Приложение № 2
к Договору об обслуживании с использованием Системы «Клиент-Банк» № ___ от «__»_____ 20 года

Регламент по использованию Системы «Клиент-Банк»
в КБ «Экономикс-Банк» (ООО)

1. Настоящий Регламент устанавливает:

1.1. Общие принципы, условия и порядок электронного документооборота, осуществляемого с помощью Системы;
1.2. Условия и порядок предоставления Банком Клиенту СКЗИ, при помощи которых Клиент подписывает электронной подписью документы, направляемые Банку по Системе;
1.3. Условия и порядок предоставления Банком Клиенту программного обеспечения Системы;
1.4. Условия обеспечения защиты от несанкционированного доступа, контроля целостности и достоверности электронных документов, направляемых по Системе.

2. Порядок и условия допуска Клиента к осуществлению документооборота в Системе.

2.1. Информационный обмен в рамках Системы осуществляется по каналу связи Интернет с использованием HTTPS. Для обеспечения конфиденциальности ЭД при передаче по открытым каналам связи, а также для обеспечения авторства и целостности ЭД, в Системе СКЗИ «Криптомодуль С» компании “ПрограмПарк”.
2.2. Клиент согласен, с тем, что использование в Системе протокола HTTPS в качестве средства обеспечения конфиденциальности при передаче ЭД, а также использование СКЗИ «Криптомодуль С» в качестве средства обеспечения подлинности и целостности ЭД, достаточными, т.е., обеспечивающими защиту интересов Клиента.
2.3. Электронный документооборот включает в себя процесс формирования электронного документа, подписания его Ключом ЭП, передачу ЭД, а также учет и хранение ЭД.
2.4. Правила и условия, установленные Регламентом, обязательны для исполнения Клиентом. Изменения Регламента, а также сроки и порядок вступления в силу этих изменений доводятся Банком до сведения Клиента посредством электронных документов путем передачи по Системе, путем публикации документа на сайте Банка, а также дополнительно иными способами, по выбору Банка, обеспечивающими получение Клиентом указанной информации, но в любом случае не позднее, чем за семь рабочих дней до даты вступления в силу данных изменений и дополнений.
2.5. Документооборот в Системе доступен Клиенту только после выполнения им всех следующих действий:
а) заключения с Банком Договора;
б) получения всех программных и аппаратных компонентов Системы, необходимых для функционирования Системы и оплаты комиссии Банка согласно действующим Тарифам Банка;;
в) выполнение предусмотренных Регламентом требований, необходимых для использования Системы;
г) формирования на рабочем месте Клиента Ключей ЭП и предоставления в Банк оригиналов Сертификатов открытых ключей ЭП всех пользователей Системы. Передача оригиналов Сертификатов открытых ключей ЭП производится Уполномоченным лицом Клиента или Представителем Клиента, действующим на основании нотариально удостоверенной доверенности, с подписанием Акта приема-передачи сертификата ключа подписи.
2.6. Для подключения к Системе Клиент подписывает со своей стороны, заверяет печатью (при наличии) и передает в Банк следующие документы:
а) Заявление на подключение к Системе “Клиент-Банк”;
б) Договор (в 2-ух экземплярах);
в) Сертификаты открытых ключей ЭП всех Владельцев сертификатов ключей ЭП Системы на бумажных носителях.
2.6. Программное обеспечение АРМ Системы передается на носителе Клиенту его Уполномоченному лицу. Передача осуществляется работником Банка лично Уполномоченному лицу Клиента или Представителю Клиента, действующему на основании нотариально удостоверенной доверенности, в помещениях Банка с подписанием Акта приема-передачи программного обеспечения Системы «Клиент-Банк» и ключевых носителей. Клиент может воспользоваться объявленными Банком доверенными источниками для получения программного обеспечения АРМ Системы в сети Интернет. Таковыми источниками являются:
а) http://www.java.com/ru/ - для получения дистрибутива программного обеспечения «Среда JAVA Runtime»,
б) https://ibank2.ru/ - для получения программного обеспечения «Драйвер для USB-Токенов и смарт-карт «iBank 2 Key»».

