ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«30» августа 2023 г. № 822-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 76558
от "22" декабря 2023 г.

О требованиях к обеспечению защиты информации, содержащейся в автоматизированной информационной системе страхования

Настоящее Положение на основании подпункта 5 пункта 7 статьи 33^{10} Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации» устанавливает требования к обеспечению защиты информации, содержащейся в автоматизированной информационной системе страхования.

1. Оператор автоматизированной информационной системы страхования (далее – АИС страхования) должен осуществлять защиту информации, содержащейся в АИС страхования, указанной в пункте 1 статьи 33^{11} Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации» (далее соответственно – защищаемая информация, Закон Российской Федерации № 4015-I), при ее получении, подготовке, обработке, хранении и предоставлении (далее – защита информации).

В случае если защищаемая информация содержит персональные данные, оператор АИС страхования должен 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» (далее – Федеральный закон от 27 июля 2006 года № 152-ФЗ) и 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»[1] (далее – приказ ФСТЭК России № 21).

2. Оператор АИС страхования должен определить во внутренних документах состав и порядок применения организационных и технических мер защиты информации в отношении эксплуатируемых им автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее при совместном упоминании – объекты информационной инфраструктуры) в рамках следующих процессов (направлений):

защиты информации при управлении доступом к объектам информационной инфраструктуры;

защиты вычислительных сетей;

контроля целостности и защищенности объектов информационной инфраструктуры;

защиты объектов информационной инфраструктуры от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносные коды);

предотвращения утечек защищаемой информации;

управления событиями, которые привели или, по оценке оператора АИС страхования, могут привести к незаконному раскрытию защищаемой информации или неоказанию услуг, связанных с получением или предоставлением защищаемой информации (далее – инциденты защиты информации);

---

[1] 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).

защиты среды виртуализации;

защиты информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств.

3. Оператор АИС страхования должен осуществлять защиту информации с помощью средств криптографической защиты информации (далее – СКЗИ) в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (далее – Федеральный закон от 6 апреля 2011 года № 63-ФЗ), Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66[1] (далее – Положение ПКЗ-2005), и технической документацией на СКЗИ.

Обеспечение защиты персональных данных с использованием СКЗИ осуществляется в соответствии с 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 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»[2] (далее – приказ ФСБ России № 378) с применением СКЗИ, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности при осуществлении

---

[1] 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).

[2] Зарегистрирован Минюстом России 18 августа 2014 года, регистрационный № 33620.

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), и обеспечивающих нейтрализацию угроз безопасности персональных данных, определенных Банком России в соответствии с частью 5 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ и подпунктом 6 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I.

Обеспечение защиты биометрических персональных данных с использованием СКЗИ осуществляется в соответствии с 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) с применением СКЗИ, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и обеспечивающих нейтрализацию угроз безопасности персональных данных, определенных приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 5 мая 2023 года № 445 «Об утверждении перечня 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 в единой биометрической системе, а также актуальных при взаимодействии информационных систем государственных органов, органов местного самоуправления, Центрального банка Российской Федерации, организаций, за исключением организаций финансового рынка,

индивидуальных предпринимателей, нотариусов с единой биометрической системой, с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных»[1] (далее – приказ Минцифры России № 445).

4. Оператор АИС страхования в случаях, предусмотренных технической документацией на СКЗИ, должен проводить оценку влияния аппаратных, программно-аппаратных и программных средств сети (системы), используемой СКЗИ с целью защиты информации при ее передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с 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».

Оператор АИС страхования должен применять СКЗИ, имеющее подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и обеспечивающие нейтрализацию угроз, определенных в соответствии с нормативным актом Банка России об определении угроз безопасности при обработке персональных данных в АИС страхования, принятым на основании подпункта 6 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I, и приказом Минцифры России № 445.

Оператор АИС страхования должен обеспечивать защиту криптографических ключей СКЗИ, используемых при обмене защищаемой информацией, в том числе ключей электронной подписи и ключей проверки электронной подписи (далее − криптографические ключи СКЗИ).

---

[1] Зарегистрирован Минюстом России 26 мая 2023 года, регистрационный № 73486. Согласно пункту 3 приказа Минцифры России № 445 данный акт действует до 1 июня 2029 года.

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. Принадлежность физическому или юридическому лицу ключа проверки электронной подписи, изготовленного средствами электронной подписи, подтверждается сертификатом ключа проверки электронной подписи, созданным и выданным удостоверяющим центром в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ.

