

# ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СИСТЕМЫ ИНТЕРНЕТ-БАНК ЕРБ

Документ описывает правила безопасного использования системы Интернет-Банк ЕРБ. Рекомендуется руководствоваться этими правилами на всех компьютерах, где будет использоваться подключение к Интернет-Банк ЕРБ.

АО «Европейско-Российский банк» (далее – «Банк») не несет ответственность за потерю данных, утечку личных сведений, а также за прочий ущерб, возникший в результате неиспользования указанных здесь рекомендаций.

Более подробную информацию о правилах, элементах или актуальных угрозах безопасности системы Интернет-Банк ЕРБ можно найти на сайте Банка.

## ЧАСТЬ ПЕРВАЯ ЭЛЕМЕНТЫ БЕЗОПАСНОСТИ И ТЕРМИНЫ

1. Интернет-Банк неотъемлемо связан с двумя интернет-порталами – Интернет-Банк ЕРБ и Сертификационным центром ЕРБ.
2. Элементы безопасности, предназначенные для входа в Интернет-Банк ЕРБ, называются Аутентификатором. Аутентификатором является Имя пользователя и цифровой сертификат или Имя пользователя, пароль и динамический SMS-ключ, отправляемый на мобильный телефон пользователя.
3. Цифровой сертификат расположен на специальном устройстве, которое подключается к компьютеру через USB порт – далее «Аппаратное оборудование».
4. Любой пользователь, который имеет доступ к счетам в Интернет-Банк ЕРБ, владельцем которых он является или получил права доступа к ним посредством Интернет-Банк ЕРБ, называется Уполномоченным пользователем.

## ЧАСТЬ ВТОРАЯ ОБЩИЕ ПРАВИЛА БЕЗОПАСНОСТИ



5. Рекомендуются использовать возможности настройки лимитов транзакций платежных поручений для всех Уполномоченных пользователей Интернет-Банк ЕРБ (подробную информацию об Уполномоченных пользователях и настройках лимитов транзакций вы найдете в Коммерческих условиях продукта Интернет-Банк).
6. Имена пользователей, пароли, а также личные сведения и Аппаратное оборудование, предназначенное для доступа в Интернет-Банк ЕРБ или любую другую часть системы Интернет-Банка (пароль для связи с HelpDesk, пароли для доступа к Центру сертификатов ЕРБ) хранить в безопасном месте.
7. Целью злоупотребления может стать и Договор об использовании услуг Интернет-Банка и его приложения. Считайте эти документы конфиденциальными, защищайте их от потери и храните в безопасном месте.
8. В случае подозрения раскрытия Имен пользователей, паролей или других конфиденциальных сведений незамедлительно свяжитесь с Банком по телефону +420 236 737 702 и потребуйте блокировку соответствующих услуг.

