Приложение № 2
к Условиям дистанционного обслуживания
клиентов с использованием Системы «iBank 2»

ТРЕБОВАНИЯ
по обеспечению безопасности при работе с Системой «iBank2».

Настоящие Требования разработаны в целях:

- Предотвращения хищения денежных средств, находящихся на банковских счетах Клиента при осуществлении расчётов с использованием Системы «iBank 2» (далее – «iBank 2»).

- Минимизации рисков проведения злоумышленниками несанкционированных платежей и других вредоносных действий с использованием Системы «iBank 2».

1. В целях обеспечения безопасности электронного устройства, на котором производится работа с Системой «iBank 2»:

- Используйте для работы в Системе «iBank 2» специально выделенное для этих целей исправное электронное устройство (компьютер/ноутбук/планшет/смартфон, далее по тексту - ЭУ);
- Исключите возможность несанкционированного доступа к ЭУ;
- На ЭУ должна быть установлена только одна операционная система;
- На ЭУ должна быть установлена парольная защита для входа в BIOS и в операционную систему. Пароли должны иметь высокий уровень сложности и меняться не реже одного раза в месяц;
- На ЭУ не должны устанавливаться средства разработки и откладки программного обеспечения;
- Крайне желательно опечатывать корпус и неиспользуемые разъёмы ЭУ с целью исключения несанкционированного подключения и установки аппаратных закладок;
- Применяйте на ЭУ только лицензионное системное, прикладное и антивирусное программное обеспечение (далее - ПО);
- Своевременно устанавливайте на ЭУ необходимые обновления системы безопасности, обновления системного, прикладного и антивирусного ПО, обновления модулей и баз антивирусного ПО;
- Еженедельно осуществляйте полную проверку ЭУ на наличие/отсутствие вредоносного кода (вирусов);
- Применяйте на ЭУ специализированные программные средства безопасности – персональные межсетевые экраны (firewall), а также средние или высокие параметры безопасности и конфиденциальности установленного на ЭУ Интернет – браузера;
- Во время работы в сети Интернет никогда не соглашайтесь на установку каких-либо дополнительных программ или компонентов, если неизвестно для чего это нужно;
- При работе с электронной почтой не открывайте письма и вложенные в них файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам;
- Исключите посещение Интернет-сайтов, за исключением сайтов банков и сайтов обновлений систем безопасности разработчиков системного, прикладного и антивирусного ПО с данного ЭУ;
- Отключайте устройства беспроводного доступа (Wi-Fi и Bluetooth), когда в них нет необходимости.

2. В целях исключения доступа посторонних лиц к ЭУ, на котором производится работа с системой «iBank 2»:

- Назначьте ответственное лицо, имеющее право использовать Систему «iBank 2»;
- Определите порядок доступа и порядок работы на данном ЭУ, исключающий доступ к данному ЭУ неуполномоченных лиц;
- Исключите обслуживание данного ЭУ нештатными специалистам.

3. В целях исключения возможности удалённого подключения к ЭУ:

- На ЭУ, предназначенном для работы в Системе «iBank 2», не должно быть установлено программ он-лайн общения (ICQ, Skype и т.п.), программ удалённого администрирования и программ удаленного доступа к данному ЭУ;
- При обычной работе на ЭУ входите в Систему «iBank 2» под учётной записью с правами ограниченного доступа (как обычный пользователь), не имеющего неограниченные права администратора системы;
- Учётная запись «Гость», в операционной системе ЭУ, должна быть выключена.

4. В целях защиты ключа электронной подписи от хищения и копирования:

- Храните USB-токен/файловое хранилище на котором содержится ключ электронной подписи в надёжном месте;
- Подключайте USB-токен/файловое хранилище и к компьютеру только на время работы с Системой «iBank 2». Отключайте и извлекайте USB-токены в то время, когда они не используются для работы с Системой «iBank 2»;
- Определите порядок доступа и места хранения USB-токенов, исключающие их несанкционированное использование неуполномоченными работниками и третьими лицами;
- Никогда не передавайте USB-токены/файловые хранилища каким-либо специалистам для проверки работы Системы «iBank 2», проверки настроек взаимодействия с Банком и т.п. При необходимости таких проверок только ответственный за работу с Системой «iBank 2» должен подключить USB-токен к ЭУ и лично ввести пароль доступа, исключая его подсматривание;
- При увольнении работника, ответственного за USB-токен/файловое хранилище, при переводе такого работника на другую должность и в других случаях, когда работник прекращает работать с USB-токеном/файловым хранилищем, незамедлительно обратитесь в Банк с просьбой временной блокировки данной учётной записи в Системе «iBank 2», сгенерируйте новые ключи электронной подписи и зарегистрируйте их в БАНКЕ.

5. В целях сохранности пароля доступа к ключу электронной подписи:

- Запомните пароль к ключу электронной подписи, который находится на USB-токене/файловом хранилище;
- Никогда не записывайте его в местах, доступных посторонним лицам;
- Периодически (желательно – 1 раз в месяц) меняйте пароль доступа к ключу электронной подписи;
- Никому и никогда не сообщайте сведения о пароле, включая работников Банка. Банк никогда не запрашивает данную информацию.

6. При работе с Системой «iBank 2» и СМС-подтверждениями платежей:

- Ограничьте доступ к телефону на номер которого приходят СМС с ключами подтверждения платежей и ключами доступа к Системе «iBank 2»;
- Перед вводом СМС ключа для подтверждения платежа, убедитесь, что информация, полученная в СМС, соответствует фактическим реквизитам платежа.

