Приложение 11
к Договору дистанционного банковского обслуживания
в системе «Интернет-банкинг» («VTB Online banking»)

Процедура по обеспечению безопасности при работе в системе «Интернет-банкинг» («VTB Online banking»)

1. Система «Интернет-банкинг» («VTB Online banking») (далее - «система «Интернет-банкинг») предназначена для удаленного управления банковским (-ими) счетом (-ами) и получения иных электронных банковских услуг через общедоступную сеть Интернет с гарантированным уровнем безопасности, основанного на механизмах шифрования информации с помощью протокола SSL (Secure Sockets Layer), который обеспечивает установление безопасного соединения между Клиентом и Банком, а также подтверждения всех операций Электронно-цифровой подписью и паролем безопасно хранящихся на специальных электронных носителях e-Token PRO 72k Java.
2. В целях обеспечения гарантированного уровня безопасности система «Интернет-банкинг» включает в себя следующие средства защиты:
   1) каналы связи предоставляются провайдером сети Интернет с применением услуг по защите от нелегитимного трафика;
   2) для сетевой безопасности Банка, а также разграничения сетевого доступа, применяются программно-аппаратные фаерволы с функциями пакетной фильтрации, а также средства аутентификации, идентификации и анализа трафика и журналов оборудования;
   3) отсутствие хранения конфиденциальной информации на опубликованном в глобальной сети Интернет Web-сервере;
   1) осуществление безопасного обмена данными между Клиентом и сервером системы «Интернет-банкинга» путем использования алгоритмов шифрования трафика, которые позволяют исключить ситуацию подмены сервера, раннее выявление недостатков в системе безопасности за счет сопоставления протоколов обмена сообщениями на стороне Клиента и сервера. Конфиденциальность передаваемой информации обеспечивается шифрацией данных посредством протокола SSL (Secure Sockets Layer), с использованием процедур аутентификации, авторизации для осуществлений входа в систему «Интернет-банкинг» и подтверждения операций, а также аппаратно-программным комплексом двухфакторной аутентификации и безопасного хранения Электронно-цифровой подписи e-Token PRO 72k Java;
   2) устройство e-Token PRO 72k Java предоставляет собой защищенный носитель, предназначенный для строгой аутентификации, безопасного хранения секретных данных, выполнения криптографических вычислений и работы с асимметричными ключами, цифровыми сертификатами, ключами шифрования и Электронно-цифровой подписи. E-Token PRO 72k Java сертифицирован и соответствует 3 (третьему) уровню безопасности по стандарту СТ РК 1073-2007, что совместно с использованием криптоаплета TumarCSP и сертификата РГП КЦМР «KISC Certificate RK-02» и позволяет превзойти 3 (третий) уровень защиты системы по СТ РК 1073-2007 *(СКЗИ третьего уровня безопасности предназначены для защиты информации, ущерб от изменения которой в объеме использования одного и того же ключа (одних и тех же ключей), не превышает 1 000 000 (один миллион) минимальных расчетных показателей.)* Устройство позволяет осуществлять механизм Электронно-цифровой подписи так, чтобы закрытый ключ безопасно хранился и никогда не покидал устройства;
   3) пароль на ключевой контейнер Клиент Банка должен изменить со стандартного при первом подключении Защищенного носителя ЭЦП - eToken PRO 72K (Java) самостоятельно. Предложение о смене пароля будет сгенерировано криптопровайдером Tumar CSP автоматически. Выполнение операций в системе «Интернет-банкинг» без смены стандартного пароля невозможно;
   4) целостность передаваемой информации обеспечивается хешированием каждого SSL пакета;
   5) подлинность информации обеспечивается применением Электронно-цифровой подписи;

6) для регистрации Клиента в качестве Пользователя системы «Интернет-банкинг» требуется наличие у Клиента открытого текущего счета в Банке, логина, пароля и устройства e-Token PRO 72k Java для входа в систему «Интернет-банкинг» с Регистрационным свидетельством Электронно-цифровой подписи, зарегистрированным в уполномоченном Удостоверяющем центре, а именно в Казахстанском центре межбанковских расчетов (КЦМР);

7) при осуществлении первого входа в систему «Интернет-банкинг», неперсонифицированным паролем, полученным при регистрации в Банке, в защищенном Пин-конверте, происходит обязательная смена пароля. Требования к паролю в целях безопасности регламентированы следующим образом:

- если компьютер после входа Клиентом/Пользователем в систему «Интернет-банкинг» остается бездействующим более 10 (десяти) минут, системой «Интернет-банкинг» осуществляется автоматический выход из системы «Интернет-банкинг» и завершение сессии;
- проверка подлинности запроса Клиента о получении электронной банковской услуги через систему «Интернет-банкинг» осуществляется Банком автоматически посредством запроса Электронно-цифровой подписи. При этом каждое действие Клиента в системе «Интернет-банкинг», требует подтверждения, посредством Электронно-цифровой подписи, хранящейся на защищенном носителе Электронно-цифровой подписи – e-Token PRO 72K (Java), при этом Клиенту, потребуется вручную вводить пароль для доступа к ключевому контейнеру Электронно-цифровой подписи, тем самым подтверждая валидность операций, что защищает Клиента от мошеннических действий злоумышленников и киберпреступников.

