Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

« » _____ 20__ г. № _____-У

г. Москва

У К А З А Н И Е

О внесении изменений в Положение Банка России от 20 апреля 2021 года № 757-П

На основании статьи 76^{4-1} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»:

1. Внести в Положение Банка России от 20 апреля 2021 года № 757-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»[1] следующие изменения:

1.1. В пункте 1.1:

1.1.1. В абзаце первом после слов «Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» дополнить словами «(далее – Федеральный закон «О Центральном банке Российской Федерации (Банке России)»)».

1.1.2. Абзац второй после слов «при осуществлении финансовых операций» дополнить словами «, совершаемых в рамках деятельности, предусмотренной

[1] Зарегистрировано Минюстом России 15 июня 2021 года № 63880.

Федеральным законом от 22 апреля 1996 года № 39-ФЗ «О рынке ценных бумаг», Федеральным законом от 29 ноября 2001 года № 156-ФЗ «Об инвестиционных фондах», Федеральным законом от 7 февраля 2011 года № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте», Федеральным законом от 21 ноября 2011 года № 325-ФЗ «Об организованных торгах», Федеральным законом от 7 декабря 2011 года № 414-ФЗ «О центральном депозитарии», Законом Российской Федерации от 27 ноября 1992 года № 4015-1 «Об организации страхового дела в Российской Федерации», Федеральным законом от 7 мая 1998 года № 75-ФЗ «О негосударственных пенсионных фондах», Федеральным законом от 2 июля 2010 года № 151-ФЗ «О микрофинансовой деятельности и микрофинансовых организациях», Федеральным законом от 18 июля 2009 года № 190-ФЗ «О кредитной кооперации», Федеральным законом от 30 декабря 2004 года № 215-ФЗ «О жилищных накопительных кооперативах», Федеральном законом от 8 декабря 1995 года № 193-ФЗ «О сельскохозяйственной кооперации», Федеральным законом от 2 августа 2019 года № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации», Федеральным законом от 31 июля 2020 года № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», Федеральным законом от 19 июля 2007 года № 196-ФЗ «О ломбардах», Федеральным законом от 20 июля 2020 года № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы»,».

1.2. В пункте 1.2:

1.2.1. Абзацы четвертый – шестой изложить в следующей редакции:

«Федеральным законом от 29 декабря 2022 года № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» (далее – Федеральный закон от 29 декабря 2022 года

№ 572-ФЗ);

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)» [2];».

1.2.2. Дополнить абзацем седьмым следующего содержания:

«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» [3] (далее – приказ ФСБ России № 378).».

1.3. Абзац третий пункта 1.3 изложить в следующей редакции:

«Безопасность процессов изготовления, использования, хранения и уничтожения 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, используемые для изготовления криптографических ключей.».

1.4. В пункте 1.4:

1.4.1. В подпункте 1.4.3:

---

[2] Зарегистрирован Минюстом России 3 марта 2005 года № 6382, с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года № 173 (зарегистрирован Минюстом России 25 мая 2010 года № 17350).

[3] Зарегистрирован Минюстом России 18 августа 2014 года № 33620.

в абзаце пятом слова «, 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» исключить;

в абзаце шестом слова «, осуществляющие деятельность по обязательному пенсионному страхованию» исключить;

абзац седьмой считать утратившим силу;

в абзацах девятом, десятом слова «и регистраторы» исключить;

дополнить абзацами пятнадцатым - шестнадцатым следующего содержания:

«регистраторы;

депозитарии, осуществляющие расчеты по результатам сделок, совершенных на торгах организаторов торговли по соглашению с такими организаторами торговли и (или) с клиринговыми организациями, осуществляющими клиринг обязательств по таким сделкам.».

1.4.2. В подпункте 1.4.4:

в абзаце третий слова «и регистраторы» исключить;

абзац девятый считать утратившим силу;

дополнить абзацами тринадцатым – пятнадцатым следующего содержания:

«микрофинансовые организации (за исключением микрофинансовых организаций предпринимательского финансирования и микрофинансовых организаций, учредителем (акционером, участником) которых является Российская Федерация, субъект Российской Федерации, муниципальное образование);

микрофинансовые организации;

операторы инвестиционной платформы, не указанные в подпункте 1.4.3 настоящего пункта.».

