ЗАО “ТОЙОТА БАНК”
109028, РОССИЯ, Г. МОСКВА
СЕРЕБРЯНИЧЕСКАЯ НАБЕРЕЖНАЯ, Д. 29
Т+7 495 644 1000 Ф+7 495 644 1024

FINANCIAL SERVICES | TOYOTA

# Памятка по информационной безопасности при использовании системы ДБО «Клиент-Банк».

Под информационной безопасностью понимается защищенность системы ДБО «Клиент-Банк» от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, а также от попыток хищения, модификации или разрушения ее компонентов.

При использовании системы ДБО «Клиент-Банк» необходимо значительное внимание уделять вопросам безопасности и надежности функционирования системы ДБО «Клиент-Банк».

Безопасность любого компонента данной системы достигается обеспечением трех его характеристик: целостности, доступности и конфиденциальности.

- Целостность компонента системы предполагает, что при функционировании системы информация может быть изменена только теми пользователями, которые имеют на это право.
- Доступность предусматривает действительную доступность компонента авторизованному (т.е. допущенному) пользователю в любое время.
- Конфиденциальность состоит в том, что определенная часть информации предоставляется только авторизованным пользователям.

Одними из важнейших аспектов проблемы обеспечения безопасности системы ДБО «Клиент-Банк» являются определение, анализ и классификация всех возможных угроз безопасности. Различают две основные группы угроз.

К первой группе относятся так называемые случайные (непреднамеренные) угрозы, которые по своей сути не зависят от человека (например, стихийные бедствия), а также угрозы, обусловленные ошибками эксплуатации аппаратных и программных средств, сбоями и отказами работы оборудования и средств передачи данных и т.д.

Вторую группу составляют преднамеренные угрозы, приводящие к непосредственному раскрытию, изменению, хищению или уничтожению данных. Этот вид угроз исходит и от внутренних участников системы (сотрудники Банка и Клиента), и от внешних, так называемых «хакеров» и других злоумышленников.

Наиболее распространенной угрозой безопасности системы ДБО «Клиент-Банк» является несанкционированный доступ в систему и к его компонентам. Поэтому для Банка важно создать надежную интегрированную многоуровневую систему защиты, включающую такие средства защиты, как правовые (законодательные), организационные, физические и программно-аппаратные. При этом наилучший успех в достижении высокой степени защищенности системы ДБО достигается только на основе их комплексного использования.

Соблюдение правил информационной безопасности обеспечивает защищенность интересов Банка и Клиентов, в условиях угроз в информационной сфере при оказании услуг дистанционного банковского обслуживания.

Защищенность достигается обеспечением совокупности свойств информационной безопасности: конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры. Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению случайных или злонамеренных воздействий.

Главный инструмент Банка и Клиента основан на опыте прогноза (составление модели угроз и модели нарушителя), а также работа с персоналом по повышению его бдительности в возможных критических условиях, готовности и способности к адекватным действиям в условиях потенциальной злоумышленной активности.

Для использования в работе с системой ДБО «Клиент-Банк» предлагаются «Рекомендации по информационной безопасности при использовании системы ДБО» (Приложение 1 к настоящей Памятке) и «Регламент использования носителей ключевой информации» (Приложение 2 к настоящей Памятке).

Приложение 1

**Рекомендации по информационной безопасности при использовании системы ДБО.**

Для минимизации рисков при дистанционном банковском обслуживании рекомендуется:

- Использовать в работе лицензионную версию системы ДБО «Клиент-Банк»;
- Производить обучение эксплуатации системы ДБО «Клиент-Банк» пользователей, работающих с системой;
- В целях снижения вероятности выполнения непреднамеренных, случайных операций организовать:
  - ✓ разграничение по пользователям системы ДБО «Клиент-Банк» прав на выполнение операции: создание документа, подпись документа, отправка документа;
  - ✓ отслеживание специального реквизита документа «Статус», который предназначен для отображения различных этапов обработки конкретного документа.
- На основе прогноза, базирующегося на анализе и оценке рисков информационной безопасности, разработать и постоянно совершенствовать Политику информационной безопасности в вопросах дистанционного банковского обслуживания, которая в обязательном порядке должна содержать:
  - ✓ требования к внешним аппаратным и программным средствам, обеспечивающим информационную безопасность каналов связи в вопросах взаимодействия в рамках дистанционного банковского обслуживания;
  - ✓ требования к обязательности предоставления провайдерами Интернет-услуг механизмов защиты;
  - ✓ последовательность необходимых действий, осуществляемых при возникновении внештатной ситуации или при подозрении на неё.
  - ✓ перечень событий, наступление которых должно повлечь за собой немедленную замену/изъятие ключей электронной цифровой подписи.
- Разработанная Политика информационной безопасности должна доводиться до сведения всех сотрудников, работа которых связана с системой ДБО «Клиент-Банк»;
- Использовать все возможности общесистемных программно-аппаратных решений, повышающих уровень безопасности, в частности:
  - ✓ ограничение на сетевом брандмауэре IP-адресов, с которых допустима работа с системой ДБО «Клиент-Банк»;

  Целесообразность ограничения диапазона IP-адресов именно на сетевом брандмауэре, вместо проверки IP- и MAC-адресов непосредственно в системе ДБО «Клиент-Банк» обусловлена следующими факторами:

  - Невозможность в большинстве случаев достоверного определения системой ДБО «Клиент-Банк» IP-адреса клиентской машины в связи с тем, что соединение между клиентской и банковской частью производится через промежуточные proxy-сервера и брандмауэры.

  - Широкое использование в настоящее время механизма динамического предоставления IP-адреса (DHCP). Необходимость указания в роли допустимого адреса широкого диапазона IP-адресов практически сводит на нет эффект от применения таких мер.

  - ✓ использование аппаратных устройств — токенов для хранения ключевой информации.
- Использовать и постоянно обновлять персональные средства защиты, антивирусного программного обеспечения, средств обнаружения вредоносных программ.

Приложение 2

## Регламент использования носителей ключевой информации.

- Установка и настройка системы ДБО «Клиент-Банк» на АРМ пользователей производится с учетом установленных требований.
- Определяется и утверждает порядок учета, хранения и использования носителей ключевой информации (ключевых дискет, ключевых идентификаторов touch memory, ключевых смарт-карточек) с секретными ключами и ключами шифрования, который должен полностью исключать возможность несанкционированного доступа к ним.
- Утверждается список лиц, имеющих доступ к секретным ключам и ключам шифрования (с указанием конкретной информации для каждого лица), и выдаются данные ключи их владельцам под роспись. Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен.
- Для хранения носителей ключевой информации с секретными ключами и (или) ключами шифрования должны использоваться надежные металлические хранилища.
- В течение рабочего дня вне времени использования секретных ключей и (или) ключей шифрования, а также по окончании рабочего дня носители ключевой информации с секретными ключами и (или) ключами шифрования помещаются владельцем ключа в хранилище.
- При транспортировке носителей ключевой информации с секретными ключами и (или) ключами шифрования соблюдаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.
- Не допускается:
    - ✓ снимать несанкционированные копии с носителей ключевой информации;
    - ✓ знакомить с содержанием носителей ключевой информации или передавать носители ключевой информации лицам, к ним не допущенным;
    - ✓ выводить секретные ключи и (или) ключи шифрования на дисплей (монитор) электронно-вычислительной машины или принтер;
    - ✓ устанавливать носитель секретных ключей и (или) ключей шифрования в считывающее устройство АРМ пользователей, программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие электронно-вычислительной машины;
    - ✓ записывать на носители ключевой информации постороннюю информацию.
- При компрометации секретного ключа и (или) ключа шифрования владелец ключей, допустивший компрометацию, обязан предпринять все меры для прекращения любых операций с использованием этого ключа и немедленно проинформировать о факте компрометации ответственное лицо Банка, который организует внеплановую смену ключей и (или) ключей шифрования.

  По факту компрометации секретного ключа и (или) ключа шифрования организовывается служебное расследование.
- В случае увольнения или перевода в другое подразделение (на другую должность), изменения функциональных обязанностей работника, имевшего доступ к секретным ключам и (или) ключам шифрования, должна быть проведена сдача ключей, к которым указанный работник имел доступ, ответственному лицу Банка.