Приложение №3 к Приказу № 17-0197 от 05.05.2017

Публичное акционерное общество «Почта Банк»
тел. 8 800 550 0770, www.pochtabank.ru

ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ АРМ ПОЛЬЗОВАТЕЛЯ

(РЕДАКЦИЯ 3.0)

Термины, указанные в настоящем документе с заглавной буквы, используются в значении, определенном в Соглашении о дистанционном обслуживании юридических лиц в ПАО «Почта Банк».

1. Общие требования

1.1. Правом доступа к АРМ Пользователя должны обладать только лица, ознакомленные с настоящими требованиями и имеющие на это полномочия.

1.2. На АРМ Пользователя необходимо соблюдать следующие требования:

- работать под учетной записью пользователя (без прав администратора на данном персональном компьютере);
- использовать только лицензионное программное обеспечение, регулярно устанавливать рекомендуемые производителями обновления, как операционной системы, так и используемых программ (браузера и иных прикладных программ);
- заблокировать доступ в Интернет, за исключением ресурсов необходимых для использования АРМ Пользователя;
- хранить и использовать идентификаторы, пароли, ключи шифрования и ЭП (далее - Ключи), Коды подтверждения с полным исключением возможности несанкционированного доступа к ним посторонних лиц, включая коллег по работе, родственников, знакомых, детей и др. Никому не передавать Ключи и пароли и не оставлять их без присмотра;
- установить лицензионное антивирусное программное обеспечение. Регулярно производить обновление и полную антивирусную проверку АРМ Пользователя;
- защитить АРМ Пользователя от сети Интернет межсетевым экраном;
- разрешить запускать только те приложения, которые необходимы для выполнения работ в рамках Соглашения о дистанционном обслуживании юридических лиц в ПАО «Почта Банк»;
- на АРМ Пользователя должна быть установлена только одна операционная система;
- на АРМ Пользователя должна быть установлена парольная защита на вход в BIOS и в операционную систему. Пароль должен обладать необходимой сложностью, исключающей его подбор по словарю;
- программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам;
- блокировать или выключать АРМ Пользователя каждый раз при покидании своего рабочего места;
- извлекать ключевой носитель каждый раз при прекращении работы с АРМ Пользователя.

1.3. В целях предотвращения несанкционированного доступа к АРМ Пользователя пользователям запрещается:

- оставлять пароли к ключевому носителю на открытом месте (столе, персональном компьютере, временно записывать куда-либо);
- оставлять без контроля АРМ Пользователя, при включенном питании и загруженном программном обеспечении. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана должно производиться с использованием пароля доступа;
- использовать для доступа к Личному кабинету гостевые компьютеры в гостиницах, интернет-кафе и других общедоступных местах (риск хищения Ключей в этом случае очень велик);
- исполнять и открывать файлы, полученные из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов;
- использовать электронную почту, за исключением случая резервного обмена информацией с Банком.

2. Правила безопасности при работе с АРМ Пользователя

2.1. Прежде чем пройти авторизацию в Личном кабинете, необходимо убедиться, что соединение происходит в защищенном режиме с использованием протокола HTTPS (появляется буква S в адресной строке: https://glk.pochtabank.ru, https://lk.pochtabank.ru или https://lk2.pochtabank.ru (в зависимости от используемого канала)), удостовериться в правильности сертификата SSL-соединения. Ссылка для входа в Личный кабинет указана на сайте Банка www.pochtabank.ru.

2.2. Не пользуйтесь АРМ Пользователя если имеется подозрение, что он заражен вирусной программой.

Симптомы заражения:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- произвольно, без участия пользователя, на персональном компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ выйти в Интернет, хотя пользователь этого не инициировал;
- частые зависания и сбои в работе персонального компьютера, медленная работа персонального компьютера при запуске программ;
- невозможность загрузки операционной системы, исчезновение файлов и каталогов или искажение их содержимого.

2.3. Одним из способов мошеннических действий является рассылка писем с указанием ссылок на поддельные web-сайты, имеющие похожие адреса, или перенаправление на них с других ресурсов. К примеру, pochta-bank.ru, pochtabahk.ru, pochtabamk.ru вместо верного pochtabank.ru. Внимательно проверяйте адрес сайта перед авторизацией или совершением операций. Если он отличается от указанного в Заявлении о присоединении, не используйте данный сайт. Для входа в Личный кабинет перейдите по ссылке с сайта Банка www.pochtabank.ru или наберите адрес в браузере вручную.

2.4. Не храните на персональном компьютере конфиденциальную информацию о Вашем логине и пароле для доступа к АРМ Пользователя.

2.5. Удаляйте конфиденциальную информацию в случае передачи АРМ Пользователя другим лицам (продажа устройства, передача в ремонт).

2.6. Ни при каких условиях не сообщайте и не передавайте информацию о Вашем логине, пароле, одноразовых паролях и иных сведениях, используемых для авторизации в АРМ Пользователя никому, включая сотрудников Банка.

2.7. При возникновении подозрений, что Ваши данные для доступа (логин или пароль) стали известны посторонним лицам, незамедлительно обратитесь в Банк для блокировки доступ к Личному кабинету и обязательно смените пароль.