1.4.3. Дополнить подпунктом 1.4.6 следующего содержания:

«1.4.6. Некредитные финансовые организации, совмещающие деятельность с деятельностью кредитной организации, иностранного банка, осуществляющего деятельность на территории Российской Федерации через свой филиал, оператора по переводу денежных средств, банковского платежного агента (субагента),

оператора услуг информационного обмена, поставщика платежных приложений, оператора платежных систем, оператора услуг платежной инфраструктуры, оператора электронных платформ и формирующие в отношении объектов информационной инфраструктуры один контур безопасности в соответствии с пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, должны применять меры защиты информации, посредством выполнения которых обеспечивается реализация наиболее высокого уровня защиты информации, установленного пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017, из предусмотренных настоящим пунктом и нормативными актами Банка России, устанавливающими на основании статьи 57.4 Федерального закона «О Центральном банке Российской Федерации (Банке России)» и части 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» требования к обеспечению защиты информации для некредитных финансовых организаций, операторов услуг информационного обмена, операторов услуг платежной инфраструктуры, операторов электронных платформ.».

1.5. В пункте 1.5:

1.5.1. В абзаце первом после слов «(далее – оценка соответствия уровня защиты информации)» дополнить словами «и оценки выполнения требований к обеспечению защиты информации, применяемых с использованием технологических мер защиты информации и применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений,».

1.5.2. Дополнить подпунктом 1.5.4 следующего содержания:

«1.5.4. Центральные контрагенты, центральный депозитарий, регистраторы финансовых транзакций, указанные в подпункте 1.4.2 пункта 1.4 настоящего Положения, а также некредитные финансовые организации, указанные в подпункте 1.4.3 пункта 1.4 настоящего Положения и совмещающие свою деятельность с деятельностью кредитных организаций, при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений должны осуществлять расчет показателей

оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении видов оценки соответствия, указанных в пунктах 4.3 и 5.3 порядка составления и представления отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации», установленной в приложении 1 к Указанию Банка России от 10 апреля 2023 года № 6406-У «О формах, сроках, порядке составления и представления отчетности кредитных организаций (банковских групп) в Центральный банк Российской Федерации, а также о перечне информации о деятельности кредитных организаций (банковских групп)»[4].

Профессиональные участники рынка ценных бумаг, не совмещающие свою деятельность с деятельностью кредитных организаций, организаторы торговли, клиринговые организации, указанные в подпункте 1.4.3 пункта 1.4 настоящего Положения, при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении видов оценки соответствия, указанных в пунктах 3.2 и 4.2 порядка и сроков составления отчетности по форме 0420433 «Сведения об оценке выполнения требований к обеспечению защиты информации профессиональными участниками рынка ценных бумаг, организаторами торговли, клиринговыми организациями», установленной в приложении 1 к Указанию Банка России от 30 сентября 2022 года № 6282-У «Об объеме, формах, сроках и порядке составления и представления в Банк России отчетности профессиональных

[4] Зарегистрировано Минюстом России 16 августа 2023 года № 74823 (с изменениями, внесенным Указанием Банка России от 8 декабря 2023 года № 6621-У, зарегистрированным Минюстом России 22 января 2024 года № 76927, Указанием Банка России от 12 марта 2024 года № 6688-У, зарегистрированным Минюстом России 29 мая 2024 года № 78345, Указанием Банка России от 10 июля 2024 года № 6800-У, зарегистрированным Минюстом России 25 октября 2024 года № 79916, Указанием Банка России от 4 сентября 2024 года № 6840-У, зарегистрированным Минюстом России 10 октября 2024 года № 79758, Указанием Банка России от 16 декабря 2024 года № 6961-У, зарегистрированным Минюстом России 19 декабря 2024 года № 80633).

участников рынка ценных бумаг, организаторов торговли и клиринговых организаций, а также другой информации»[5].

