ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

ПОЛОЖЕНИЕ

«17» октября 2022 г. № 808-П

г. Москва

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 71409
от "07" декабря 2022 г.

О требованиях к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательных для лиц, оказывающих профессиональные услуги на финансовом рынке, к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона «О кредитных историях», при ее обработке, хранении и передаче сертифицированными средствами защиты, а также к сохранности информации, полученной в процессе деятельности кредитного рейтингового агентства

Настоящее Положение на основании статьи 76^{9-6} Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»[1], части 2 статьи 7 Федерального закона от 30 декабря 2004 года № 218-ФЗ «О кредитных историях»[2], части 13 статьи 9 Федерального закона от 13 июля 2015 года № 222-ФЗ «О деятельности кредитных рейтинговых агентств в Российской Федерации, о внесении

[1] Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2021, № 27, ст. 5187.
[2] Собрание законодательства Российской Федерации, 2005, № 1, ст. 44; 2020, № 31, ст. 5061.

изменения в статью 76[1] Федерального закона «О Центральном банке Российской Федерации (Банке России)» и признании утратившими силу отдельных положений законодательных актов Российской Федерации»[1] 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;

требования к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона от 30 декабря 2004 года № 218-ФЗ «О кредитных историях»[2], при ее обработке, хранении и передаче сертифицированными средствами защиты;

требования к сохранности и защите информации, полученной в процессе деятельности кредитного рейтингового агентства.

Глава 1. Требования к обеспечению защиты информации при осуществлении деятельности в сфере оказания профессиональных услуг на финансовом рынке в целях противодействия осуществлению незаконных финансовых операций, обязательные для лиц, оказывающих профессиональные услуги на финансовом рынке

1.1. Лица, оказывающие профессиональные услуги на финансовом рынке, должны обеспечить защиту информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой лицами, оказывающими профессиональные услуги на финансовом рынке, с использованием автоматизированных систем, программного обеспечения,

---

[1] Собрание законодательства Российской Федерации, 2015, № 29, ст. 4348.
[2] Собрание законодательства Российской Федерации, 2005, № 1, ст. 44; 2022, № 13, ст. 1960.

средств вычислительной техники, телекоммуникационного оборудования (далее при совместном упоминании – объекты информационной инфраструктуры) в рамках:

обеспечения защиты информации при управлении доступом;

обеспечения защиты вычислительных сетей;

контроля целостности и защищенности объектов информационной инфраструктуры;

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

предотвращения утечек информации;

управления инцидентами защиты информации;

защиты среды виртуализации;

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

1.2. Лица, оказывающие профессиональные услуги на финансовом рынке, должны определить во внутренних документах состав и порядок применения организационных и технических мер в рамках процессов (направлений) защиты информации, указанных в пункте 1.1 настоящего Положения.

1.3. Лица, оказывающие профессиональные услуги на финансовом рынке, должны осуществлять свою деятельность в рамках процессов (направлений) защиты информации, указанных в пункте 1.1 настоящего Положения, с помощью средств криптографической защиты информации (далее – СКЗИ) в соответствии с технической документацией на СКЗИ, а также в соответствии со следующими федеральными законами и иными нормативными правовыми актами Российской Федерации:

Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной

подписи»[1] (далее – Федеральный закон «Об электронной подписи»);

Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»[2] (далее – Федеральный закон «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»[3];

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»[4];

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)»[5] (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

---

[1] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2022, № 79, ст. 5306.
[2] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233.
[3] Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257.
[4] Зарегистрирован Минюстом России 14 мая 2013 года, регистрационный № 28375, с изменениями, внесенными приказом ФСТЭК России от 23 марта 2017 года № 49 (зарегистрирован Минюстом России 25 апреля 2017 года, регистрационный № 46487), приказом ФСТЭК России от 14 мая 2020 года № 68 (зарегистрирован Минюстом России 8 июля 2020 года, регистрационный № 58877).
[5] 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).

каждого из уровней защищенности»[1].

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

1.5. Требования к обеспечению защиты информации, установленные в пунктах 1.1–1.3, в абзаце первом пункта 1.4 настоящего Положения, не распространяются на лиц, осуществляющих актуарную деятельность.

Лица, осуществляющие актуарную деятельность, должны осуществлять мероприятия по защите информации от воздействия вредоносных кодов.

При применении усиленной квалифицированной электронной подписи лица, осуществляющие актуарную деятельность, должны выполнять требования эксплуатационной документации к средствам электронной подписи.

---

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

Глава 2. Требования к обеспечению бюро кредитных историй защиты информации, указанной в статье 4 Федерального закона от 30 декабря 2004 года № 218-ФЗ «О кредитных историях», 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, хранении и передаче сертифицированными средствами защиты, в том числе при взаимодействии бюро кредитных историй с пользователями кредитных историй, источниками формирования кредитных историй, субъектами кредитных историй (далее соответственно – защищаемая информация, субъекты взаимодействия).

