Приложение

Рекомендации по информационной безопасности для клиентов РНКБ Банк (ПАО), использующих системы «Банк-Клиент» и «Интернет Банк-Клиент»

Системы **«Банк-Клиент»** и **«Интернет Банк-Клиент»** (далее – «Система»/«Системы») предназначены для подготовки, передачи по каналам связи и хранения финансовых документов, представленных в электронном виде (далее – «Электронный документ»).

Безопасность обмена Электронными документами обеспечивается посредством шифрования таких документов, использования электронной цифровой подписи (далее – «ЭЦП»), которая является аналогом собственноручной подписи, а также наличием защищенного канала передачи информации.

Шифрование и подпись Электронных документов осуществляется с помощью секретного ключа ЭЦП, находящегося на специально предназначенном для этого внешнем носителе, например, дискете, флеш-носителе, USB-токене (далее – «Внешний носитель»). Доступ к секретному ключу защищен паролем, известным только владельцу ключа ЭЦП. Не имея в распоряжении секретного ключа и не зная пароля доступа к нему, невозможно сформировать ЭЦП под Электронным документом.

Выполнение нижеследующих рекомендаций является необходимым условием обеспечения безопасности расчетов в Системах.

Для исключения доступа посторонних лиц к Вашим секретным ключам ЭЦП необходимо соблюдать следующие **меры безопасности ключевых носителей:**

1. Не храните ключи ЭЦП на жестком диске компьютера. Храните ключи ЭЦП только на Внешнем носителе в недоступном для посторонних лиц месте.
2. Используйте USB-токен для хранения ключа ЭЦП, так как использование USB-токена значительно повышает уровень сохранности Ваших ключей.
3. Пароль доступа к Внешнему носителю с ключом ЭЦП следует хранить отдельно. Не записывайте пароль доступа к секретному ключу на этикетках Внешних носителей.
4. Подключайте Внешний носитель с ключом ЭЦП только в момент подписания Электронных документов. Не оставляйте Внешний носитель с ключом ЭЦП постоянно подключенным к компьютеру.
5. Используйте Внешний носитель с ключами ЭЦП только для подписания Электронных документов.
6. Не используйте Внешний носитель с ключами ЭЦП для каких-либо других целей, в частности, не храните на них информацию произвольного содержания, не относящегося к работе с Системами.
7. Не копируйте содержимое Внешнего носителя и не передавайте его никому даже на короткое время.
8. Закончив работу в Системе или прервав ее (даже на несколько минут), не забудьте извлечь Внешний носитель и убрать его в доступное только Вам место.
9. В случае замены лица, например, при увольнении сотрудника, использующего ЭЦП, незамедлительно сообщите об этом администратору Систем в Банке по телефону: +7(495)232-90-85, 8 800 100-90-850 (звонок по России бесплатный) и произведите генерацию новых ключей ЭЦП.
10. В случае если Внешний носитель с ключами ЭЦП утерян, или у Вас имеется подозрение, что такие ключи оказались у посторонних лиц, даже на короткое время, незамедлительно

сообщите об этом администратору Систем в Банке по телефону: +7(495)232-90-85, 8 800 100-90-850 (звонок по России бесплатный)

При выборе пароля доступа к секретному ключу ЭЦП рекомендуем выполнять следующие **правила выбора пароля:**

1. Выбирайте свой пароль самостоятельно и никому его не сообщайте.
2. Постарайтесь запомнить свой пароль. Если Вы все-таки записали пароль на бумаге, храните его в месте, недоступном для посторонних лиц.
3. Пароль должен содержать не менее 6 различных символов. Чем сложнее будет пароль, тем труднее его будет подобрать.
4. Обязательно смените пароль в том случае, если он стал известен постороннему лицу.
5. Не используйте в качестве пароля:
   - 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.

Необходимо обеспечить **меры по защите компьютера**, с которого осуществляется работа в Системах:

1. Обеспечьте безопасность помещения и ограничьте доступ сотрудников и посторонних лиц к ключам ЭЦП и компьютерам с установленной Системой. Доступ должны иметь только доверенные лица.
2. Используйте лицензионное программное обеспечение из проверенных и надежных источников. Регулярно выполняйте обновления операционной системы и прикладного программного обеспечения, особенно в части безопасности.
3. На компьютере должно быть установлено антивирусное программное обеспечение с регулярно обновляемыми базами. Периодически осуществляйте полную проверку компьютера на предмет наличия вирусов.
4. На компьютере не должны запускаться программы, полученные из непроверенных источников (особую опасность могут представлять программы, полученные по электронной почте или через Интернет).
5. Крайне желательно установить на компьютер персональный межсетевой экран.