Негосударственные пенсионные фонды, указанные в подпункте 1.4.3 пункта 1.4 настоящего Положения, при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении видов оценки соответствия, указанных в пунктах 3 и 4.1 порядка и сроков составления отчетности по форме 0420266 «Сведения об оценке выполнения требований к обеспечению защиты информации негосударственным пенсионным фондом», установленной в приложении 1 к Указанию Банка России от 28 июня 2024 года № 6796-У «О формах, сроках и порядке составления и представления в Банк России отчетности, в том числе о требованиях к отчетности по обязательному пенсионному страхованию, негосударственных пенсионных фондов, а также о порядке сообщения негосударственными пенсионными фондами Банку России информации о лицах, которым поручено проведение идентификации, упрощенной идентификации, обновление информации о клиентах, представителях клиентов, выгодоприобретателях и бенефициарных владельцах»[6].

Операторы инвестиционной платформы, операторы финансовой платформы, операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, не совмещающие свою деятельность с деятельностью кредитных организаций, операторы обмена цифровых финансовых активов, не совмещающие свою деятельность с деятельностью кредитных организаций, указанные в подпункте 1.4.3 пункта 1.4 настоящего Положения, при проведении

[5] Зарегистрировано Минюстом России 10 февраля 2023 года № 72319 (с изменениями, внесенными Указанием Банка России от 15 ноября 2023 года № 6606-У, зарегистрированным Минюстом России 21 декабря 2023 года № 76534, Указанием Банка России от 28 июня 2024 года № 6793-У, зарегистрированным Минюстом России 25 октября 2024 года № 79929).

[6] Зарегистрировано Минюстом России 31 октября 2024 года № 79989.

оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении видов оценки соответствия, указанных в пунктах 3 и 4.1 порядка составления отчетности по форме 0420722 «Сведения об оценке выполнения требований к обеспечению защиты информации оператором инвестиционной платформы, оператором финансовой платформы, оператором информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператором обмена цифровых финансовых активов», установленной в приложении 1 к Указанию Банка России от 10 июля 2024 года № 6798-У «О порядке и сроках составления и представления в Банк России отчетов операторов инвестиционных платформ, отчетности операторов финансовых платформ, операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и операторов обмена цифровых финансовых активов, форме отчетов операторов инвестиционных платформ и составе включаемых в них сведений, составе и формах отчетности операторов финансовых платформ, а также о порядке сообщения операторами инвестиционных платформ, операторами финансовых платформ, операторами информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторами обмена цифровых финансовых активов Банку России информации о лицах, которым поручено проведение идентификации, упрощенной идентификации, обновление информации о клиентах, представителях клиентов, выгодоприобретателях и бенефициарных владельцах»[7].

Страховые организации, указанные в подпункте 1.4.3 пункта 1.4 настоящего Положения, при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного

[7] Зарегистрировано Минюстом России 2 ноября 2024 года № 80008.

обеспечения автоматизированных систем и приложений должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении видов оценки соответствия, указанных в пунктах 3 и 4.1 порядка и сроков составления отчетности по форме 0420175 «Сведения об оценке выполнения требований к обеспечению защиты информации страховой организацией», установленной в приложении 1 к Указанию Банка России от 15 июля 2024 года № 6805-У «О формах, сроках и порядке составления и представления в Банк России отчетности страховщиков»[8].».

1.6. В пункте 1.8:

1.6.1. В абзаце первом слова «(далее – оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений)» заменить словами «(далее – проведение оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения)».

1.6.2. В абзацах втором, третьем после слов «определять необходимость сертификации или» дополнить словом «проведения», после слов «автоматизированных систем и приложений» дополнить словами «, а также отдельного программного обеспечения».

1.6.3. В абзацах четвертом, пятом, шестом после слов «прикладного программного обеспечения автоматизированных систем и приложений» дополнить словами «, а также отдельного программного обеспечения,».

1.6.4. Дополнить абзацами седьмым − девятым следующего содержания:

«Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать проведение оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения при каждом внесении изменений в исходный текст программного обеспечения и приложений,

[8] Зарегистрировано Минюстом России 8 ноября 2024 года № 80089.