3. В целях обеспечения гарантированного уровня безопасности при работе в системе «Интернет-банкинг», Клиенту/Пользователю (-ям) системы «Интернет-банкинг» необходимо на своем рабочем месте обеспечивать должный уровень безопасности, включая, но не ограничиваясь:

1) при входе в систему «Интернет-банкинг» вводить только имя Пользователя, логин и пароль. Никакой другой информации Банк не запрашивает;

2) использовать отдельный компьютер с ограниченным физическим доступом, исключительно для работы в системе «Интернет-банкинг», другие действия на этом компьютере осуществляться не должны, а именно, такие как работа с другими программами, электронной почтой, посещения сайтов в Интернете;

3) осуществлять безопасное хранение Комплекта ключей только на съемном носителе (USB Flash - eToken PRO 72k Java), использование которого осуществлять при условии недопущения передачи вторым лицам (включая работников Банка и работников Клиента или их родственников). Установка USB eToken на рабочее место допускается только непосредственно на время работы с системой «Интернет-банкинг»;

4) в случае использования нескольких ключей при работе в системе «Интернет-банкинг» (первой и второй подписи) не переносить эти ключи на один USB eToken, а также не подключать одновременно различные USB eToken **(**ключевые носители) к компьютеру;

5) обеспечивать недопущение разглашения личного логина и любого из паролей, сформированных для работы в системе «Интернет-банкинг» вторым лицам (включая работников Банка и работников Клиента или их родственников);

6) обеспечивать недопущение использования различного нелицензионного, стороннего, сомнительного, а также не проверенного программного обеспечения на наличие вредоносных программ;

7) обеспечивать обязательное использование лицензионного, своевременно обновляющегося антивирусного программного обеспечения. Действие вирусов может быть направлено на перехват идентификационной информации Пользователя и передаче ее злоумышленникам;

8) обеспечивать использование современных операционных систем своего компьютера, с автоматическим своевременным обновлением, рекомендуемым компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполнять обновления (патчи) операционной системы и браузера Вашего компьютера, что значительно повышает уровень безопасности;

9) не подключать к компьютеру не проверенные на наличие вирусов отчуждаемые носители информации;

10) в целях обеспечения дополнительной безопасности Пользователь при вводе пароля может использовать «Виртуальную клавиатуру», исключая тем самым возможность перехвата вводимых символов;

11) не использовать в пароле свое имя, дату рождения, только цифры или простые слова, длина пароля должна быть не менее 8 (восеми) символов. Необходимо стараться применять в сочетании заглавные буквы, цифры и специальные символы;

12) срок действия между обязательной смены пароля составляет 30 (тридцать) календарных дней;

13) никогда не сохранять пароль (-и) в программах, устанавливающих Интернет-соединение, в текстовых файлах на компьютере либо на других электронных носителях информации, так как при этом существует риск его кражи и компрометации;

14) после окончания работы необходимо закрывать окно системы «Интернет-банкинг» с помощью кнопки «Выход» и никогда не оставлять компьютер с текущей сессией в системе «Интернет-банкинг» без присмотра;

15) производить замену ключей ЭЦП до истечения срока их действия. Кроме того, необходимо проводить замену ключей ЭЦП во всех случаях увольнения и\или смены лиц, имеющих доступ к системе «Интернет-банкинг», а также руководителей с правом подписи доверенностей на получение ключей ЭЦП, и в случае подозрения на их компрометацию;

16) в случае сбоев в работе компьютера или его поломки во время работы с системой «Интернет-банкинг» или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска и т.п.), следует немедленно извлечь ключи и выключить компьютер, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции;

17) при возникновении любых сомнений в правильности функционирования системы «Интернет-банкинг» незамедлительно обратиться в Банк;

18) в случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении системы «Интернет-банкинг» отложите совершение операций и обратитесь в Группу поддержки пользователей Банка.

4. После 3 (трех) попыток неверного ввода пароля, Банк автоматически осуществляет блокирование пароля Пользователя сроком на 30 (тридцать) минут. Если данное событие происходит повторно в течение полутора часов система «Интернет-банкинг» автоматически формирует почтовое сообщение сотрудникам Управления безопасности, которые принимают меры и при необходимости блокируют Пользователя в системе «Интернет-банкинг». Если Пользователь по каким-либо причинам не может вспомнить свой пароль, то ему необходимо обратиться в подразделение Банка для получения неперсонифицированного пароля в Пин-конверте и осуществить вход в систему «Интернет-банкинг» с последующей сменой пароля.
5. По желанию Пользователя возможно предусмотреть дополнительные меры по реализации защиты и безопасности информации при работе в системе «Интернет-банкинг», например, такие как: организация фильтрации доступов по идентификационным признакам (фильтрация внутренних IP, фильтрация внешних IP, фильтрация по MAC адресам), а также настройка доступа по временным критериям.
6. Для осуществления анализа спорных ситуаций, Банком обеспечивается ведения архива всех отосланных/принятых Пользователем Клиента и Банком Электронных документов. Все действия Пользователей Клиента в системе «Интернет-банкинг» записываются в электронные журналы, сформированные системой «Интернет-банкинг».
7. При обнаружении несанкционированного доступа и/или попыток такого доступа к информации, составляющей банковскую тайну, ее несанкционированного изменения, осуществления несанкционированного платежа или перевода денег и иных несанкционированных действий, а также ситуаций, представляющих угрозу информационной безопасности Банка и Клиента, возникающих при предоставлении Банком электронных банковских услуг, Банк уведомляет об этом Клиента, не позднее следующего рабочего дня после их обнаружения путем направления таких уведомлений по уполномоченным электронным каналам связи и незамедлительно принимает все необходимые меры для устранения их последствий и предотвращения их появления в будущем.
8. В случае возникновения несанкционированных действий, указанных в пункте 7 настоящих Процедур, Банк вправе приостановить предоставление электронных банковских услуг посредством системы «Интернет-банкинга».