Утвержден
Генеральным директором АО «БКИ СБ» О.И. Лагуткиным
Приказ № 2026/05/04-1 от «04» мая 2026 г.

Приложение № 2 к Договору об оказании информационных услуг (договор присоединения) (далее – Договор)

Регламент электронного взаимодействия

Термины и определения

В настоящем Регламенте используются следующие термины и определения:

Администратор Партнера – работник (иное уполномоченное лицо) Партнера, на которого возложена ответственность за взаимодействие с Бюро и контролю над Операторами Партнера, а также за взаимодействие с файл-сервером Бюро;

Администратор файл-сервера – работник (иное уполномоченное лицо) Партнера, на которого возложена ответственность за взаимодействие с файл-сервером Бюро;

База данных – специальным образом структурированная обновляемая электронная база данных Бюро, хранящая кредитные истории субъектов кредитной истории;

Безопасность информации (информационная безопасность):

1) состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п.

2) состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз;

Бюро – Акционерное общество «Бюро кредитных историй «Скоринг Бюро» ИНН 7708429953, ОГРН 1247700058319.

Ключ (Криптографический ключ) – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований;

Ключевой носитель – любой электронный носитель информации, на котором хранится секретный ключ;

Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но, не ограничиваясь, следующие: утрата ключевых носителей; утрата ключевых носителей с последующим обнаружением; увольнение сотрудников, имевших доступ к ключевой информации; нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа; возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи; нарушение печати на сейфе с ключевыми дискетами; случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника);

Оператор Партнера – работник (иное уполномоченное лицо) Партнера, на которого возложена функция направления запросов в Бюро на получение кредитных отчетов;

Программное обеспечение (ПО) – совокупность данных, команд, предназначенных для функционирования ЭВМ;

Система – автоматизированная система Бюро, с помощью которой оказываются услуги по формированию, обработке и хранению кредитных историй, а также по предоставлению кредитных отчетов и сопутствующих услуг;

СКЗИ – средства криптографической защиты информации;

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1. Общие положения

1.1. Настоящий Регламент описывает процессы взаимодействия Сторон в целях организации безопасной передачи электронных документов, подписанных Электронной подписью, между Сторонами в рамках, определенных Договором, заключенным между Сторонами, и устанавливает обязательства Сторон по обеспечению информационной безопасности при обмене электронными документами.

1.2. Термины, применяемые в настоящем Регламенте, если из контекста не следует иное, понимаются в смысле, указанном в Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи». Стороны признают, что методы и системы защиты информации, шифрования, используемые между Сторонами в соответствии с настоящим Регламентом достаточны для обеспечения конфиденциальности, подтверждения целостности передаваемых сообщений, подлинности авторства, а также разбора конфликтных ситуаций по ним. Стороны принимают к использованию для осуществления электронной передачи документов в Системе программное средство криптографической защиты, сертифицированное ФСБ России.

1.3. Для электронного взаимодействия Стороны используют усиленную неквалифицированную электронную подпись. В случаях, если в Договоре и иных документах применительно к договору между Сторонами, используется термины «электронно-цифровая подпись» и (или) «электронная подпись» и не указано иное, то имеется в виду усиленная неквалифицированная электронная подпись.

1.4. Стороны признают, что используемые во взаимоотношениях между Бюро и Партнером электронные документы, подписанные действующей на момент передачи Электронной подписью отправителя, подготовленные и переданные с помощью программного обеспечения Системы в соответствии со всеми процедурами защиты информации, предусмотренными настоящим Регламентом и эксплуатационной документацией на средства криптографической защиты информации (СКЗИ), признаются равнозначным документам на бумажном носителе, подписанным уполномоченным лицом организации-отправителя с проставлением печати (при ее наличии), и имеют соответствующую юридическую силу, в частности, могут порождать для Сторон соответствующие права и обязанности.

1.5. Порядок формирования и проверки Электронной подписи должен соответствовать следующим требованиям:
- сертификат ключа проверки электронной подписи действителен на момент подписания электронного документа (при наличии достоверной информации о моменте подписания электронного документа) или на день проверки действительности указанного сертификата, если момент подписания электронного документа не определен;

- имеется положительный результат проверки принадлежности владельцу сертификата ключа проверки электронной подписи, с помощью которой подписан электронный документ, и подтверждено отсутствие изменений, внесенных в этот документ после его подписания;
- электронная подпись используется с учетом ограничений, содержащихся в сертификате ключа проверки электронной подписи лица, подписывающего электронный документ (если такие ограничения установлены).

1.6. Формирование и проверка Электронной подписи электронного документа осуществляется с использованием сертифицированного средства электронной подписи.

1.7. Стороны признают, что применение усиленной неквалифицированной электронной подписи Партнера, выданной Бюро, а также усиленной неквалифицированной электронной подписи Бюро является безусловным доказательством того, что электронный документ действительно исходит от соответствующей Стороны, и сформирован и подписан уполномоченным лицом и не претерпел изменений при информационном взаимодействии Сторон.

1.8. Такие сведения, как персональные адреса электронной почты, идентификационные пароли, регистрационные номера, пароли и криптографические ключи обеих Сторон, используемые для разграничения доступа, передачи и защиты информации, а также материалы разбора конфликтных ситуаций являются конфиденциальной информацией и не подлежат разглашению Сторонами.

2. Обеспечение защищенного соединения для взаимодействия с Бюро

2.1. Для обеспечения безопасного взаимодействия Стороны организуют защищенное соединение на основе криптоалгоритмов между программными средствами Партнера и Системы Бюро через информационно-телекоммуникационную сеть «Интернет».

2.2. Стороны соглашаются, что обеспечение защищенного соединения между программными средствами Партнера и Системы Бюро через информационно-телекоммуникационную сеть «Интернет» реализуется следующим способом: посредством TLS-соединения с использованием криптографических алгоритмов ГОСТ, с аутентификацией Партнера по клиентскому сертификату защищенного соединения.