реализующий технологию обработки защищаемой информации в соответствии с пунктом 1.10 настоящего Положения.

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, вправе не проводить сертификацию или оценку соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения (за исключением прикладного программного обеспечения, взаимодействующего с СКЗИ) в отношении разрабатываемого ими программного обеспечения и приложений, если прошли сертификацию процессов безопасной разработки программного обеспечения ФСТЭК России на соответствие требованиям в части реализации безопасного жизненного цикла разработки программного обеспечения и приложений, указанным в национальном стандарте Российской Федерации ГОСТ Р 56939-2024 «Защита информации Разработка безопасного программного обеспечения. Общие требования», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 года № 1504-ст[9].

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны осуществлять планирование применения, применение, контроль применения и совершенствование применения мер, направленных на реализацию требований, установленных настоящим пунктом.».

1.7. Пункт 1.9 изложить в следующей редакции:

«1.9. Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить целостность электронных сообщений.

В целях обеспечения целостности электронных сообщений некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать реализацию мер по использованию любого вида усиленной электронной подписи, предусмотренной частью 4 статьи 5 Федерального закона

[9] М.: ФГБУ «Институт стандартизации», 2024.

от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи»), или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.

При использовании усиленной неквалифицированной электронной подписи в целях обеспечения целостности электронных сообщений некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечить использование усиленной неквалифицированной электронной подписи, созданной с использованием средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, при осуществлении регулирования в соответствии с пунктом «ш» части первой статьи 13 Федерального закона от 3 апреля 1995 года № 40-ФЗ «О федеральной службе безопасности» (далее – требования, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности).

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 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.

1.9[1]. Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, должны обеспечить подтверждение составления электронных сообщений уполномоченным на это лицом.

Некредитные финансовые организации в целях подтверждения составления электронных сообщений уполномоченным на это лицом должны:

обеспечить использование электронной подписи в соответствии с Федеральным законом «Об электронной подписи»;

осуществлять признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, в соответствии со статьей 6 Федерального закона «Об электронной подписи».

При использовании усиленной неквалифицированной электронной подписи в целях подтверждения составления электронных сообщений уполномоченным на это лицом некредитные финансовые организации должны обеспечить использование усиленной неквалифицированной электронной подписи, созданной с использованием средств электронной подписи и средств удостоверяющего центра, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности.

В целях обеспечения целостности электронных сообщений некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать реализацию мер по использованию любого вида усиленной электронной подписи, предусмотренной частью 1 статьи 5 Федерального закона «Об электронной подписи», или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией отправителя сообщения.».

1.8. В пункте 1.10:

1.8.1. В абзаце первом слова «должны обеспечивать регламентацию, реализацию, контроль (мониторинг) технологии безопасной обработки защищаемой информации, указанной» заменить словами «должны обеспечивать планирование, регламентацию, реализацию, контроль (мониторинг) и совершенствование мер и мероприятий, направленных на реализацию технологий безопасной обработки защищаемой информации, указанных».

1.8.2. Абзац второй подпункта 1.10.2 изложить в следующей редакции:

«в случае использования государственной информационной системы «Единая система идентификации и аутентификации физических лиц с использованием биометрических персональных данных» (далее – единая биометрическая система) –

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»[10], приказом ФСБ России № 378 технических и организационных мер, а также применение шифровальных (криптографических) средств, указанных в части 1 статьи 19 Федерального закона от 29 декабря 2022 года № 572-ФЗ, в целях нейтрализации угроз безопасности, актуальных при обработке биометрических персональных данных, векторов единой биометрической системы, проверке и передаче информации о степени соответствия векторов единой биометрической системы предоставленным биометрическим персональным данным физического лица при взаимодействии информационных систем организаций финансового рынка с единой биометрической системой;».

1.8.3. Абзац третий подпункта 1.10.2 дополнить словами «, а также отключение возможности использования клиентом технологии единого входа (однократной аутентификации) для совершения действий, связанных с осуществлением финансовых операций. При каждой идентификации, аутентификации, авторизации клиентов с использованием единой системы идентификации и аутентификации для осуществления финансовых операций некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровень защиты информации, должны запрашивать новое подтверждение идентификации и аутентификации клиента.».

