Приложение № 3 к
Политике антивирусной защиты
АО «РУНА-БАНК»

Рекомендации по защите информации от воздействия вредоносного кода
АО «РУНА-БАНК»

Уважаемые Клиенты!

Информируем Вас, что в информационно-телекоммуникационной сети "Интернет" (далее - сеть «Интернет») зафиксированы случаи распространения вирусов-шпионов (троянских программ), подключающихся на этапе авторизации клиента в Систему дистанционного банковского обслуживания «Интернет-Банк». Некоторые из троянских программ при обнаружении ими подключения компьютера клиента к банковским сайтам могут отслеживать информацию, вводимую на клавиатуре, и передавать ее злоумышленникам, а также совершать от Вашего имени платежи в пользу других клиентов («дроповский платеж»). Так же участились случаи удаленного управления компьютерами клиента.

Обращаем Ваше внимание на необходимость соблюдения определенных правил при работе с банковскими системами через сеть Интернет

- следить за нарушением сквозной нумерации, т.е. за последовательностью нумерации документов;
- на рабочих местах Клиента использовать только лицензионное программное обеспечение;
- на системное программное обеспечение и Интернет-браузер должны быть установлены последние критические обновления. Обновления Интернет-браузеров скачиваются и устанавливаются с сайтов производителей Интернет-браузеров;
- необходимо использовать антивирусное программное обеспечение, с обновлением сигнатур вирусных баз не реже раза в сутки, в режиме мониторинга и проведением периодических антивирусных проверок компьютеров;
- необходимо отключить на автоматизированных рабочих местах Клиента автозагрузку со сменных носителей (дискет, флэш-накопителей, оптических дисков) как потенциальный источник угроз;
- необходимо отключить на автоматизированных рабочих местах Клиента у пользователей сетевой удалённый доступ (т.е. когда технический специалист может удалённо подключаться к компьютеру);
- необходимо использовать программы сетевых экранов (брандмауэров) для блокировки нежелательных и/или неиспользуемых ресурсов сети «Интернет»;
- необходимо регулярно, не реже одного раза в день, проверять состояние счета;
- ключевой носитель нельзя передавать третьим лицам, оставлять без присмотра, хранить в доступном месте;
- не работать на компьютере с правами администратора;
- все учетные записи на компьютере должны быть с паролем;
- Подключение Token’а производить только для входа в систему Клиент-Банк и подписания документов;
- не использовать компьютер с системой Клиент-Банк для просмотра электронной почты и сайтов в сети «Интернет»;
- не заходить в систему Клиент-Банк в Интернет-кафе и с других непроверенных компьютеров;
- в случае возникновения нештатных ситуаций на компьютере с системой Клиент-Банк (зависание, нет возможности войти в систему, зафиксированная попытка мошенничества в системе Клиент-Банк другого банка и т.п.) необходимо сразу обратиться в Банк;
- не использовать удаленное управление на компьютере с системой Клиент-Банк.