Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

« » _____ 2021 г. №_____-П

г. Москва

Об установлении обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, требований к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, за исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами

На основании статьи 76^{9-6} Федерального закона Российской Федерации от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 1, ст. 53), части 2 статьи 7 Федерального закона от 30 декабря 2004 года № 218-ФЗ «О кредитных историях» (Собрание законодательства Российской Федерации, 2005, № 1, ст. 44; 2020, № 31, ст. 5061) настоящее Положение устанавливает обязательные для лиц, оказывающих профессиональные услуги на финансовом рынке, требования к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, за

исключением требований к обеспечению защиты информации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами, в том числе требования к обеспечению бюро кредитных историй защиты информации при ее обработке, хранении и передаче сертифицированными средствами защиты.

Глава 1. Общие требования к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций

1.1. Лица, оказывающие профессиональные услуги на финансовом рынке, за исключением бюро кредитных историй, вправе принять решение о необходимости соблюдения в отношении автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее – объекты информационной инфраструктуры) требований национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2017) (далее – ГОСТ Р 57580.1-2017), соответствующих минимальному уровню защиты информации.

1.2. Обеспечение защиты информации с помощью средств криптографической защиты информации (далее - СКЗИ) лица, оказывающие профессиональные услуги на финансовом рынке, должны осуществлять в соответствии с технической документацией на СКЗИ, а также следующими федеральными законами и иными нормативными правовыми актами

Российской Федерации:

Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27; 2021, № 9, ст. 1467) (далее – Федеральный закон «Об электронной подписи»);

Федеральным законом «О персональных данных»;

постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257);

приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)», зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года № 6382, 25 мая 2010 года № 17350 (далее – Положение ПКЗ-2005);

приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», зарегистрированным Министерством юстиции Российской Федерации 18 августа 2014 года № 33620.

1.3. В случае наличия в технической документации на СКЗИ требований к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований лица, оказывающие профессиональные

услуги на финансовом рынке, должны обеспечить проведение указанной оценки в соответствии с Положением ПКЗ-2005 по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности.

В случае если лица, оказывающие профессиональные услуги на финансовом рынке, применяют СКЗИ российского производства, СКЗИ должны иметь сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности.

Безопасность процессов изготовления криптографических ключей СКЗИ должна обеспечиваться комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

Глава 2. **Особенности обеспечения бюро кредитных историй защиты информации при ее обработке, хранении и передаче сертифицированными средствами защиты**

2.1. Бюро кредитных историй должны осуществлять защиту информации, указанной в статье 4 Федерального закона от 30 декабря 2004 года № 218-ФЗ «О кредитных историях» (далее – Федеральный закон «О кредитных историях»), содержащейся в автоматизированных системах, используемых бюро кредитных историй, при ее обработке, передаче и хранении сертифицированными средствами защиты, в том числе при взаимодействии бюро кредитных историй с пользователями кредитных историй, источниками формирования кредитных историй, субъектами кредитных историй (далее соответственно – защита информации, защищаемая информация, субъекты взаимодействия).

В дополнение к настоящим требованиям бюро кредитных историй должны применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2021, № 1, ст. 58) (далее – Федеральный закон «О персональных данных»).

2.2. Бюро кредитных историй должны обеспечивать формирование для субъектов взаимодействия рекомендаций по защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее – вредоносный код), в целях противодействия неправомерному разглашению и незаконному использованию защищаемой информации.

Бюро кредитных историй должны обеспечивать доведение до субъектов взаимодействия следующей информации:

о возможных рисках получения несанкционированного доступа к защищаемой информации лицами, не обладающими правом ее обработки, хранения и передачи;

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

2.3. Защита информации в отношении объектов информационной инфраструктуры, должна осуществляться бюро кредитных историй в соответствии с требованиями ГОСТ Р 57580.1-2017 с соблюдением следующих требований.

2.3.1. Требования ГОСТ Р 57580.1-2017, соответствующие

стандартному уровню защиты информации, должны соблюдать квалифицированные бюро кредитных историй.