2.7. Доступ Клиента в Систему осуществляется Администратором Системы Банка в течение трех рабочих дней после заключения Клиентом с Банком Договора и оплаты комиссий Банка согласно действующим Тарифам Банка.
2.8. Установка АРМ Системы проводится Клиентом самостоятельно.
2.9. По заявлению Клиента возможна установка АРМ Системы работником Банка на рабочем месте Клиента при соблюдении следующих условий:

а) готовности технических средств Клиента в соответствии с техническими требованиями к организации АРМ Системы;

б) наличия Заявление на подключение к Системе «Клиент-Банк»;

в) оплате комиссии Банка согласно действующим Тарифам Банка.

Дата и время установки АРМ Системы специалистом (работником) Банка назначается Клиентом и согласовывается с Администратором Системы.

Клиент по результатам установки АРМ Системы работником Банка и проверки работоспособности Системы обязан подписать и заверить печатью (при наличии) Акт приема-сдачи работ в 2-х экземплярах (согласно Приложению № 5 к Договору). Два экземпляра Акта приема-сдачи работ Клиент обязан передать в Банк для подписания. После подписания Банком один экземпляр Акта приема-сдачи работ передается Клиенту.
2.10. После установки АРМ Системы Клиент формирует самостоятельно Ключи ЭП, заполняет 2 экземпляра Сертификата открытых ключей ЭП для каждого пользователя Системы. Сертификаты открытых ключей ЭП передаются в Банк для регистрации открытых ключей ЭП Клиента. Регистрация открытых ключей ЭП Системы производится в течение 2-х (Двух) рабочих дней с момента получения Банком оригиналов Сертификатов открытых ключей ЭП.

3. Технические требования к организации АРМ Системы.

3.1. Для работы в Системе Клиент должен использовать персональный или переносной компьютер с предустановленной операционной системой:

- Windows 2000 Professional,
- Windows XP, Windows Vista,
- Windows 7,
- Mac OS X.

3.2. Для доступа к серверу Системы Клиентом могут быть использованы браузеры:

- Microsoft Internet Explorer версии 6.0 и выше
- Mozilla FireFox 8.0 И выше
- Опера 10.0 и выше.

3.3. В качестве ключевого носителя используется USB-Токен iBank2 Key.
3.4. Компьютер, на котором осуществляется работа Клиента с Системой, должен быть оборудован программными средствами антивирусной защиты с ежедневным обновлением базы данных антивирусного программного обеспечения. Работа в сети Интернет на компьютере пользователя Системы не должна допускать посещения сайтов сомнительного содержания, развлекательных ресурсов, сайтов социальных сетей, игровых интернет-ресурсов. Не допускается запуск на компьютере пользователя Системы программ несанкционированного снятия защиты программного обеспечения (лицензионной или парольной). Также не допускается установка программного обеспечения, позволяющая осуществлять перехват, преобразование данных Системы.
3.5. Периодически (не реже одного раза в месяц) работником Клиента, квалифицированным для административной работы с компьютерной техникой, на компьютере пользователя Системы должен производиться аудит работы программного обеспечения (операционной системы, прикладного программного обеспечения) для:

- выявления ошибок в работе программного обеспечения,
- обнаружения посторонних неизвестных программ,
- обнаружения замедления работы операционной системы,
- контроля работоспособности дополнительных защитных прикладных программ (сетевых экранов и антивирусных средств).

3.6. Администратор Системы имеет право осуществлять дистанционный контроль отсутствия на компьютере пользователя Системы признаков программного обеспечения, позволяющего осуществлять преобразование данных Системы. В случае наличия подозрения на присутствие указанного программного обеспечения Администратор Системы имеет право направить письменное уведомление Клиенту с требованием удаления указанного программного обеспечения.
3.7. Банк не несет ответственности за нарушение электронного документооборота с Клиентом, если:

а) данное нарушение было вызвано вмешательством вирусного программного обеспечения в процесс обмена электронными документами;

б) данное нарушение было вызвано вмешательством программного обеспечения для преобразования данных Системы, которое произошло после получения Клиентом письменного уведомления от Банка о подозрении наличия указанного программного обеспечения;

в) данное нарушение было вызвано несоблюдением мер информационной безопасности при работе с Системой на компьютере пользователя Системы (отсутствие актуального работоспособного антивирусного программного обеспечения, посещение интернет-ресурсов сомнительного или развлекательного характера, недостаточная квалификация лица, осуществляющего систематический контроль работы программного обеспечения Клиента).