3. Порядок подключения и работы Партнера в Системе Бюро

3.1. Партнер предоставляет Бюро заявку на подключение к Системе по форме, указанной в Приложении № 1 к настоящему Регламенту (в случае если Партнер является юридическим лицом или индивидуальным предпринимателем) или Приложении № 1а к настоящему Регламенту (в случае если Партнер является арбитражным управляющим). При подключении Партнера к Системе Бюро в заявке необходимо указать номер мобильного телефона Администратора Партнера.

3.2. Процедура **получения сертификата защищенного соединения:**

3.2.1. Партнер формирует файл запроса на получение сертификата защищенного соединения по инструкции (которая предоставляется Бюро на этапе переговоров и (или) заключения Договора) по форме, указанной в Приложении № 3 к настоящему Регламенту, и отправляет его и соответствующие сопроводительные документы на электронную почту сотрудника Департамента продаж Бюро, являющегося контактным лицом для Партнера.

3.2.2. Бюро отправляет сертификат защищенного соединения на электронную почту Партнеру. Под «сертификатом защищенного соединения» понимается соответствующий файл, использование которого на ЭВМ Партнера требуется для обеспечения защищенного соединения в рамках выбранной процедуры в соответствии с инструкциями Бюро.

3.3. Подробные инструкции Администратора Партнера и Оператора Партнера изложены в соответствующих документах и доступны Партнеру для скачивания на соответствующем веб-ресурсе.

3.4. Для добавления Администратора Партнера и (или) Администратора файл-сервера Партнеру необходимо направить в Бюро заявление, форма которого приведена в Приложении № 5.1 к настоящему Регламенту. Для блокировки Администратора Партнера и (или) Администратора файл-сервера Партнеру необходимо направить в Бюро заявление, форма которого приведена в Приложении № 5.2 к настоящему Регламенту.

3.5. Для изменения данных Администратора Партнера и (или) Администратора файл-сервера Партнеру необходимо направить в Бюро заявление, форма которого приведена в Приложении № 6 к настоящему Регламенту. Добавление/блокировка и изменение данных Администраторов Партнера и Администраторов файл-сервера при этом осуществляется Бюро.

3.6. Администратор Партнера выполняет действия по добавлению/блокировке/разблокировке или изменению данных Операторов Партнера самостоятельно.

3.7. Бюро оставляет за собой право добавлять учетные записи, которые могут использоваться при регистрации в Системе Бюро предоставляемого Партнеру открытого ключа шифрования и ЭП.

4. Формирование ключей шифрования и электронной подписи

4.1. Полномочия лиц, осуществляющих формирование индивидуальной ключевой информации и сертификацию открытых ключей, определяются на основании доверенности, форма которой приведена в Приложении № 2 к настоящему Регламенту. В случае использования иной формы доверенности она должна содержать в своём тексте формулировки полномочий тождественные или аналогичные указанным в форме доверенности.

4.2. Формирование ключей шифрования и ЭП Партнера осуществляется на автоматизированном рабочем месте Администратора Партнера при помощи программного обеспечения, имеющего действующий сертификат соответствия ФСБ России на момент формирования ключей шифрования и ЭП Партнера. Соответствующие инструкции по установке и применению ПО приведены в отдельных документах, высылаемых Партнеру по запросу в службу технической поддержки Бюро.

4.3. Регистрационная карточка запроса на сертификат открытого ключа шифрования и ЭП распечатывается в двух экземплярах и заверяется подписью и печатью (при ее наличии) уполномоченного лица Партнера, один экземпляр хранится у Партнера, второй высылается в Бюро. В карточке запроса необходимо указать *код запроса,* который сгенерировало используемое ПО СКЗИ. Форма регистрационной карточки запроса на сертификат открытого ключа шифрования и ЭП приведена в Приложении № 3 к настоящему Регламенту.

4.4. Бюро предоставляет Партнеру сертификат открытого ключа шифрования.

4.5. Для отзыва сертификата открытого ключа шифрования и ЭП Партнеру необходимо направить в адрес службы технической поддержки Бюро заявление на отзыв сертификата, форма которого приведена в Приложении № 4 к настоящему Регламенту.

4.6. Партнер при необходимости, совместно со службой технической поддержки Бюро, проводит установку и настройку необходимого для подключения к Системе ПО.

5. Правила формирования файлов кредитных историй для передачи в Бюро

5.1. Партнеру предоставляется возможность передавать файлы содержащие кредитные истории в Бюро в формате b2b – после предварительного тестирования на условиях, определённых соглашением Сторон.

5.2. Порядок передачи и описания форматов взаимодействия приведены в отдельных документах, высылаемых Партнеру по его запросу в службу технической поддержки Бюро.

6. Порядок формирования запросов для запроса кредитной истории

6.1. Партнеру предоставляется возможность осуществлять запросы кредитных отчетов в Бюро следующими способами:
- в формате b2b;
- через web-интерфейс Бюро.

6.2. Все инструкции и описания форматов приведены в отдельных документах, высылаемых Партнеру по запросу в службу технической поддержки Бюро.

7. Права и обязанности Сторон

7.1. Права и обязанности Партнера.

7.1.1. Партнер назначает своих ответственных должностных лиц, имеющих право работать с Системой, с указанием их полномочий и срока действия таких полномочий.

7.1.2. Партнер обязуется выдавать доверенность лицам, уполномоченным Партнером для обмена электронными документами в рамках электронного взаимодействия с Системой, и предоставить их в Бюро либо предоставить документы, подтверждающие правомочия лица выступать от имени Партнера без доверенности. Партнер обязан самостоятельно следить за изменениями и истечением срока полномочий, указанных в настоящем пункте лиц, своевременно информировать Бюро об этих изменениях в письменном виде, предоставлять новые документы по истечении срока действия предыдущих. При этом отслеживание актуальности полномочий является обязанностью Партнера.
Риск неправомерного подписания электронного документа третьими лицами с использованием электронной подписи Партнера несет Партнер, которому принадлежит электронная подпись. Бюро не несет ответственности перед Стороной в случае неправомерного подписания электронного документа третьими лицами и с использованием электронной подписи Партнера.

7.1.3. Партнер обязуется использовать ключи электронной подписи исключительно для электронного взаимодействия с Системой в соответствии с настоящим Регламентом электронного взаимодействия, и прекратить их использование в случае прекращения действия соответствующих договоров. Ответственность за использование ключей электронной подписи в иных целях лежит на Партнере.