2.3.2. Требования ГОСТ Р 57580.1-2017, соответствующие минимальному уровню защиты информации, должны соблюдать бюро кредитных историй, не являющиеся квалифицированными.

2.3.3. Бюро кредитных историй должны осуществлять ежегодное тестирование объектов информационной инфраструктуры, обрабатывающих защищаемую информацию при приеме электронных сообщений, содержащих защищаемую информацию (далее – электронные сообщения) субъектов кредитных историй в автоматизированных системах и приложениях с использованием информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), а также на официальном сайте бюро кредитных историй в сети «Интернет» на предмет проникновений и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

Бюро кредитных историй вправе установить во внутренних документах форму результатов ежегодного тестирования объектов информационной инфраструктуры.

2.4. Бюро кредитных историй должны обеспечивать проведение оценки соответствия уровня защиты информации требованиям, предусмотренным пунктом 2.3 настоящего Положения, с соблюдением следующих требований.

2.4.1. Бюро кредитных историй должны осуществлять оценку соответствия уровня защиты информации с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (Собрание

законодательства Российской Федерации, 2012, № 7, ст. 863; 2020, № 49, ст. 7943) (далее – проверяющая организация).

2.4.2. Бюро кредитных историй должны осуществлять оценку соответствия уровня защиты информации в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года № 156-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2018) (далее – ГОСТ Р 57580.2-2018).

2.4.3. Оценка соответствия уровня защиты информации должна осуществляться бюро кредитных историй, не являющимися квалифицированными, – не реже одного раза в три года, квалифицированными бюро кредитных историй не реже одного раза в два года.

2.5. Бюро кредитных историй должны хранить отчет, составленный проверяющей организацией по результатам оценки соответствия уровня защиты информации, в течение не менее чем трех лет с даты его выдачи проверяющей организацией.

2.6. Бюро кредитных историй должны обеспечить уровень соответствия не ниже третьего уровня соответствия, предусмотренного подпунктом «г» пункта 6.9 ГОСТ Р 57580.2-2018.

Бюро кредитных историй должны обеспечить уровень соответствия не ниже четвертого уровня соответствия, предусмотренного подпунктом «д» пункта 6.9 ГОСТ Р 57580.2-2018.

2.7. Бюро кредитных историй, не являющиеся квалифицированными, должны обеспечить использование для обработки, хранения и передачи защищаемой информации прикладного программного обеспечения автоматизированных систем и приложений, распространяемых бюро кредитных историй субъектам кредитных историй для совершения действий в

целях обработки, хранения и передачи защищаемой информации, в том числе за плату, прошедших сертификацию в системе сертификации Федеральной службы по техническому и экспортному контролю или оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД 4, предусмотренного пунктом 7.6 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014).

В отношении прикладного программного обеспечения и приложений, не указанных в абзаце первом настоящего пункта, бюро кредитных историй, не являющиеся квалифицированными, должны самостоятельно определять необходимость сертификации или оценки соответствия.

По решению бюро кредитных историй, не являющегося квалифицированным, оценка соответствия в прикладном программном обеспечении автоматизированных систем и приложений проводится самостоятельно или с привлечением проверяющей организации.

2.8. Бюро кредитных историй должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить их целостность и подтвердить их составление уполномоченным на это лицом.

В целях обеспечения контроля целостности электронных сообщений и подтверждения составления электронного сообщения уполномоченным на это лицом бюро кредитных историй должны обеспечивать использование усиленной квалифицированной электронной подписи или усиленной неквалифицированной электронной подписи при передаче электронных сообщений между:

бюро кредитных историй и источниками формирования кредитных

историй;

бюро кредитных историй и пользователями кредитных историй;

бюро кредитных историй и поднадзорными Банку России организациями, с которыми у бюро кредитных историй заключен договор в соответствии с частью 3 статьи 9 Федерального закона «О кредитных историях»;

бюро кредитных историй между собой;

бюро кредитных историй и Банком России.

В целях обеспечения контроля целостности электронных сообщений и подтверждения составления электронного сообщения уполномоченным на это лицом бюро кредитных историй должны обеспечивать использование электронной подписи, иных аналогов собственноручной подписи, кодов, паролей и других средств при передаче электронных сообщений между субъектами кредитных историй и бюро кредитных историй.

