ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

«28» октября 2025 г.

УКАЗАНИЕ

№ 7219-У

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
г. Москва
ЗАРЕГИСТРИРОВАНО
Регистрационный № 85262
от "6" февраля 2026.

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] (далее – Положение Банка России № 757-П) следующие изменения:

1.1. Абзац первый пункта 1.1 после слов «(Банке России)» дополнить словами «(далее – Федеральный закон «О Центральном банке Российской Федерации (Банке России)»)».

1.2. Пункт 1.2 изложить в следующей редакции:

«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:

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

Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон «Об электронной подписи»);

Федеральным законом «О персональных данных»;

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»;

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)» (зарегистрирован Минюстом России 3 марта 2005 года, регистрационный № 6382) с изменениями, внесенными приказом ФСБ России от 12 апреля 2010 года № 173 (зарегистрирован Минюстом России 25 мая 2010 года, регистрационный № 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» (зарегистрирован Минюстом России 18 августа 2014 года, регистрационный № 33620) (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:

абзацы пятый и шестой изложить в следующей редакции:

«страховые организации;

негосударственные пенсионные фонды;»;

абзац седьмой признать утратившим силу;

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

в абзаце одиннадцатом слова «инвестиционной платформы» заменить словами «инвестиционных платформ»;

в абзаце двенадцатом слова «финансовой платформы» заменить словами «финансовых платформ»;

дополнить абзацами следующего содержания:

«регистраторы;

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

1.4.2. В подпункте 1.4.4:

в абзаце третьем слова «и регистраторы» исключить;

абзац девятый признать утратившим силу;

дополнить абзацами 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);

операторы инвестиционных платформ, не указанные в подпункте 1.4.3 настоящего пункта;

микрофинансовые организации.».

1.5. В пункте 1.5:

1.5.1. Абзац первый изложить в следующей редакции:

«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) 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, с соблюдением следующих требований:».

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, совмещающие свою деятельность с деятельностью кредитной организации, при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений при составлении отчетности по форме 0409071 «Сведения об оценке выполнения кредитными

организациями требований к обеспечению защиты информации», установленной приложением 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)» (зарегистрировано Минюстом России 16 августа 2023 года, регистрационный № 74823) с изменениями, внесенными Указаниями Банка России от 8 декабря 2023 года № 6621-У (зарегистрировано Минюстом России 22 января 2024 года, регистрационный № 76927), от 12 марта 2024 года № 6688-У (зарегистрировано Минюстом России 29 мая 2024 года, регистрационный № 78345), от 10 июля 2024 года № 6800-У (зарегистрировано Минюстом России 25 октября 2024 года, регистрационный № 79916), от 4 сентября 2024 года № 6840-У (зарегистрировано Минюстом России 10 октября 2024 года, регистрационный № 79758), от 16 декабря 2024 года № 6961-У (зарегистрировано Минюстом России 19 декабря 2024 года, регистрационный № 80633), от 17 апреля 2025 года № 7047-У (зарегистрировано Минюстом России 24 июля 2025 года, регистрационный № 83051) (далее – Указание Банка России № 6406-У), 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 подпункте 4.3 пункта 4 и подпункте 5.3 пункта 5 Порядка составления и представления отчетности по форме 0409071 «Сведения об оценке выполнения кредитными организациями требований к обеспечению защиты информации», установленного приложением 1 к Указанию Банка России № 6406-У.

Профессиональные участники рынка ценных бумаг, 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 при составлении отчетности (отчета) по форме 0420433 «Сведения об оценке выполнения требований к обеспечению защиты информации профессиональными участниками рынка ценных бумаг, организаторами торговли, клиринговыми организациями», установленной приложением 1 к Указанию Банка России от 30 июня 2025 года № 7119-У «О формах, сроках и порядке составления и представления в Банк России отчетности профессиональных участников рынка ценных бумаг, об объеме, формах, сроках и порядке составления и представления в Банк России отчетов организаторов торговли и клиринговых организаций, а также о порядке сообщения профессиональными участниками рынка ценных бумаг Банку России информации о лицах, которым поручено проведение идентификации, упрощенной идентификации, обновление информации о клиентах, представителях клиентов, выгодоприобретателях и бенефициарных владельцах» (зарегистрировано Минюстом России 26 ноября 2025 года, регистрационный № 84279) (далее – Указание Банка России № 7119-У), должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении показателей оценки соответствия, указанных в подпункте 3.2 пункта 3 и подпункте 4.1 пункта 4 Порядка и сроков составления отчетности (отчета) по форме 0420433 «Сведения об оценке выполнения требований к обеспечению защиты информации профессиональными участниками рынка ценных бумаг, организаторами торговли, клиринговыми организациями», установленных приложением 1 к Указанию Банка России № 7119-У.

