуществления финансовых операций, должна обеспечивать следующие мероприятия:

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 в Приказе 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, Приказе 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 выполнение требований к обеспечению защиты информации в соответствии техническими требованиями к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия в соответствии с Приказом Министерства цифрового развития, 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.

1.11.3. Технология обработки защищаемой информации, применяемая при формировании (подготовке), передаче и приеме электронных сообщений, должна обеспечивать следующие мероприятия:

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 защищаемой информации при ее передаче по каналам связи.

1.11.4. 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 клиентом способом, указанным в пункте 1.10 настоящего Положения;

получение от клиента подтверждения совершаемой финансовой операции.

1.11.5. 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.

1.12. 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:

дату (день, месяц, год) и время (часы, минуты, секунды) осуществления финансовой операции, а для клиентов – совершение действий в целях осуществления финансовой операции;

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

код, соответствующий технологическому участку;

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

идентификационную информацию, используемую для идентификации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления финансовых операций: для работников (клиентов) – сетевой адрес компьютера и (или) коммуникационного устройства (маршрутизатора) работника (клиента); для клиентов – 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.

1.13. Некредитные финансовые организации должны осуществлять регистрацию инцидентов, связанных с обеспечением защиты информации при осуществлении деятельности в сфере финансовых рынков (далее – инциденты защиты информации), а также представлять сведения о выявленных инцидентах защиты информации должностному лицу (отдельному структурному подразделению), ответственному за управление рисками, при наличии указанного должностного лица (отдельного структурного подразделения) в соответствии с внутренними документами указанных некредитных финансовых организаций при соблюдении следующих требований.

1.13.1. Некредитные финансовые организации к инцидентам защиты информации должны относить события, которые привели или могут по оценке указанных некредитных финансовых организаций 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» (далее – перечень типов инцидентов).

1.13.2. По каждому инциденту защиты информации некредитные финансовые организации должны осуществлять регистрацию следующей информации:

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 и иного имущества клиента некредитной финансовой организации.

1.14. 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 1.12 настоящего Положения, и информации об инцидентах защиты информации;

целостность и доступность информации, указанной в абзаце первом 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 – на срок, установленный законодательством Российской Федерации, регулирующим деятельность некредитных финансовых организаций.

1.15. Некредитные финансовые организации должны информировать Банк России:

о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный некредитной финансовой организацией или Банком России инцидент защиты информации;

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

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 должны предоставлять сведения, указанные в абзаце втором настоящего пункта по запросу Банка России при выявлении Банком России инцидентов защиты информации, включенных в перечень типов инцидентов.

Некредитные финансовые организации должны предоставлять в Банк России сведения, указанные в настоящем пункте, с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае возникновения технической невозможности взаимодействия некредитных финансовых организаций с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России некредитные финансовые организации 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. В состав требований к обеспечению защиты информации при осуществлении деятельности оператора финансовой платформы, регистратора финансовых транзакций включаются следующие требования.

2.2. 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:

информация, обрабатываемая оператором финансовой платформы при совершении финансовых сделок с использованием финансовых платформ;

информация, обрабатываемая регистратором финансовых транзакций при осуществлении репозитарной деятельности в отношении финансовых сделок;

информация, содержащаяся в электронных сообщениях, составляемых

потребителем финансовых услуг, оператором финансовой платформы и регистратором финансовых транзакций при заключении и исполнении финансовых сделок с использованием финансовой платформы, в том числе содержащаяся в электронных сообщениях - указаниях потребителей финансовых услуг при совершении финансовых сделок с использованием финансовых платформ;

информация обо всех совершенных с использованием финансовых платформ финансовых сделках, о расчетах по финансовым сделкам, предоставленная оператором финансовой платформы регистратору финансовых транзакций;

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

2.3. В дополнение к мерам технологии обработки защищаемой информации, указанным в пункте 1.11 настоящего Положения, операторы финансовой платформы, регистраторы финансовых транзакций должны обеспечивать реализацию следующих мер.