## **ЧАСТЬ ТРЕТЬЯ**

### **СПЕЦИФИЧЕСКИЕ ПРАВИЛА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ УСЛУГИ ИНТЕРНЕТ-БАНК ЕРБ**

9. Защита системы Интернет-Банка является настолько сильной, насколько сильной является ее самая слабая часть. Система Интернет-Банка состоит из серверов банка, сети Интернет, сети GSM, компьютера пользователя, мобильного телефона пользователя и человеческого фактора.
10. Серверы банка защищены сертификатами серверов, системой файрволов, защитных зон, оборудования мониторинга и другими механизмами, которые во всей системе Интернет-Банка являются очень сильной частью.
11. Потенциально наиболее опасная часть – Интернет, достаточна сильно защищена благодаря зашифрованной связи между сервером банка и компьютером пользователя.
12. Сеть GSM используется только для передачи части информации, которая сама по себе не может использоваться для нарушения защиты Интернет-Банка.
13. Две другие части – компьютер пользователя и мобильный телефон – являются потенциально наиболее уязвимыми местами всей системы, и это по причине того, что за их защиту не может отвечать и не отвечает Банк. Защиту мобильного телефона можно обеспечить относительно просто, телефон рекомендуется иметь постоянно при себе, а данные в его памяти защитить PIN кодом или другими защитными средствами, которые имеются в конкретном аппарате.
14. Более сложным для обычного пользователя является обеспечение безопасности компьютера. Необходимо обеспечить защиту от установки программ позволяющих осуществлять дистанционное управление, считывание данных с клавиатуры (получение пароля), копирование файлов (сертификатов), или же изменение отображаемой информации. По возможности проконсультируйтесь со специалистом о настройках безопасности.
15. Относительно самостоятельной частью и потенциально самым слабым местом защиты является человеческий фактор. Уполномоченный пользователь может предоставить важные части защиты потенциальному нарушителю, который может злоупотребить ими. Защита Интернет-Банк ЕРБ (и других его частей) должна быть настолько совершенной, чтобы даже в случае раскрытия конфиденциальных сведений постороннему лицу не могло произойти злоупотребление Интернет-Банк ЕРБ. Система элементов безопасности всегда состоит из одного или нескольких сведений, которые должен знать только Уполномоченный пользователь и оборудования, которое служит для проверки его подлинности (Аппаратное оборудование или мобильный телефон). Каждый Уполномоченный пользователь должен



осознавать важность сведений, которые служат для проверки его подлинности при использовании Интернет-Банк ЕРБ, и ни при каких обстоятельствах не разглашать эти сведения. Банк ни при каких обстоятельствах не будет требовать от Уполномоченного пользователя эти сведения без использования Интернет-Банк ЕРБ (или связанных приложений), за исключением пароля для коммуникации с HelpDesk.

## ЧАСТЬ ЧЕТВЕРТАЯ РЕКОМЕНДОВАННЫЕ ДЕЙСТВИЯ И НАСТРОЙКИ

16. Рекомендуется периодически менять пароль для входа в Интернет-Банк ЕРБ (рекомендуется менять пароль минимально один раз в месяц)
17. При выборе пароля не использовать легко угадываемую комбинацию, например, имена, даты рождения, телефонные номера и т.п.
18. Никому не передавать свой пароль для входа и предотвращать разглашение при его вводе.
19. Предназначенный для проверки подлинности пользователя сертификат расположен на Аппаратном оборудовании, специфика которого не позволяет злоупотребление им. Доступ к устройству дополнительно защищен с помощью PIN кода. Из этого также следует факт, что для правильной работы этого устройства необходимо, чтобы на компьютере были установлены приложения, позволяющие считывание данных из его памяти. Это фактически предотвращает то, чтобы Аппаратное оборудование простым образом использовалось на чужих и публичных компьютерах. В случае использования мобильного телефона для проверки подлинности, не рекомендуется использовать Интернет-Банк ЕРБ на публичных или чужих компьютерах, особенно на тех, где нельзя гарантировать или обеспечить защиту данного компьютера.
20. Не забывать периодически один раз в год обновлять действие сертификата. Сертификат всегда выдается сроком на один год. В случае, когда Уполномоченный пользователь не провел своевременно обновления, в Интернет-Банк ЕРБ будет закрыт любой доступ. В таком случае пользователь руководствуется указаниями, регулирующими потерю пароля/обновление сертификата.
21. В случае потери Аппаратного оборудования необходимо отменить действие сертификата. Отмена производится в Центре сертификатов ЕРБ пользователем или клиентским работником после проверки этого требования на HelpDesk.
22. В случае, когда будет потерян мобильный телефон, на который отправляются SMS ключи, незамедлительно сообщите об этом в HelpDesk. Клиентский работник заблокирует возможность отправки SMS ключей на номер этого мобильного телефона.
23. В своем браузере используйте максимальное шифрование (128 бит)
24. При коммуникации с сервером банка используйте протокол TLS или SSL 3.0
25. Установите антивирусное программное обеспечение и постоянно (минимально один раз в неделю) обновляйте его.
26. Установите antispyware программное обеспечение и постоянно (минимально один раз в неделю) обновляйте его.
27. При применении антивирусного программного обеспечения уделяйте внимание возможным изменениям в системных файлах, здесь могут проявиться нападения типа троянских коней (вирус импортированный, например, файлом, присоединенным к электронному сообщению).
28. Для текущей работы, особенно при работе с сетью Интернет, не используйте пользовательский профиль с правами администратора.
29. Перед подключением к Интернет-Банк ЕРБ закрывайте все окна интернет-браузера, а потом снова запустите браузер (это предотвратит некоторых виды нападений).