5. Оператор АИС страхования должен формировать для пользователей АИС страхования рекомендации по защите информации от воздействия вредоносного кода в целях противодействия неправомерному разглашению и незаконному использованию защищаемой информации.

Оператор АИС страхования должен доводить до пользователей АИС страхования информацию о возможных рисках несанкционированного доступа к защищаемой информации лицами, не обладающими правом ее обработки, хранения и передачи (далее – информация о рисках), путем размещения информации о рисках на официальном сайте оператора АИС страхования в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), предусмотренном подпунктом 10 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I, для целей обеспечения ознакомления с ней пользователей АИС страхования.

6. Оператор АИС страхования должен осуществлять не реже одного раза в два года:

тестирование объектов информационной инфраструктуры, обрабатывающих защищаемую информацию при приеме электронных сообщений, содержащих защищаемую информацию (далее – электронные сообщения), в автоматизированных системах и приложениях с использованием сети «Интернет», а также на официальном сайте оператора АИС страхования в сети «Интернет», предусмотренном подпунктом 10 пункта 7 статьи 33^{10} Закона

Российской Федерации № 4015-I, на предмет возможности несанкционированного доступа к обрабатываемой защищаемой информации;

анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

В случае выявления уязвимостей информационной безопасности объектов информационной инфраструктуры оператор АИС страхования должен устранять выявленные уязвимости в порядке и сроки, установленные во внутренних документах оператора АИС страхования.

7. Оператор АИС страхования при использовании прикладного программного обеспечения автоматизированных систем и приложений, распространяемых оператором АИС страхования среди пользователей АИС страхования для совершения действий в целях обмена защищаемой информацией, а также программного обеспечения, обрабатывающего защищаемую информацию при приеме электронных сообщений к исполнению в автоматизированных системах и приложениях в сети «Интернет», должен обеспечить проведение сертификации в системе сертификации федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации при осуществлении регулирования в соответствии с подпунктом 13 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 года № 1085 (далее – сертификация), или оценки соответствия требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД4[1] (далее – оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения).

[1] Подраздел 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 приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст (М., ФГУП «Стандартинформ», 2014) и введенного в действие 1 сентября 2014 года.

По решению оператора АИС страхования оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения проводится самостоятельно или с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации, на проведение работ и предоставление 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.

В отношении программного обеспечения и приложений, не указанных в абзаце первом настоящего пункта, оператор АИС страхования должен самостоятельно определять необходимость сертификации или оценки соответствия прикладного программного обеспечения автоматизированных систем и приложений, а также отдельного программного обеспечения.

Оператор АИС страхования в случае принятия решения о сертификации программного обеспечения автоматизированных систем и приложений, не указанных в абзаце первом настоящего пункта, должен обеспечить сертификацию программного обеспечения автоматизированных систем и приложений не ниже 4 уровня доверия в соответствии с приказом Федеральной службы по техническому и экспортному контролю от 2 июня 2020 года № 76[1].

8. Оператор АИС страхования в целях обеспечения контроля целостности исходящих электронных сообщений и подтверждения составления исходящего электронного сообщения уполномоченным на это работником оператора АИС страхования (далее – работник) при передаче исходящего электронного сообщения оператором АИС страхования должен использовать усиленную квалифицированную электронную подпись (далее – УКЭП).

---

[1] 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).

В целях обеспечения защиты информации оператор АИС страхования должен хранить входящие электронные сообщения и средства, обеспечивающие проверку электронной подписи входящих электронных сообщений, в течение срока, указанного в подпункте 1 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I.

В целях обеспечения защиты информации оператор АИС страхования должен хранить исходящие электронные сообщения, подписанные УКЭП, и средства, обеспечивающие проверку электронной подписи исходящих электронных сообщений, не менее пяти лет с даты подписания электронных сообщений. Класс используемых в таких случаях средств электронной подписи и средств удостоверяющего центра определяется исходя из угроз безопасности при обработке персональных данных в АИС страхования, определенных нормативным актом Банка России об определении угроз безопасности при обработке персональных данных в АИС страхования, принятым на основании подпункта 6 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I, и приказом Минцифры России № 445.

