Утверждено Решением Правления ООО
КБ «Центрально-Европейский Банк”
(протокол № 43/2017 от 01.12.2017г)

Рекомендации по обеспечению информационной безопасности при работе в системе «iBank2»

Уважаемый Клиент!

В целях обеспечения информационной безопасности при работе в системе «iBank2», необходимо исполнять следующие требования:

1. Реализовать следующие организационные меры защиты информации при назначении функциональных прав и обязанностей сотрудников и использовании средств электронной подписи:

1.1. Назначить лиц, допущенных к работе в системе «iBank2» и имеющих право подписи электронных документов.

1.2. По возможности запретить доступ к электронному устройству, предназначенному для работы с системой «iBank2» (далее – ЭУ), лиц, не допущенных к работе в системе«iBank2».

1.3. Предоставить пользователю, работающему в системе «iBank2» с использованием данного ЭУ, минимальные необходимые права (наличие прав администратора нежелательно).

1.4. Не привлекать для администрирования и обслуживания ЭУ, предназначенного для работы в системе «iBank2», технических специалистов на условиях предоставления им удаленного доступа к ЭУ.

1.5. Разрешить доступ к НКИ и к другим средствам защиты только сотрудникам, являющимся владельцами ключей ЭП.

1.6. Исключить возможность использования НКИ вне ЭУ, предназначенных для работы в системе «iBank2».

1.7. Хранить НКИ в месте, недоступном для посторонних лиц. Подключение НКИ к ЭУ допускается только непосредственно на время работы в системе «iBank2». После окончания сеанса работы в системе «iBank2» НКИ должен быть незамедлительно извлечен из ЭУ!

1.8. Обеспечить неразглашение паролей, используемых в системе «iBank2». Не передавать пароли к ключам ЭП третьим лицам, не записывать пароли и не сохранять их вместе с НКИ. Не делать простых и легких паролей (111111,12345,abcdefg,qwerty и т.п.). Не следует выбирать в качестве пароля дату рождения, номер телефона и другие данные, которые легко узнать.

1.9. Производить замену ключей ЭП до истечения срока их действия. Кроме того, проводить замену ключей ЭП во всех случаях увольнения и/или смены лиц, имеющих доступ к системе «iBank2», а также в случаях подозрений на компрометацию ключей ЭП .

2. Реализовать следующие технологические меры защиты информации:

2.1. Использовать на ЭУ только лицензионное ПО. Своевременно устанавливать обновления операционной системы ЭУ, рекомендуемые компанией-производителем, в целях устранения выявленных в нем уязвимостей. Регулярно выполнять обновления (установка патчей) Web - браузера и ПО Java на ЭУ, так как данные действия значительно повысят его уровень безопасности. Для обновления системного и прикладного ПО необходимо использовать только источники, гарантирующие отсутствие вредоносных программ.

2.2. На ЭУ, используемых для работы в системе «iBank2», рекомендуется выполнить следующие настройки:

- Запретить в свойствах Web - браузера:
  - автоматическую загрузку файлов из сети Интернет;
  - автоматический запуск файлов из сети Интернет;
  - автоматическую загрузку не подписанных элементов ActiveX.
- Отключить загрузку с гибкого диска, привода CD-ROM, загрузку с внешних USB-носителей, загрузку по сети.
- Отключить учетную запись для гостевого входа (Guest/Гость).
- Исключить использование режима автоматического входа пользователя в операционную систему при ее загрузке.
- Отключить режимы отображения окна всех зарегистрированных на ЭУ пользователей и быстрого переключения пользователей.
- Запретить в настройках операционной системы удаленный доступ к этому ЭУ.

3. Реализовать следующие меры для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования ЭУ (далее – вредноносный

код):

3.1. Установить и регулярно обновлять на ЭУ следующие лицензионные технические средства защиты информации, предназначенные для предотвращения воздействия вредоносного кода:

- антивирусное программное обеспечение с ежедневно обновляемыми базами данных сигнатур вредоносных кодов;
- персональные межсетевые экраны (firewall);
- средства защиты от несанкционированного доступа и пр.