30. Не позволяйте другому лицу подключаться к сети с использованием Вашего профиля пользователя; отходя от компьютера всегда блокируйте его или завершите все соединения между Вашим компьютером и сервером; поместите в безопасное место Аппаратное оборудование, которое служит хранилищем сертификатов; всегда держите у себя телефон для получения SMS кодов.
31. Интернет-Банк ЕРБ и Центр сертификатов ЕРБ не позволяют сохранять пароли и другую тайную информацию, которая используется при работе с ними; это особенно важно если вы работаете с публичного терминала, интернет-кафе или любого другого ненадежного компьютера.
32. Рекомендуется защищать компьютер программами типа «Personal firewall», в первую очередь для подключения к сети Интернет по телефонному кабелю (посредством кабельного телевидения и т.п.).
33. Не рекомендуется устанавливать программное обеспечение, полученное из неблагонадежных источников (публичные библиотеки программного обеспечения, приложения в электронных сообщениях и т.п.). Нелегально полученное программное обеспечение может содержать так называемых «троянских коней», и отправлять ваши пароли автору этих программ. Уделяйте повышенное внимание при получении электронных сообщений с приложениями. Распространяемые по электронной почте сообщения часто содержат так называемых «воров паролей».
34. На компьютере, где используется Интернет-Банк ЕРБ, не рекомендуется использовать так называемые «instant messenger», то есть приложения для коммуникации в реальном времени, например, ICQ, AIM, GoogleTalk, Microsoft MSN messenger или VoIP, Skype. Эти системы имеют ряд недостатков безопасности и ошибок, большинство из них сложно обновляется и имеется высокий риск установки версии с внесенным вредоносным программным кодом. Эти программы можно легко использовать для определения введенных паролей и для скачивания любого файла из компьютера.
35. Если по какой-либо причине вы должны использовать программы типа instant messaging, то рекомендуется не запускать эти программы вместе с системой, Перед использованием Интернет-Банк ЕРБ перезапустите компьютер и не запускайте эти программы, пока вы не завершите работу с Интернет-Банк ЕРБ. Если в рамках этих систем вы получите любое сообщение, содержащее ссылку, перед нажатием на нее необходимо убедиться что речь идет о достоверном источнике.
36. Устанавливайте важные обновления для операционной системы и других программ от компаний производителей.
37. Отнесите сервер Интернет-Банка АО «Европейско-Российский банк» к зоне надежных серверов.
38. В настройках интернет-браузера для зоны общего Интернета установите:
  - запрет скачивания ActiveX объектов (неподписанных и подписанных)
  - запрет инициализации и запуска элементов, необозначенных безопасными
  - запрет запуска ActiveX объектов, необозначенных безопасными
  - у MS VM – Разрешение для языка JAVA: высокий уровень безопасности
  - запрет доступа к датам в разных доменах
  - запрет установки части рабочего стола
  - запрет запуска файлов и программ в IFRAME
  - запрет использования подфреймов в рамках различных доменов
  - высокий уровень безопасности у Software channel permissions
  - запрет внесения в буфер обмена с помощью скриптов
  - запрет запуска java апплетов
39. Далее мы рекомендуем:



- не использовать инструменты, расширяющие возможности браузера (например, MyIE, Maxthon)
- периодически удалять временные файлы Интернет
- проверять действительность сертификатов серверов
- разрешить предупреждение о недействительных сертификатов серверов
- разрешить предупреждение о перенаправлении при отправке форм
- разрешить предупреждение о переходе между защищенным и незащищенным соединением

Помните, когда вы предоставите кому-либо доступ к своим личным сведениям или средствам безопасности, вы дадите такому лицу возможность злоупотребления этими данным или передачи их третьему лицу.