Признание электронных сообщений, подписанных электронной подписью, равнозначными сообщениям на бумажном носителе, подписанным собственноручной подписью, должно осуществляться в соответствии со статьей 6 Федерального закона «Об электронной подписи».

Требования настоящего пункта распространяются на бюро кредитных историй в случае если федеральными законами не установлено иное.

2.9. Бюро кредитных историй в части требований к обеспечению защиты информации, применяемых в отношении технологии обработки информации, обрабатываемой, передаваемой и хранимой на участках идентификации, аутентификации и авторизации субъектов взаимодействия при совершении действий в целях обработки, хранения и передачи защищаемой информации; формирования (подготовки), передачи и приема электронных сообщений; удостоверения права субъектов взаимодействия на совершение действий с защищаемой информацией; осуществления действий в целях обработки, хранения и передачи защищаемой информации (далее – действия с кредитными историями); учета результатов осуществления

действий с кредитными историями; хранения электронных сообщений и информации об осуществленных действиях с защищаемой информацией (далее – технологические участки), должны обеспечивать:

целостность и достоверность защищаемой информации;

регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации;

регистрацию результатов совершения действий, связанных с осуществлением доступа к защищаемой информации.

2.9.1. Технология обработки защищаемой информации, применяемая бюро кредитных историй на всех технологических участках, должна обеспечивать целостность и неизменность защищаемой информации, в том числе путем взаимной (двухсторонней) аутентификации с субъектами взаимодействия средствами вычислительной техники бюро кредитных историй и субъектов взаимодействия.

2.9.2. Технология обработки защищаемой информации, применяемая при идентификации, аутентификации и авторизации субъектов кредитных историй – физических лиц в целях предоставления кредитных отчетов, должна обеспечивать выполнение в случае использования единой системы идентификации и аутентификации соблюдение требований к обеспечению защиты информации в соответствии с Техническими требованиями к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия, утвержденными приказом Министерства связи и массовых коммуникаций Российской Федерации от 23 июня 2015 года № 210 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия», зарегистрированным Министерством юстиции Российской Федерации 25 августа 2015 года № 38668, 2 июня 2017 года № 46934.

2.9.3. Технология обработки защищаемой информации, применяемая при формировании (подготовке), передаче и приеме электронных сообщений,

должна обеспечивать следующие мероприятия:

проверку правильности заполнения полей электронного сообщения и прав владельца электронной подписи (входной контроль);

структурный контроль электронных сообщений;

защиту защищаемой информации при ее передаче по каналам связи.

2.9.4. Технология обработки защищаемой информации, применяемая при удостоверении права субъектов взаимодействия бюро кредитных историй на совершение действий с защищаемой информацией, должна обеспечивать получение электронных сообщений субъекта взаимодействия, подписанных субъектом взаимодействия способом, указанным в пункте 2.8 настоящего Положения.

2.10. Бюро кредитных историй должны обеспечивать регистрацию результатов совершения следующих действий, связанных с осуществлением доступа к защищаемой информации:

идентификация, аутентификация и авторизация субъектов взаимодействия при совершении действий с кредитными историями;

прием электронных сообщений от субъектов взаимодействия;

направление электронных сообщений субъектам взаимодействия;

прием (передача) электронных сообщений при взаимодействии бюро кредитных историй с субъектами взаимодействия и другими бюро кредитных историй, в том числе для удостоверения права субъектов взаимодействия осуществлять действия с защищаемой информацией и для учета результатов осуществления действий с кредитными историями;

осуществление доступа работников бюро кредитных историй (далее – работники) к защищаемой информации и осуществление действий субъектами взаимодействия с защищаемой информацией, выполняемых с использованием автоматизированных систем, программного обеспечения.

Регистрации подлежат следующие данные о действиях, выполняемых работниками с использованием автоматизированных систем, программного обеспечения:

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

присвоенный работнику идентификатор, позволяющий установить работника в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат совершения работником действия с защищаемой информацией (успешно или неуспешно);

информация, используемая для идентификации устройств, при помощи которых либо в отношении которых осуществлен доступ к автоматизированной системе, программному обеспечению в целях совершения работником действий с защищаемой информацией.

