Рекомендации по безопасности при работе с системой «Интернет-банк»

В целях обеспечения необходимого уровня защищенности Клиентов при проведении операций по системе «Интернет-банк» (далее – Система) и предотвращения попадания на компьютер, используемый для работы в Системе, вредоносного программного обеспечения, РОСКОМСНАББАНК (ПАО) рекомендует следующие организационно-технические меры защиты:

1. Общие требования

Для обеспечения высокого уровня информационной безопасности при эксплуатации Системы в организации необходимо:

1.1. Четко определить компьютеры, предназначенные для работы в Системе, и ответственных сотрудников, уполномоченных для работы в Системе.
1.2. Ограничить доступ к компьютерам посторонних лиц и неуполномоченных на работу в Системе сотрудников.
1.3. Любые работы на компьютерах проводить под наблюдением ответственного сотрудника организации.
1.4. При увольнении ответственного сотрудника или ИТ-специалиста организации, имеющих доступ к компьютеру или к секретным ключам, срочно обратиться в Банк для блокировки ключей и их перегенерации.
1.5. Использовать выделенный только для целей работы в Системе компьютер.
1.6. Определить места хранения личной ключевой информации ответственного сотрудника, исключающие доступ к ним других лиц.
1.7. Назначить ответственного за соблюдение требований информационной безопасности при работе в системе, который должен постоянного контролировать соблюдение мер информационной безопасности, выявлять в результате проведения проверочных мероприятий, устранять и информировать руководство организации обо всех выявленных нарушениях, проводить необходимые мероприятия по усилению безопасности в соответствии с информационными сообщениями Банка.
1.8. Регулярно контролировать платежные документы и состояние счета.

2. Требования к автоматизированным рабочим местам (компьютерам)

2.1. Использовать только лицензионное системное и прикладное ПО, регулярно обновляемое в автоматическом режиме из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.
2.2. Использовать только лицензионное и регулярно обновляемое в автоматическом режиме специализированное ПО для защиты информации: антивирусное ПО, персональные межсетевые экраны (файрволы), средства защиты от несанкционированного доступа и пр.
2.3. Устанавливать и использовать на компьютере только ПО, необходимое для работы с Системой.
2.4. В целях снижения вероятности заражения, работать в операционной системе компьютера с минимально необходимыми правами «Пользователя»; ограничить использование портов и приводов компьютера (USB, FDD, CD/DVD, Wifi, Bluetooth и т.д.).
2.5. В целях снижения вероятности использования злоумышленником уязвимостей Web-браузера (обозревателя Интернета) задать для него максимальный уровень безопасности по умолчанию (запрет языка Java, сценариев, загрузки элементов ActiveX, автоматической загрузки файлов из сети Интернет, автоматического запуска файлов из сети Интернет, автоматической загрузки не подписанных элементов ActiveX). Для тех сайтов, которые требуют разрешения исполнения соответствующих элементов (в частности, сайт Системы), необходимо индивидуально разрешить их исполнение, добавив сайт в список надежных.
2.6. Обращать внимание на нестандартные действия компьютера, сообщения, зависания и. т.п. – это может быть проявлением действий специального вредоносного ПО. В таких случаях необходимо провести проверку состояния счета.

3. Требования к парольной защите

3.1. Не использовать простые пароли (111111, 12345, abcdefg, qwerty, дата рождения, номер телефона и т.п.) – такие пароли легко можно угадать либо подбирать при помощи специального

программного обеспечения. Пароль должен содержать прописные и строчные буквы русского и латинского алфавита, а также цифры и специальные символы.
3.2. Периодически менять пароль для входа в Систему (наиболее оптимальным сроком действия пароля является 2-3 месяца).
3.3. Никому не распространять пароли, не записывать их.
3.4. Незамедлительно сообщать в Банк о фактах невозможности получения доступа к Системе по причине несовпадения пароля на вход в систему. Обычной практикой злоумышленников является смена пароля в целях маскировки своих действий и получения дополнительного времени для успешного выполнения операций от имени Клиента.

