ПАМЯТКА КЛИЕНТУ
по соблюдению мер информационной безопасности при использовании Системы «Интернет Банк-Клиент» ЦМРБанк (ООО)

Общая безопасность использования Системы «Интернет Банк-Клиент» ЦМРБанк (ООО) (далее – Система ИБК) складывается из учета всех требований безопасности при эксплуатации Системы ИБК в совокупности и требует соблюдение требований безопасности работы со стороны Клиента.

Технологии защиты операций в Системе ИБК используют современные механизмы обеспечения безопасности и предоставляют удобство пользования услугой, обеспечивая при этом высокий уровень её надежности и безопасности. Вместе с тем эффективность данных механизмов зависит также от выполнения Клиентом следующих рекомендаций:

1. Установите и регулярно обновляйте лицензионное антивирусное программное обеспечение на Вашем компьютере, используемом для работы в Системе ИБК (далее –Компьютер). Действие вирусов может быть направлено на перехват Вашей персональной информации и передачу её злоумышленникам.

2. Своевременно устанавливайте обновления операционной системы и браузера Компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей, так как данные действия значительно повысят его уровень безопасности.

3. Установите и настройте персональный брандмауэр (firewall) на Компьютере. Это позволит Вам запретить несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа.

4. Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Компьютера – программы поиска шпионских компонентов.

5. После окончания сеанса работы в Системе ИБК съемный ключевой носитель должен быть незамедлительно извлечен из Компьютера.

6. Если Вы используете несколько ключей при работе в Системе ИБК (например, первая и вторая подписи или ключи с правом подписи и без права подписи (просмотр и создание платежного документа)) – не сохраняйте/не переносите эти ключи на один съемный ключевой носитель, а также не подключайте одновременно различные ключевые носители к одному компьютеру.

ВАЖНО! ***Перед окончательным подписанием электронно-цифровой подписью платежного документа, созданного в том числе с использованием Вашего персонального шаблона документа, внимательно проверяйте все реквизиты получателя (включая, но не ограничиваясь: номер счета получателя, его ИНН, БИК банка получателя), сумму платежа и другие значимые параметры документа.***

7. Для контроля доступа к съемному ключевому носителю рекомендуется на него установить пароль.

ВАЖНО! ***Не сообщайте никому пароль для доступа к съемному ключевому носителю (включая сотрудников Банка и Ваших родственников).***

8. После окончания работы в Системе ИБК обязательно корректно завершите работу (выйдите из Системы ИБК, используя кнопку «Выход») и/или закройте браузер.

ВАЖНО! ***Извлеките из Вашего компьютера съемный ключевой носитель!***

9. Исключите посещение с Вашего компьютера 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.

10. Категорически не рекомендуется работать с Системой ИБК из мест, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатные беспроводные сети Wi-Fi и т.п.), так как это существенно увеличивает риск кражи Ваших персональных данных.

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

12. Для работы в Системе ИБК рекомендуется использовать выделенный компьютер, ноутбук, при этом на Компьютере не рекомендуется устанавливать иное программное обеспечение, кроме необходимого для работы в Системе ИБК.

13. Права пользователя, работающего в Системе ИБК, на данном компьютере должны быть минимально необходимыми (наличие прав администратора нежелательно).

14. Не привлекайте для администрирования и обслуживания компьютера с установленной на нем Системой ИБК технических специалистов на условиях предоставления им удаленного доступа к компьютеру.

15. Логины и пароли для работы в Системе ИБК – это Ваша персональная конфиденциальная информация. Ни при каких обстоятельствах не раскрывайте свой логин и пароль никому, включая сотрудников Банка и Ваших родственников. При обращении к Вам лиц от имени Банка по телефону, электронной почте с просьбой предоставления конфиденциальной информации (пароли, кодовые слова, и т.д.) ни при каких обстоятельствах не следует сообщать данную информацию.

16. Не сохраняйте Ваш логин и пароль в текстовых файлах на жестком диске компьютера, либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.

17. В случае сбоев в работе Компьютера или его поломки во время/после работы в Системе ИБК (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), следует **НЕМЕДЛЕННО** извлечь ключи и выключить компьютер, а также обратиться в Банк(-и) убедиться, что от Вашего имени не производились несанкционированные операции.

18. Обращайте внимание на любые изменения в привычных для Вас процессах установления соединения с Системой ИБК или функционирования Системы ИБК. При возникновении любых сомнений в правильности функционирования Системы ИБК незамедлительно обратитесь в Банк.

19. Перед работой в Системе ИБК убедитесь, что защищенное соединение по протоколу "https" установлено именно с официальным сайтом услуги (https://ibank.cmrbank.ru/). Настоятельно не рекомендуется переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка, https://ibank.cmrbank.ru/) или поступивших по электронной почте писем.

20. В случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении к Системе ИБК отложите совершение операций и обратитесь в службу поддержки Банка по телефонам 8 (800) 250-09-22; 8 (495) 980-80-44 доб.44744 либо отправьте сообщение на электронный адрес help@cmrbank.ru**.**

ВАЖНО! ***Обращаем Ваше внимание, что одним из распространенных мошеннических методов завладения средствами клиента является изменение вирусной программой в реально подготовленном Вами платежном документе перед его окончательным подписанием электронно-цифровой подписью реквизитов получателя (например, номера счета получателя, его ИНН и БИК банка получателя без изменения наименования получателя). Настоятельно рекомендуем, с учетом вышеизложенных мер технической и антивирусной защиты, перед окончательным подписанием документов электронно-цифровой подписью внимательно проверять все реквизиты получателей, сумму платежа и другие значимые параметры документа.***

Соблюдайте вышеизложенные простые рекомендации при работе с Системой ИБК, это позволит Вам значительно снизить возможность несанкционированного доступа к Вашим данным третьих лиц!