ПАМЯТКА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ ДЛЯ ЮРИДИЧЕСКИЙ ЛИЦ «КЛИЕНТ-БАНК»

В настоящее время увеличилось число хищений денежных средств клиентов банков, работающих в системе дистанционного банковского обслуживания для юридических лиц (далее – ДБО), за счет неправомерного получения персональной информации пользователей системы ДБО «Клиент-Банк»: логинов, паролей, секретных ключей средств шифрования.

Согласно статистике, наиболее часто попытки хищения средств осуществляются:

– сотрудниками организаций, в том числе уволенными, имеющими или имевшими доступ к носителям ключей электронной подписи (дискетам, флеш-носителям, жестким/сетевым дискам и пр.), а также доступ к компьютерам, с которых осуществляется работа с системой ДБО;

– ИТ-специалистами (штатными и внештатными), оказывающими (или оказывавшими ранее, в т.ч. однократно) различные ИТ-услуги по поддержке, подключению к сети Интернет, установке, обновлению и поддержке различных программ (бухгалтерских, правовых, информационных и др.) на компьютерах, с которых осуществляется работа с системой ДБО;

– мошенниками, с использованием сети Интернет, путем заражения компьютеров различными вирусами и вредоносным программным обеспечением (используя «бреши» в безопасности компьютеров и корпоративной сети организации), с последующим хищением через Интернет ключей электронной подписи (ЭП) и средств доступа к системе ДБО.

После того, как Банк передал Вам средства доступа к системе ДБО (логин/пароль) и ключи ЭП, конфиденциальность полученных Банком данных по системе ДБО полностью зависит от того насколько ответственно Вы отнесётесь к их использованию и хранению, а также к защите компьютеров, с которых осуществляется работа с системой ДБО.

В данных условиях соблюдение Вами рекомендаций, приведенных в настоящей Памятке, позволяет минимизировать риск мошеннических действий при использовании системы ДБО для юридических лиц «Клиент-Банк» (далее – система «iBank 2»).

Рекомендации по обеспечению безопасности компьютера, на котором установлена система «iBank 2»

1. Ограничьте доступ к компьютеру с системой «iBank 2»: компьютер установите в недоступном для посторонних лиц месте, в закрываемом на ключ помещении.
2. Для работы с системой «iBank 2» используйте только лицензионное программное обеспечение, что снижает риск «взлома» (например, операционных систем, пакетов для офисной работы и т.п.).
3. Осуществляйте своевременную (по возможности, автоматическую) загрузку и установку всех последних обновлений операционной системы, а также регулярное обновление другого системного и прикладного программного обеспечения по мере появления новых версий (Интернет обозреватели – Internet Explorer, Opera, Firefox и др., почтовые клиенты и т.п.).
4. Отключите режим автозапуска на сменных носителях (CD, флеш-накопителях

и т.п.). Всегда проверяйте посторонние сменные носители на отсутствие вирусов и иных вредоносных программ, а также свои флеш-накопители, если они подключались к другим компьютерам.

5. На компьютере, на котором установлена система «iBank 2», должна быть установлена и регулярно обновляться программа антивирусной защиты. Осуществляйте еженедельную полную антивирусную проверку компьютера. Антивирусное программное обеспечение должно быть запущено постоянно с момента загрузки компьютера.

6. При работе в сети Интернет не соглашайтесь на установку каких-либо дополнительных программ с неизвестных Вам сайтов.

7. Не используйте компьютер, на котором развернута система «iBank 2» для развлекательных целей (посещение Интернет ресурсов, не относящихся к системе «iBank 2», воспроизведение мультимедиа файлов и т.п.).

8. При работе с электронной почтой не открывайте письма и прикрепленные к ним файлы, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

9. На компьютере, на котором установлена система «iBank 2» не рекомендуется работать под учетной записью с правами администратора и Power User («Опытный пользователь»); все учетные записи пользователей должны быть защищены паролем не менее восьми символов, состоящим из цифр и букв. Гостевая учетная запись (в операционной системе Windows учетная запись типа «Гость») должна быть отключена.

10. Для исключения ошибочных и преднамеренных действий пользователя, приводящих к снижению защищенности системы и рискам финансовых потерь, необходимо средствами политик безопасности операционной системы или специализированными средствами защиты ПК от несанкционированного доступа (НСД) обеспечить для пользователя функционально-замкнутую среду, позволяющую ему запускать и работать только с разрешенными программами без доступа к файловой системе и реестру ОС.

11. По возможности применяйте специализированные программные средства безопасности:

- персональные межсетевые экраны, файерволы (Personal Firewall);
- антишпионское программное обеспечение (Anti-Malware software) и другое специализированное ПО, использующееся для обеспечения информационной безопасности.

При настройке межсетевого экрана, файервола разрешайте доступ только к доверенным ресурсам сети Интернет и только для доверенных приложений.

12. Не используйте компьютер с системой «iBank 2» в публичных (проводных/беспроводных) сетях, предоставляющих доступ к сети Интернет, так как в таких сетях значительно повышается риск хищения и последующего неправомерного использования персональной информации пользователей системы ДБО «iBank 2».

13. Необходимо исключить установку на компьютер с системой «iBank 2» ПО, полученного из не заслуживающих доверия источников, а также нелицензионного и свободно-распространяемого ПО.

14. Не привлекайте для администрирования и обслуживания компьютер с системой «iBank 2» ИТ-персонал на условиях предоставления ему удаленного доступа.

