Рекомендации по информационной безопасности для клиентов банка, использующих в своей деятельности системы Интернет-Банк.

Уважаемые клиенты!

В течение последних лет продолжились и участились попытки противоправного завладения денежными средствами клиентов банков, использующих в своей деятельности системы дистанционного обслуживания. По прогнозам аналитиков в области компьютерной безопасности, в будущем ожидается рост такого рода преступлений. Разработчиками систем дистанционного обслуживания и сотрудниками АО БАНК "МОСКВА-СИТИ" проводится работа по обеспечению безопасности этих систем, однако, без реализации защитных мер непосредственно Вами, как клиентами нашего банка, она не даст желаемого результата.

Практика показала, что злоумышленники чаще всего не пытаются взламывать компьютерные сети банков, а захватывают управление компьютерами клиентов, и, получая доступ к ключам электронно-цифровой подписи и паролям доступа, осуществляют платежи от их имени. Существенную опасность представляют также уволенные или недобросовестные сотрудники организаций, имеющие или имевшие ранее доступ к системе «Интернет-банк».

Заботясь о безопасности наших клиентов, опираясь на действующие законодательство, а также в соответствии с рекомендациями Банка России, наш банк разработал следующие рекомендации по реализации защитных мер на персональных компьютерах клиентов банка, использующих в своей работе системы дистанционного обслуживания:

1. Настоятельно рекомендуется использовать лицензионно-чистое программное обеспечения (далее ПО), включая операционную систему, установленное на компьютере, используемом для работы с системой дистанционного обслуживания (далее – системой «Интернет-Банк»). Использование нелицензионных копий операционных систем и любых иных программных продуктов крайне нежелательно по следующим причинам:
- в том случае, если они получены не из доверенного источника, например, приобретены на компьютерном рынке, скачаны из файлообменной сети и т.д., они могут уже быть заражены вирусными программами, или иметь «черные ходы», используемые злоумышленниками;
- программы-«активаторы», как правило, используемые для обхода систем проверки подлинности, в большинстве своем используют вирусные механизмы и нарушают механизмы самозащиты систем, что может привести к заражению операционной системы вирусными программами или установке в нее троянской компоненты, используемой злоумышленниками для получения несанкционированного доступа к компьютеру;
- возможно нарушение в работе систем автоматического обновления операционной системы и связанных программных продуктов, что оказывает негативное влияние на механизм обеспечения безопасности.

Используя нелегальное программное обеспечение на компьютере, предназначенному для эксплуатации систем «Интернет-Банк», Вы подвергаете себя неоправданному риску, поскольку потери в результате хищений могут быть значительно больше, чем экономия на приобретении легального программного обеспечения.

Для операционных систем семейства Microsoft Windows версия операционной системы должна быть не ниже Windows XP с установленным Service pack 3 и всеми актуальными на момент установки системы «Интернет-Банк» обновлениями

операционной системы. Также обязательно должна быть включена функция автоматической загрузки и установки обновлений операционной системы. Для прочих программных продуктов должна быть включена возможность автоматической установки обновлений для данного программного обеспечения, если это предусмотрено производителем программного продукта. Недопустимо использование программ-генераторов инсталляционных ключей или программ снятия защиты от несанкционированного доступа на компьютере с установленной системой «Интернет-Банк».

2. Должно быть установлено и включено программное обеспечение для защиты от вредоносного кода. Использование бесплатных, условно-платных программ, либо программ с ограниченной функциональностью не рекомендуется. Обязательно использование средств автоматической загрузки и обновления версий защитного ПО и баз данных сигнатур вредоносного кода. По возможности, программное обеспечение для защиты от вредоносного кода и межсетевой экран должны быть настроены способом, обеспечивающим надлежащий уровень реакции на возникающие угрозы без участия пользователя.

3. На компьютере с системой «Интернет-Банк» должен быть установлен и настроен лицензионно-чистый межсетевой экран. Его настройки должны разрешать только необходимые для работы соединения. При использовании собственных маршрутизаторов, прокси-серверов, другого оборудования и ПО для доступа в сеть интернет из локальной сети предприятия также необходимо использовать межсетевой экран, ограничивающий трафик для компьютера с системой «Интернет-Банк» возможность просмотра ресурсов сети Интернет должна быть ограничена ресурсами, необходимыми в рабочей деятельности. Настройки безопасности программ, применяемых для просмотра ресурсов Интернет, должны быть установлены в максимально возможный уровень, не препятствующий исполнению пользователем своих служебных обязанностей.