Негосударственные пенсионные фонды при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений при составлении отчетности по форме 0420266 «Сведения об оценке выполнения требований к обеспечению защиты информации негосударственным пенсионным фондом»,

установленной приложением 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» (зарегистрировано Минюстом России 31 октября 2024 года, регистрационный № 79989) с изменениями, внесенными Указанием Банка России от 13 марта 2025 года № 7010-У (зарегистрировано Минюстом России 16 апреля 2025 года, регистрационный № 81874) (далее – Указание Банка России № 6796-У), должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении показателей оценки соответствия, указанных в пункте 3 и подпункте 4.1 пункта 4 Порядка и сроков составления отчетности по форме 0420266 «Сведения об оценке выполнения требований к обеспечению защиты информации негосударственным пенсионным фондом», установленных приложением 1 к Указанию Банка России № 6796-У.

Операторы инвестиционных платформ, операторы финансовых платформ, операторы информационных систем, в которых осуществляется выпуск цифровых финансовых активов, операторы обмена цифровых финансовых активов, 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 при составлении отчетности (отчета) 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 приложением 1 к Указанию Банка России от 30 июня 2025 года № 7122-У «О порядке и сроках составления и представления (предоставления) 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» (зарегистрировано Минюстом России 4 декабря 2025 года, регистрационный № 84444) (далее – Указание Банка России № 7122-У), должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении показателей оценки соответствия, указанных в пункте 3 и подпункте 4.1 пункта 4 Порядка составления отчетности (отчета) 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», установленного приложением 1 к Указанию Банка России № 7122-У.

Страховые организации при проведении оценки выполнения требований к технологии обработки защищаемой информации и требований в отношении прикладного программного обеспечения автоматизированных систем и приложений при составлении отчетности по форме 0420175 «Сведения об оценке выполнения требований к обеспечению защиты информации страховой организацией», установленной приложением 1 к Указанию Банка России от 30 июня 2025 года № 7124-У «О формах, сроках и порядке составления и представления в Банк России отчетности страховщиков, о порядке сообщения страховщиками Банку России информации о лицах, которым поручено проведение идентификации, упрощенной идентификации, обновление информации о клиентах, представителях клиентов, выгодоприобретателях и бенефициарных владельцах, о порядке сообщения страховщиками в Банк России сведений об опубликовании годовой бухгалтерской (финансовой) отчетности страховщика, а также о порядке и сроках представления страховщиками в Банк России сведений и документов в отношении их филиалов, представительств и иных обособленных подразделений» (зарегистрировано Минюстом России 30 октября 2025 года, регистрационный № 84011) (далее – Указание Банка России № 7124-У), должны осуществлять расчет показателей оценки выполнения требований к технологическим мерам защиты информации и прикладному программному обеспечению автоматизированных систем и приложений в отношении показателей оценки соответствия, указанных в пункте 3 и подпункте 4.1 пункта 4 Порядка и сроков составления отчетности по форме 0420175 «Сведения об оценке выполнения требований к обеспечению защиты информации страховой организацией», установленных приложением 1 к Указанию Банка России № 7124-У.».

1.6. Пункты 1.8 и 1.9 изложить в следующей редакции:

«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 в соответствии с порядком, установленным Положением о сертификации средств защиты информации, утвержденным постановлением Правительства Российской Федерации от 26 июня 1995 года № 608 (далее – сертификация), или оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже, чем ОУД 4, предусмотренный пунктом 7.6 раздела 7 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 и введенного в действие с 1 сентября 2014 года приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст (М.: ФГУП «Стандартинформ», 2014) (далее соответственно – ГОСТ Р ИСО/МЭК 15408-3-2013, оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения).

Некредитные финансовые организации, не указанные в абзаце первом настоящего пункта, должны самостоятельно определять необходимость сертификации или проведения оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего пункта, некредитные финансовые организации

должны самостоятельно определять необходимость сертификации или проведения оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

По решению некредитной финансовой организации оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения 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, а также отдельного программного обеспечения 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 ФСТЭК России от 2 июня 2020 года № 76 (зарегистрирован Минюстом России 11 сентября 2020 года, регистрационный № 59772) с изменениями, внесенными приказом ФСТЭК России от 18 апреля 2022 года № 68 (зарегистрирован Минюстом России 20 июля 2022 года, регистрационный № 69318) (далее – приказ ФСТЭК России № 76).