3.8. На основании HTTPS и электронного адреса Клиента Администратор Системы имеет право отключить Клиента от электронного обмена при обнаружении попыток несанкционированного доступа постороннего программного обеспечения к серверу Банка.

3.9. При установке рабочего места Системы используется программное обеспечение, предоставленное Банком, либо полученное из указанных в настоящем Регламенте доверенных источников.

4. Организация электронного документооборота.

4.1. Перечень электронных документов, передаваемых по Системе:

- Платежное поручение;
- Заявление об отказе от акцепта;
- Заявление об акцепте;
- Заявление на получение наличных;
- Заявление на перевод иностранной валюты;
- Поручение на обязательную продажу валюты;
- Поручение на продажу иностранной валюты;
- Поручение на покупку иностранной валюты;
- Поручение на конвертацию иностранной валюты;
- Поручение на обратную продажу иностранной валюты;
- Распоряжение на списание с транзитного счета;
- Паспорт сделки по контракту;
- Паспорт сделки по кредитному договору;
- Справка о валютных операциях;
- Справка о поступлении валюты РФ;
- Справка о подтверждающих документах;
- Справка о расчетах через счета за рубежом;
- Рублевые и валютные выписки;
- Письмо (Запрос);
- Сообщение сводного формата.

4.1.1. Электронный документооборот включает:

а) формирование ЭД и его подпись;

б) отправку и доставку ЭД;

в) проверка подлинности доставленного ЭД;

г) подтверждение получения ЭД;

д) отзыв ЭД;

е) хранение ЭД.

4.2. Формирование ЭД осуществляется в следующем порядке:

а) ЭД оформляется путем заполнения стандартной формы документа, предусмотренной в Системе для данного вида ЭД. При оформлении ЭД Систем осуществляет автоматический контроль присутствия обязательной информации в соответствующих полях формы документа. Ключевыми полями ЭД являются все обязательные для данного вида ЭД реквизиты, без наличия которых надлежащее исполнение ЭД является невозможным.

б) Сформированный ЭД подписывается Клиентом с использованием Ключа ЭП.

4.3. Отправка и доставка ЭД:

4.3.1. В отношениях между Клиентом и Банком ЭД считается исходящим от Клиента, если:

а) ЭД подписан действующим Ключом ЭП Клиента;

б) Банк не уведомлен о компрометации действующего Ключа ЭП.

4.3.2. ЭД не считается исходящим от Клиента, если:

а) ЭД не прошел проверку на целостность текста и подлинность ЭП;

б) Банк уведомлен о компрометации Ключей ЭП Клиента.

4.4. Проверка подлинности доставленного ЭД включает в себя:

а) проверку ЭД на соответствие установленному формату для данного вида ЭД;

б) проверку подлинности ЭП (осуществляется преобразование строк, содержащих данные ЭД, с помощью действующего Открытого ключа ЭП Клиента на сервере Банка. Производится сравнение строки ЭП, полученной от Клиента, и строки, полученной в результате преобразования. ЭП считается верной, если результат преобразований идентичен строке ЭП ЭД Клиента);

в) проверку соответствия параметров ЭД требованиям Договора между Банком и Клиентом, а также требованиям законодательства Российской Федерации, в том числе нормативных документов Банка России. В случае положительного результата проверки, ЭД принимается к исполнению. В случае, если ЭД не проходит контроль правильности оформления, или не подтверждается его ЭП, Банк не принимает данный ЭД к исполнению. Документ при этом получает статус «Отвергнут».

4.5. Подтверждение получения ЭД представляет собой статус ЭД, имеющий визуальное представление «В обработке». Если иное не предусмотрено отдельными договорами (соглашениями) между Банком и Клиентом, то ЭД считается неполученным Банком до тех пор, пока ЭД не получил статуса «На исполнении».

Примечание: Подтверждение может быть получено только во время сеанса связи с Банком по Системе.

4.6. Отзыв РЭД может производиться как по инициативе Клиента, так и по инициативе Банка.

4.6.1. Клиент вправе отозвать отправленный РЭД. В тексте отзыва должен содержаться текст отзыва и указываться номер, сумма, дата отзываемого РЭД.

