Инструкция пользователя
системы электронного банкинга "StarAccess"

Рекомендации по информационной безопасности при работе с системой "StarAccess"

(версия 3)

2011 г.

Используемые сокращения.

StarAccess (Система) - система электронного банкинга "StarAccess" (компьютерная программа "iBank 2 UA").
Банк – АО "УкрСиббанк".
Клиент – юридическое или физическое лицо – клиент банка, эксплуатирующий систему "StarAccess".

Для криптографических преобразований в системе используется библиотека "Гепард 1.0". Подробная информация о сертификации и соответствии стандартам приведена на официальном сайте Государственной службы специальной связи и защиты информации Украины[1]. На сайте Банка размещена информация о лицензиях, сертификатах и экспертных заключениях[2].

Общие рекомендации при работе с системой при выявлении или подозрении на выявление угроз.

В случае подозрений возникновения следующих ситуаций при работе с системой:

- расхождения санкционированных клиентом операций с данными по счету, предоставленными банком (подозрение на несанкционированное управление счетом);
- подозрении на компрометацию пароля и/или секретного ключа;
- обнаружение писем от Банка с просьбами посетить вложенные в письмо гиперссылки или просьбами ввести пароль и/или предоставить другую конфиденциальную информацию,

Клиенту рекомендуется выполнить следующие действия:

1. Немедленно разорвать соединение рабочей станции с сетью Интернет, локальной, беспроводной и любой иной сетью (физически отключить сетевой кабель или кабель модема от системного блока / ноутбука, bluetooth-адаптер, Wi-Fi и т.п.).

2. Немедленно связаться с сотрудниками Контакт-Центра Банка (0 800 505 800 - по Украине (звонки со стационарных телефонов на территории Украины бесплатны) или +380 44 590 06 55 – по всему миру) и обратиться в обслуживающее отделение Банка, изложив суть возникших подозрений.

3. Предоставить сотрудникам банка наиболее полную информацию, суть проблемы и при каких обстоятельствах она возникла, какие действия проводились с рабочей станцией.

4. В случае подтверждения подозрений на несанкционированное управление счетом (списания) подготовить и срочно доставить письмо в Банк с описанием сложившейся проблемы и заявление в правоохранительные органы.

5. Не подключая компьютер к сети Интернет, локальной или беспроводной сети, проверить систему на предмет наличия / отсутствия вирусов и другого вредоносного ПО. Один из способов – использование регулярно обновляющейся бесплатной утилиты DrWeb CureIT-: необходимо предварительно скачать из сети Интернет (http://www.drweb.ru/download/) свежую версию с помощью **другой** рабочей станции (если другая рабочая станция отсутствует – в Интернет-кафе, компьютерном клубе, любым другим доступным путем) и скопировать утилиту на рабочую станцию с системой с помощью внешнего носителя (например, USB-накопитель или компакт-диск). Перед копированием утилиты внешний носитель следует проверить с помощью вышеуказанной утилиты.

6. Если проверка не обнаружит вирусов и вредоносного ПО – подключить рабочую станцию к сети Интернет и **немедленно обновить антивирусную базу** установленного антивирусного ПО.

7. Не начинать работу с системой до тех пор, пока не убедитесь в отсутствии угрозы, а в случае несанкционированного управления счетом выключить компьютер и никого не подпускать к нему до прибытия сотрудников правоохранительных органов.

8. Не используйте носитель с секретными ключами до тех пор, пока не убедитесь в отсутствии угрозы.

9. Когда убедитесь в отсутствии угроз и начнете использовать систему, **немедленно** сгенерируйте новые секретные ключи, обязательно сменив пароль.

10. Продолжать использование системы только после того, как убедитесь, что рабочая станция не заражена вирусами и/или вредоносным ПО, остатки на Ваших счетах не изменились и ключевая информация не скомпрометирована, либо Вами произведена перегенерация ключа (ключей).

11. При дальнейшем использовании системы контролировать регулярность обновлений антивирусного ПО и остатки денежных средств на Ваших счетах.

Внимание! Каждый клиент обязан ограничить доступ третьих лиц к ключевой информации и паролям. Ключевая информация должна храниться на внешних носителях (например, флеш-картах, дискетах и т.п.) в недоступных другим лицам местах (например: сейф, закрываемые тумбы и т.п.).

Рекомендации по соблюдению мер информационной безопасности.