Некредитные финансовые организации, реализующие стандартный уровень защиты информации, в случае сертификации прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения 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.

Некредитные финансовые организации, реализующие усиленный и стандартный уровни защиты информации, должны обеспечивать сертификацию или оценку соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения при каждом внесении изменений в исходный текст программного обеспечения и приложений, 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 указанные организации обеспечили сертификацию процессов безопасной разработки программного обеспечения ФСТЭК России на соответствие требованиям в части реализации безопасного жизненного цикла разработки программного обеспечения и приложений, указанным в разделах 4 и 5 национального стандарта Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденным и введенным в действие с 20 декабря 2024 года приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 года № 1504-ст (М.: ФГБУ «Институт стандартизации», 2024), при осуществлении полномочий в соответствии с подпунктами 13, 13^2 пункта 8, подпункта 9 пункта 9 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 года № 1085.

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.

1.9. 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 1 статьи 5 Федерального закона «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).

Указанное в абзаце втором настоящего пункта требование по реализации мер по использованию усиленной квалифицированной электронной подписи, усиленной неквалифицированной электронной подписи или СКЗИ, реализующих функцию имитозащиты информации с аутентификацией

отправителя сообщения, не применяется 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.».

1.7. Дополнить пунктами 1.9^1 и 1.9^2 следующего содержания:

«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, реализующие усиленный, стандартный и минимальный уровни защиты информации, 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, реализующие усиленный, стандартный и минимальный 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.

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.

1.9[2]. Некредитные финансовые организации, реализующие усиленный, стандартный и минимальный уровни защиты информации, в случае использования единой системы идентификации и аутентификации, определенной пунктом 5 статьи 2 Федерального закона от 29 декабря 2022 года № 572-ФЗ (далее – единая система идентификации и аутентификации), должны реализовывать 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 уровни защиты информации, должны запрашивать новое подтверждение идентификации и аутентификации клиента.».

1.8. В пункте 1.10:

1.8.1. В абзаце первом слова «регламентацию, реализацию, контроль (мониторинг) технологии» заменить словами «планирование, регламентацию, реализацию, контроль (мониторинг) и совершенствование мер и мероприятий, направленных на реализацию технологий».

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», определенной пунктом 4 статьи 2 Федерального закона от 29 декабря 2022 года № 572-ФЗ (далее – единая биометрическая система), – реализацию установленных приказом ФСТЭК России 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» (зарегистрирован Минюстом России 14 мая 2013 года, регистрационный № 28375) с изменениями, внесенными приказами ФСТЭК России от 23 марта 2017 года № 49 (зарегистрирован Минюстом России 25 апреля 2017 года, регистрационный № 46487), от 14 мая 2020 года № 68 (зарегистрирован Минюстом России 8 июля 2020 года, регистрационный № 58877), 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. 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 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 информации при ее передаче по каналам связи.».

1.8.4. В подпункте 1.10.4:

в абзаце втором слова «в пункте 1.9» заменить словами «в пункте 1.9^1»;

дополнить абзацем следующего содержания:

«Указанное в абзаце третьем настоящего подпункта требование не применяется центральными контрагентами, организаторами торговли, клиринговыми организациями, репозитариями, не являющимися регистраторами финансовых транзакций, центральным депозитарием, депозитариями, специализированными депозитариями инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов, регистраторами, 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. Абзац пятый пункта 1.11 изложить в следующей редакции:

«сведения, идентифицирующие технологический участок;».

1.10. 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 сети «Интернет» должны регистрировать следующую информацию о действиях клиентов:

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», принятого и введенного в действие с 1 января 2000 года постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 18 марта 1999 года № 78 (М.: ИПК «Издательство стандартов», 1999), 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 применением 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», принятого и введенного в действие с 1 июля 1998 года постановлением Государственного комитета Российской Федерации по стандартизации и метрологии от 19 августа 1997 года № 286 (М.: ИПК «Издательство стандартов», 1997) (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 адрес на транспортном уровне (порт) автоматизированной системы, используемой некредитной финансовой организацией, предусмотренные разделом 11 ГОСТ Р ИСО 7498-3-97).».

1.11. В пункте 1.12:

в абзаце первом слова «и стандартный» заменить словами «, стандартный и минимальный»;

в абзаце втором слова «пункта 1.1 настоящего Положения» заменить словами «пункта 1.1, пункте 1.11^1 настоящего Положения».

