Уважаемые клиенты!

За последнее время система дистанционного банковского обслуживания (ДБО) «Банк-Клиент» стала неотъемлемой частью взаимодействия коммерческих организаций с банками. Удобство применения такой системы трудно недооценить: она позволяет снизить издержки и повысить оперативность проведения финансовых операций.

Однако, по данным МВД, только в Москве каждый месяц происходит больше десятка успешных мошеннических операций с использованием системы ДБО «Банк-Клиент». Ущерб клиентов банков составляет сотни миллионов рублей. Жертвами мошенничества являются как крупные фирмы, так и имеющие на расчетных счетах 10 или 30 тысяч рублей, не застрахован никто. Предпринимаемые банками мероприятия пресекаются многие попытки мошенничества. Но без заинтересованности **и организованности** самих клиентов банков исключить попытки мошенничества не возможно.

Кража денежных средств может быть произведена как сотрудниками организации, так и абсолютно не имеющими к ней отношения людьми. В большинстве случаев компрометация электронных ключей происходит с помощью вредоносного ПО, которое проникает через Интернет. Этот код обнаруживает, что на данном ПК ведется работа с системой ДБО, и осуществляет копирование ключей и логина/пароля пользователя, а затем передает данную информацию злоумышленникам. Кроме того, возможны случаи, когда перевод денежных средств осуществляется непосредственно с ПК жертвы **посредством ПО, также установленного** мошенниками через сеть Интернет.

Хранение ключей на жестком диске компьютера или незащищенном внешнем носителе (дискете, USB-flash-диске) существенно упрощает получение несанкционированного доступа к ним. Как правило, компания узнает, что с ее счета были украдены денежные средства, уже после того, как деньги прошли через несколько счетов юридических и физических лиц и были успешно обналичены. При этом злоумышленники прикладывают все усилия к уничтожению доказательств своей преступной деятельности и препятствуют доступу компании-жертвы к счетам. Для этого используются различные способы вывода из строя персонального компьютера, с которого производилась кража ключей и логина/пароля пользователя. Также часто применяются DDoS-атаки на серверы банков и интернет-шлюзы компании-жертвы для затруднения доступа к счетам через систему ДБО.

Чтобы предотвратить хищение секретного (закрытого) ключа ЭЦП и пароля доступа к ключу, необходимо:

Организационные меры (не требуют дополнительных финансовых затрат).

1. Разработать и строго соблюдать регламент доступа своих сотрудников к персональным компьютерам, с которых осуществляется работа с системой ДБО.
2. Периодически (раз в месяц) менять пароль для доступа к системе «Банк-Клиент».
3. Регулярно, не реже одного раза в полугодие, производить перегенерацию ключей ЭЦП.
4. Максимально ограничить доступ к компьютерам с системой ДБО, т.е. допускать к компьютерам только ответственных штатных IT-сотрудников (для обслуживания компьютеров) и только ответственных сотрудников, владельцев персональных ключей ЭЦП. Исключить работу на компьютере других лиц из-за угрозы заражения вредоносными программами, компрометации ключей и парольной информации.
5. Закрепить каждый ключ ЭЦП за сотрудником персонально и под роспись ознакомить его с мерой ответственности за нарушение правил сохранности ключа.
6. Не хранить пароль для входа в систему «Банк-Клиент» на жестком диске, записанным на стикерах.
7. Подключать носители с секретными ключами СКЗИ только на время выполнения криптографических операций. Отключать, извлекать носители с ключами ЭЦП, если они не используются для работы с системой «Банк-Клиент». Хранить ключи в сейфе или металлическом запираемом шкафу.
8. Не использовать ключи ЭЦП и другую аутентификационную информацию для входа в систему «Банк-Клиент» с гостевых рабочих мест (интернет-кафе и т.д.). Не использовать при работе с системой «Банк-Клиент» удалённое подключение к компьютеру, удалённое использование криптографических ключей.

9. При обслуживании компьютера IT-сотрудниками – обеспечивать контроль за выполняемыми ими действиями.
10. При увольнении сотрудника, имевшего технический доступ к секретному (закрытому) ключу ЭЦП, обязательно сменить ключ ЭЦП.
11. Не передавать ключи ЭЦП IT-сотрудникам для проверки работы системы «Банк-Клиент», проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМа системы, и лично ввести пароль, исключая его подсматривание.
12. Не использовать компьютер, используемый для работы с системой «Банк-Клиент», для получения электронной почты и посещения сайтов Интернет, за исключением сайта системы «Банк-Клиент».
13. При возникновении любых подозрений на компрометацию (копирование) секретных (закрытых) ключей ЭЦП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) – обязательно позвонить в банк и заблокировать ключи ЭЦП.

Технические меры.

1. Для хранения ключей использовать устройства, с которых невозможно скопировать ключи (RuToken).
2. Не использовать ключи ЭЦП и другую аутентификационную информацию для входа в систему «Банк-Клиент» с гостевых рабочих мест (интернет-кафе и т.д.). Не использовать при работе с системой «Банк-Клиент» удалённое подключение к компьютеру, удалённое использование криптографических ключей.
3. На компьютерах, используемых для работы с системой «Банк-Клиент», исключить загрузку и установку нелицензионного ПО и т.п. Перейти к использованию лицензионного ПО (операционные системы, офисные пакеты и пр.), обеспечить регулярное обновление системного и прикладного ПО после проверки на тестовой рабочей станции (при отсутствии возможности тестирования – включить автоматическое обновление). Использовать только ПО, полученное из надежных источников и реально необходимое для работы на компьютере с системой «Банк-Клиент». Не должно быть установлено программных средств удаленного доступа к компьютеру.
4. Применять на рабочем месте лицензионные средства антивирусной защиты, обеспечить возможность автоматического обновления антивирусных баз. Проводить периодическую полную проверку на вирусы.
5. Применять на рабочем месте специализированные программные средства безопасности: персональные межсетевые экраны, антишпионское программное обеспечение и т.п.
6. Постоянную работу в операционной системе осуществлять с правами обычного пользователя, вход в операционную систему с правами администратора осуществлять только в случае необходимости проведения технических работ. Учётная запись «Гость» должна быть отключена.
7. При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с системой «Банк-Клиент», принять меры для обеспечения отсутствия вредоносных программ на компьютерах.
8. Отключить на рабочем месте неиспользуемые порты, протоколы, сервисы и службы.
9. Использовать 2 подписи ЭЦП системы «Банк-Клиент», подписание осуществлять с 2-х разных компьютеров.
10. Использовать дополнительные средства защиты, например генератор одноразовых паролей.
11. На компьютерах, используемых для работы с системой «Банк-Клиент», установить файервол, блокирующий исходящий и входящий трафик на любые IP-адреса, отличающиеся от адреса системы «Банк-Клиент».