Рекомендации по информационной безопасности для клиентов РНКБ Банк (ПАО), при использовании систем дистанционного банковского обслуживания

В целях обеспечения информационной безопасности при работе в системах дистанционного банковского обслуживания РНКБ Online, Интернет Банк-Клиент (ИБК), а также для минимизации рисков информационной безопасности, обращаем Ваше внимание на необходимость выполнения следующих рекомендаций:

1. Обеспечение безопасности персонального компьютера (ПК).

- Управление и регистрация доступа третьих лиц к ПК, путем создания персонифицированных(личных) учетных записей, с ограничением прав на выполнение и установку постороннего ПО.
- Обеспечить безопасность помещения и исключить бесконтрольный доступ к ПК, используемому для работы в системе ИБК. Доступ к ПК должны иметь только доверенные лица.
- Использовать на ПК только лицензионные операционные системы или сертифицированные свободно распространяемые операционные системы с актуальными установленными обновлениями, в том числе обновлениями безопасности.
- Устанавливать на ПК для работы в системе ИБК минимально возможный набор программ, необходимых для работы в Системе ИБК. На компьютере не должны запускаться программы, полученные из непроверенных источников (особую опасность могут представлять программы, полученные по электронной почте или через Интернет).
- На компьютере обязательно должно быть установлено антивирусное программное обеспечение с регулярно обновляемыми базами. Периодически осуществляйте полную проверку компьютера на предмет наличия вирусов.
- Рекомендуется установить на компьютер персональный межсетевой экран.
- Работать в операционной системе только под правами пользователя. Использовать учетные записи с правами «администратор» / «локальный администратор» не рекомендуется.
- На компьютере не должны быть заведены учетные записи без паролей или с паролями по умолчанию. Учетная запись «Гость» должна быть заблокирована.
- Исключить доступ к ресурсам ПК для работы в Системе ИБК с других ПК локальной вычислительной сети. Не работать в системе ИБК с недоверенных компьютеров (Интернет-кафе и т.д.).
- Не устанавливать и не использовать программы удаленного доступа к компьютеру (TeamViewer, RAdmin и аналогичные). Ограничить доступ «Удаленного помощника».
- Осуществлять постоянный контроль отправляемых платежных документов при работе в Системе ИБК, а также состояние своего расчетного счета.

2. Обеспечение безопасности соединения с сетью Интернет.

- Компьютер, с которого осуществляется подготовка и отправка Электронных документов в Банк, необходимо выделить в отдельную доверенную зону, исключив его из общей локальной сети организации (Выделить ПК для работы в системе ИБК в отдельный сегмент локальной вычислительной сети). Для выделенной доверенной зоны установить полный запрет на доступ к ресурсам сети Интернет, за исключением настроек, необходимых для корректной работы в системе ИБК.
- В Браузере адрес Онлайн-сервисов Банка обязательно должен начинаться с https:// (а не http://).
- Ограничить обращения в браузере к нецелевым Интернет-ресурсам, кроме доступа в систему ИБК.

- Проверять информацию об IP-адресе, с которого осуществлялся предыдущий вход в Систему ИБК.
- Проверять в Браузере совпадение адреса страницы с Онлайн-сервисами с указанным на Официальном сайте Банка https://www.rncb.ru.
- Желательно подключить дополнительные услуги безопасности при работе в Системе ИБ:
  - подключение в Систему ИБК с определенного фиксированного набора ip-адресов;
  - СМС или телефонное подтверждение платежей;
  - услуга подтверждения клиентом платежей на новых получателей.
- Используйте надежные и проверенные проводные и беспроводные точки доступа к Сети Интернет. Не рекомендуется использовать непроверенные, общедоступные точки доступа Wi-Fi, Ehternet.

3. Обеспечение безопасности при работе с USB-токеном и его хранении.