Регистрации подлежат следующие данные о действиях, выполняемых субъектами взаимодействия с использованием автоматизированных систем, программного обеспечения:

дата (день, месяц, год) и время (часы, минуты, секунды) совершения субъектом взаимодействия действий с защищаемой информацией;

присвоенный субъекту взаимодействия идентификатор, позволяющий установить субъекта взаимодействия в автоматизированной системе, программном обеспечении;

код, соответствующий технологическому участку;

результат совершения субъектом взаимодействия действия с защищаемой информацией (успешно или неуспешно);

информация, используемая для идентификации устройств, при помощи которых либо в отношении которых осуществлен доступ к автоматизированной системе, программному обеспечению в целях совершения субъектом взаимодействия действий с защищаемой информацией.

2.11. Бюро кредитных историй должны осуществлять регистрацию событий, которые привели или по их оценке могут привести к неоказанию услуг, предоставляемых бюро кредитных историй, связанных с нарушением

требований к обеспечению защиты информации, в том числе включенных в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и размещаемый Банком России на официальном сайте Банка России в сети «Интернет» (далее соответственно – инциденты защиты информации, перечень типов инцидентов), а также представлять сведения о выявленных инцидентах защиты информации должностному лицу (отдельному структурному подразделению), ответственному за управление рисками, при наличии указанного должностного лица (отдельного структурного подразделения) в соответствии с внутренними документами указанных бюро кредитных историй при соблюдении следующих требований.

По каждому инциденту защиты информации бюро кредитных историй должны осуществлять регистрацию следующей информации:

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

результата реагирования на инцидент защиты информации.

2.12. Бюро кредитных историй должны осуществлять информирование Банка России:

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

о принадлежащих бюро кредитных историй и (или) администрируемых в их интересах сайтах в сети «Интернет», которые используются бюро кредитных историй для осуществления своей деятельности;

о планируемых мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах в сети «Интернет», в отношении инцидентов защиты информации

не позднее одного рабочего дня до дня проведения мероприятия.

Бюро кредитных историй должны предоставлять в Банк России сведения, указанные в абзацах втором – четвертом настоящего пункта, с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае технической невозможности взаимодействия бюро кредитных историй с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России бюро кредитных историй должны предоставлять в Банк России сведения с использованием резервного способа взаимодействия. Информация о технической инфраструктуре (автоматизированной системе) Банка России, резервном способе взаимодействия, форме и сроках направления сведений размещается на официальном сайте Банка России в сети «Интернет».

2.13. Бюро кредитных историй должны обеспечивать:

хранение защищаемой информации, информации о регистрации данных, указанных в пункте 2.10 настоящего Положения, и информации об инцидентах защиты информации;

целостность и доступность защищаемой информации, информации о регистрации данных, указанных в пункте 2.10 настоящего Положения, и информации об инцидентах защиты информации в течение пяти лет с даты ее формирования бюро кредитных историй (даты поступления в бюро кредитных историй), а в случае если законодательством Российской Федерации, регулирующим деятельность бюро кредитных историй установлен иной срок – на срок, установленный законодательством Российской Федерации, регулирующим деятельность бюро кредитных историй.

Глава 3. **Заключительные положения**

3.1. Настоящее Положение не распространяется на отношения,

регулируемые Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736).

3.2. Настоящее Положение в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от ___№ __) вступает в силу с 1 октября 2022 года, за исключением положений, для которых настоящим пунктом установлены иные сроки вступления их в силу.

Пункты 2.3, 2.4, 2.7 настоящего Положения вступают в силу с 1 октября 2023 года.

Абзац первый пункта 2.6 настоящего Положения вступает в силу с 1 октября 2023 года и действует до 1 октября 2024 года.

Абзац второй пункта 2.6 настоящего Положения вступает в силу с 1 октября 2024 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Согласовано:

Директор
Федеральной службы безопасности
Российской Федерации А.В. Бортников

Директор
Федеральной службы по техническому
и экспортному контролю В.В. Селин