1.8.4. Подпункт 1.10.3 изложить в следующей редакции:

«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) исходящих электронных

[10] Зарегистрирован Минюстом России 14 мая 2013 года № 28375 (с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 года № 49, зарегистрированного Минюстом России 25 апреля 2017 года № 46487, приказом ФСТЭК России от 14 мая 2020 года № 68, зарегистрированного Минюстом России 8 июля 2020 года № 58877).

сообщений (двойной контроль);

структурный и логический контроль входящих электронных сообщений, в том числе проверку правильности заполнения полей электронного сообщения (входной контроль);

контроль дублирования входящих электронных сообщений;

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

Указанные в абзаце пятом настоящего пункта требования по реализации мер по криптографической защите информации при ее передаче по каналам связи не применяются в случае, если 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.».

1.8.5. Подпункт 1.10.4 дополнить абзацем четвертым следующего содержания:

«Указанные в абзаце третьем настоящего пункта требования по получению от клиента подтверждения совершаемой финансовой операции не применяются центральными контрагентами, организаторами торговли, клиринговыми организациями, некредитными финансовыми организациями, осуществляющими репозитарную деятельность, депозитариями при осуществлении операций по результатам сделок, совершенных на торгах организаторов торговли, иных операций по распоряжению (поручению) клиринговой организации, а также операторами информационных систем, в которых осуществляется выпуск цифровых финансовых активов, при осуществлении операций по результатам взаимодействия с оператором обмена цифровых финансовых активов.».

1.9. В пункте 1.11:

1.9.1. Абзац пятый изложить в следующей редакции:

«сведения, идентифицирующие технологический участок;».

1.9.2. Дополнить пунктом 1.11^1 следующего содержания:

«1.11[1] Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» должны регистрировать следующую информацию о действиях клиентов, выполняемых на технологическом участке идентификации, аутентификации и авторизации клиентов при совершении действий в целях осуществления финансовых операций:

дата (день, месяц, год) и время (часы, минуты, секунды) начала соединения и окончания соединения сессии транспортного уровня в соответствии с эталонной моделью взаимосвязи открытых систем, предусмотренной пунктом 1.7 раздела 1 государственного стандарта Российской Федерации ГОСТ Р ИСО/МЭК 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»[11], при авторизации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления финансовых операций;

идентификационная информация, используемая для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления финансовых операций (адрес на сетевом уровне и адрес на транспортном уровне (порт) компьютера и (или) коммуникационного устройства (маршрутизатора), предусмотренные разделом 11 государственного стандарта Российской Федерации ГОСТ Р ИСО 7498-3-97 «Информационная технология. Взаимосвязь открытых систем базовая эталонная модель. Часть 3. Присвоение имен и адресация»[12] (далее – ГОСТ Р ИСО 7498-3-97);

идентификационная информация, используемая для адресации автоматизированной системы, программного обеспечения, к которым осуществлен доступ с целью осуществления финансовых операций (адрес на сетевом уровне и

[11] Принят постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78 и введен в действие 1 января 2000 года (М., ИПК «Издательство стандартов», 1999).

[12] Принят и введен в действие с 1 июля 1998 года постановлением Комитета Российской Федерации по стандартизации, метрологии и сертификации от 19 августа 1997 года № 286.

адрес на транспортном уровне (порт) автоматизированной системы, используемой некредитной финансовой организацией, предусмотренные разделом 11 ГОСТ Р ИСО 7498-3-97).».

1.10. В абзаце втором пункта 1.12 после слов «хранение информации, указанной в абзацах втором и четвертом пункта 1.1» дополнить словами «, пункте 1.11^1».

1.11. Подпункт 1.14.2 пункта 1.14 изложить в следующей редакции:

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

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

сведений, позволяющих выявить причину возникновения инцидента защиты 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.».