В случае если защищаемая информация содержит персональные данные, бюро кредитных историй должны применять меры по обеспечению безопасности персональных данных при их обработке в соответствии со статьей 19 Федерального закона «О персональных данных»[1].

2.2. Бюро кредитных историй должны формировать для субъектов взаимодействия рекомендации по защите информации от воздействия вредоносных кодов в целях противодействия неправомерному разглашению и незаконному использованию защищаемой информации.

Бюро кредитных историй должны доводить до субъектов взаимодействия следующую информацию:

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

---

[1] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2022, № 29, ст. 5233.

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, по контролю конфигурации устройства, с использованием которого субъектом взаимодействия совершаются действия в целях обработки, хранения и передачи защищаемой информации, и своевременному обнаружению воздействия вредоносных кодов.

2.3. 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 использовать для обработки, хранения и передачи защищаемой информации прикладное программное обеспечение автоматизированных систем и приложений, распространяемых бюро кредитных историй среди субъектов кредитных историй для совершения действий в целях обработки, хранения и передачи защищаемой информации, прошедших сертификацию в системе сертификации федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, 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[1].

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

По решению бюро кредитных историй оценка соответствия в прикладном программном обеспечении автоматизированных систем и приложений проводится самостоятельно или 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[2].

2.5. 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 использовать установленные нормативными актами Банка России, регулирующими деятельность бюро кредитных историй, виды усиленной электронной подписи при передаче электронных сообщений между:

бюро кредитных историй и источниками формирования кредитных

---

[1] М., ФГУП «Стандартинформ», 2014.

[2] Собрание законодательства Российской Федерации, 2012, № 7, ст. 863; 2016, № 26, ст. 4049.

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»[1];

бюро кредитных историй и субъектами кредитных историй;

бюро кредитных историй между собой;

бюро кредитных историй и Банком России.

Бюро кредитных историй могут обеспечить использование простой электронной подписи при передаче в бюро кредитных историй электронных сообщений от субъектов кредитных историй.

В случае если бюро кредитных историй при передаче электронных сообщений между субъектами, указанными в настоящем пункте, использует усиленную неквалифицированную электронную подпись, то для ее создания и проверки должны применяться СКЗИ и средства удостоверяющего центра, имеющие сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности в соответствии с пунктом 2 части 4 статьи 5 Федерального закона «Об электронной подписи»[2].

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»[3].

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

2.6. Бюро кредитных историй в части требований к защите информации, применяемых в отношении технологии обработки информации, обрабатываемой, передаваемой и хранимой на участках идентификации,

---

[1] Собрание законодательства Российской Федерации, 2005, № 1, ст. 44; 2020, № 31, ст. 5061.
[2] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2016, № 1, ст. 65.
[3] Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; 2019, № 52, ст. 7794.

аутентификации и авторизации субъектов взаимодействия при совершении действий в целях обработки, хранения и передачи защищаемой информации, формированию (подготовке), передаче и приему электронных сообщений, удостоверению права субъектов взаимодействия на совершение действий с защищаемой информацией, осуществлению действий в целях обработки, хранения и передачи защищаемой информации (далее – действия с кредитными историями), учету результатов осуществления действий с кредитными историями, хранению электронных сообщений и информации об осуществленных действиях с защищаемой информацией (далее – технологические участки) должны обеспечивать:

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.

2.6.1. 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.

2.6.2. 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[1].

2.6.3. 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.

2.6.4. Технология обработки защищаемой информации, применяемая при удостоверении бюро кредитных историй права субъектов взаимодействия на совершение действий с защищаемой информацией, должна обеспечивать получение электронных сообщений субъекта взаимодействия, подписанных субъектом взаимодействия способом, указанным в пункте 2.5 настоящего Положения.

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

идентификации, аутентификации и авторизации субъектов взаимодействия при совершении действий с кредитными историями;

приема (передачи) 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;

осуществления доступа работников бюро кредитных историй (далее – работники) к защищаемой информации и осуществления субъектами взаимодействия действий с защищаемой информацией,

---

[1] Зарегистрирован Минюстом России 25 августа 2015 года, регистрационный № 38668, с изменениями, внесенными приказом Минкомсвязи России от 22 февраля 2017 года № 71 (зарегистрирован Минюстом России 2 июня 2017 года, регистрационный № 46934).

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 субъект 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.

2.8. 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 следующего требования.

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

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

результата реагирования на инцидент защиты информации.

2.9. 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) об

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».