15. При работе в системе «iBank 2» не оставляйте компьютер с активной системой «iBank 2» без присмотра, выходите из системы «iBank 2», даже если необходимо отойти на непродолжительное время.

16. Если заметите подозрительную активность на компьютере с установленной системой «iBank 2» (самопроизвольные движения мышью, открытие/закрытие окон, набор текста) – немедленно выключите компьютер и сообщите в ООО Пир Банк по телефону: *+7 (485) 691-69-32* о возможной попытке несанкционированного доступа к системе.

Рекомендации, направленные на защиту от копирования ключевой и парольной информации в системе «iBank 2»

1. Не храните логин и пароль для доступа к системе «iBank 2» на компьютере (в электронном виде) и там, где злоумышленник может их легко обнаружить вне компьютера.
2. При первом входе в систему «iBank 2» измените пароль доступа и храните его в секрете. При этом не назначайте пароль, используемый в системе «iBank 2», в любых других системах и сервисах. Целесообразно осуществлять плановую смену пароля не реже одного раза в 1 месяц.
3. Используйте надежные пароли – длиной не менее 8 символов, содержащие буквы из различных регистров (заглавные и строчные), специальные символы (*, &, ^, % и т.п.) и цифры. Не используйте очевидные сочетания (имя, фамилия, дата рождения, номер телефона).
4. Не передавайте неуполномоченным лицам ключевые носители, логины и пароли доступа, в том числе ИТ-специалистам для проверки работы системы, настроек взаимодействия с Банком и т.п. При необходимости таких проверок владелец ЭП (уполномоченное лицо) обязан лично подключать носитель с ключами ЭП к компьютеру.
5. В случае необходимости отлучиться от рабочего места поместите носители с ключами ЭП в защищённое место (например, в сейф).
6. Не вводите конфиденциальные данные, если окно для ввода или его оформление (логотип, надписи, шрифт и тому подобное) отличается от стандартных окон системы «iBank 2» или отображается не так, как всегда. Внимательно следите за сообщениями, которые появляются на экране компьютера.
7. Необходимо выполнять незамедлительную блокировку и смену ключей ЭП в случаях их компрометации (в том числе утере (даже с последующим обнаружением), в случае обнаружения каких-либо вредоносных программ на компьютере, используемом для работы в системе «iBank 2», и т.п.), а также по истечении срока действия ключей с периодичностью, установленной договорами и документацией.
8. Необходимо заменять ключи ЭП во всех случаях увольнения или смены руководителей юридического лица, подписывавших распоряжения (доверенности) о предоставлении сотрудникам организации полномочий подписания ЭП электронных документов.
9. При обращении от имени ООО ПИР Банк по телефону, электронной почте, через SMS-сообщения, а так же с использованием писем на «официальном» бланке лиц с просьбами сообщить или передать конфиденциальную информацию (ключи, пароли и пр.) ни при каких обстоятельствах *не сообщать* данную информацию.
10. Рекомендуется использовать для хранения ключей ЭП внешние носители, а не жесткие/сетевые диски компьютера. При этом необходимо хранить данный носитель в условиях, исключающих доступ к нему третьих лиц (например, использовать для хранения личный сейф).
11. Не используйте носители с ключами ЭП для каких-либо других целей (в частности, не храните на них любую другую информацию).
12. Извлекайте носители с ключами ЭП из компьютера каждый раз после завершения их использования (т.е. носители с ключами ЭП должны находиться в компьютере только в момент подписания) – даже если работа в системе «iBank 2» продолжается, носители должны быть извлечены из компьютера сразу после окончания подписания документов.
13. Не оставляйте без присмотра сотрудников сторонних организаций, которые производят сервисные работы на компьютере с установленной системой «iBank 2».

Рекомендации по контролю несанкционированных списаний

1. Следует регулярно контролировать состояние своих счетов и незамедлительно информировать обслуживающее подразделение ООО ПИР Банк обо всех подозрительных или несанкционированных операциях по телефонам ООО ПИР Банк.
2. В случае неожиданного выхода из строя компьютера, либо пропадания на нем программного обеспечения системы «iBank 2», необходимо прекратить на компьютере работу, отключив его от всех видов сетей, включая локальную корпоративную сеть, и модемов, срочно запросить в ООО ПИР Банк выписку по счету. При обнаружении несанкционированных платежных операций написать заявление в ООО ПИР Банк, а также обратиться с соответствующим заявлением в правоохранительные органы. Работоспособность поврежденного компьютера не восстанавливать до проведения технической экспертизы. Переустановку ПО системы «iBank 2» проводить на новом компьютере. После переустановки ПО системы «iBank 2» произвести немедленную смену всех своих ключей ЭП.
3. Появление на экране компьютера во время отсутствия соединения с Банком сообщений, провоцирующих на установление такого соединения, свидетельствует о наличии на компьютере вредоносного ПО.
4. В данной ситуации установление соединения с Банком может привести к отправке фальшивого документа. При появлении подобного сообщения необходимо провести контроль платежных документов.

Соблюдение Вами этих мер позволит существенно снизить риски, связанные с использованием системы «iBank 2» и предотвратить несанкционированный доступ к Вашим денежным средствам.

Успешного Вам бизнеса и финансового процветания!

С уважением, ООО ПИР Банк

Телефон службы поддержки системы «Клиент-Банк»:
+7 (495) 691-69-32