1.12. В пункте 1.15:

в абзаце втором после слов «о выявленных инцидентах защиты информации» дополнить словами «и компьютерных атаках»;

дополнить абзацем шестым следующего содержания:

«Предоставление информации, указанной в абзаце втором настоящего пункта, некредитными финансовыми организациями, реализующими усиленный, стандартный и минимальный уровни защиты информации, Банку России осуществляется в сроки, установленные приложением к настоящему Положению.».

1.13. В главе 2:

в абзаце четвертом пункта 2.1 слово «потребителей» заменить словом «получателей»;

в абзаце шестом пункта 2.1 слово «потребителя» заменить словом «получателя»;

в абзаце третьем подпункта 2.2.1 пункта 2.2 слово «потребителей» заменить словом «получателей»;

в подпункте 2.2.2 пункта 2.2 слово «потребителей» заменить словом «получателей»;

в пункте 2.3 слово «потребителем» заменить словом «получателем»;

дополнить пунктом 2.4 следующего содержания:

«2.4. Оператор финансовой платформы, регистратор финансовых транзакций должны осуществлять деятельность по планированию применения, применению, контролю применения и совершенствованию применения мер, направленных на реализацию требований, установленных подпунктами 2.2.1, 2.2.2 пункта 2.2, пунктом 2.3 настоящего Положения.».

1.14. Главу 3 дополнить пунктом 3.4 следующего содержания:

«3.4. Оператор информационной системы, в которой осуществляется выпуск цифровых финансовых активов, оператор обмена цифровых финансовых активов должны осуществлять деятельность по планированию применения, применению, контролю применения и совершенствованию применения мер, направленных на реализацию требований, установленных пунктами 3.2 и 3.3 настоящего Положения.».

1.15. Дополнить приложением в редакции приложения к настоящему Указанию.

2. Настоящее Указание подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от ____ года № ПСД-___) вступает в силу с 1 января 2027 года, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления их в силу.

Абзац шестой подпункта 1.4.2 пункта 1.4 настоящего Указания вступает в силу с 1 января 2028 года.

Абзац пятый подпункта 1.4.2 пункта 1.4 настоящего Указания действует по 31 декабря 2028 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Указанию Банка России
от __.__.2024 № _____
«О внесении изменений в Положение Банка России от 20 апреля 2021 года № 757-П»

Приложение
к Положению Банка России
от 20 апреля 2021 года № 757-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»

Сроки предоставления некредитными финансовыми организациями Банку России сведений о выявленных инцидентах защиты информации, о принятых мерах и проведенных мероприятиях по реагированию на выявленный некредитной финансовой организацией или Банком России инцидент защиты информации

Вид сведений	Срок предоставления
1	2
Сведения о выявлении инцидента защиты информации	В течение 3 часов с момента выявления инцидента защиты информации и (или) выявлении незаконного раскрытия информации ограниченного доступа и (или) защищаемой информации, указанной в пункте 1.1 настоящего Положения, некредитной финансовой организацией, реализующей усиленный или стандартный уровни защиты информации в соответствии с ГОСТ Р 57580.1-2017. В течение 24 часов с момента выявления инцидента защиты информации некредитной финансовой организацией, реализующей минимальный уровень защиты информации в соответствии с ГОСТ Р 57580.1-2017.
Сведения о выявлении незаконного раскрытия информации ограниченного доступа и (или) защищаемой информации, указанной в пункте 1.1 настоящего Положения	
Сведения о результатах расследования инцидента защиты информации или незаконного раскрытия информации ограниченного доступа и (или) защищаемой информации, указанной в пункте 1.1 настоящего Положения	В течение 30 дней с момента направления в Банк России данных о выявлении инцидента защиты информации или незаконного раскрытия информации ограниченного доступа и (или) защищаемой информации, указанной в пункте 1.1 настоящего Положения

Сведения о компьютерных инцидентах (в соответствии с пунктом 5 статьи 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»)	В течение 3 часов с момента выявления компьютерного инцидента в случае его связи с функционированием значимого объекта критической информационной инфраструктуры. В течение 24 часов с момента выявления компьютерного инцидента во всех иных случаях