4.6.2. РЭД может быть отозван отправителем только до окончания периода электронного обмена по Системе текущего операционного дня в Системе или до выполнения действий, в результате которых отзыв РЭД невозможен. Если отзыв исполнен, отзываемый РЭД принимает статус «Удален».

4.7. Клиент обязан своевременно, до окончания операционного дня в Системе, проконтролировать состояние направленных РЭД.

5. Смена Ключей ЭП вследствие компрометации.

5.1. В случае компрометации Ключей ЭП Клиент направляет в Банк Уведомление о компрометации ключа ЭП (далее - «Уведомление»), составленное по форме Приложения № 4 к настоящему Договору. Уведомление может быть направлено в Банк в виде письменного документа, заверенного печатью (при наличии) и подписанного собственноручной подписью уполномоченного лица Клиента. Документ может быть доставлен в Банк лично или передан по факсу. Передача Уведомления по факсу требует подтверждения путем последующего предоставления Клиентом его оригинала на бумажном носителе в Банк не позднее 5 (Пяти) рабочих дней. После направления Уведомления Клиент должен связаться с Администратором Системы для подтверждения получения Банком Уведомления.

5.2. В случае наличия у Клиента нескольких ЭП, допускается направление Уведомления посредством Системы на не скомпрометированных Ключах ЭП, путем передачи ЭД «Письмо» с указанием в поле «Тема» - «Уведомление о компрометации Ключа ЭП». Передача Уведомления посредством Системы требует подтверждения путем последующего предоставления Клиентом его оригинала на бумажном носителе в Банк не позднее 5 (Пяти) рабочих дней.

5.3. При получении от Клиента (Уполномоченного лица Клиента) Уведомления на бумажном носителе, работник Банка указывает на Уведомлении дату и время его получения Банком и передает Клиенту (Уполномоченному лицу Клиента) копию соответствующего Уведомления, содержащего отметку о дате и времени его получения Банком. С этого момента все ЭД, подписанные компрометированным Ключом ЭП, считаются недействительными и Банком не принимаются. При отправке Клиентом Уведомления в виде ЭД по Системе, дата и время получения Уведомления фиксируется средствами Системы автоматически. Направление Уведомления означает требование Клиента прекратить прием и исполнение любых ЭД, подписанных компрометированным Ключом ЭП в сроки, предусмотренные условиями Договора или иными договорами (соглашениями), заключенными между Банком и Клиентом.

5.4. Клиент самостоятельно производит замену Ключей ЭП. Клиент обязан предоставить в Банк после смены Ключей ЭП оригиналы Сертификатов открытых ключей ЭП в 2 (Двух) экземплярах для регистрации открытых ключей ЭП Клиента на сервере Банка. Сертификаты открытых ключей ЭП передаются в Банк Уполномоченным лицом Клиента или Представителем Клиента, действующим на основании нотариально удостоверенной доверенности, с подписанием Акта приема-передачи сертификата ключа электронной подписи (Приложение № 7 к настоящему Договору).

5.5. Открытые ключи ЭП, соответствующие скомпрометированным Ключам ЭП, Банком не удаляются и хранятся на сервере Банка в Системе в соответствии со сроками хранения документов, подписанных Ключами ЭП Клиента.

6. Процедуры разрешения конфликтных ситуаций.

6.1. Рассматривается конфликт типа: «Банк утверждает, что получил от Клиента корректно подписанный электронный документ, Клиент утверждает, что не подписывал (не отправлял) этот документ» (в дальнейшем «Отказ Клиента от подписи под электронным документом»).
6.2. Для рассмотрения конфликтных ситуаций по письменному заявлению одной из Сторон создается экспертная комиссия. В комиссию в равном числе входят представители Банка и представители Клиента. Со стороны Банка обязательно входит Администратор Системы Банка. Экспертная комиссия осуществляет свою работу на территории Банка, с использованием персонального компьютера, эталонного программного обеспечения и ключевых носителей, участвующих в конфликте Сторон. Эталонное программное обеспечение состоит из операционной системы и Системы, действующей на момент рассмотрения конфликта экспертной комиссией версии со встроенной криптографической библиотекой, используемой при подписании Клиентом спорного документа. Эталонное оборудование и программное обеспечение предоставляется Банком.
Замечание: до подачи заявления Сторонам рекомендуется проверить, что причиной возникновения конфликта не является нарушение целостности программного обеспечения, а также причиной не является несанкционированный доступ к Системе с использованием вредоносного программного обеспечения. Для этого Клиент в присутствии независимых экспертов с соответствующей квалификации формирует копию жесткого диска, где была размещена Система, копию жесткого диска, где была размещена операционная система. Информация, сохраненная на образах дисков, не должна быть изменена с момента обнаружения несанкционированного доступа в Систему, кроме того, должны быть сохранены неизменными журналы работы операционной системы, журналы обновления и работы антивирусного программного обеспечения.
6.3. В ходе разрешения конфликта может возникать спор об актуальности используемого Ключа ЭП между Клиентом и УЦ Банка. Открытый ключ ЭП считается актуальным и принадлежащим Владельцу сертификата ключа ЭП, если он был зарегистрирован в УЦ Банка и действовал в момент, когда произошел конфликт. В данном разделе описан также порядок разрешения спора об актуальности открытого ключа ЭП Клиент.