В целях обеспечения контроля целостности входящих электронных сообщений и подтверждения составления электронного сообщения пользователем АИС страхования оператор АИС страхования должен при получении электронного сообщения, содержащего запрос о предоставлении содержащейся в АИС страхования защищаемой информации, осуществить проверку на принадлежность пользователю АИС страхования соответствующего вида электронной подписи и сертификата ключа проверки электронной подписи (далее – контроль электронной подписи).

В целях обеспечения защиты информации оператор АИС страхования должен хранить результаты контроля электронной подписи и обеспечивать их целостность в течении сроков, указанных в абзаце втором настоящего пункта.

9. Оператор АИС страхования должен обеспечить целостность предоставленной в АИС страхования информации, подписанной УКЭП

и признаваемой в соответствии с частью 1 статьи 6 Федерального закона от 6 апреля 2011 года № 63-ФЗ электронным документом, равнозначным документу на бумажном носителе (далее – предоставленная в АИС страхования информация), при ее хранении в течение срока, указанного в подпункте 1 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I, посредством подписания предоставленной в АИС страхования информации с помощью УКЭП работника по истечении сроков действия соответствующих квалифицированных сертификатов ключей проверки электронной подписи.

10. Оператор АИС страхования в части требований к защите информации, применяемых в отношении технологии обработки защищаемой информации, должен обеспечить конфиденциальность, целостность и достоверность защищаемой информации, регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации, регистрацию результатов совершения действий, связанных с осуществлением доступа к защищаемой информации, на следующих технологических участках:

идентификации, аутентификации и авторизации пользователей АИС страхования при совершении действий в целях обработки, хранения и передачи защищаемой информации (далее – действия с защищаемой информацией),

формирования (подготовки), передачи и приема электронных сообщений;

удостоверения права пользователей АИС страхования на совершение действий с защищаемой информацией;

осуществления действий с защищаемой информацией, учета результатов осуществления действий с защищаемой информацией, а также хранения электронных сообщений и информации об осуществленных действиях с защищаемой информацией.

10.1. Технология обработки защищаемой информации, применяемая оператором АИС страхования при идентификации, аутентификации и авторизации пользователей АИС страхования при совершении действий с

защищаемой информацией, в случае использования единой биометрической системы, определенной в соответствии с пунктом 4 статьи 2 Федерального закона от 29 декабря 2022 года № 572-ФЗ, должна предусматривать:

реализацию технических и организационных мер, установленных приказом ФСТЭК России № 21, приказом ФСБ России № 378;

применение шифровальных (криптографических) средств, указанных в пункте 1 части 1 статьи 19 Федерального закона от 29 декабря 2022 года № 572-ФЗ, в целях нейтрализации угроз безопасности, определенных приказом Минцифры России № 445.

10.2. Технология обработки защищаемой информации, применяемая при формировании (подготовке), передаче и приеме электронных сообщений, составляемых при взаимодействии оператора АИС страхования и пользователя АИС страхования, должна предусматривать:

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

проверку правильности формирования (подготовки) исходящих электронных сообщений;

использование для подписания исходящего электронного сообщения средств электронной подписи, имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и обеспечивающих нейтрализацию угроз, определенных нормативным актом Банка России об определении угроз безопасности при обработке персональных данных в АИС страхования, принятым на основании подпункта 6 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I, и приказом Минцифры России № 445;

защиту информации, в том числе обеспечение ее целостности и конфиденциальности шифровальными (криптографическими) средствами, при ее передаче по каналам связи;

использование сертификатов безопасности, подтверждающих принадлежность ключа аутентификации сайту в сети «Интернет» и используемых для установления с данным сайтом криптографически защищенного соединения, выданных информационной системой национального удостоверяющего центра, предназначенной для обеспечения устойчивости взаимодействия устройств в российском сегменте сети «Интернет», определенной в абзаце семнадцатом подпункта «а» пункта 2 Положения об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме, утвержденного постановлением Правительства Российской Федерации от 8 июня 2011 года № 451.

10.3. Технология обработки защищаемой информации, применяемая при удостоверении оператором АИС страхования права пользователя АИС страхования на совершение действий с защищаемой информацией, должна предусматривать контроль подписания электронного сообщения пользователем АИС страхования посредством мероприятия, указанного в абзаце четвертом подпункта 10.2 настоящего пункта, и проверку прав владельца электронной подписи.