3.2. Использовать дополнительное программное обеспечение, позволяющее повысить уровень защиты ЭУ – программы поиска шпионских компонент, программы защиты от «спам» - рассылок.

4. Реализовать следующие меры для защиты информации при использовании сети Интернет:

4.1. На ЭУ, используемых для работы в системе «iBank2», исключить посещение Интернет-сайтов сомнительного содержания и любых других Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), загрузку и установку нелицензионного ПО, и т. п.

4.2. Не работать в системе «iBank2» из мест, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.).

4.3. При работе в системе «iBank2» убедится, что защищенное соединение по протоколу https установлено именно с официальным сайтом услуги (https://ibank2.cebbank.ru), не переходить на данную страницу по ссылке с Интернет-ресурсов (за исключением официального ресурса Банка, www.cebbank.ru) или по электронной почте писем.

4.4. Ограничить список IP-адресов, с которых будет разрешена работа в системе «iBank2». Наиболее предпочтительно использовать при работе в системе «iBank2» статические IP-адреса, что позволяет задействовать встроенный в систему механизм IP-фильтрации в полной мере.

4.5. В случае появления предупреждений Web - браузера о перенаправлении Вас на другой сайт при подключении к системе «iBank2» отложить совершение операций и обратится в службу технической поддержки Банка.

5. Предпринимать следующие дополнительные меры защиты информации при осуществлении работы в системе «iBank2»:

5.1. При входе в систему «iBank2» обращать внимание на информацию о последних сеансах работы в системе «iBank2». Данная информация включает в себя дату и время сеанса, номер ключа и IP-адрес, с которого осуществлялся сеанс. Если информация не соответствует Вашим действиям в системе «iBank2», нужно незамедлительно поставить об этом в известность службу технической поддержки Банка с целью блокировки ключей ЭП.

5.2. Если при входе в систему «iBank2» окно для ввода пароля отличается от стандартных окон системы «iBank2» (логотип другого банка, другие надписи, шрифт и т.д.) или отображается не так как всегда (нарушен порядок работы в системе «iBank2»), не вводить имена и пароли.

5.3. В случае сбоев в работе ЭУ или его поломки во время/после работы в системе «iBank2» (проблемы с загрузкой операционной системы, выход из строя жесткого диска, «странное» поведение ЭУ, медленная работа), следует **НЕМЕДЛЕННО** извлечь НКИ и выключить ЭУ, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции.

5.4. Обращать внимание на любые изменения в привычных процессах установления соединения с системой «iBank2» или в функционировании системы «iBank2». При возникновении любых сомнений в правильности функционирования системы «iBank2» незамедлительно обращаться в Банк.

5.5. Не отвечать на письма с просьбой выслать ключ ЭП и пароль. Банк никогда не запрашивает у Клиентов такую информацию. Такое письмо может быть направлено только злоумышленниками с целью завладеть Вашим ключом ЭП.

5.6. Регулярно контролировать состояние счетов, зарегистрированных в системе «iBank2», и незамедлительно сообщать сотрудникам Банка обо всех подозрительных или несанкционированных операциях.

ВНИМАНИЕ!

Незамедлительное обращение в Банк с предоставлением полной информации о несанкционированном списании денежных средств с Ваших счетов может позволить оперативно приостановить транзакцию и предотвратить финансовые потери.

При любых подозрениях на мошеннические действия (компрометацию ключей ЭП, логинов, паролей и т.д.), а также при нестабильной работе системы «iBank2» (зависание системы «iBank2», самопроизвольное выключение системы «iBank2», ЭУ и т.д.), следует незамедлительно прекратить работу в системе «iBank2», извлечь из ЭУ НКИ, и обратиться в Банк.