ПАО Банк «Кузнецкий» постоянно совершенствует комплексную защиту системы дистанционного банковского обслуживания (далее – Система ДБО), поскольку любые операции с использованием Интернета сопряжены с рисками, в том числе угрозами хакерских атак и несанкционированного доступа к денежным средствам. От того, насколько неукоснительно будут соблюдаться приведенные ниже рекомендации, зависит безопасность Ваших операций и Ваших средств в Системе ДБО. С данными требованиями необходимо ознакомить сотрудников Вашей организации, непосредственно работающих с Системой ДБО, а также Ваших специалистов по информационным технологиям и по обеспечению безопасности, в том числе информационной.

В целях снижения риска хищения денежных средств с использованием Системы ДБО рекомендуем придерживаться приведенных ниже правил:

1. Не использовать при работе с Системой ДБО компьютер с установленной операционной системой Windows XP.
2. Использовать для работы с Системой ДБО современные браузеры, поддерживающие работу по протоколу не ниже TLS 1.1 (например, Internet Explorer 11, Microsoft Edge, Yandex Browser, Mozila FireFox 27, Chrome 30, Opera 17)…
3. Осуществлять смену пароля на доступ к Системе ДБО при первом входе в систему и в последующем не реже 1 раза в 3 месяца.
4. Осуществлять работу в системе ДБО под учетной записью пользователя с минимальными правами доступа к операционной системе (пользователь, осуществляющий работу в системе ДБО должен отсутствовать в группе Администраторы).
5. Использовать для хранения файлов с секретными ключами ЭП отчуждаемые носители eToken ГОСТ, ruToken-ЭЦП 2.0, jaCarta-ГОСТ и систему SafeTouch.
6. Отключать, извлекать носители с ключами ЭП из компьютера, после приема или передачи информации.
7. Хранить вне сеансов связи носители с ключами ЭП в сейфе или другом, недоступном для посторонних лиц месте.
8. Ограничить физический и логический доступ (завести персонифицированные учетные записи) к компьютеру, используемому для работы с системой ДБО. Исключить на данном компьютере посещение Интернет сайтов отличных от Системы ДБО, загрузку и установку нелицензионного программного обеспечения и развлекательного контента, электронной почты.
9. Применять на рабочем месте специализированные лицензионные программные средства безопасности: антивирусное программное обеспечение, персональные межсетевые экраны, программы антиспам и антишпион.
10. Ограничить доступ из локальной сети к ресурсам компьютера, предназначенного для работы в Системе ДБО.
11. Установить и настроить персональный брандмауэр (firewall). Это позволит запретить несанкционированный удаленный доступ 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://dbo2.kuzbank.ru).
12. При работе с Системой ДБО убедитесь, что защищенное соединение по протоколу https установлено именно с официальным сайтом услуги (https://dbo2.kuzbank.ru).
13. 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.
14. Категорически не рекомендуется работать с Системой ДБО с компьютеров, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.), так как это существенно увеличивает риск кражи Ваших учетных данных и платежной и ключевой информации.
15. Не хранить ключи ЭП на незащищенных от копирования носителях информации (жесткий диск компьютера, реестр компьютера, USB-флэш накопитель и т.п.).
16. Исключить возможность использования средств удаленного администрирования на компьютере, предназначенном для работы в Системе ДБО.
17. Использовать только лицензионное программное обеспечение (операционные системы, офисные пакеты и пр.).
18. Обеспечить автоматическое обновление операционной системы и прикладного программного обеспечения,
19. Обеспечить автоматическое обновление антивирусных баз и модулей антивирусной программы.
20. Для контроля доступа к съемному ключевому носителю рекомендуется на него установить пароль.

ВАЖНО: Не сообщайте никому пароль для доступа к Системе ДБО, съемному ключевому носителю (включая сотрудников Банка и сотрудников Вашей организации или Ваших родственников)!

21. При формировании пароля следует руководствоваться требованиями по сложности пароля:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дата рождения и т.д.), а также общепринятые сокращения;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

ВНИМАНИЕ! Изменение пароля доступа к секретному ключу ЭП не защищает от использования злоумышленником ранее похищенного ключа.

22. Не рекомендуется записывать пароли и другие параметры доступа на бумажных и иных носителях и оставлять их в общедоступных местах. Также не рекомендуется записывать или сохранять в незащищенных файлах информацию о паролях.

23. При увольнении ответственного сотрудника, имевшего доступ (технический доступ) к секретному ключу ЭП, необходимо заблокировать ключ ЭП и инициировать внеплановую смену ключа ЭП.

24. При возникновении любых подозрений на компрометацию секретных ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно позвонить в Банк для блокирования ключей ЭП.

25. Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте сотрудникам Банка обо всех подозрительных или несанкционированных операциях.

26. При обнаружении факта или подозрений на несанкционированное списание денежных средств со счета, немедленно:

- сообщите в Банк о возможной попытке несанкционированного доступа к Системе ДБО (или о списании денежных средств, если оно состоялось);
- сверьте последние отправленные в Банк платежные документы, при обнаружении несанкционированных платежей напишите заявление на приостановление/ограничение действия ключей ЭП;
- выключите и не включайте компьютер до выяснения всех обстоятельств происшествия для сохранения возможных следов действий злоумышленников;
- предпримите меры по сохранению лог файла работы в сети Интернет (данные с прокси-сервера, брандмауэра или запросите у оператора).

27. Значительно повысить уровень безопасности системы ДБО позволит применение следующих мер:

- установка ограничений по IP-адресам (доступ к системе ДБО с определенного сетевого адреса);
- установка ограничений по MAC-адресам (доступ к системе ДБО с определенного компьютера);
- установка лимитов на проведение операций с использованием системы ДБО, таких как ограничение на максимальную сумму одного платежа или максимальную сумму платежей за определенный период;
- блокировка счета в системе ДБО на время длительного отсутствия (отпуск, командировка при отсутствии необходимости в использовании системы);
- использование виртуальной клавиатуры для ввода пароля, что позволит избежать перехват информации, вводимой с клавиатуры.

28. В случае сбоев в работе компьютера или его поломки во время / после работы с Системой 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 Сектор дистанционного банковского обслуживания и убедиться, что от Вашего имени не производились несанкционированные операции.

29. Логины и пароли для работы в Системе ДБО – это Ваша персональная 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. При возникновении подобных инцидентов, сообщите об этом на горячую линию.

Вся ответственность за конфиденциальность секретных данных (паролей и ключей) полностью лежит на их владельце.

Банк не осуществляет рассылку электронных писем или звонков с просьбой прислать секретный ключ ЭП или пароль.

Банк не рассылает по электронной почте программы для установки на компьютеры.

По любым вопросам, связанным с работой Системы ДБО, можно обратиться в Банк по следующим контактным данным:

Отдел дистанционного банковского обслуживания:

8-800-100-64-10,
(8412) 23-18-12,
(8412) 23-18-13

e-mail: dbo@kuzbank.ru
Адрес: 440000, г. Пенза, ул. Красная, 104, комната 317