а) Администратор Системы предоставляет:

- спорный ЭД в Системе;
- открытые ключи ЭП в Системе, для проверки ЭП под электронными сообщениями,
- Сертификаты ключей ЭП на бумажном носителе.

б) Клиент предоставляет:

- личные ключевые носители;
- журналы операционной системы и антивирусного программного обеспечения на дату отправки спорного ЭД.

в) Экспертная комиссия убеждается в работоспособности персонального компьютера и программного обеспечения. На основании полученных файлов производится проверка подписи Ключем ЭП программными средствами для разбора конфликтных ситуаций разработчика Системы.
6.4. Администратор Системы по решению экспертной комиссии осуществляет выгрузку данных журнала обработки спорного ЭД в Системе.
6.5. Экспертная комиссия оформляет свое решение о подлинности ЭД в виде акта, который оформляется на бумажном носителе и подписывается всеми членами экспертной комиссии. Акт экспертной комиссии является окончательным и пересмотру не подлежит. Действия, вытекающие из него, являются обязательными для участников конфликтной ситуации. Акт экспертной комиссии является основанием для предъявления претензий к лицам, виновным в возникновении конфликта.

9. Прекращение и возобновление обслуживания в Системе.

9.1. Обслуживание Клиента в Системе может быть прекращено временно (приостановлено) или окончательно.
9.2. Временное прекращение обслуживания Клиента в Системе происходит по собственному желанию Клиента или при блокировке Системы, вызванной:

- срабатыванием системы защиты от подбора пароля к Системе;
- несвоевременной оплатой Клиентом комиссии за обслуживание в Системе в соответствии с действующими Тарифами Банка;
- по иным причинам, предусмотренным Договором.

9.3. Для временного прекращения обслуживания в Системе по собственному желанию Клиент оформляет Заявление на приостановку обслуживания в Системе свободного формата за подписью Уполномоченного лица и заверенного печатью (при наличии) Клиента (допускается направление Заявки ЭД произвольного формата в Системе) и передает его в Банк.

После получения Заявления на приостановку обслуживания в Системе Банком, в течение следующего рабочего дня производится блокировка Ключа ЭП Клиента в Системе на стороне Банка. Обслуживание Клиента в Системе считается приостановленным на второй рабочий день после принятия Банком Заявления на приостановку обслуживания в Системе. Для возобновления обслуживания в Системе Клиент оформляет

Заявление свободного формата на возобновление обслуживания в Системе за подписью уполномоченного лица и заверенного печатью (при наличии) Клиента и передает его в Банк. Данное Заявление на возобновление обслуживания в Системе является основанием возобновления взимания с Клиента комиссии за обслуживание в Системе. Возобновление обслуживания производится в течение одного рабочего дня, следующего за днем приема Банком Заявления на возобновление обслуживания в Системе.
9.4. В случае прекращения обслуживания по Системе в связи со срабатыванием системы защиты от подбора пароля Клиент производит формирование новых Ключей ЭП. Новые Ключи ЭП Клиент формирует самостоятельно.

10. Обеспечение информационной безопасности.

10.1. Обеспечение конфиденциальности и сохранности электронного документооборота обеспечивается:

1) Использованием протокола обмена HTTPS по каналам связи сети Интернет для шифрования данных при обмене.

2) Использованием сертифицированных ФСБ России средств криптографической защиты информации при подписи ЭД на основании ГОСТ Р34.10–2001.