1.12. Подпункт 1.14.2 пункта 1.14 изложить в следующей редакции:

«1.14.2. По каждому инциденту защиты информации, незаконному раскрытию защищаемой информации, указанной в пункте 1.1 настоящего Положения, и (или) информации, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации, а также компьютерному инциденту, определенному пунктом 5 статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», 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;

результата расследования инцидента защиты информации, незаконного раскрытия защищаемой информации, указанной в пункте 1.1 настоящего Положения, и (или) информации, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации.».

1.13. В пункте 1.15:

абзац второй после слов «инцидентах защиты информации» дополнить словами «и компьютерных атаках»;

в третьем предложении абзаца пятого слова «и сроках» исключить;

дополнить абзацем 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, содержащиеся в приложении к настоящему Положению.».

1.14. В пункте 2.1:

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

в абзаце шестом слово «потребителя» заменить словом «получателя».

1.15. В абзаце третьем подпункта 2.2.1 и в подпункте 2.2.2 пункта 2.2 слово «потребителей» заменить словом «получателей».

1.16. В пункте 2.3 слово «потребителем» заменить словом «получателем», слова «требованиями пункта 1.9» заменить словами «требованиями пунктов 1.9 и 1.9^1».

1.17. Главу 2 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.».

1.18. 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.».

1.19. Пункт 4.2 изложить в следующей редакции:

«4.2. Некредитные финансовые организации при совмещении деятельности в сфере финансового рынка и (или) совмещении своей деятельности 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 электронной платформы, 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 пунктом 1.4 настоящего Положения 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 кредитных организаций, операторов по переводу денежных средств, банковских платежных агентов (субагентов), операторов услуг информационного обмена, поставщиков платежных приложений, операторов платежных систем, операторов услуг платежной инфраструктуры, операторов электронных платформ.».

1.20. 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 12 сентября 2025 года № ПСД-27) вступает в силу с 1 января 2027 года, за исключением абзацев седьмого и восьмого подпункта 1.4.2 пункта 1 настоящего Указания.

Абзац пятнадцатый подпункта 1.4.4 пункта 1.4 Положения Банка России № 757-П (в редакции настоящего Указания) вступает в силу с 1 января 2028 года.

Абзац тринадцатый подпункта 1.4.4 пункта 1.4 Положения Банка России № 757-П (в редакции настоящего Указания) действует по 31 декабря 2027 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Указанию Банка России
от 28 октября 2025 года № 7219-У
«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, принятых мерах и проведенных мероприятиях по реагированию на выявленный некредитной финансовой организацией или Банком России инцидент защиты информации

№ п/п	Вид сведений	Срок предоставления
1	2	3
1	Сведения о выявлении инцидента защиты информации	В течение 3 часов с момента выявления инцидента защиты информации некредитной финансовой организацией, реализующей усиленный и стандартный уровни защиты информации, предусмотренные пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017. В течение 24 часов с момента выявления инцидента защиты информации некредитной финансовой организацией, реализующей минимальный уровень защиты информации, предусмотренный пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017

1	2	3
2	Сведения о выявлении незаконного раскрытия защищаемой информации, указанной в пункте 1.1 настоящего Положения, и (или) информации, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации	В течение 3 часов с момента выявления незаконного раскрытия защищаемой информации, указанной в пункте 1.1 настоящего Положения, и (или) информации, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации, некредитной финансовой организацией, реализующей усиленный и стандартный уровни защиты информации, предусмотренные пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017. В течение 24 часов с момента выявления незаконного раскрытия защищаемой информации, указанной в пункте 1.1 настоящего Положения, и (или) информации, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации, некредитной финансовой организацией, реализующей минимальный уровень защиты информации, предусмотренный пунктом 6.7 раздела 6 ГОСТ Р 57580.1-2017
3	Сведения о результатах расследования инцидента защиты информации или незаконного раскрытия защищаемой информации, указанной в пункте 1.1 настоящего Положения, и (или) информации, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации	В течение 30 календарных дней со дня направления в Банк России данных о выявлении инцидента защиты информации или незаконного раскрытия защищаемой информации, указанной в пункте 1.1 настоящего Положения, и (или) информации, доступ к которой ограничен федеральными законами и актами Президента Российской Федерации
4	Сведения о компьютерных инцидентах (в соответствии с пунктом 5 статьи 2 Федерального закона от 26 июля 2017 года № 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

».