4. Не рекомендуется использование компьютера с системой «Интернет-Банк» для каких-либо целей, отличных от связанных с исполнением должностных обязанностей, например, развлекательных.

5. Работа пользователя на данном компьютере должна происходить в режиме непривилегированного пользователя (классификация в системе Microsoft Windows - USER). Работа в роли пользователя, обладающего административными правами, локальными или иными, должна допускаться только при выполнении действий, требующих данных прав.

6. Должна быть отключена возможность автозапуска программ со всех устройств хранения информации и сменных носителей. Загрузка компьютера должна осуществляться с установленного в нем жесткого диска, возможность первичной загрузки с иных устройств (CD/DVD, внешних накопителей, сетевая загрузка и прочее) должна быть отключена средствами BIOS компьютера. Доступ к BIOS компьютера должен быть закрыт паролем.

7. Не допускается вход в систему любого из пользователей данного компьютера без ввода пароля, причем, количество неудачных попыток его ввода должно быть обязательно ограничено. Пароли пользователей должны иметь длину не менее 8 символов и содержать символы, цифры и спецсимволы латинского алфавита в различном регистре ввода, таким же образом должны формироваться и пароли к системе «Интернет-Банк». Пароли к ключам системы «Интернет-Банк» и компьютеру, обеспечивающему её

функционирование, должны храниться в условиях, не допускающих их попадание к посторонним лицам. Срок действия паролей и ключей целесообразно ограничивать сроком в 1-2 месяца. Также желательно переименование учетных записей пользователей с административными правами.

8. После установки на компьютер системного и прикладного программного обеспечения, требующего для этого административного уровня доступа, целесообразно произвести очистку кэша паролей (в случае использования систем MS WINDOWS), с целью недопущения попадания паролей административных учетных записей в руки злоумышленников.

9. Если это возможно, то компьютер должен быть физически отключен от сети предприятия или же не входить в сетевой домен (домены) или рабочие группы, существующие в сети предприятия.

10. Использование локальных беспроводных сетей не рекомендуется. Так же не рекомендуется использование беспроводных сетей для подключения к провайдерам Интернет.

11. При использовании беспроводных сетей не допускается отключение шифрования канала передачи данных или использование стандарта безопасности WEP. Пароли к точкам доступа, ключи сетей и действия с ними должны соответствовать требованиям, изложенным в п.7 настоящего документа. Также желательно установить контроль доступа по MAC-адресам устройств. Идентификатор сети желательно назначить таким образом, чтобы избежать даже косвенной ассоциации точки доступа с объектом, на котором она установлена, или сотрудником предприятия.

12. Не допускается установка или активация на данном компьютере программ дистанционного управления или каких-либо их компонентов. Также необходимо отключить системы дистанционного управления аппаратным обеспечением, путем внесения соответствующих изменений в настройки BIOS компьютеров.

13. Недопустимо предоставление ресурсов данного компьютера в общий доступ, если же избежать этого не представляется возможным, то пароль доступа к предоставляемым ресурсам должен соответствовать требованиям, указанным в п.7 настоящего документа. Предоставление в общий доступ логических дисков с установленной системой «Интернет-Банк» категорически запрещается. Также запрещается предоставление в общий доступ устройств, используемых для хранения ключей системы «Интернет-Банк», или же портов компьютера, к которым они подключаются.

14. Не допускается наличие на сменном носителе, используемом для хранения ключей электронно-цифровой подписи системы «Интернет-Банк» иной информации, кроме как ключевой. Любое устройство, используемое для хранения ключей системы «Интернет-Банк» или подписи документов этой системы, должно подключаться к компьютеру исключительно на время работы с системой «Интернет-Банк», после чего должно отключаться в штатном порядке и перемещаться в место, предназначенное для его безопасного хранения (металлический шкаф, сейф и т.д.).

15. В том случае, если это возможно, необходимо использовать для подписи документов пару ключей, например, ключ бухгалтера и ключ директора, размещаемые на разных носителях данных. Эта мера, в сочетании с прочими, способна уменьшить

вероятность совершения хищения, поскольку злоумышленнику необходимо будет завладеть уже двумя ключами и двумя паролями к ним.

16. Для хранения ключевой информации и шифрования данных обязательно использование защищенных носителей ключей RuToken, обеспечивающих больший уровень защиты от попыток несанкционированного использования систем «Интернет-Банк». Также защищенные носители обязательно применять в тех случаях, когда осуществляется подключение к системе «Интернет-Банк» из потенциально опасного места, например, с использованием компьютера в гостинице, аэропорту, интернет-кафе или открытой публичной точки доступа Wi-Fi. Однако, они не являются панацеей, поскольку, если злоумышленник получил удаленный доступ к компьютеру (например, в результате нарушения положений п.12), то его действия будут неотличимы от штатных действий пользователя.