7.1.4. Партнер обеспечивает доработку своей автоматизированной системы для организации безопасного взаимодействия с Бюро.

7.1.5. Партнер обязан:
- Соблюдать положения документов, регламентирующих функционирование Системы со встроенными средствами криптографической защиты информации.
- Эксплуатировать сертифицированные средства криптографической защиты информации в соответствии с условиями сертификатов на данные средства.
- Выполнять условия и требования эксплуатационной документации на средства криптографической защиты информации.
- Допускать к эксплуатации СКЗИ только уполномоченных сотрудников, прошедших необходимую подготовку по применению данных средств и допущенных к работе с ними на основании приказа Партнера, обеспечить персонализацию выдачи и внутреннего учета логинов, используемых ответственными сотрудниками по работе с Бюро.
- Обеспечить соответствие Рекомендациям Бюро по обеспечению информационной безопасности, указанным в Приложении № 7 к настоящему Регламенту (далее – Рекомендации Бюро по обеспечению информационной безопасности).
- Обеспечивать безопасность полученной от Бюро информации при ее дальнейшей обработке, в т.ч. при хранении.
- Обеспечивать сохранность и целостность программного обеспечения Системы.
- Сохранять конфиденциальность и подлинность своих секретных ключей и паролей.
- Нести риск последствий, вызванных нарушением конфиденциальности и подлинности ключей и паролей.
- Извещать Бюро обо всех случаях компрометации криптографических ключей Партнера.
- Письменно уведомить Бюро о необходимости замены ключа СКЗИ.
- Обеспечить эксплуатацию автоматизированных рабочих мест, подключенных к Системе, в соответствии с инструкциями Бюро.
- Размещать автоматизированные рабочие места, подключенные к Системе, в охраняемом помещении, оборудованной системой охранной сигнализации, исключающей доступ в помещение посторонних лиц.
- Хранить носители с криптографическими ключами в металлических шкафах (сейфах), исключающих несанкционированный доступ к ним посторонних лиц.
- Оборудовать системные блоки компьютеров автоматизированных рабочих мест средствами защиты от несанкционированного вскрытия.
- Учитывать криптографические ключи и их носители в выделенных для этих целей журналах.
- При уничтожении полученной от Бюро информации, в т.ч. электронных сообщений, использовать методы, гарантирующие невозможность восстановления уничтоженной информации.
- Предоставить по запросу Бюро в срок, не превышающий 2 (две) недели с момента получения запроса Бюро, документы и (или) сведения, подтверждающие соблюдение Партнером Рекомендаций Бюро по обеспечению информационной безопасности.
- Предоставлять по запросу Бюро, в срок, указанный в запросе, сведения и (или) документы, подтверждающие факт наличия законных оснований для передачи персональных данных работников или представителей Партнера.
- Не использовать по отношению к Системе:
  - сканеры портов и анализаторы трафика;
  - ПО, предназначенное для сокрытия или внедрения дополнительной информации в цифровые объекты (в том числе реализующее методы стеганографии);

- ПО для обхода средств защиты, включая средства подбора и восстановления паролей, поиска уязвимостей;
- специализированные программные средства, оказывающее влияние на сетевые настройки средств вычислительной техники, серверов и сетевого оборудования.

- Незамедлительно письменно уведомлять Бюро об изменении данных Администратора Партнера и (или) Администратора файл-сервера по форме, утвержденной Приложением № 6 к настоящему Регламенту. Партнер несет риск юридических последствий, связанных с неуведомлением Бюро об изменении данных Администратора Партнера и (или) Администратора файл-сервера.

7.2. Права и обязанности Бюро.

7.2.1. Бюро обязано:

- Оказывать консультативную поддержку Партнеру по телефону и по электронной почте в рабочие часы Бюро по московскому времени.
- Сохранять конфиденциальность и подлинность используемых секретных ключей и паролей.
- Протоколировать все случаи и попытки нарушения безопасности Системы. При возникновении таких случаев принимать все возможные меры для предотвращения и/или ликвидации их последствий вплоть до приостановления функционирования Системы.
- В случае компрометации криптографических ключей Партнера заблокировать открытые криптографические ключи Партнера до завершения внеплановой смены криптографических ключей.
- Своевременно информировать Партнера об изменениях порядка осуществления приема/передачи электронных документов и другой информации по Системе.
- Оказывать консультационные услуги Партнеру по вопросам функционирования Системы и использования СКЗИ.
- Соблюдать положения документов, регламентирующих функционирование Системы.
- За 1 (один) календарный месяц до истечения срока действия сертификата направить Партнеру электронное письмо с напоминанием о скором истечении срока действия сертификата.
- Направить уведомление Администратору Партнера о приостановке приема сведений и необходимости направления достоверных сведений в случае, если переданные Партнером в Бюро сведения в отношении субъекта кредитной истории отвечают признакам недостоверности, установленным Банком России. Уведомление направляется на e-mail Администратора Партнера, указанный в заявке на подключение к автоматизированной системе (Приложения № 1, № 1а к настоящему Регламенту), а в случае изменения данных – на уточненный e-mail, указанный в заявлении на изменение данных Администратора Партнера (Приложение № 6 к настоящему Регламенту). Электронные файлы, содержащие сведения о выявленных Бюро фактах передачи Партнером недостоверных сведений размещаются на файл-сервере в отдельную директорию в папке Партнера.
- Возобновить прием сведений от Партнера в отношении субъекта кредитной истории, в информации о котором были установлены признаки недостоверности, не позднее рабочего дня, следующего за днем предоставления Партнером достоверных сведений.

7.2.2. Бюро вправе:

- Осуществлять документарную проверку соблюдения Партнером Рекомендаций Бюро по обеспечению информационной безопасности в случае возникновений инцидентов информационной безопасности со стороны Партнера или когда есть весомые основания полагать, что подключение Партнера может повлиять на безопасность Системы и/или ИТ-инфраструктуру Бюро.
- Прекратить доступ Партнера к Системе, в случае, когда есть основания полагать, что со стороны Партнера либо под его контролем (в том числе вследствие его бездействия) осуществляются действия по несанкционированному Бюро доступу к серверам Бюро и (или) данным на них, в том числе в случае несоблюдения Рекомендаций Бюро по обеспечению информационной безопасности и требований настоящего Регламента.
- Направлять запросы Партнеру о предоставлении сведений и (или) документов, подтверждающих факт наличия законных оснований для передачи персональных данных работников или представителей Партнера.

