РЕКОМЕНДАЦИИ
при обнаружении признаков наличия вредоносного программного обеспечения на рабочей станции, предназначенной для работы с системой iBank2

1. Назначение документа

1.1. Настоящие рекомендации разработаны с целью оказания методической помощи клиентам ПАО АКБ «Приморье» (далее – Банк), использующим систему iBank2, и обнаружившим как самостоятельно, так и с помощью Банка, признаки наличия вредоносного программного обеспечения.

2. Основные понятия

2.1. Под признаками наличия вредоносного программного обеспечения (далее ВПО) подразумевается совокупность факторов, прямо или косвенно указывающим на заражение рабочей станции вредоносным кодом. Основные признаки наличия ВПО приведены в п.3.

2.2. В случае выявления таких признаков ВПО следует незамедлительно прекратить работу на ПК, вынуть USB-токен, отключить рабочую от сети и сообщить об этом в Банк с целью блокирования ключей ЭП и проведения сверки платежей.

2.3. Для дальнейшего продолжения работы с ПК необходимо провести удаление вредоносного ПО и настройку ПК в соответствии с рекомендациями Банка. Во избежание повторно заражения так же необходимо провести проверку и других рабочих станций локальной сети. **Для проведения такого рода работ необходимо привлечение квалифицированных IT специалистов!**

3. Признаки наличия ВПО

3.1. Основными признаками наличия ВПО являются:

- наличие платежных поручений, созданных или отправленных в Банк, которые Клиент самостоятельно не создавал;
- уведомления от антивируса и прочих средств защиты информации;
- наличие программ удаленного администрирования, как то Radmin, VNC, TeamViewer, AmmyAdmin и пр.;
- нетипичное поведение ПК: мерцающие и сворачивающиеся окна, дергание мыши, выдача ошибок или дополнительных окон, которые ранее не появлялись;
- наличие в автозагрузки посторонних процедур;
- наличие посторонних процессов в диспетчере процессов;
- изменение в свойствах обозревателя нетипичных настроек прокси-сервера;
- уведомление из Банка о подозрении на наличие ВПО.

4. Удаление ВПО и безопасная работа с системой iBank2

4.1. Следует провести полную переустановку операционной системы с форматированием загрузочного диска ПК и переустановкой всех программ с эталонных копий из источников, отличных от данного ПК.

4.2. Механизмы очистки компьютера с помощью антивируса не дают 100% гарантии удаления всех путей и средств, используемых злоумышленников и не гарантируют отсутствие повторного заражения ПК.

4.3. После переустановки операционной системы необходимо провести настройку ПК в соответствии с «Памяткой о мерах по защите информации при использовании системы iBank2».

4.4. В первую очередь необходимо:

- установить лицензионное антивирусное ПО, настроив автоматическое обновление и автоматическое удаление ВПО;
- ограничить возможность использования сети Интернет, разрешив только соединение с сервером банка, с серверами обновлений операционной системы, средств антивирусной защиты и прочих средств защиты информации;
- осуществлять работу в системе под учетной записью пользователя, не имеющего права администратора на данном ПК;
- сменить стандартный пароль на административной учетной записи.

4.5. Необходимо помнить, что только выполнение ВСЕХ пунктов «Требования по защите информации при использовании системы Интернет Клиент-Банк «iBank2» и ответственное отношение пользователя к их выполнению дает гарантию безопасной работы с системой «iBank2».