2.10. Бюро кредитных историй должны:

хранить защищаемую информацию, информацию о регистрации данных, указанных в пункте 2.7 настоящего Положения, и информацию об инцидентах защиты информации;

обеспечивать целостность и доступность защищаемой информации, информации о регистрации данных, указанных в пункте 2.7 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. Требования к сохранности и защите информации, полученной в процессе деятельности кредитного рейтингового агентства

3.1. Кредитное рейтинговое агентство на постоянной основе должно обеспечивать сохранность следующей информации:

информации, полученной кредитным рейтинговым агентством в процессе своей деятельности, включая договоры кредитного рейтингового агентства, протоколы (записи) встреч представителей кредитного рейтингового агентства с представителями рейтингуемых лиц, переписку представителей кредитного рейтингового агентства с рейтингуемыми лицами, отчетность и иную информацию рейтингуемых лиц, представленную кредитному рейтинговому агентству, сведения (сообщения, данные) независимо от формы их представления, полученные кредитным рейтинговым агентством от рейтингуемого лица;

информации, полученной кредитным рейтинговым агентством в процессе рейтинговой деятельности, включая информацию о рейтинговых действиях до раскрытия такой информации в соответствии со статьей 14 Федерального закона от 13 июля 2015 года № 222-ФЗ «О деятельности кредитных рейтинговых агентств в Российской Федерации, о внесении изменения в статью 76^1 Федерального закона «О Центральном банке Российской Федерации (Банке России)» и признании утратившими силу отдельных положений законодательных актов Российской Федерации»[1], информацию, связанную с подготовкой и осуществлением рейтинговых действий, осуществляемых группой рейтинговых аналитиков, включая ее председателя, принимающей решение о рейтинговых действиях (далее – рейтинговый комитет), в том числе материалы анализа, проводимого рейтинговыми аналитиками, включая рейтинговые отчеты, материалы заседаний рейтинговых комитетов;

информации ограниченного доступа, определяемой в качестве таковой в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ

[1] Собрание законодательства Российской Федерации, 2015, № 29, ст. 4348.

«Об информации, информационных технологиях и о защите информации»[1] и (или) с договором с рейтингуемым лицом.

3.2. В целях обеспечения сохранности защищаемой информации, указанной в пункте 3.1 настоящего Положения (далее – защищаемая информация, полученная в процессе деятельности кредитного рейтингового агентства), кредитное рейтинговое агентство должно:

предупреждать неправомерный доступ, уничтожение, модифицирование, блокирование, копирование, представление, распространение защищаемой информации, полученной в процессе деятельности кредитного рейтингового агентства;

обеспечивать полноту, точность и актуальность защищаемой информации, полученной в процессе деятельности кредитного рейтингового агентства;

не допускать воздействие на объекты информационной инфраструктуры, в том числе на официальный сайт кредитного рейтингового агентства в сети «Интернет», в результате которого нарушается их функционирование;

хранить защищаемую информацию, полученную в процессе деятельности кредитного рейтингового агентства, на территории Российской Федерации и обеспечивать возможность ее восстановления в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники, в том числе создавать ее резервные копии в электронном виде с периодичностью, установленной кредитным рейтинговым агентством, но не реже одного раза в семь дней;

размещать резервные копии защищаемой информации, полученной в процессе деятельности кредитного рейтингового агентства, в местах, отличных от мест размещения ее носителей;

обеспечивать сохранность защищаемой информации, полученной в процессе деятельности кредитного рейтингового агентства, при взаимодействии с третьими лицами, которым предоставляется к ней доступ;

разработать внутренние документы, регламентирующие порядок обеспечения сохранности защищаемой информации, полученной в процессе

[1] Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2022, № 29, ст. 5292.

деятельности кредитного рейтингового агентства, определяющие ее состав, а также состав лиц, ответственных за ее хранение и уничтожение, место и форму ее хранения, порядок работы с ней, включающий следующие процедуры:

документирование защищаемой информации, полученной в процессе деятельности кредитного рейтингового агентства, в том числе в ходе подготовки и проведения заседаний рейтингового комитета, методологического комитета, работы органов внутреннего контроля;

хранение защищаемой информации, полученной в процессе деятельности кредитного рейтингового агентства, в течение сроков, установленных Федеральным законом от 22 октября 2004 года № 125-ФЗ «Об архивном деле в Российской Федерации»[1], но не менее пяти лет;

уничтожение защищаемой информации, полученной в процессе деятельности кредитного рейтингового агентства.

Глава 4. **Заключительные положения**

4.1. При обеспечении безопасности объектов информационной инфраструктуры, эксплуатация и использование которых осуществляются бюро кредитных историй 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»[2].

4.2. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 12 мая 2022 года № ПСД-32) вступает в силу с 1 апреля 2023 года, за исключением пункта 2.4 настоящего Положения.

Пункт 2.4 настоящего Положения вступает в силу с 1 апреля 2024 года.

---

[1] Собрание законодательства Российской Федерации, 2004, № 43, ст. 4169; 2022, № 29, ст. 5306.
[2] Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736.

4.3. Со дня вступления в силу настоящего Положения признать утратившим силу Указание Банка России от 20 мая 2016 года № 4023-У «О требованиях к сохранности и защите информации, полученной в процессе деятельности кредитного рейтингового агентства»[1].

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

СОГЛАСОВАНО:

Директор
Федеральной службы безопасности
Российской Федерации

_____ А.В. Бортников

_____ 2022 г.

Директор
Федеральной службы по техническому
и экспортному контролю

_____ В.В. Селин

_____ 2022 г.

[1] Зарегистрировано Минюстом России 10 июня 2016 года, регистрационный № 42511.