Приложение 2.3.
к Договору о комплексном банковском обслуживании
юридических лиц, индивидуальных предпринимателей
и лиц, занимающихся частной практикой,
в АО Банк «Венец»

Рекомендации по обеспечению безопасной работы в Системе ДБО «ВЕНЕЦ-БИЗНЕС»

АО Банк «Венец» рекомендует соблюдать требования по информационной безопасности при работе с Системой ДБО, а именно:

1. **Вход в Систему ДБО Банка осуществляйте только с официального сайта Банка.**
   Не входите в Систему ДБО по ссылкам, размещенным на ресурсах в сети Интернет, отличных от официальных ресурсов Банка, так как мошенники часто публикуют фишинговые сайты (сайты-двойники) для хищения учетных данных от Системы ДБО (логин, пароль) и, как следствие в дальнейшем, финансовой информации. При обнаружении сайта-двойника немедленно сообщите об этом в Отдел по работе с клиентами Банка по номеру 8-800-707-55-99 (звонок по России бесплатный) и перешлите ссылку, по которой осуществлялся вход на сайт-двойник, для проведения расследования нашими специалистами по адресу info@venets-bank.ru

2. **Избегайте входа в Систему ДБО Банка в местах, где услуги Интернета являются общедоступными.**
   Например, Интернет-кафе, а также с неизвестных Вам компьютеров. В случае, если Вам все же пришлось осуществить вход в Систему ДБО с компьютера общего пользования, мы рекомендуем сменить пароль от Системы ДБО сразу после того, как Вы завершили работу. Это важно, поскольку существует риск перехвата мошенниками Ваших учетных данных от Системы ДБО (логин, пароль) или иной информации (номера банковской карты) без Вашего ведома при помощи вредоносного программного обеспечения и вирусов.

3. **Перед осуществлением передачи Вашей конфиденциальной информации через вебсайт** убедитесь в наличии защищенного соединения с сайтом по протоколу https. Обязательно в адресной строке браузера должно быть установлено защищенное соединение с использованием сертификата. Данный символ указывает на то, что сайт работает в защищенном режиме и все передаваемые данные будут защищены.

4. **Никому и никогда не сообщайте свой пароль к Системе ДБО**, ПИН-код карты и CVV/CVC (секретный трёхзначный код для осуществления операций с использованием Вашей банковской карты в Интернет). Запомните, АО Банк «Венец» никогда и ни при каких обстоятельствах не запрашивает указанную информацию у Клиентов.

5. **Осуществляйте вход и работу в Системе ДБО Банка только с защищенного лицензионным антивирусным программным обеспечением компьютера** и своевременно производите обновление антивирусных баз. Антивирусное программное обеспечение и персональный firewall требуют постоянного обновления для своевременной и надежной защиты Вашей информации от вредоносных программ, и атак из сети Интернет. Использование персонального firewall особенно важно на компьютерах с высокоскоростным доступом в Интернет. Помните, что даже если Вы не посещаете сайты сомнительного содержания, это не гарантирует вирусной чистоты компьютера, так как регулярно выявляются случаи вирусного заражения общеизвестных сайтов (включая новостные и финансовые).

Используйте антивирусное ПО проверенных и хорошо зарекомендовавших себя производителей (Kaspersky Anti-Virus, Symantec, ESET Software, Trend Micro, McAfee, Microsoft, Panda Software и др.).

Несмотря на то, что большинство современных антивирусных продуктов имеет режим постоянной проверки (резидентный режим) компьютера на вирусы **не стоит пренебрегать периодической полной проверкой всего содержимого компьютера.** Как правило, при установке антивирусного ПО создаются задачи проверки компьютера по расписанию.

6. **Используйте функцию подтверждения операций в Системе ДБО кодом подтверждения (Разовым паролем),** отправляемым на Ваш мобильный телефон. Даже если логин и пароль для входа в Систему ДБО скомпрометированы и стали известны злоумышленникам, получить доступ к SMS-сообщениям Вашего телефона они не смогут, как и отключить функцию их отправки.

7. **Используйте функцию IP-фильтрации при работе в Системе ДБО**.
   Данный функционал позволят работать в Системе ДБО только с тех ip-адресов, которым Вы доверяете и с которых Вы постоянно работаете, это не позволит злоумышленникам при компрометации учетных данных от Системы ДБО воспользоваться ими и войти в Систему ДБО с других ip-адресов.

8. **Решив закончить работу с Системой ДБО Банка**, делайте это в соответствии с установленными процедурами. Не закрывайте Интернет-браузер просто так. Выполняйте последовательное завершение сеанса работы посредством нажатия на клавишу «Выход».

9. **Не работайте на компьютере под учетной записью с правами администратора системы**. Помните, что атакующее Ваш компьютер вредоносное ПО при работе с административными правами также может получить максимальные привилегии в Системе, и этим значительно облегчить задачу злоумышленников. Возьмите за правило регистрировать и использовать для постоянной работы учетную запись с ограниченными правами, а учетной записью администратора Системы пользоваться лишь при необходимости (например, для установки новых программ или перенастройки компьютера).

10. **Не отключайте без особой необходимости средства обеспечения безопасности Вашего компьютера**.
    К ним относятся: антивирусное ПО, межсетевой экран (firewall), системы обеспечения безопасного повышения привилегий (например, UAC в ОС Microsoft Windows), системы поиска и установки обновлений ПО.

11. **Не используйте взломанное либо нештатным образом активированное ПО, полученное из сомнительных источников.**
    Нет никаких гарантий, что взлом защитных механизмов ПО не привел к ослаблению штатной защиты ПО от неблагоприятных внешних воздействий, и, более того, что взломщики сами не встроили в дистрибутив ПО вредоносные компоненты.

12. **По возможности, не используйте предлагаемую браузером функцию сохранения паролей к сайтам**, в том числе к сайту Системы ДБО, так как сохраненная информация может стать легкой добычей злоумышленников при проведении атаки на браузер.

13. **Не храните на серверах электронной почты (в особенности, бесплатных ресурсов вебпочты) письма, содержащие конфиденциальную информацию,** в частности, переписку с Банком, хранимая в почте информация может стать сравнительно легкой добычей злоумышленников и быть использованной ими против Вас. Регулярно производите очистку папок веб-почты, не забывая про папки «Черновики», «Отправленные», «Удаленные» и/или «Корзина».

14. **Не открывайте неизвестные или вызывающие подозрение вложения в почтовые письма, полученные от незнакомых отправителей**.
Даже если отправитель Вам знаком, не лишним будет проверить файл антивирусной системой перед его запуском.

15. **В случае, если компьютер ведет себя странно** (появляются сообщения об ошибках в программах, программы самопроизвольно запускаются либо завершаются, их выполнение занимает больше, чем обычно, времени, появляются вплывающие окна в браузере на тех сайтах, где их не должно быть, вместо указанного в адресной строке браузера адреса открываются другие ресурсы и т.п.) настоятельно рекомендуется немедленно прекратить использование компьютера и провести внеочередную полную антивирусную проверку.

16. **Обеспечьте конфиденциальность учетной информации от Системы ДБО**.
Храните ключевые носители (Смарт-ключи) в месте, недоступном посторонним лицам. Храните в тайне пароль доступа к Смарт-ключу и логину.