7.2.3. Стороны обязуются обеспечить условия сохранения ключевых носителей и условия хранения и использования программного обеспечения СКЗИ, исключающие порчу и утрату ключевых носителей, а также их использование любыми другими лицами.

8. Персональные данные

8.1. Стороны договорились о том, что в соответствии с настоящим Регламентом они могут передавать друг другу персональные данные, относящиеся к работникам, представителям, уполномоченным лицам, и иным контактным лицам Сторон, в объеме, необходимом для заключения и исполнения Договора, подключения к Системе, предоставления и администрирования доступа, электронного взаимодействия Сторон.

8.2. Стороны заверяют и гарантируют правомерность передачи персональных данных друг другу и последующей обработки полученных друг от друга персональных данных в соответствии с настоящим Регламентом с соблюдением требований применимого законодательства, а также наличие надлежащих правовых оснований для такой передачи и последующей обработки, включая получение согласия субъекта персональных данных и (или) его надлежащее уведомление в случаях, когда это требуется применимым законодательством.

8.3. Если иное прямо не предусмотрено отдельным договором, приложением к договору, поручением на обработку персональных данных либо иным письменным соглашением Сторон применительно к конкретной услуге, каждая из Сторон признает, что является самостоятельно действующим оператором в отношении персональных данных, передаваемых Сторонами друг другу в рамках настоящего Регламента.

8.4. Обработка персональных данных иных субъектов персональных данных, а также обработка персональных данных в рамках отдельных услуг, по которым между Сторонами согласованы специальные условия обработки персональных данных, осуществляется на основании соответствующего договора, приложения к договору, поручения на обработку персональных данных или иного письменного соглашения Сторон. В соответствующей части такие специальные условия имеют приоритет над положениями настоящего Регламента.

8.5. Стороны заверяют и гарантируют обеспечение конфиденциальности и безопасности получаемых друг от друга персональных данных при их обработке в соответствии с требованиями применимого законодательства.

9. Порядок действий при компрометации ключей

9.1. Сторона, допустившая утрату ключевого носителя с ключевой информацией СКЗИ, независимо от наличия или отсутствия сведений о ее несанкционированном использовании, незамедлительно сообщает об этом другой Стороне и прекращает работу с использованием СКЗИ до момента регистрации и ввода в действие новых ключей. Вышедший из-под контроля ключевой носитель может использоваться в дальнейшем только после применения к нему операции форматирования.

9.2. Сторона, допустившая порчу или утрату ключевых носителей, незамедлительно сообщает об этом другой Стороне и прекращает работу с использованием СКЗИ до момента приобретения новых ключевых носителей, регистрации и ввода в действие новых ключей.

10. Отзыв сертификатов

10.1. Отзыв сертификатов производится Бюро по письменному заявлению Партнера на отзыв сертификата, форма которого приведена в Приложении № 4 к настоящему Регламенту, в случае утраты/повреждения/невозможности использования/невостребованности ключевых носителей или в случае досрочного прекращения полномочий представителя.

10.2. Отзыв сертификатов в случае подозрений на компрометацию или в случае истечения срока полномочий доверенного лица Партнера, указанного в доверенности, может выполняться Бюро без получения от Партнера заполненного заявления на отзыв сертификата с уведомлением об этом Партнера.

11. Порядок действий при разрешении спорных ситуаций, связанных с подлинностью электронных документов

11.1. При возникновении спорных ситуаций между Сторонами, связанными с подлинностью электронных документов, несогласная Сторона должна в течение 3 (трех) рабочих дней направить другой Стороне письменное заявление, в котором должны быть изложены ее претензии.

11.2. Не позднее 10 (десяти) рабочих дней со дня получения другой Стороной заявления Бюро созывает согласительную экспертную комиссию (далее – Комиссия).

11.3. Состав Комиссии формируется из двух представителей каждой из Сторон.

11.4. Комиссия по договоренности Сторон работает на территории одной из Сторон и на ее компьютерном оборудовании. Конфигурация компьютерного оборудования, необходимая для дальнейшей экспертизы, должна соответствовать требованиям, согласованным Комиссией.

11.5. Экспертиза оспариваемого электронного документа осуществляется в присутствии всех членов Комиссии. Экспертиза осуществляется в три этапа:

11.5.1. Подготовка оборудования и программного обеспечения, тестирование их работоспособности.

11.5.2. Контроль целостности оспариваемого электронного документа путем проверки электронной подписи при помощи сертификата ключа проверки электронной подписи, предоставленного Стороной-заявителем.

11.5.3. Аутентификация отправителя оспариваемого электронного документа путем проверки принадлежности, актуальности и целостности сертификата ключа проверки электронной подписи, использованного Комиссией для проверки электронной подписи.

11.6. Подтверждением подлинности оспариваемого электронного документа является единовременное выполнение следующих условий:

11.6.1. Проверка электронной подписи оспариваемого электронного документа на сертификате ключа проверки подписи, файл которого предъявлен Стороной-заявителем, дала положительный результат.

11.6.2. Подтверждена принадлежность, актуальность и целостность сертификата ключа проверки подписи Стороны-заявителя, с помощью которого проводится проверка электронной подписи оспариваемого электронного документа.

11.7. Результаты экспертизы в течение 3 (трех) рабочих дней оформляются в виде письменного заключения – Акта экспертной комиссии, подписываемого всеми членами Комиссии (далее – Акт). Акт составляется в двух экземплярах, по одному для каждой Стороны. Акт является окончательным и пересмотру не подлежит.

11.8. Акт, составленный Комиссией, является доказательством при дальнейшем разбирательстве спора в суде.

12. Порядок внесения изменений в настоящий Регламент

12.1. Внесение изменений и дополнений в настоящий Регламент, в том числе во все приложения к нему, производится Бюро в одностороннем порядке.