- Подключать USB-токен с ключом ЭЦП необходимо только на время проведения операций. Не оставляйте USB-токен с ключом ЭЦП постоянно подключенным к ПК.
- В нерабочее время USB-токен необходимо хранить в сейфе или хранилище исключающем доступ посторонних лиц к USB-токену.
- Блокировать ключи ЭЦП и производить перевыпуск новых ключей ЭПЦ при замене должностных лиц, уполномоченных подписывать документы в системе ИБК.
- Не хранить два и более ключей ЭЦП с правами первой и второй подписи на одном USB-токене. На одном USB-токене должен быть записан только один ключ ЭЦП доступа в Систему ИБК.
- Необходимо незамедлительно сообщить в Банк в случае если USB-токен с ключами ЭЦП утерян, или у Вас имеется подозрение, что USB-токен оказались у посторонних лиц, даже на короткое время.

4. Обеспечение безопасности при работе с паролями.

- Стартовые пароли на USB-токен должны быть сменены на личные.
- Выбирайте свой пароль самостоятельно и никому его не сообщайте, в том числе сотрудникам Банка. Обязательно смените пароль в том случае, если он стал известен постороннему лицу.
- Пароль должен содержать не менее 8 символов. Желательно, чтобы пароль одновременно содержал символы в нижнем и верхнем регистрах, цифры и спецсимволы (!, @, &, *, %, …).
- Не хранить пароль от USB-токена в файлах на ПК или этикетках, прикрепленных к USB-токену, клавиатуре, ПК. В случае записали пароля на бумаге, храните его в месте, недоступном для посторонних лиц
- Не используйте в качестве пароля легко угадываемые комбинации символов:
  - последовательности символов состоящие из одних цифр (в том числе даты, номера телефонов и т.п.);
  - последовательности повторяющихся букв или цифр;
  - подряд идущие в раскладке клавиатуры или в алфавите символы;
  - имена и фамилии.
- Не сообщайте постоянный или одноразовые пароли, в том числе полученные в SMS-сообщениях или Push-уведомлениях никому, включая сотрудников Банка.
- При получении от Банка на Мобильном устройстве SMS-сообщения или Push-уведомления с одноразовым паролем на подтверждение операции, проверьте соответствие указанных в сообщении реквизитов с реквизитами, указанными Вами при формировании операции.

- При смене доверенного номера телефона, на который приходят SMS-сообщения или Push-уведомления необходимо **незамедлительно** обратиться в Банк и сообщить о смене номера.
- В случае утери телефона как можно скорее заблокируйте SIM-карту или Интернет-банк.

5. Действия при обнаружении попыток несанкционированного доступа

При обнаружении попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, необходимо незамедлительно отключить от ПК USB-токен и сообщить об этом в Банк по контактам, указанным на Официальном сайте Банка https://www.rncb.ru для блокировки ключей ЭЦП, используемых для работы в Системе ИБК.

Для предупреждения несанкционированного доступа к Системе ИБК важно обращать внимание на нестандартную работу ПК. Типичными признаками несанкционированного доступа к ПК Клиента являются:

- В строке Браузера адрес системы ИБК отличается от адреса, указанного на Официальном сайте Банка https://www.rncb.ru
- Наличие измененного интерфейса Системы ИБК при условии отсутствия уведомлений об обновлении со стороны Банка.
- Соединение устанавливается не по защищенному протоколу (в строке запроса браузера отображается **http://** вместо **https://**).
- Наличие ошибок сертификата сайта.
- Имеется подозрение на проникновение третьих лиц в ПК или удаленное управление ПК.
- Система 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 или несоответствие ранее установленной нумерации.
- В списке рабочих документов или выписке обнаружены посторонние расчетные документы, которые Клиентом не создавались.
- Внезапное отсутствие действующего закрытого ключа ЭЦП на USB-токене.
- Выход из строя ПК (отказ в работе, сбой в операционной системе или антивирусного ПО, отказ Системы ИБК в обслуживании по неустановленным причинам).

Обращаем внимание на то, что выполнение вышеуказанных рекомендаций позволит минимизировать риски несанкционированного списания денежных средств.

При любых подозрениях на несанкционированные действия следует незамедлительно отключить ПК от Сети Интернет, отключить от ПК USB-токен, обратиться в Банк по номерам телефонов, указанным на Официальном сайте Банка для блокировки ключей ЭЦП, используемых для работы в Системе ИБК.