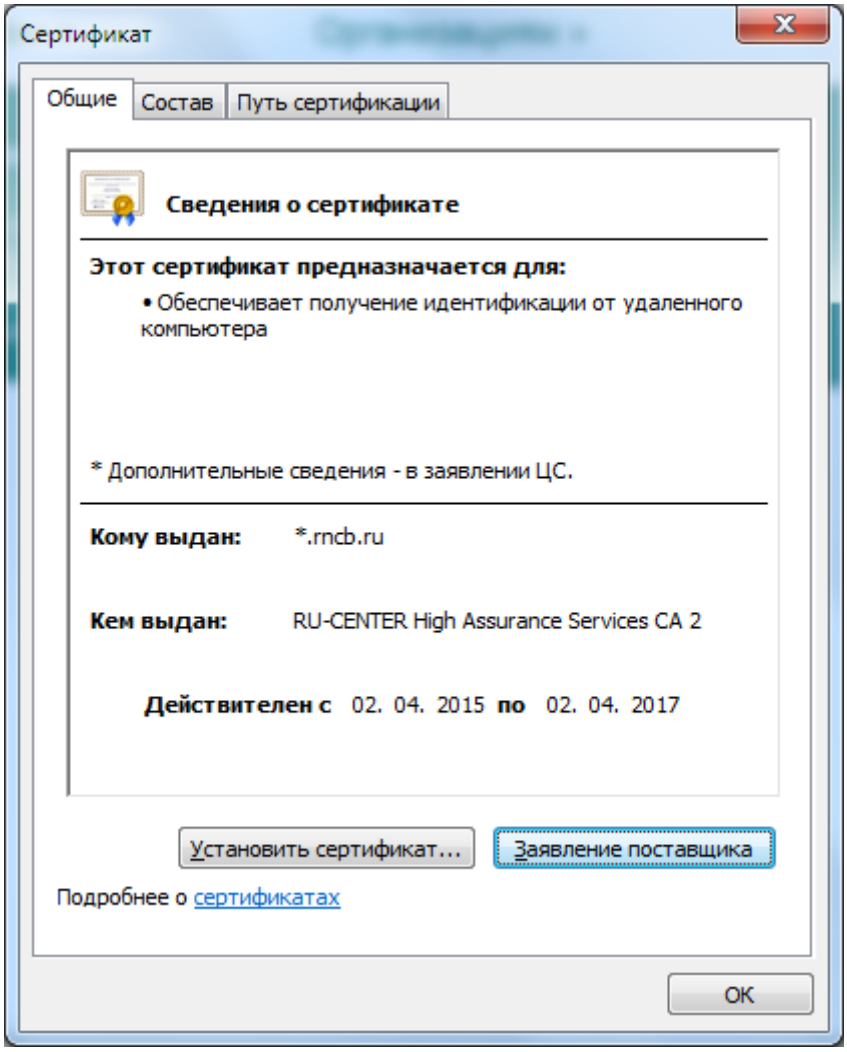
Для исключения возможности удаленного захвата управления вашим компьютером, с которого осуществляется обмен электронными платежами, мы рекомендует соблюдать **дополнительные меры** обеспечения безопасности, основанные на требованиях ЦБ РФ:

1. Компьютер, с которого осуществляется подготовка и отправка Электронных документов в Банк, необходимо выделить в отдельную доверенную зону, исключив его из общей локальной сети организации.
2. В зависимости от выбора канала передачи информации (TCP/IP, модем) настроить удаленную связь с Банком с учетом специфики их работы. Для модема – телефонная линия, для TCP/IP – шифрованный канал по заранее определенному порту.

3. Для выделенной доверенной зоны установить полный запрет на доступ к ресурсам сети Интернет, за исключением настроек, необходимых для корректной работы транспортной подсистемы Систем.
4. Крайне желательно использовать пароль на вход в клиентскую часть программного обеспечения системы «Банк-Клиент».
5. Осуществляйте постоянный контроль отправляемых платежных документов при работе с Системами, а также состояние своего расчетного счета.
6. Старайтесь не работать с недоверенных компьютеров (Интернет-кафе, киоски и т.д.).
7. Проверяйте информацию об IP-адресе, с которого осуществлялся предыдущий вход в систему «Интернет Банк-Клиент».
8. При обнаружении Вами попыток несанкционированного доступа или в случае мотивированных опасений, что такие попытки могут быть осуществлены, просим Вас:
   - незамедлительно сообщить об этом в Банк по телефону: +7(495)232-90-85, 8 800 100-90-850 (звонок по России бесплатный)
   - блокировать ключи ЭЦП, используемые для работы в Системе.

Пользователям системы **«Интернет Банк-Клиент»** рекомендуется соблюдать **меры по обеспечению безопасности соединения в сети Интернет**:

1. Используйте адрес https://ibank.rncb.ru/ (ip: 195.3.246.178) для входа на стартовую страницу Системы;
2. После входа на стартовую страницу Системы проверьте соответствие сертификата соединения приведенному ниже рисунку (для этого используете символ замка в окне браузера):



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