7. Будьте осторожны и внимательны при работе в Системе «iBank 2»:

- Внимание! Если возникло подозрение, что компьютер заражён (неадекватная реакция на действия пользователя, непонятные окна и сообщения, получение незапрашиваемых СМС с ключом для входа или для проведения операции и т.п.) - немедленно прекратите работу в Системе «iBank 2», извлеките USB-токен/файловое хранилище и обратитесь к ИТ-специалисту для выяснения причин происходящего.
- Не пользуйтесь Системой «iBank 2» до выяснения причин происходящего.
- Не пользуйтесь Системой «iBank 2» через публичные компьютерные сети (интернет-кафе, компьютерные салоны, и любые другие общественные места);
- Особое внимание следует обратить на недопустимость использования Системы «iBank 2» через публичные Wi-Fi сети;
- Не работайте с Системой «iBank 2», используя чужие ЭУ;
- Прежде чем ввести пароль в Системе «iBank 2», убедитесь, что соединение установлено именно с сервером БАНКА - в адресной строке должен отображаться адрес **https://ibank.russitabank.ru/**. Злоумышленники часто используют похожие сайты, например, https://ibank.rositabank.ru/;
- Если при подключении к Системе «iBank 2» появляется предупреждение Интернет-браузера о перенаправлении на другой сайт, немедленно прекратите все операции и обратитесь в службу технической поддержки БАНКА по телефону +7 (495) 933-46-00;
- Обращайте особое внимание на любые изменения в привычных процессах установления соединения с Системой «iBank 2». При возникновении любых сомнений в правильном функционировании Системы «iBank 2», немедленно обращайтесь по телефону +7 (495) 933-46-00 в службу технической поддержки БАНКА;
- Регулярно контролируйте состояние своих счетов в Системе «iBank 2» и незамедлительно сообщайте работникам Банка по телефону +7 (495) 933-46-00 обо всех подозрительных или несанкционированных финансовых операциях;
- При возникновении любых подозрений на компрометацию ключа электронной подписи или на наличие в ЭУ вредоносных программ – незамедлительно заблокируйте Вашу учетную запись в Системе «iBank 2», сгенерируйте новые ключи электронной подписи и зарегистрируйте их в БАНКЕ;

- В случае обнаружения на ЭУ посторонних, незнакомых и необычных программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках все работы на данном ЭУ должны быть прекращены;
- В случае сбоев в работе ЭУ, его поломки во время работы с Системой «iBank 2», или сразу после сеанса работы (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), немедленно обратитесь в Банк по телефону +7 (495) 933-46-00 и убедитесь, что от имени вашей организации не производились несанкционированные переводы денежных средств;
- В случае утери, хищения или повреждения USB-токена/файлового хранилища немедленно свяжитесь с БАНКОМ.

8. Пользователю системы «iBank 2» запрещается:

- обрабатывать предоставленными Банком ключами электронной подписи информацию, содержащую государственную тайну;
- после ввода ключевой информации либо иной конфиденциальной информации оставлять без контроля ЭУ, на которых ведётся работа с системой «iBank 2»;
- разглашать содержимое USB-токенов или передавать USB-токены/файловые хранилища лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации (за исключением случаев, предусмотренных соответствующими соглашениями между Банком и Клиентом);
- использовать USB-токены/файловые хранилища в режимах, не соответствующих соглашениям между Банком и Клиентом;
- записывать на ключевые носители постороннюю информацию;
- производить дублирование ключевых носителей.

9. Общие рекомендации по использованию и хранению USB-токенов:

- Необходимо оберегать USB-токены от сильных механических воздействий (падения с высоты, сотрясения, вибрации, удары);
- USB-токены необходимо оберегать от воздействия высоких и низких температур;
- При резкой смене температур (вносе охлажденного устройства с мороза в теплое помещение) не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждений из-за сконденсированной на электронной схеме влаги;
- Необходимо оберегать USB-токены от попадания на них прямых солнечных лучей;
- Необходимо оберегать USB-токены от воздействия влаги и агрессивных сред;
- Недопустимо воздействие на USB-токены сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;
- При подключении USB-токена к компьютеру не прилагайте излишних усилий;
- USB-токен в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем USB-токена пыли, грязи и влаги;
- При засорении разъема токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо;
- Не разбирайте USB-токены;
- Необходимо избегать скачков напряжения питания ЭУ ;
- Не извлекайте USB-токен из USB-порта во время записи и считывания;
- В случае неисправности или неправильного функционирования USB-токенов обращайтесь в Банк.

10. Важно! Обратите внимание!

- МКИБ "РОССИТА-БАНК" ООО не имеет доступа к секретным ключам клиентов;
- У МКИБ "РОССИТА-БАНК" ООО отсутствует возможность подписания документов электронной подписью от имени какого-либо клиента;
- В МКИБ "РОССИТА-БАНК" ООО хранятся только сертификаты открытого ключа электронной подписи клиентов, сформированные и переданные клиентами в Банк при подключении к системе «iBank 2». Данные сертификаты пригодны только для проверки электронной подписи платежных документов, полученных от клиентов;
- МКИБ "РОССИТА-БАНК" ООО никогда не запрашивает у клиентов конфиденциальную информацию, информацию о паролях и ключах;
- МКИБ "РОССИТА-БАНК" ООО не несёт ответственности за сохранность ключевой информации клиентов (она хранится только у клиентов и только клиент является её единственным владельцем), а

также за возможный ущерб, который может понести клиент в случае исполнения МКИБ "РОССИТА-БАНК" ООО платёжных документов, инициированных неуполномоченными лицами, но подписанных действительной электронной подписью клиента.