2.3.1. Технология обработки защищаемой информации, применяемая оператором финансовой платформы при идентификации, аутентификации и авторизации в соответствии с подпунктом 1.11.2 пункта 1.11 настоящего Положения, должна распространяться на деятельность по идентификации 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», и аутентификацию участников финансовой платформы при заключении и исполнении финансовых сделок.

2.3.2. 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.

2.4. 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 их целостность и подтвердить их составление уполномоченным на это лицом, реализуемым в соответствии с требованиями пункта 1.10 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. В состав требований к обеспечению защиты информации при осуществлении деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператора обмена цифровых финансовых активов включаются следующие требования.

3.2. 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:

информация, обрабатываемая оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, на основании которой осуществляется выпуск и обращение цифровых финансовых активов, в том числе информация, содержащаяся 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»);

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

информация, обрабатываемая оператором информационной системе, 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;

информация, обрабатываемая 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 сделок с цифровыми финансовыми активами.

3.3. В дополнение к мерам технологии обработки защищаемой информации, указанным в пункте 1.11 настоящего Положения, операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторы обмена цифровых финансовых активов должны обеспечивать реализацию следующих мер в рамках выпуска и обращения цифровых финансовых активов:

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;

защиту защищаемой информации при ее хранении 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 информации;

реализацию системы управления жизненным циклом сделки, указанной в части 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 сделки, указанной в части 2 статьи 4 Федерального закона «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»;

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

3.4. В дополнение к мерам технологии обработки защищаемой информации, указанным в пункте 1.11 настоящего Положения и пункте 3.3 настоящего Положения, операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторы обмена цифровых финансовых активов должны обеспечивать реализацию следующих мер в рамках выпуска и обращения цифровых финансовых активов в информационной системе на основе распределенного реестра:

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(ов), обеспечивающего(их) 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;

применение криптографических алгоритмов с учетом оценки их стойкости к актуальным угрозам безопасности информации для предотвращения атак, направленных на криптографические алгоритмы и протоколы;

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, не относящаяся к некредитным финансовым организациям, реализующим усиленный, стандартный и минимальный уровни защиты информации, выявила соответствие требованиям, указанным в пунктах 1.5.2, 1.5.3, 1.5.4 настоящего Положения, такая некредитная финансовая организация должна обеспечить соответствие требованиям, указанным в пунктах 1.5.2, 1.5.3 и 1.5.4 и пунктах 1.6–1.12, 1.14, 2.1 – 2.4, 3.1 – 3.4 настоящего Положения, в срок не позднее девяти месяцев со дня выявления соответствия требованиям, указанным в пунктах 1.5.2, 1.5.3, 1.5.4 настоящего Положения.

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. 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).

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

Абзац четвертый подпункта 1.5.2 пункта 1.5, абзацы десятый, одиннадцатый, двенадцатый, тринадцатый, четырнадцатый подпункта 1.5.3 пункта 1.5, абзацы третий, четвертый, пятый подпункта 1.5.4 пункта 1.5, пункты 2.1 – 2.4, пункты 3.1 – 3.4 настоящего Положения вступают в силу с 1 января 2022 года.

Подпункт 1.5.5 пункта 1.5, пункты 1.6, 1.7, 1.9-1.12, 1.14 настоящего Положения применяются к некредитным финансовым организациям, указанным в абзаце четвертом подпункта 1.5.2 пункта 1.5, абзаце десятом, одиннадцатом, двенадцатом, тринадцатом, четырнадцатом подпункта 1.5.3 пункта 1.5, подпункте 1.5.4 пункта 1.5 настоящего Положения, с 1 января 2022 года.

Абзац первый пункта 1.8 настоящего Положения вступает в силу с 1 января 2022 года и действует по 30 июня 2023 года включительно.

Абзац второй пункта 1.8 настоящего Положения вступает в силу с 1 июля 2023 года.

4.5. Настоящее Положение не распространяется на лиц, осуществляющих актуарную деятельность.

4.6. Со дня вступления в силу настоящего Положения признать утратившими 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