Приложение № 1
к Приказу № 194 от 23 октября 2019 г.
«Об утверждении рекомендаций
по защите информации и о
порядке их доведения до клиентов »

Рекомендации клиентам ООО «АвтоКредитБанк» по защите информации

I. Рекомендации по защите информации от воздействия вредоносного кода (вредоносных программ) при использовании систем дистанционного банковского обслуживания

С целью исключения возможности появления на персональных электронных вычислительных машинах (далее - ПЭВМ), с которых клиентами осуществляется работа с системами дистанционного банковского обслуживания (далее – система ДБО), вредоносных программ (далее – ВК, вредоносный код), направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения ПЭВМ либо на похищение информации, в том числе файлов с ключами электронной цифровой подписи и паролей, рекомендуем Вам придерживаться следующих правил

1. Выделяйте, по возможности, отдельную ПЭВМ, используемую только для работы в системе ДБО.

2. Используйте ПЭВМ с установленным лицензионным программным обеспечением, своевременно обновляйте установленные операционную систему и программное обеспечение.

3. Установите и своевременно обновляйте на ПЭВМ средства защиты от ВК (антивирусное программное обеспечение). При этом:

- средства защиты от ВК должны запускаться автоматически при загрузке операционной системы,

- не реже одного раза в неделю, согласно расписанию, установленному в настройках средства защиты от ВК, в автоматическом режиме должна осуществляться полная проверка отсутствия ВК на ПЭВМ,

- любая информация, получаемая по телекоммуникационным каналам (Интернет и пр.) или на съемных носителях, должна подвергаться проверке на отсутствие ВК, при наличии технической возможности в автоматическом режиме,

- при обнаружении ВК его обезвреживание должно осуществляться средством защиты от ВК в автоматическом режиме, не требующем ответов пользователя.

4. Ограничивайте информационный обмен в сети Интернет только доверенными ресурсами и проверенными корреспондентами электронной почты или используйте сетевые экраны, разрешив доступ только к доверенным ресурсам.

5. При работе в сети Интернет не соглашайтесь на установку каких-либо сомнительных программ.

6. При работе с электронной почтой не открывайте сообщения и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких сообщениях ссылкам.

7. Воздерживайтесь от использования программ онлайнового общения на ПЭВМ, используемой для работы в системе ДБО.

8. Не используйте на ПЭВМ, используемой для работы в системе ДБО, средства удаленного администрирования.

9. При наличии признаков возможного наличия ВК на ПЭВМ (включая, но не ограничиваясь такими как: неправильная работа установленных приложений, вывод на экран монитора ПЭВМ сообщений или изображений, не запланированных действиями пользователя или действиями программ работающих в данный момент, открытие искаженных меню и диалоговых окон, произвольный запуск программ, исчезновение файлов или каталогов, искажается информация в некоторых файлах или каталогах, появление файлов или каталогов со странными именами и т.п.), а также при соответствующих сообщениях средств защиты от ВК исключите использования системы ДБО до исправления ситуации.

10. Помните, что в соответствии с условиями договоров, предметом которых является предоставление клиентам услуг ДБО, Банк не несёт ответственность в случаях финансовых потерь, понесённых клиентами в связи с нарушением и (или) ненадлежащим исполнением ими требований по защите от ВК клиентских ПЭВМ, используемых для работы в системе ДБО.

II. Рекомендации по защите информации при использовании сети Интернет для осуществления переводов денежных средств от несанкционированного доступа путем использования ложных ресурсов сети Интернет

При осуществлении операций с использованием систем дистанционного банковского обслуживания существует, в частности, риск получения злоумышленниками несанкционированного доступа к защищаемой информации путем использования ложных (фальсифицированных) ресурсов сети Интернет. Ложные (фальсифицированные) ресурсов сети могут имитировать программный интерфейс используемой Банком системы ДБО и (или) использовать зарегистрированные товарные знаки и наименование Банка.

Попадание на такие ресурсы возможно, например, с различных внешних ссылок, на которых установлена переадресация на сайт злоумышленника. Введение Ваших учетных данных на таких ресурсах может привести к получению этих данных злоумышленниками и в конечном итоге привести к хищению Ваших денежных средств.

С целью снижения указанного риска рекомендуем Вам придерживаться следующих правил:

1. Обращайте внимание, какие перенаправления совершаются при обработке Ваших запросов.

2. При входе в систему ДБО всегда проверяйте, чтобы в адресной строке интернет-браузера отображался адрес, начинающийся с https://online.autokreditbank.ru. Если адрес отличается хотя бы на один символ, незамедлительно сообщите об этом в Банк по телефону (843) 294-98-66 и проконсультируйтесь со специалистом.

3. Обращайте внимание на сообщения о действительности используемых сайтами цифровых сертификатов;

4. Если при использовании системы ДБО появляются предупреждение об ошибке сертификата безопасности, проверьте, кому принадлежит сертификат, и если владелец сертификата не ООО «АвтоКредитБанк», незамедлительно сообщите об этом в Банк по телефону (843) 294-98-66.

5. В случае обнаружения фальсифицированного сайта, копирующего дизайн официального сайта или системы ДБО, пожалуйста, незамедлительно сообщите об этом в Банк по телефону (843) 294-98-66.

III. Рекомендации по предотвращению несанкционированного доступа к защищаемой информации, используемой при доступе к системе ДБО

В целях предотвращению несанкционированного доступа к защищаемой информации, используемой при доступе к системе ДБО, что в конечном итоге может привести к хищению Ваших денежных средств, рекомендуем Вам придерживаться следующих правил:

1. Храните пароль для входа в систему ДБО в недоступном для посторонних лиц месте. Не сохраняйте информацию о пароле для входа в систему ДБО на любых носителях, включая ПЭВМ. Регулярно меняйте пароль, используя для их создания сложные сочетания не связанных букв и цифр.

2. Никому не разглашайте пароль от системы ДБО. Банк не рассылает электронных писем, SMS или других сообщений с просьбой уточнить Ваши конфиденциальные данные (в т.ч. пароли т.п.).

3. Не пересылайте файлы с конфиденциальной информацией для работы в системе ДБО по электронной почте или через SMS-сообщения.

4. Использование ключевых носителей системы ДБО должно осуществляться исключительно их владельцами.

5. Храните ключевые носители системы ДБО в недоступном для посторонних лиц месте.

6. Извлекайте ключевые носители из ПЭВМ, если они не используются для работы в ДБО.

7. Исключите возможность доступа посторонних лиц к ПЭВМ, с которой Вы осуществляете работу в системе ДБО

8. Принимайте меры по контролю конфигурации ПЭВМ, используемой для работы в системе ДБО, не допуская несанкционированных программно-аппаратных изменений конфигурации.

9. Контролируйте количество, сумму отправленных электронных документов и их получателей и незамедлительно сообщайте в Банк по телефону (843) 294-98-66 обо всех подозрительных или несанкционированных изменениях.

10. В случае если Вы получили уведомление системы ДБО об операции, которую Вы не совершали, незамедлительно сообщите об этом в Банк по телефону (843) 294-98-66

11. В случае утраты (потере, хищении) ПЭВМ, с использованием которого Вы осуществляете перевод денежных средств, незамедлительно сообщите об этом в Банк по телефону (843) 294-98-66

12. В случае выбытия ПЭВМ, на котором ранее была установлена система ДБО, гарантированно удалите с него всю информацию, имеющую отношение к работе в системе ДБО.