3. Правила безопасности по использованию носителей ключевой информации

3.1. Уделите вопросу хранения ключа электронной подписи должное внимание. Помните, что наличие ключа позволяет заверить от Вашего имени документ и передать его на исполнение в Банк. Для большей безопасности храните ключи на съемных защищенных ключевых носителях в сейфе или ином хранилище, обеспечивающем сохранность ключевой информации. Ключевые носители с ключами электронных подписей должны хранится раздельно для обеспечения условия невозможности их одновременной компрометации.

3.2. Подключайте ключевой носитель к компьютеру только на время подписи документов. Не держите ключевые носители постоянно подключенными к компьютеру. Ни в коем случае не храните ключи на жестком диске персонального компьютера.

3.3. При вводе ключа и пароля обращайте особое внимание на правильность отображение названия ключа. При компрометации Ключей незамедлительно сообщите об этом в Банк.

3.4. Не храните вместе пароли и ключевой носитель (физически близкое расположение);

3.5. Владелец ключевого носителя несет полную ответственность за его сохранность и использование.

3.6. В случае компрометации Ключей должна быть произведена их замена.

3.7. Владельцу необходимо произвести замену Ключа заблаговременно до истечения срока его действия.

4. Правила безопасности по использованию паролей

4.1. Для доступа в учетную запись к АРМ Пользователя необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

- длина пароля должна быть не менее 7 символов. Пароль должен содержать символы минимум из следующих символьных групп: цифры, заглавные и строчные буквы латинского алфавита;
- пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые слова и комбинации букв (dddddd, 333444555, qwerty, 12345, abc123, passw0rd, pochta и т.п.);
- пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, и т.п.);

- пароль не должен совпадать с предыдущими паролями и не должен совпадать с логином, а также не должен быть копией пароля, используемого Вами в других системах (операционная система персонального компьютера, электронная почта, развлекательные ресурсы в Интернет и т.п.).

4.2. Никогда не сообщайте свой пароль третьим лицам, в том числе коллегам, родственникам и сотрудникам Банка.

4.3. Не записывайте свой пароль там, где доступ к нему могут получить третьи лица. Запрещается сохранять логин и пароль на персональный компьютер, мобильном устройстве, а также на иных электронных носителях, доступ к которым могут получить третьи лица.

4.4. Рекомендуется осуществлять смену пароля для доступа к АРМ Пользователя не реже одного раза в 3 (Три) месяца.

4.5. При возникновении подозрений, что Ваш пароль стал известен третьим лицам, необходимо незамедлительно сменить пароль или обратиться в Банк для блокировки доступа в Личный кабинет.

5. Дополнительные рекомендации

5.1. При утрате мобильного телефона, на который направляются одноразовые пароли, незамедлительно обратитесь к своему оператору сотовой связи для блокировки SIM-карты и в Банк для блокировки доступа к Личному кабинету.

5.2. Для изменения номера телефона, используемого для получения одноразовых паролей необходимо обратиться в Банк с письменным заявлением.

5.3. Банк никогда не связывается по телефону и не осуществляет рассылку сообщений по СМС или e-mail с просьбой предоставить, подтвердить или уточнить Вашу конфиденциальную информацию (пароли, логины, номер мобильного телефона, на который приходят одноразовые пароли и другие конфиденциальные данные). Не отвечайте на такие сообщения.

5.4. Банк никогда не связывается с просьбой установить или обновить программное обеспечение, в своих электронных письмах никогда не рассылает программы. Не открывайте подозрительные файлы, присланные вам по электронной почте.

5.5. При получении подозрительного сообщения не отвечайте на него, не переходите по ссылкам, указанным в подозрительном сообщении.

5.6. Если вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль для входа в Личный кабинет.

5.7. Обращайте внимание на появление подозрительной активности на АРМ Пользователя, например, самопроизвольные движение курсора на экране, набор текста и т.п. Обращайте внимание на невозможность зайти на сайт Личного кабинета, при том, что другие интернет-сайты у Вас загружаются, а также на невозможность войти в Личный кабинет по причине несовпадения логина и пароля, при том, что они корректны. Данные факты могут свидетельствовать о заражении Вашего АРМ Пользователя вредоносными программами.

5.8. Запрещено работать с зараженным вирусами АРМ Пользователя.

5.9. Банк рекомендует отслеживать информацию по вопросам информационной безопасности в связи с видоизменением способов мошеннических действий и информационных угроз.

Вам могут быть полезны следующие ресурсы:

- «Управление «К» предупреждает: будьте осторожны и внимательны!»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/broshyura_k_01_02_20121.pdf
- «Вредоносные программы в интернете»: http://mvd.ru/upload/site1/mvd/mvd2/mvd3/liflets_out_1.pdf
- «Пользователям интернета»: http://mvd.ru/upload/site1/mvd1/liflets_out_3.pdf
- «Телефонные мошенники»: http://mvd.ru/upload/site1/mvd1/liflets_out_4.pdf

5.10. Для обнаружения необходимости установки обновлений браузера рекомендуем Вам использовать сервис обнаружения уязвимостей: http://www.surfpatrol.ru/.

5.11. При несанкционированном доступе к Ключам или паролям, при подозрении на возможность такого доступа, при увольнении сотрудника, имевшего доступ к Ключам, утере ключевого носителя владелец обязан незамедлительно связаться с сотрудником технической поддержки Банка по телефонам для блокировки Ключей и проведения внеплановой смены Ключей.