Приложение 3 к Условиям предоставления
ПАО КБ «Центр-инвест» услуги
«Дистанционное банковское обслуживание»

Рекомендации по обеспечению информационной безопасности в системе дистанционного банковского обслуживания

Клиент в полном объеме несет ответственность за информационную безопасность и сохранность оборудования (АРМ клиента), с которого осуществляется доступ к СДБО, а также за обеспечение доступа к носителям ключевой информации, СКЗИ с неизвлекаемыми ключами и другим средствам ЭП и защиты информации круга доверенных лиц, обладающих правом ЭП.

- Клиент обязуется не допускать загрузку *на устройстве используемом для работы с СДБО* резидентных или иных программ, допускающих несанкционированный доступ к устройствам накопления информации и устройствам ввода/вывода и (или) способных вмешиваться в работу СДБО.
- Клиент обязуется обеспечить информационную безопасность *устройства используемого для работы с СДБО*, включая отсутствие на оборудовании с которого осуществляется использования системы банк-клиент компьютерных вирусов, “троянских программ” и иного вредоносного программного обеспечения.
- Клиент несет ответственность за режим доступа к *устройства используемого для работы с СДБО*, сохранность и конфиденциальность отчуждаемого носителей ключевой информации, СКЗИ с неизвлекаемыми ключами и других средств ЭП и защиты информации, реквизитов доступа и других средств защиты информации используемых при работе с СДБО.

Банк считает необходимым соблюдение Клиентами следующего комплекса мер по защите информации:

1. Обеспечение безопасности компьютера, с использованием которого осуществляется работа в системе ДБО:

- *Устанавливайте, используйте и регулярно обновляйте только лицензионное программное обеспечение*, а также свободное программное обеспечение поддерживаемое разработчиками или сообществом. Это позволит снизить риск использование уязвимостей злоумышленниками.
- *Установите и регулярно обновляйте* антивирусное программное обеспечение. При выборе рекомендуется отдавать предпочтение комплексным решениям (содержащим в своем составе персональный брэндмауэр, модули поиска шпионских компонент, а также защиты электронной почты) ведущих разработчиков антивирусного программного обеспечения. Это позволит снизить риск действия вредоносных программ.
- *Своевременно устанавливайте обновления операционной системы своего компьютера*, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей. Регулярно выполняйте обновления (патчи) операционной системы и браузера Вашего компьютера, что значительно повысит его уровень безопасности.
- *Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере или используйте комплексное антивирусное решение содержащее брандмауэр в своем составе***.** Это позволит Вам снизить риск несанкционированного удаленного доступа к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа. Дополнительно можно настроить брандмауэр на доступ только по адресам системы ДБО (https://dbo.centrinvest.ru).
- *Не устанавливайте и не применяйте на устройстве, используемом для работы с СДБО* программное обеспечение полученное из сомнительных источников.
- *Минимизируйте количество используемых браузерных плагинов на устройстве используемом для работы с СДБО*, а также внимательно относитесь к источникам их установки.
- В обязательном порядке следует отключать Автозапуск в операционной системе (для OS Windows: «Панель управления» -> «Администрирование» -> «Службы»; необходимо найти в закладке «Расширенный» службу «Определение `оборудования оболочки» и установить «Отключено»).
- *Исключите посещение с устройства, используемого для работы с СДБО, сайтов сомнительного содержания и любых других Интернет-ресурсов* (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов от недостоверных источников. *Использование устройства используемого для работы с СДБО для интернет-серфинга, а также работы с электронной почтой* существенно повышает риски использования системы СДБО.

- *Категорически не рекомендуется работать с системой ДБО с компьютеров, не заслуживающих доверия* (интернет-кафе), т.к. это существенно увеличивает риск хищения Ваших персональных данных.
- *Регулярно контролируйте состояние своих счетов* и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.
- *На компьютере не рекомендуется устанавливать иное программное обеспечение*, кроме необходимого для работы в системе ДБО. Рекомендуется использовать для работы с Банком выделенный компьютер.
- *Права пользователя, работающего с системой ДБО, на данном компьютере должны быть минимально необходимыми* (наличие прав администратора нежелательно).
- Клиент должен исключать установку *на устройстве используемом для работы с СДБО* программами и/или сервисов удаленного доступа и (или) администрирования и не привлекайть для администрирования и обслуживания компьютера с системой ДБО технических специалистов на условиях предоставления им удаленного доступа к устройству.
- При наличии технической возможности (если вы работаете стационарно и имеете статический IP-адрес), ограничьте доступ в СДБО по IP адресу, передав в банк заявление приведенное в приложении 11.

