ПАМЯТКА
по информационной безопасности при работе с системой «Клиент-Банк»
(для клиентов ООО «Русский Национальный Банк»)

Безопасность использования дистанционного банковского обслуживания (далее по тексту – ДБО) складывается из совокупности всех требований безопасности при работе с ДБО и зависит от соблюдения их Клиентом.

Соблюдайте простые рекомендации по работе с ДБО, это позволит Вам избежать несанкционированного доступа к вашим данным со стороны третьих лиц.

Требования к паролю персональной рабочей станции, подключаемой к ДБО (далее по тексту – ПЭВМ):
- Никогда не записывайте логин и пароль ПЭВМ в местах, доступных третьим лицам, а лучше просто запомните их.
- Создавайте свой пароль с применением заглавных и строчных букв, а также цифр, не используйте простые для разгадывания пароли, пример: QWERTY, 123, 12345678 и т.д. и т.п.
- Периодически меняйте пароль доступа. Если у вас возникли подозрения, что кто-либо владеет информацией о вашем логине и пароле, обязательно смените пароль.
- Никогда не сообщайте информацию о логине и пароле никому, включая работников Банка.

Требования к программному обеспечению ПЭВМ:
- Используйте строго лицензионное программное обеспечение, установленное или планируемое к установке на ПЭВМ.
- Своевременно обновляйте операционную систему ПЭВМ и прикладное программное обеспечение ПЭВМ с использованием автоматического обновления или только из доверенных источников, гарантирующих отсутствие вредоносных программ. Помните, что при использовании не обновленных или старых версий программного обеспечения, неисправленными ошибками в программном обеспечении будут пользоваться злоумышленники для захвата управления ПЭВМ.
- Используйте и оперативно обновляйте лицензионное специализированное программное обеспечение для защиты информации – антивирусные программы, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр. Помните, что вредоносное программное обеспечение (компьютерные вирусы, «трояны», и т.д.) зачастую используют возможность отправки конфиденциальных данных или позволяют дистанционно управлять ПЭВМ злоумышленникам.
- При выборе и приобретении лицензионного антивирусного программного обеспечения для использования на ПЭВМ, рекомендуем использовать программное обеспечение следующих разработчиков:
• Kaspersky Lab;
• Eset;
• DrWeb;
• Symantec;
• Microsoft.

Требования по обеспечению безопасной установки и работы ПО ДБО:
- Перед установкой ПО ДБО на ПЭВМ необходимо проверить ПЭВМ на отсутствие вредоносного программного обеспечения, программ удаленного доступа к ресурсам ПЭВМ (TeamViewer, BeTwin, RAdmin и др.), программ работы с вирусоопасными ресурсами и сервисами сети Интернет.
- При работе с ПО ДБО у пользователей ПЭВМ в ОС не должно быть административных прав и прав Power User («Опытный пользователь»).
- Для исключения ошибочных и преднамеренных действий пользователя ПЭВМ, приводящих к снижению защищенности ПЭВМ и рискам финансовых потерь, необходимо средствами политик безопасности ОС или специализированными средствами защиты ПЭВМ от несанкционированного доступа обеспечить для пользователя ПЭВМ функционально-замкнутую среду, позволяющую ему запускать и работать только с разрешенными программами без доступа к файловой системе и реестру ОС.

Требования по ограничению доступа к ПЭВМ, логинам, паролям и носителям секретных ключей:
- Строго соблюдайте регламент ограниченного доступа к ПЭВМ. Помните, что любой физический доступ к ПЭВМ – это потенциальная возможность установки на ПЭВМ вредоносной программы (через съемный носитель или путем доступа к вредоносному ресурсу сети Интернет), с возможностью ее использования в последующем злоумышленниками для хищения денежных средств через ДБО.
- Соблюдайте регламент доступа к носителям секретных ключей (с ключевыми носителями и ПЭВМ должны работать только доверенные лица клиента).
- Подключайте к компьютеру носитель с ключом Электронной подписи только на время проведения сеансов связи с банком, а после их завершения необходимо немедленно отключить носитель от ПЭВМ и убрать в недоступное посторонним лицам место хранения (сейф). Сохранность ключа является главным фактором в обеспечении информационной безопасности при работе с системой ДБО.

Общие рекомендации:
- Никогда не открывайте подозрительные файлы, присланные вам по электронной почте.
- Не отвечайте на подозрительные письма электронной почты или телефонные звонки с просьбой сообщить логин ДБО, любые пароли, Кодовое слово и другие Ваши конфиденциальные данные (работники Банка никогда и ни при каких условиях не запросят у Вас подобную информацию).

Незамедлительно информируйте Банк о внештатных ситуациях и подозрениях на нарушение безопасности ПЭВМ (заражение компьютера вирусами, попытка несанкционированного доступа к рабочему месту ДБО, компрометация ключа подписи)!