12.2. При изменении положений настоящего Регламента Бюро обязано не менее чем за 30 (тридцать) календарных дней до вступления изменений в силу поместить новую редакцию настоящего Регламента на сайте Бюро в информационно-телекоммуникационной сети «Интернет» www.scoring.ru;

12.3. Изменения вступают в силу по истечении 30 (тридцати) календарных дней с даты размещения новой редакции настоящего Регламента на сайте Бюро в информационно-телекоммуникационной сети «Интернет» www.scoring.ru. Любые изменения и дополнения с момента вступления в силу равно распространяются на всех лиц, заключивших с Бюро Договор, в том числе и ранее даты вступления изменений в силу.

Список приложений

Приложение № 1	Заявка на подключение к автоматизированной системе Акционерного общества «Бюро кредитных историй «Скоринг Бюро».
Приложение № 1а	Заявка на подключение к автоматизированной системе Акционерного общества «Бюро кредитных историй «Скоринг Бюро» (для Арбитражных управляющих).
Приложение № 2	Доверенность (образец).
Приложение № 3	Регистрационная карточка запроса на сертификат открытого ключа шифрования и ЭП, и (или) сертификата защищенного соединения.
Приложение № 4	Заявление на отзыв сертификата.
Приложение № 5.1	Заявление на добавление Администратора Партнера/Администратора файл-сервера.
Приложение № 5.2	Заявление на блокировку Администратора Партнера/Администратора файл-сервера.
Приложение № 6	Заявление на изменение данных Администратора Партнера/Администратора файл-сервера.
Приложение № 7	Рекомендации Бюро по обеспечению информационной безопасности.

Приложение № 1

Генеральному директору
АО «БКИ СБ»
Лагуткину О.И.

Заявка на подключение к автоматизированной системе Акционерного общества «Бюро кредитных историй «Скоринг Бюро»

_____

(наименование организации для юридического лица

_____

или ИП ФИО индивидуального предпринимателя)

в лице _____

(должность и ФИО руководителя или ФИО индивидуального предпринимателя)

действующего на основании _____

(Устав или доверенность (номер и дата) для юридического лица

_____

или свидетельство (номер и дата) о регистрации в качестве индивидуального предпринимателя/лист записи (номер и дата) для индивидуального предпринимателя)

направляет заявку на подключение и сообщает следующее:

Ответственными лицами назначены:

По техническим вопросам (ФИО (при наличии отчества), адрес электронной почты, телефон):	Укажите ФИО, адрес электронной почты, телефон
По вопросам выгрузки данных в БКИ (ФИО (при наличии отчества), адрес электронной почты, телефон):	Укажите ФИО, адрес электронной почты, телефон
По вопросам корректировок кредитных историй (ФИО (при наличии отчества), адрес электронной почты, телефон):	Укажите ФИО, адрес электронной почты, телефон
По запросам субъектов кредитных историй (ФИО (при наличии отчества), адрес электронной почты, телефон)*: * возможно указание более одного ответственного лица	Укажите ФИО, адрес электронной почты, телефон

Администратор Партнера:

Администратор Партнера выполняет функции управления учетными записями Операторов Партнера (создание, блокирование, разблокирование и редактирование) и составления статистики по запросам.

Фамилия Имя Отчество *(при наличии отчества)*	Укажите ФИО
Адрес электронной почты	Укажите адрес электронной почты
мобильный телефон	Укажите номер мобильного телефона

Данные Партнера – юридического лица (ЮЛ)

Полное наименование ЮЛ	Укажите полное наименование юр. лица
Сокращенное наименование ЮЛ	Укажите сокращенное наименование юр. лица
Фирменное наименование ЮЛ	Укажите фирменное наименование юр. лица
Дата создания ЮЛ (Дата регистрации в качестве ЮЛ)	Укажите дату регистрации в качестве юр. лица
Тип организации (Код источника/пользователя КИ)	Выберите элемент
Признак резидентства	☐ Резидент ☐ Нерезидент
Адрес постоянно действующего исполнительного органа ЮЛ, по которому осуществляется связь	Укажите адрес
Адрес местонахождения (индекс, город/населенный пункт/поселок, улица, дом)	Укажите адрес местонахождения
Почтовый адрес (индекс, город/населенный пункт/поселок, улица, дом)	Укажите почтовый адрес
Номер(-а) телефона(-ов) постоянно действующего исполнительного органа ЮЛ	Укажите номер (-а) телефона (-ов)
Адрес электронной почты	Укажите адрес электронной почты

ОКПО	Укажите ОКПО
Основной государственный регистрационный номер (ОГРН)	Укажите ОГРН
Идентификационный номер налогоплательщика (ИНН)	Укажите ИНН
Код причины постановки на учет (КПП)	Укажите КПП
Наименование банка	Укажите наименование банка
БИК	Укажите БИК
корреспондентский счет	Укажите корреспондентский счет
расчетный счет	Укажите расчетный счет
Идентификатор LEI	*Для ЮЛ нерезидентов РФ указывается международный код идентификации ЮЛ LEI*

Данные Партнера – индивидуального предпринимателя (ИП)

Фамилия Имя Отчество *(при наличии отчества)*	Укажите ФИО
Дата рождения	Укажите дату рождения
Адрес регистрации	Укажите адрес регистрации
Почтовый адрес (индекс, город/населенный пункт/поселок, улица, дом)	Укажите почтовый адрес
Номер(-а) телефона(-ов)	Укажите номер (-а) телефона (-ов)
Адрес электронной почты	Укажите электронную почту
Вид документа, удостоверяющего личность	
Серия и номер документа, удостоверяющего личность	Укажите серию и номер документа
Дата выдачи документа, удостоверяющего личность	Укажите дату выдачи документа
Наименование органа, выдавшего документ, удостоверяющий личность	Укажите наименование органа, выдавшего документ
Код органа, выдавшего документ, удостоверяющий личность	Укажите код органа, выдавшего документ
Регистрационный номер (ОГРНИП)	Укажите ОГРНИП
Дата регистрации в качестве ИП	Укажите дату регистрации в качестве ИП
Номер налогоплательщика (ИНН)	Укажите ИНН
Наименование банка	Укажите наименование банка
БИК	Укажите БИК
корреспондентский счет	Укажите корреспондентский счет
расчетный счет	Укажите расчетный счет
Страховой номер индивидуального лицевого счета, указанный в документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС)	Укажите СНИЛС

****Все поля обязательны для заполнения**, *кроме полей, выделенных курсивным шрифтом*

Настоящим Партнер проинформирован и понимает, что указываемая в настоящей заявке информация содержит персональные данные ответственных лиц (представителей) Партнера, и гарантирует наличие правовых оснований для передачи указанных персональных данных в Акционерное общество «Бюро кредитных историй «Скоринг Бюро» в целях подключения и использования автоматизированной системы Акционерного общества «Бюро кредитных историй «Скоринг Бюро».