3) Использование Клиентом защищенного хранилища ЭП типа USB-Токен с невозможностью копирования Ключа ЭП.

4) Использованием ЭП (в том числе без права подписи) при авторизации в Системе.

5) Возможностью по желанию Клиента ограничить обмен с определенного перечня внешних статических IP адресов.

6) Отображением информации об IP адрес последнего соединения в Системе.

7) Разграничением прав Владельцев сертификатов ключей ЭП на проведение операций (первая и вторая подпись).

10.2. Рекомендации по обеспечению информационной безопасности.

а) При работе с компьютером:

1) Учетная запись, под которой производится работа с Системой, не должна иметь прав локального администратора.

2) Не посещайте сайты сомнительного содержания, развлекательные интернет-ресурсы, социальные сети, онлайн игры с рабочего места Системы. Воздержитесь от посещения форумов развлекательного характера.

3) Не устанавливайте программное обеспечение развлекательного характера (анимированные изображения рабочего стола, свободно распространяемые игры, веб-сервисы получения электронных почтовых уведомлений (Mail.RU агент, Я-Онлайн и пр.)).

4) Не скачивайте и не устанавливайте программы подбора паролей, снятия лицензионной защиты.

5) Обращайте особое внимание на ежедневное обновления антивирусного программного обеспечения.

6) Обращайте внимание на неожиданное поведение компьютера (частые зависания программ, объем трафика при интернет-соединении сильно возрос за последнее время, прекращено обновление антивирусного программного обеспечения, нет доступа на сайты антивирусных решений, запускаются неизвестные программные компоненты, при попытке входа в Систему появляется предупреждение о технических работах без предварительного уведомления от Банка, погас экран или выключился компьютер в момент начала работы с Системой).

б) При работе с ЭП:

1) При подключении к Системе регистрируйте двух и более пользователей Системы. При этом не устанавливайте одному пользователю право единственной подписи ЭД.

2) ключевой носитель ЭП используйте только в момент работы с Системой.

3) Не передавайте права на перегенерацию ЭП постороннему лицу (включая специалиста, обслуживающего компьютерную технику). Формирование ключей ЭП должно производиться Владельцем сертификата ключа ЭП самостоятельно!

4) Произведите смену Ключей ЭП после увольнения Владельца ЭП или системного администратора.

5) Плановая смена ЭП должна производиться в обязательном порядке не реже одного раза в 2 (Два) года.

6) ключевой носитель ЭП не оставляйте без присмотра даже на очень короткое время!

7) Заблокируйте Ключ ЭП в Системе, если Владелец сертификата ключа ЭП планирует отсутствовать длительное время: в командировке, дальней поездке, отпуске. Сообщите в Банк время возвращения Владельца сертификата ключа ЭП для разблокировки учетной записи.

Внимание! Не допускайте беспричинной потери контроля управления в Системе, невозможности входа в Систему длительное время без объективных причин! В случае возникновения подобных ситуаций незамедлительно сообщите об этом в Банк!

10.3. Прекратите работу с Системой и обратитесь незамедлительно в Банк, если:

1) Несмотря на то, что предыдущий заход в Систему был успешный, Система сообщает о блокировке учетной записи или некорректности пароля.

2) При попытке обновления антивирусного программного обеспечения работа антивирусной программы неожиданно прекращается или база антивирусного программного обеспечения не обновляется.

3) В момент захода в Систему отключился компьютер, и загрузить вновь его не удается.

4) Интерфейс Системы изменен без уведомления со стороны Банка, появились дополнительные поля ввода.

5) Без уведомления со стороны Банка при попытке захода в Систему предлагается установка неизвестного программного обеспечения.

6) При попытке соединения с Системой интернет-браузер сообщает о недействительности Сертификата HTTPS .

В вышеуказанных ситуациях целесообразно временно заблокировать учетную запись в Системе до выяснения причин нарушения работы компьютера.

10.4. Для обеспечения работоспособности Системы Банк руководствуется следующими законодательными актами:

а) Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

б) Приказом ФАПСИ от 13.06.2001 г. N 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

в) «Стандартом Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2010».

Внимание! Работники Банка, включая Администратора Системы, ни при каких условиях не запрашивают пароль для авторизации в Системе!