17. Запрещается хранение ключей системы «Интернет-Банк» непосредственно на жестких дисках компьютера или иных встроенных в него устройствах хранения данных.

18. При подключении к сети Интернет рекомендуется использовать услугу по предоставлению статического IP адреса. В этом случае необходимо сообщить банку IP-адрес, идентифицирующий компьютер, или компьютерную сеть клиента, или его провайдера в сети Интернет для ограничения доступа с других адресов. Эта мера позволит снизить вероятность успешных действий злоумышленников, даже в том случае, если они завладели ключами и паролями к системе «Интернет-Банк».

Организационные меры защиты:

19. При увольнении сотрудников, имевших любой доступ к секретным ключам электронной подписи и их носителям, обслуживающих систему «Интернет-Банк» или обеспечивающих информационно-техническую поддержку предприятия, необходимо незамедлительно заблокировать текущие и создать новые ключи системы «Интернет-Банк», сменив также пароли доступа к используемому в работе с данной системой компьютеру. Также необходимо провести полную его антивирусную проверку, а также проверку на предмет запланированного исполнения каких-либо программ или наличия программ или компонентов программ удаленного доступа.

20. Ключи и пароли доступа к системе «Интернет-Банк», равно как и пароли к компьютеру, обеспечивающему функционирование этой системы, должны обязательно меняться в случае заражения данного компьютера вредоносными программами, даже в том случае, если было проведено успешное их удаление, вне зависимости от того, выполнялась или нет переустановка системного и прикладного программного обеспечения.

21. Лицо, уполномоченное для работы с системой «Интернет-Банк», не должно ни в коем случае передоверять свои обязанности иным лицам при любых обстоятельствах и для решения любых задач.

22. Следует определить внутренними документами порядок и ответственных за следующие мероприятия: настройку безопасности операционной системы, систем антивирусной защиты, настройку межсетевых экранов; настройку и ограничение прав доступа; организацию парольной защиты; установку и выполнение требований по хранению ключевой информации; организацию реагирования на инциденты, связанные с информационной безопасностью.

Защита от социального инжиниринга.

Обращаем внимание пользователей системы!

23. Не отвечайте на сообщения, письма или телефонные звонки, якобы от имени банка, с просьбой выслать секретный ключ, пароль и другие конфиденциальные данные. Банк никогда не запрашивает у клиентов конфиденциальную информацию! При общении с сотрудниками банка пользуйтесь только теми телефонами, которые указаны на нашем сайте, либо получены Вами от сотрудников банка лично.

24. Банк никогда не осуществляет рассылку писем, содержащих ссылки для перехода на страницы в сети Интернет, или для загрузки какого-либо программного обеспечения или данных. Необходимое для работы системы «Интернет-Банк» программное обеспечение можно получить на официальном сайте банка или у сотрудников банка в офисах.

25. В случае если при включении или в процессе работы системы «Интернет-Банк» будут обнаружены какие-то не имевшие ранее места события, такие, как нештатные информационные окна, сообщения, платежи, Вами не проводившиеся или не санкционированные, сообщения об ошибках, сообщения о неверном ключе доступа или пароле, и т.п. – лицу, ответственному за работу с системой, надлежит зафиксировать суть события, прекратить работу, выключить компьютер и незамедлительно уведомить о событии сотрудников банка. Эти же действия необходимо выполнить и в случае появления признаков заражения компьютера вирусными программами.

26. Если невозможно избежать использования систем обмена сообщениями или e-mail на данном компьютере, то необходимо соблюдать максимальную осторожность при работе с ними: не открывать письма или сообщения, полученные из неизвестных источников, не устанавливать и не запускать программы, прилагающиеся к письмам и не переходить по ссылкам из писем или сообщений.

Приведенные в данном документе правила, требования и рекомендации предполагают, что их реализация будет поручена лицам, имеющим надлежащую квалификацию и опыт работы. Они способны дать реальный эффект лишь при комплексном использовании и надлежащем контроле за их реализацией и постоянном выполнении.

Соблюдение Вами этих мер позволит существенно снизить риски, связанные с использованием систем «Интернет-Банк» и предотвратить несанкционированный доступ к Вашим денежным средствам.