Заявка оформлена:

Должность	Подпись	Фамилия и инициалы
Укажите должность		Укажите фамилию и инициалы
_____	_____	_____

мп

«___» _____ 20_ г.

Приложение № 1а

Генеральному директору
АО «БКИ СБ»
Лагуткину О.И.

Заявка на подключение к автоматизированной системе Акционерного общества «Бюро кредитных историй «Скоринг Бюро» (для Арбитражных управляющих)

Настоящим Заявлением арбитражный управляющий (далее – Пользователь):

данные Пользователя

Фамилия Имя Отчество *(при наличии отчества)*	Укажите ФИО
Дата рождения	Укажите дату рождения
Место рождения	Укажите место рождения
Вид документа, удостоверяющего личность	Укажите вид документа, удостоверяющего личность
Серия и номер паспорта (без пробелов)	Укажите серия и номер паспорта (без пробелов)
Дата выдачи паспорта	Укажите дату выдачи паспорта
Кем выдан паспорт	Укажите кем выдан паспорт
Код подразделения	Укажите код подразделения
Идентификационный номер налогоплательщика (ИНН)	Укажите ИНН
Страховой номер индивидуального лицевого счета, указанный в документе, подтверждающем регистрацию в системе индивидуального (персонифицированного) учета (СНИЛС)	Укажите СНИЛС
Адрес местонахождения (индекс, город/населенный пункт/поселок, улица, дом)	Укажите адрес местонахождения
Почтовый адрес (индекс, город/населенный пункт/поселок, улица, дом)	Укажите почтовый адрес
Мобильный телефон	Укажите мобильный телефон
Адрес электронной почты	Укажите адрес электронной почты
Дата вступления в СРО	Укажите дату вступления в СРО
Номер протокола вступления в СРО	Укажите номер протокола вступления в СРО
Номер Арбитражного управляющего в реестре СРО	Укажите номер Арбитражного управляющего в реестре СРО
Номер Арбитражного управляющего в Росреестре	Укажите номер Арбитражного управляющего в Росреестре

действующий на основании Федерального закона от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях» и являющийся членом саморегулируемой организации (далее – СРО):

данные СРО

Наименование	Укажите наименование СРО
Регистрационный номер СРО	Укажите регистрационный номер СРО
ИНН	Укажите ИНН СРО
КПП	Укажите КПП СРО
ОГРН	Укажите ОГРН СРО
Адрес	Укажите адрес СРО
Телефон	Укажите телефон СРО

выражает намерение установить программное обеспечение с использованием криптографической защиты информации (СКЗИ) и подключиться к Системе Акционерного общества «Бюро кредитных историй «Скоринг Бюро».

Оборудование и помещения, предназначенные для установки программного обеспечения Системы с встроенными средствами криптографической защиты информации (СКЗИ), удовлетворяют техническим требованиям необходимым для поддержания информационной безопасности.

Подпись _____ Фамилия и инициалы _____

«___» _____ 20__ г.

Приложение № 2
ОБРАЗЕЦ

ДОВЕРЕННОСТЬ

г. Москва «_____» _____20__ г.

_____
(полное наименование Партнера, ОГРН, ИНН Партнера)

_____
(с указанием местонахождения)
в лице

_____
(фамилия, имя, отчество (при наличии отчества))

действующего на основании _____

ДОВЕРЯЕТ

_____
(фамилия, имя, отчество (при наличии отчества))

формировать и подписывать электронной подписью (ЭП) файлы и запросы, направляемые в бюро кредитных историй, а также выполнять все необходимые процедуры по получению, применению и учету сертификатов ключей проверки электронной подписи, сертификатов защищенного соединения и шифрованию в рамках данных процессов, в том числе формировать и подписывать сопровождающие Акты, а также подписывать любые заявления и документы в целях осуществления действий в рамках Регламента электронного взаимодействия Акционерного общества «Бюро кредитных историй «Скоринг Бюро».

Настоящая Доверенность действительна в течение 10 (десяти) лет либо до момента ее отмены.

Должность _____ ФИО _____

Подпись _____
МП

Приложение № 3

Генеральному директору
АО «БКИ СБ»
О.И. Лагуткину

«___» _____ 20__ г.

Регистрационная карточка запроса на сертификат открытого ключа шифрования и ЭП, и (или) сертификата защищенного соединения (нужное подчеркнуть)

[Вставьте в данное поле криптографическую последовательность запроса: откройте файл запроса *.pem, скопируйте содержимое файла и вставьте в данное поле]

Полное наименование юридического лица или фамилия, имя, отчество (при наличии отчества) индивидуального предпринимателя/арбитражного управляющего: _____ ОГРН (для Партнера – юридического лица) /ОГРНИП (для Партнера – индивидуального предпринимателя) _____ , ИНН _____ (далее – Партнер) в лице _____ (далее – Ответственное лицо Партнера), действующего на основании _____.

Должность владельца сертификата:
_____

ФИО владельца сертификата:
_____

Подпись владельца сертификата
_____

Настоящим, Партнер проинформирован и понимает, что указываемая в регистрационной карточке информация содержит персональные данные ответственных лиц (представителей) Партнера, и гарантирует наличие правовых оснований для передачи указанных персональных данных в Акционерное общество «Бюро кредитных историй «Скоринг Бюро» в целях выпуска сертификата открытого ключа шифрования и ЭП, и (или) сертификата защищенного соединения.