В целях защиты своих конфиденциальных данных рекомендуется соблюдать следующие меры

[1] http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=72121&cat_id=72110&mustWords=%D0%93%D0%B5%D0%BF%D0%B0%D1%80%D0%B4&searchPublishing=1

[2] https://my.ukrsibbank.com/ua/sme/operations/staraccess/licenses/ - для клиентов среднего и малого бизнеса, https://corporate.ukrsibbank.com/ua/cash_management/internet_banking/licenses/ - для клиентов корпоративного бизнеса.

безопасности:

1. Требования к настройкам системы и программному обеспечению (ПО):

- использовать исключительно легальное (лицензионное) ПО;
- запретить использование любых служб и средств удаленного управления рабочей станцией (например, беспроводная настройка, служба терминалов, Telnet, диспетчер сеанса справки для удаленного рабочего стола, удаленный реестр и т.п.);
- настроить и запустить в работу программные средства ограничения доступа;
- срок действия пароля учетной записи не должен превышать 30 дней;
- пароль должен удовлетворять рекомендациям, изложенным ниже;
- пользователь не должен работать под технологическими учетными записями (Администратор и т.д.);
- должны быть запущены службы контроля безопасности (журналы доступа и запуска приложений и т.п.).

2. Требования к ПО:

- на рабочей станции (компьютере и т.п.) необходимо использовать только легальное и/или лицензионное антивирусное ПО, необходимо проводить своевременное обновление такого ПО и обновление антивирусных баз;
- на рабочей станции не должно быть установлено / запускаться игровое и развлекательное ПО;
- не допускать установки нелицензионного ПО, своевременно производить установку обновлений ПО;
- не рекомендуется использование интернет-пейджеров (на пример ICQ, Miranda и т.п.) с возможностью передачи / принятия файлов;

3.Общие рекомендации:

- настоятельно рекомендуется использование лицензионного / легального (законно приобретенного в использование) межсетевого экрана (firewall);
- недопустимо использование рабочей станции для посещения развлекательных сайтов (непристойного содержания, видео, фото, игры и т.п.) и сайтов содержащих информацию о способах "взлома" информационных систем, программ, паролей и т.п.;
- недопустимо предоставление доступа к рабочей станции третьим лицам;
- недопустима передача паролей и носителей с ключевой информацией третьим лицам, хранение их в доступном для третьих лиц виде и месте;
- недопустимо хранение ключевой информации в нерабочее время в неприспособленных для этого местах (вне сейфов ответственных работников);
- недопустимо хранение ключевой информации в памяти или на жестком диске рабочих станций;
- недопустимо оставлять подключенным к рабочей станции (компьютеру и т.п.) носитель с ключевой информацией, если не производятся операции в системе удаленного обслуживания или осуществляется «выход» в сеть Интернет;
- использование ключевой информации рекомендуется учитывать в соответствующих журналах (генерация, использование, хранение);
- при генерации нового ключа необходимо произвести смену пароля доступа к нему.

Рекомендации по созданию надежных (устойчивых) паролей.

При выборе пароля пользователю необходимо руководствоваться предлагаемыми правилами:

- не использовать атрибуты пользователя - имена и фамилии пользователей, памятные даты и любую другую легкодоступную информацию (например, номера телефонов, адреса и т.п.);
- запрещено использование комбинации символов / знаков с клавишей Ctrl;
- пароли должны составляться путем комбинации двух или более слов;
- длина пароля должна составлять не менее 8 символов;
- пароль должен содержать не менее 3-х из 4-х следующих символов – заглавные буквы, прописные буквы, цифры, спецсимволы;
- запрещено использовать слова из реальных словарей (например, английский, французский, японский и т.п.) и вымышленных (например, эльфийский Р. Р. Толкиена и т.п.);
- пароль необходимо изменять не реже чем каждые 30 календарных дней.

Ниже приведен один из возможных вариантов (примеров) выбора пароля:

- составьте список простых слов, например, цветок, лист, ручка и т.д.
- выберите первые три буквы и общее количество букв в словах;
- объедините полученные результаты, добавьте одну цифру и один из специальных символов ("&'{([-_@)]}$*% !:/ ;., ?+-=) и сделайте одну из букв заглавной;
- при смене пароля используйте приведенные рекомендации с другим набором слов.

Пример: яблоко, груша и наберите их в латинском регистре:

Z,k?uhe1

Внимание! Не используйте в качестве пароля приведенные примеры!

Безусловно, для создания пароля могут использоваться другие методы создания надежного пароля,

но выбранный пароль не должен быть слабее предложенной степени стойкости.

Внимание! Помните, что ни при каких обстоятельствах Ваш пароль не должен быть известен третьим лицам, никто не имеет права требовать от Вас раскрытие пароля, даже сотрудники Банка.