10.4. Технология обработки защищаемой информации, применяемая при осуществлении действий с защищаемой информацией, учете результатов осуществления действий с защищаемой информацией, а также хранении электронных сообщений и информации об осуществленных действиях с защищаемой информацией, должна предусматривать:

проверку соответствия (сверку) исходящих электронных сообщений соответствующим входящим электронным сообщениям;

регистрацию исполненных запросов о предоставлении защищаемой информации пользователям АИС страхования;

создание резервных копий баз данных, содержащих защищаемую информацию, в целях обеспечения доступности защищаемой информации;

хранение и целостность предоставленной в АИС страхования информации в соответствии с требованиями пункта 9 настоящего Положения.

11. В целях обеспечения защиты информации оператор АИС страхования должен регистрировать результаты совершения следующих действий, связанных с осуществлением доступа к защищаемой информации:

идентификации, аутентификации и авторизации пользователей АИС страхования при совершении действий с защищаемой информацией;

приема (передачи) электронных сообщений при взаимодействии оператора АИС страхования с пользователями АИС страхования, в том числе для удостоверения права пользователей АИС страхования осуществлять действия с защищаемой информацией и для учета результатов осуществления действий с защищаемой информацией;

осуществления доступа работников к защищаемой информации и осуществления пользователями АИС страхования действий с защищаемой информацией, выполняемых с использованием автоматизированных систем, программного обеспечения, в том числе подлежат регистрации следующие данные:

дата (день, месяц, год) и время (часы, минуты, секунды) совершения работником (пользователем АИС страхования) действий с защищаемой информацией;

присвоенный работнику (пользователю АИС страхования) идентификатор, позволяющий установить работника (пользователя АИС страхования) в автоматизированной системе, программном обеспечении;

сведения, идентифицирующие технологический участок;

результат совершения работником (пользователем АИС страхования) действия с защищаемой информацией («успешно» или «неуспешно»);

информация, используемая для идентификации устройств, при помощи которых осуществлен доступ к защищаемой информации, или устройств,

к которым осуществлен доступ работниками (пользователями АИС страхования) с использованием автоматизированных систем, программного обеспечения;

сведения, идентифицирующие сертификат ключа проверки электронной подписи, обладателем которого является работник (пользователь АИС страхования), использующий его для подписания электронных сообщений.

12. Оператор АИС страхования должен в соответствии со своими внутренними документами осуществлять регистрацию инцидентов защиты информации, а также представлять сведения о выявленных инцидентах защиты информации должностному лицу (отдельному структурному подразделению), ответственному за управление рисками, при соблюдении требований, предусмотренных абзацами вторым – пятым настоящего пункта.

По каждому инциденту защиты информации оператор АИС страхования должен 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.

13. В целях реализации требований к обеспечению защиты информации оператор АИС страхования должен информировать Банк России:

о выявленных оператором АИС страхования инцидентах защиты информации, причинах возникновения инцидента защиты информации;

о принятых мерах и проведенных мероприятиях по реагированию на выявленный оператором АИС страхования или Банком России инцидент защиты информации;

о принадлежащих оператору АИС страхования и (или) администрируемых в его интересах сайтах в сети «Интернет», которые используются оператором АИС страхования для осуществления своей деятельности;

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

Оператор АИС страхования должен представлять в Банк России указанные в абзацах втором – пятом настоящего пункта сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры (автоматизированной системы) Банка России), информация о которых размещается на официальном сайте Банка России в сети «Интернет».

14. В целях обеспечения защиты информации оператор АИС страхования должен осуществлять хранение:

защищаемой информации в течение срока, указанного в подпункте 1 пункта 7 статьи 33^{10} Закона Российской Федерации № 4015-I;

информации об инцидентах защиты информации и данных, указанных в абзацах четвертом – десятом пункта 11 настоящего Положения, не менее пяти лет с даты их формирования оператором АИС страхования (даты поступления в АИС страхования).

15. При обеспечении безопасности объектов информационной инфраструктуры, эксплуатация и использование которых осуществляются оператором АИС страхования в рамках своей деятельности и которые являются объектами критической информационной инфраструктуры Российской Федерации, применяются в том числе требования и порядок, установленные органами государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры в соответствии со статьей 6 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

16. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 23 июня 2023 года № ПСД-23) вступает в силу с 1 апреля 2024 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Согласовано:

Директор
Федеральной службы безопасности
Российской Федерации
_____ А.В. Бортников
_____ 2023 г.

Директор
Федеральной службы по техническому
и экспортному контролю
Российской Федерации
_____ В.В. Селин
_____ 2023 г.