Подпись Ответственного лица Партнера _____ Расшифровка подписи _____

мп

Приложение № 4

Генеральному директору
АО «БКИ СБ»
О.И. Лагуткину

Заявление на отзыв сертификата

Настоящим Заявлением _____ *(наименование организации/фамилия, имя, отчество (при наличии отчества) индивидуального предпринимателя или арбитражного управляющего)* _____ОГРН (для Партнеров – юридических лиц) или ОГРНИП (для Партнеров – индивидуальных предпринимателей) _____, ИНН _____ в лице_____, действующего на основании _____, выражает намерение отозвать сертификат(ы):

1. **Серийный номер сертификата** (указывается Ф.И.О. (отчество при наличии) владельца сертификата, если сертификат выдан с указанием конкретного лица и серийный номер сертификата не известен);
2. **Серийный номер сертификата** (указывается Ф.И.О. (отчество при наличии) владельца сертификата, если сертификат выдан с указанием конкретного лица и серийный номер сертификата не известен);
3. **Серийный номер сертификата** (указывается Ф.И.О. (отчество при наличии) владельца сертификата, если сертификат выдан с указанием конкретного лица и серийный номер сертификата не известен).

Причина отзыва сертификата: _____

Должность	Подпись	Фамилия и инициалы
_____	_____	_____
	мп	

«___» _____ 20 __ г.

Приложение № 5.1

Генеральному директору
АО «БКИ СБ»
О.И. Лагуткину

Заявление на добавление Администратора Партнера/Администратора файл-сервера

Настоящим Заявлением _____ *(наименование организации или фамилия, имя, отчество (при наличии отчества) индивидуального предпринимателя/арбитражного управляющего)* _____ _____ОГРН (для Партнеров – юридических лиц)/ ОГРНИП (для Партнеров – индивидуальных предпринимателей) _____, ИНН _____ в лице_____ _____, действующего на основании _____, выражает намерение добавить Администратора Партнера/Администратора файл-сервера (нужное подчеркнуть) в Систему АО «БКИ СБ»:

Администратор Партнера/Администратора файл-сервера (нужное подчеркнуть)

Фамилия Имя Отчество (при наличии отчества)	
Адрес электронной почты	
Мобильный телефон	
Роль (*нужное подчеркнуть*)	*Администратор Партнера (полный доступ) / Администратор файл-сервера (доступ только на файл-сервер)*

Настоящим, Партнер проинформирован и понимает, что указываемая в настоящем заявлении информация содержит персональные данные ответственных лиц (представителей) Партнера, и гарантирует наличие правовых оснований для передачи указанных персональных данных в Акционерное общество «Бюро кредитных историй «Скоринг Бюро» в целях подключения и использования автоматизированной системы Акционерного общества «Бюро кредитных историй «Скоринг Бюро».

Должность представителя	Подпись представителя	Фамилия и инициалы
_____	_____ мп	_____

«____» _____20__ г.

Приложение № 5.2

Генеральному директору
АО «БКИ СБ»
О.И. Лагуткину

Заявление на блокировку Администратора Партнера/Администратора файл-сервера

Настоящим Заявлением _____ *(наименование организации или фамилия, имя, отчество (при наличии отчества) индивидуального предпринимателя/арбитражного управляющего)* _____ _____ОГРН(для Партнеров – юридических лиц)/ ОГРНИП (для Партнеров – индивидуальных предпринимателей) _____, ИНН _____ в лице_____ _____, действующего на основании _____, выражает намерение заблокировать Администратора Партнера/Администратора файл-сервера в Системе АО «БКИ СБ»:

Администратор Партнера/Администратор файл-сервера

Фамилия Имя Отчество (при наличии отчества)	
Адрес электронной почты	
Роль (*нужное подчеркнуть*)	*Администратор Партнера (полный доступ) / Администратор файл-сервера (доступ только на файл-сервер)*

Должность	Подпись	Фамилия и инициалы
_____	_____	_____
	мп	

«____» _____20__ г.

Приложение № 6

В Акционерное общество
«Бюро кредитных историй «Скоринг Бюро»
129090, г. Москва, Каланчевская ул., д. 16, стр. 1
Генеральному директору
АО «БКИ СБ»
О.И. Лагуткину

Заявление на изменение данных Администратора Партнера/Администратора файл-сервера

Настоящим Заявлением _____
(наименование организации или фамилия, имя, отчество (при наличии отчества) индивидуального предпринимателя или арбитражного управляющего)
ОГРН (для Партнеров – юридических лиц)/ОГРНИП (для Партнеров – индивидуальных предпринимателей):
_____, ИНН: _____
(ОГРН или ОГРНИП, ИНН)
в лице_____,
(должность (для представителей юридических лица), фамилия, имя, отчество (при наличии отчества))
действующего на основании _____,
(устава или доверенности (номер и дата))
выражает намерение изменить данные Администратора Партнера/Администратора файл-сервера в Системе АО «БКИ СБ»:

	Старые данные	**Новые данные**
Логин		
Фамилия Имя Отчество		
Адрес электронной почты		
Мобильный телефон		

***укажите в соответствующем поле старые и новые данные или удалите текстовое поле, если соответствующие этому полю данные не изменяются.**
Настоящим, Партнер проинформирован и понимает, что указываемая в настоящем заявлении информация содержит персональные данные ответственных лиц (представителей) Партнера, и гарантирует наличие правовых оснований для передачи указанных персональных данных в Акционерное общество «Бюро кредитных историй «Скоринг Бюро» в целях подключения и использования автоматизированной системы Акционерного общества «Бюро кредитных историй «Скоринг Бюро».

Заявка оформлена

Должность	Подпись	Фамилия и инициалы
_____	_____	_____
	мп	

«___» _____ 20 __ г.

