Уважаемые Клиенты!

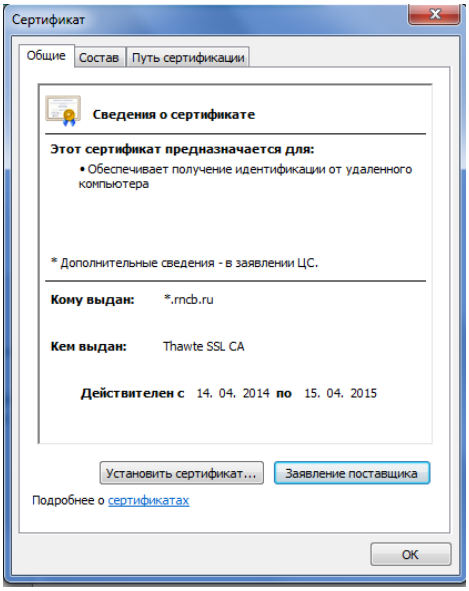
В целях обеспечения информационной безопасности рабочей станции Клиента при работе в системе дистанционного банковского обслуживания «Интернет-Банк-Клиент» РНКБ Банк (ПАО)[1] (далее – ИБК), обращаем Ваше внимание на необходимость выполнения следующих мер безопасности:

1. **Обеспечение безопасности при хранении и работе с USB-токеном:**

- Пароль доступа к секретному ключу хранить отдельно от USB-токена.
- Создавать пароль самостоятельно, не менее чем из 6 (Шести) различных символов. Если пароль стал известен любому другому лицу, необходимо блокировать старый и создать новый пароль.
- Использовать USB-токен с ключами электронной подписи (ЭП) только для входа и для подписания документов.
- Подключать USB-токен к компьютеру только на время проведения операций. После завершения операций/действий, требующих ЭП, извлекать USB-токен из соответствующего порта компьютера.
- Блокировать ключи ЭП и производить генерацию новых ключей ЭП при замене должностных лиц, уполномоченных подписывать документы в ИБК, а также при утере или при наличии подозрений, что ключи оказались у неуполномоченных лиц.

2. **Обеспечение безопасности соединения в сети Интернет:**

- Использовать адрес https://ibank.rncb.ru (ip: 195.200.209.5) для входа на стартовую страницу ИБК.
- Не использовать и не создавать ярлык на рабочем столе компьютера для прямого перехода на стартовую страницу ИБК.
- После входа на стартовую страницу проверять соответствие сертификата соединения приведенному ниже рисунку (для этого используется символ замка в окне браузера):



3. **Обеспечение безопасности персонального компьютера:**

- Выделить компьютер в отдельную доверенную зону, в т.ч. обеспечить безопасность помещения и исключить доступ к компьютеру, используемому для работы с ИБК неуполномоченным лицам.
- Использовать компьютер, работающий с системой ИБК, только для работы с ИБК. Исключить использование прикладных программ и нелицензионного программного обеспечения, пользовательского удаленного доступа, а также обращения к нецелевым Интернет-ресурсам, кроме как к сайту Банка для доступа в ИБК. Своевременно осуществлять обновление установленного программного обеспечения.
- Использовать на рабочей станции - компьютере лицензионное антивирусное программное обеспечение, применяющее как сигнатурные методы защиты, так и проактивные.
- Не работать в ИБК в местах большого скопления людей и через Wi-Fi точки доступа к сети Интернет (Интернет-кафе, Интернет-киоски и т.д.).

[1] Наименование организационно-правовой формы Банка приведено в соответствие с Уставом РНКБ Банк (ПАО) и действующим законодательством, с учетом Приказа по Банку от 25.05.2015 г. № 253.

- Обновление антивирусных баз должно производиться не реже одного раза в сутки, полная проверка компьютера и используемых носителей информации на предмет наличия вирусов не реже одного раза в неделю, с обновлением баз не реже одного раза в неделю.
- Осуществлять постоянный контроль отправляемых по ИБК документов, а также состояния банковского счета.
- Работать в операционной системе только под правами пользователя. Использовать администраторские учетные записи только в крайне необходимости.
- На компьютере не должны быть заведены учетные записи без паролей или с паролями по умолчанию. Учетная запись «Гость» должна быть заблокирована.
- Использовать межсетевой экран, установленный как на сетевом оборудовании, так и на компьютере, с которого осуществляется работа в ИБК.
- В обязательном порядке выполнять рекомендации по информационной безопасности для клиентов РНКБ Банк (ПАО), использующих системы «Интернет Банк-Клиент».

Банк обращает Ваше внимание на то, что выполнение вышеуказанных рекомендаций позволит существенно минимизировать риски несанкционированного списания денежных средств с Ваших банковских счетов.

Для предупреждения несанкционированного доступа к ИБК важно обращать внимание на нестандартную работу персонального компьютера Клиента. Типичными признаками несанкционированного доступа к компьютеру Клиента являются:

- Наличие измененного интерфейса ИБК при условии отсутствия уведомлений об обновлении со стороны Банка.
- Наличие ошибок сертификата сайта.
- Соединение устанавливается не по защищенному протоколу (в строке запроса браузера отображается **http** вместо **https**).
- Имеется подозрение на проникновения третьих лиц в компьютер.
- ИБК отказывается присваивать расчетному документу Клиента следующий порядковый номер в связи с нахождением в системе иного расчетного документа с аналогичным номером.
- Сбой порядка нумерации расчетных документов Клиента или не соответствие ранее установленной нумерации.
- В списке рабочих документов и/или выписке обнаружены посторонние расчетные документы, которые Клиентом не создавались.
- Внезапное отсутствие действующего закрытого ключа на USB-токене.
- Выход из строя ПК (отказ в работе, сбой в операционной системе и/или антивирусного ПО, отказ ИБК в обслуживании по неустановленным причинам).

При обнаружении Вами попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, просим Вас последовательно осуществить следующие действия:

- Незамедлительно сообщить об этом в обслуживающее Вас подразделение Банка или по телефонам: **+7 (495) 232-90-00 или 8-800-234-27-27** (звонок по России бесплатный).
- Заблокировать ключи ЭП, используемые для работы в ИБК.
- По возможности отключить сетевой кабель (Ethernet) от системного блока, для предотвращения удаленного доступа.
- Ни в коем случае не сканировать на вирусы до прихода специалистов или полиции. **В данном случае компьютер и система представляет собой улику.**
- Не допускать к компьютеру посторонних лиц, включая сотрудников компании не имеющих соответствующих полномочий, до прихода руководства компании, сотрудников службы безопасности компании или полиции.
- Отключить компьютер, выдергивая шнур питания без завершения сеанса работы.
- В обязательном порядке сделать запрос в обслуживающее Вас отделение Банка с целью проверки транзакций за последнюю неделю, проверки ликвидности платежей и остатков по банковским счетам.

Памятка пользователя по обеспечению информационной безопасности при эксплуатации и хранении USB-токена

При эксплуатации и хранении USB-токена пользователь должен соблюдать ряд правил и требований, которые обеспечат сохранность конфиденциальной информации пользователя.

- Не разбирайте USB-токен.
- Не передавайте USB-токен третьим лицам.
- Не сообщайте третьим лицам пароли от ключей ЭП.
- Подключайте USB-токен к компьютеру только на время работы с системой «iBank 2».
- Не оставляйте компьютер с подключенным USB-токеном без принятия мер по защите от несанкционированного доступа к нему.
- Не допускайте использование одного и того же USB-токена несколькими лицами.
- Храните USB-токен в сейфе индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.
- В случае утери (хищения) или повреждения USB-токена немедленно свяжитесь с банком.