ПОЛОЖЕНИЕ о минимальных требованиях по предоставлению удаленного/дистанционного обслуживания в Кыргызской Республике (утверждено постановлением Правления Нацбанка КР от 15 апреля 2015 года N 22/3)

Информация для пользователя

(В редакции постановления Правления Нацбанка КР от 8 июня 2017 года № 2017-П-14/23-14)

Для обеспечения безопасности в процессе проведения операций в рамках удаленных/дистанционных обслуживаний и защиты персональных данных, пользователи должны быть проинформированы о своих обязанностях и ответственности.

1. Пользователь при использовании интернет-банкинга должен:

1) использовать безопасный логин и пароль/персональный идентификационный номер, при этом не раскрывать посторонним лицам свой логин, пароль и персональный идентификационный номер;

- не хранить свой логин, пароль и персональный идентификационный номер на устройствах доступа (персональный компьютер, мобильный телефон, и т.д.) или других незащищенных носителях;

- периодически менять код, пароль и персональный идентификационный номер, не использовать пароли с низким уровнем защиты, такие как имя или дата рождения. Пароль должен содержать комбинацию, состоящую из не менее 6 знаков: букв (прописных и заглавных), специальных символов и цифр;

2) обеспечить конфиденциальность личной информации, при этом:

- не раскрывать личную информацию (номер телефона или паспорта, номер банковского счета или адрес электронной почты) посторонним лицам;

3) сохранять информацию об электронных операциях, при этом:

- необходимо регулярно проверять историю операций и выписки для отслеживания ошибок или неавторизированных операций по счету;

- незамедлительно информировать поставщика удаленного/дистанционного обслуживания о любых случаях неавторизированного использования счета или проведения операций;

4) проверять правильность и безопасность веб-страницы, при этом:

- перед осуществлением любых он-лайн операций или предоставление личной информации должен убедиться, что используется правильная веб-страница интернет-банкинга и мобильного банкинга. Необходимо остерегаться фальшивых веб-страниц, созданных в целях мошенничества;

- должен убедиться в безопасности веб-страницы, проверив наличие Унифицированных Указателей Ресурсов (URL), которые должны начинаться с "https", а на статусе интернет-браузера должен появиться знак защищенного соединения;

- всегда вводить URL веб-страницы непосредственно в интернет-браузер. Избегать перенаправления или ссылки на другие ненадежные страницы;

- по возможности, использовать программу, которая автоматически шифрует или кодирует передаваемую информацию в процессе осуществления электронных операций;

5) защитить свое устройство доступа (персональный компьютер, мобильный телефон и т.д.) от несанкционированного доступа и вредоносных программ, при этом следить за регулярным обновлением антивирусной программы и ее постоянной работой;

6) необходимо покинуть сайт, где осуществляются электронные операции, даже если компьютер оставлен без присмотра на короткий срок;

- не забывать выходить из системы после осуществления электронных операций;

7) ознакомиться с политикой безопасности системы интернет-банкинга:

- необходимо внимательно ознакомиться с условиями системы интернет-банкинга относительно осуществления платежей, переводов, дебетования/кредитования счета и другими условиями банковского обслуживания;

- перед вводом личной финансовой информации системы интернет-банкинга, необходимо внимательно ознакомиться с условиями использования или распространения данной информации.

2. Пользователь при использовании мобильного банкинга должен:

- не раскрывать посторонним лицам свой персональный идентификационный номер (ПИН), пароль, пароль от электронной почты, иные сведения, которые могут способствовать несанкционированному доступу при удаленном/дистанционном обслуживании от имени пользователя;

- периодически менять свой персональный идентификационный номер, используемый для мобильного банкинга;

- не позволять другим использовать свой мобильный телефон, через который осуществляется банковская операция;

- при потере или краже мобильного телефона, нужно незамедлительно сообщить в обслуживающий банк/оператору связи/оператора платежной системы;

- не отправлять свою личную информацию, особенно пароль или персональный идентификационный номер через электронную почту, социальные сети и другие средства электронного обмена данными;

- незамедлительно сообщить поставщику услуг при возникновении любых вопросов относительно безопасности банковского счета.

Необходимые меры для обеспечения безопасного хранения карт, их реквизитов, персонального идентификационного номера и безопасности других данных определены в нормативных правовых актах Национального банка.