Приложение № 7

Рекомендации Бюро по обеспечению информационной безопасности

1. Настоящие рекомендации действуют по отношению к Партнеру, осуществляющему электронное взаимодействие с Акционерным обществом «Бюро кредитных историй «Скоринг Бюро» в целях организации безопасной передачи и обработки электронных документов (далее – защищаемая информация), в рамках, определенных Договором, заключенным между Сторонами.
В случаях наступления инцидентов защиты информации, в т.ч. реализации рисков получения несанкционированного доступа к защищаемой информации, их негативные последствия могут привести к быстрому развитию системного кризиса, нанести существенный ущерб интересам собственников и клиентов Партнера и Бюро. Поэтому угрозы безопасности информации представляют существенную опасность, а обеспечение защиты информации является одним из основополагающих аспектов деятельности Бюро и его Партнеров.

1.1. Рекомендации по организационному обеспечению безопасности:

- в организации Партнера должны быть выделены должностные лица, ответственные за обеспечение информационной безопасности;
- в организации Партнера должны быть разработаны локальные нормативные документы, регламентирующие вопросы информационной безопасности.

1.2. Рекомендации по подключению автоматизированных рабочих мест Партнера и/или серверов, взаимодействующих с Бюро и обрабатывающих защищаемую информацию, к локальным сетям и сетям общего пользования (Internet):

- необходимо исключить прямое подключение автоматизированных рабочих мест Партнера и/или серверов, взаимодействующих с Бюро и обрабатывающих защищаемую информацию к сетям общего пользования (Internet);
- автоматизированные рабочие места Партнера и/или сервера, взаимодействующие с Бюро, должны располагаться за средствами межсетевого экранирования (фаерволом) во внутренней сети Партнера или в демилитаризованной зоне;
- автоматизированные рабочие места Партнера и/или сервера, и/или базы данных, обрабатывающие защищаемую информацию, должны располагаться за средствами межсетевого экранирования (фаерволом) во внутренней сети Партнера;
- входящий и исходящий сетевой трафик должен фильтроваться средствами межсетевого экранирования (фаервола);
- к защищенной подсети Партнера необходимо разрешить доступ только с рабочих мест Партнера и/или серверов и по протоколам, имеющим прямое отношение к организации безопасной передачи и обработки электронных документов;
- на автоматизированных рабочих местах Партнера и/или серверах, взаимодействующих с Бюро, обрабатывающих защищаемую информацию, должны быть настроены механизмы оповещения о попытках несанкционированного доступа;
- не реже одного раза в неделю должны проводиться мероприятия по мониторингу состояния информационной безопасности автоматизированных рабочих мест Партнера и/или серверов, взаимодействующих с Бюро, обрабатывающих защищаемую информацию, согласно методам мониторинга, принятым у Партнера.

1.3. Рекомендации по выбору и использованию паролей:

- Пароль является средством защиты от несанкционированного доступа к информации или средствам ее обработки, хранения, передачи, и эффективен только при правильном его использовании.
- Партнеру следует соблюдать парольную политику в части удовлетворения любого пароля следующим требованиям:
    - длина пароля должна быть не менее 10 символов;
    - пароль должен содержать в себе символы из четырех категорий: буквы нижнего регистра (от a до z), буквы верхнего регистра (от A до Z), цифры (от 0 до 9) и спецсимволы (например: $, #, %);
    - пароль не должен совпадать с логином и повторять предыдущие 10 паролей для данной учетной записи Партнера;
    - пароль не должен включать осмысленные слова, словосочетания, общепринятые аббревиатуры, а также основываться на доступных данных о Партнере и его работниках (наименование Партнера, фамилии, дате рождения, именах родственников, номеров телефонов и др.) или легко угадываемом алгоритме смены (H0u$e!, H1u$e!, H2u$e! и т.д.);
    - пароль не должен содержать широко известные или легко угадываемые слова и последовательности символов (12345678, password, qwerty, aaabbb и т.д.);
    - пароль по умолчанию (созданный при создании учетной записи Партнера) должен быть изменен пользователем при первом входе;
    - пароль должен изменяться не реже чем 1 раз в 90 дней с момента последнего изменения;
    - в случае разглашения или компрометации пароль должен быть незамедлительно изменен.
- Соблюдать правила обращения с паролями:
    - не записывать пароль на предметах и материальных носителях, а также не хранить его в файле в открытом виде;
    - не использовать один и тот же пароль для различных учетных записей;
    - не передавать кому-либо (в т.ч. коллегам и руководителям, а также работникам Бюро) свой пароль, равно как и не использовать чужие пароли;
    - не осуществлять попытки подбора паролей (в том числе автоматизированными способами), не пытаться завладеть паролями других лиц.

1.4. Рекомендации к автоматизированным рабочим местам Партнера, серверам, базам данным и/или сетевому оборудованию, взаимодействующих с Бюро и обрабатывающих защищаемую информацию:

- автоматизированные рабочие места Партнера и/или сервера, взаимодействующие с Бюро и обрабатывающие защищаемую информацию, должны быть защищены стойкими методами аутентификации;
- автоматизированные рабочие места Партнера и/или сервера, взаимодействующие с Бюро и обрабатывающие защищаемую информацию, должны быть защищены средствами антивирусной защиты;
- автоматизированные рабочие места Партнера, сервера, базы данных и/или сетевое оборудование, взаимодействующие с Бюро и обрабатывающие защищаемую информацию, должны своевременно получать обновления безопасности установленной операционной системы и всего установленного программного обеспечения;
- на автоматизированных рабочих местах Партнера, серверах и/или сетевом оборудовании, взаимодействующих с Бюро и обрабатывающих защищаемую информацию, должны быть изменены значения параметров и пароли, заданные поставщиками по умолчанию, и отключены или удалены учетные записи по умолчанию перед взаимодействием с Бюро;
- на автоматизированных рабочих местах Партнера, серверах, базах данных и/или сетевом оборудовании, взаимодействующих с Бюро и обрабатывающих защищаемую информацию, следует настроить параметры безопасности таким образом, чтобы исключить возможность некорректного использования системы.

2. В случае обнаружения Партнером инцидента информационной безопасности, способного привести к негативным последствиям для Системы и доступной Партнеру ИТ-инфраструктуры Бюро, а также нанести репутационный ущерб Бюро, Партнер обязуется незамедлительно уведомить об этом Бюро.

Контакты Бюро для оповещения об инцидентах информационной безопасности:
Телефон **+7 (495) 646-04-30**
security@scoring.ru