2. Соблюдение правил безопасности при работе с ключевыми носителями:

- *Храните ключи только на съемном (отчуждаемом) носителе.* По возможности используйте съемные защищенные носители информации или СКЗИ с неизвлекаемыми ключами. Хранение ключевых носителей должно быть организовано в месте, недоступном для посторонних лиц. Установка ключевых носителей на рабочее место допускается только непосредственно на время работы с системой ДБО.
  ВАЖНО: *После окончания сеанса работы в системе ДБО съемный ключевой носитель должен быть незамедлительно извлечен из компьютера!*
- Ключевой носитель или СКЗИ с незивлекаемыми ключами не должны быть доступен по сети, храниться и (или) применяться в качестве сетевого ресурса. Допускается только локальное применение ключевого носителя на устройстве, используемом для работы в СДБО. Подключение отчуждаемого носителя ключевой информации или СКЗИ с неизвлекаемыми ключами по локальной сети не допускается.
- Генерацию ключей ЭП осуществляйте лично с записью ключевой информации на съемный носитель или используйте для этих целей СКЗИ с неизвлекаеымми ключами. Не допускайте копирования сгенерированных ключей ЭП.
- *После окончания работы в системе ДБО обязательно корректно завершите работу* (выйдите из системы ДБО с использованием кнопки «Выход») и/или закройте используемый для работы с ДБО браузер.
  ВАЖНО: *Извлеките из компьютера съемный ключевой носитель!*
- *Производите замену ключей ЭП заблаговременно до истечения срока их действия.* Кроме того, проводите замену ключей ЭП во всех случаях увольнения и/или смены лиц, имеющих доступ к системе ДБО, а также руководителей с правом подписи доверенностей на получение ключей ЭП, и в случае подозрений на их компрометацию.

3. Соблюдение правил безопасности при использовании средств доступа (логинов/паролей):

- Логины и пароли для работы в системе ДБО – это Ваша персональная (учетная) конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте свой логин и пароль никому, включая сотрудников Банка. При обращении от имени Банка по телефону, электронной почте, через SMS лиц с просьбами сообщить конфиденциальную информацию (пароли, кодовые слова, и т.д.) ни при каких обстоятельствах не следует сообщать данную информацию.
- Не сохраняйте Ваш логин и пароль в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.
- Не используйте механизмы сохранения паролей в браузерах и (или) программные продукты (сервисы) по менеджменту паролей для учетных данных системы СДБО.

4. Выполнение правил безопасности при работе в системе ДБО:

- *В случае сбоев в работе компьютера или его поломки во время работы в системе ДБО или сразу после сеанса* (проблемы с загрузкой операционной системы, выход из строя жесткого

диска, и т.п.), *следует НЕМЕДЛЕННО извлечь ключи ЭП и выключить компьютер, а также обратиться в Банк* и убедиться, что от Вашего имени не производились несанкционированные операции (путём сверки операций за день).

- *Обращайте внимание на любые изменения в привычных для Вас процессах установления соединения с системой ДБО или в функционировании системы ДБО*. При возникновении любых сомнений в правильности функционирования системы ДБО незамедлительно обратитесь в Банк.
- При работе с системой ДБО (сервис «Интернет-Клиент») убедитесь, что защищенное соединение по протоколу https установлено именно с официальным сайтом услуги (https://dbo.centrinvest.ru/) и проконтролируйте корректно ли указан его адрес. Настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка www.centrinvest.ru) или поступивших по электронной почте писем. После входа на сайт, перед началом работы, убедитесь в корректности сертификата безопасности банка.
- В случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении к системе ДБО Банка, отложите совершение операций и обратитесь в службу поддержки Банка.
- В случае утраты ключевого носителя (или СКЗИ с неизвлекаемыми ключами), утраты ключей от хранилища в момент нахождения в нем ключевого носителя, а также в случае возникновения ситуации, связанной с временным доступом посторонних лиц к ключевому носителю (или СКЗИ с неизвлекаемыми ключами) либо в связи с подозрением, что такой доступ имел место, необходимо незамедлительно обратиться в Банк в связи с компрометацией ключа ЭП. Аналогичные действия следует предпринимать в случае компрометации имени пользователя и пароля СДБО, либо утраты TAN-карты или OTP-токена.

ВНИМАНИЕ!
Незамедлительное обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств со счетов может позволить оперативно приостановить транзакцию и предотвратить финансовые потери.