4. Правила безопасной работы в сети Интернет

4.1. Не использовать компьютер, с которого осуществляется работа в Системе, для развлечений и Интернет-серфинга, не посещать сайты сомнительного содержания – наибольшие источники распространения вредоносных программ.
4.2. Не использовать для работы в Системе компьютеры общего пользования (в интернет-кафе, бизнес-центрах и т.д.).
4.3. Обращать внимание на наличие «https:» в начале адреса страницы обозревателя, который свидетельствует о наличии защищенного соединения, и правильность самого адреса Системы: https://dbo.bashkomsnabbank.ru:1023/.
4.4. Не открывать, не сохранять и не устанавливать подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях. Такие файлы лучше немедленно удалять. В случае необходимости загрузки файла, необходимо убедиться, что он проверен антивирусом.
4.5. Не вводить конфиденциальные данные, если окно для ввода отличается от стандартных окон Системы (логотип другого банка, другие надписи, шрифт и тому подобное) или отображается не так как всегда (нарушен порядок работы в системе) – внимательно следить за сообщениями, которые появляются на экране компьютера.
4.6. При работе со средствами электронной связи следует обращать особое внимание на отправителя корреспонденции, будь то работа с почтой через Web-интерфейс одной из известных почтовых систем mail.ru, yandex.ru и т.п., или в локально установленных программах типа Outlook, Outlook Express, The Bat! и т.д., или в службах мгновенного обмена сообщениями ICQ, Instant Messaging, Mail.ru-агент и т.д. Если отправитель сообщения неизвестен, открывать вложение из такого сообщения категорически не рекомендуется. Даже если отправитель Вам известен, и Вы давно ведете с ним переписку, это не гарантия, что вложение безопасно. В таких случаях рекомендуется сохранять вложения в специально созданную папку на жестком диске и предварительно проверять их антивирусом. После успешной проверки вложения антивирусом открывать его уже из этой папки. Необходимо учитывать, что никакие обновления для компьютеров и Системы не распространяются по почте.

5. Требования к использованию ключей Системы

5.1. Обеспечить надежное хранения ключей Системы – наличие ключа позволяет заверить от Вашего имени документ и передать его на исполнение в Банк.
5.2. Никому не передавать ключи Системы, в том числе Вашим ИТ-специалистам.
5.3. Использовать для хранения ключевой информации только рекомендованные Банком аппаратные ключевые носители eToken с неизвлекаемыми ключами – не хранить ключи на жестком диске компьютера, дискетах и флеш-носителях, иначе к ним могут получить доступ злоумышленники. Использовать средства визуализации подписываемых документов SafeTouch – средства защиты последнего поколения, позволяющие исключить все известные на сегодняшний день виды мошенничества.
5.4. В случае использования средства визуализации подписываемых документов, внимательно сверять реквизиты каждого платежа, отображаемого на экране Safe Touch, перед его подписанием и отправкой в Банк.
5.5. Не держать носители ключей постоянно вставленными в компьютер – использовать их только в случае необходимости подписания документов.
5.6. Обязательно использовать пароли на доступ к секретным ключам. Наличие пароля усложняет возможность использования ключа в случае его похищения злоумышленником.
5.7. При возможности внедрить использование для отправки документов двух обязательных электронных подписей. Украсть два ключа сложнее, чем один.
5.8. При вводе ключа и пароля обращать внимание на правильное отображение названия ключа.
5.9. При компрометации или подозрении на компрометацию секретных ключей срочно обратиться в Банк для блокировки ключей и их перегенерации.

5.10. Учитывать, что Банк никогда не осуществляет рассылку электронных сообщений, содержащих компьютерные программы; а также рассылку сообщений или телефонных звонков с просьбой предоставить конфиденциальную информацию (логины, пароли, ключи и т.д.).

Помните: ответственность за обеспечение сохранности и секретности ключей и паролей Системы ложится на пользователя Системы; · в случае обнаружения несанкционированных списаний необходимо незамедлительно обратиться в обслуживающее Вас подразделение Банка с заявлением, а также обратиться с соответствующим заявлением в правоохранительные органы, при этом дальнейшая работа на компьютере крайне нежелательна – необходимо отключить от него все сети связи и электропитания.