Рекомендации по информационной безопасности
ПАО «САРОВБИЗНЕСБАНК»
при работе с Системой дистанционного банковского обслуживания Faktura.ru

**В целях недопущения хищения и несанкционированного использования Вашего СЕКРЕТНОГО КЛЮЧА ЭП злоумышленниками, требуется придерживаться приведенных ниже правил:**

1. **Не передавайте пароли** к СЕКРЕТНЫМ КЛЮЧАМ, не записывайте их и не сохраняйте вместе с носителем ключа, или в телефоне.
2. **Не делайте простых паролей** (111111,12345,abcdefg,qwerty и т.п.), не следует выбирать в качестве пароля дату рождения, номер телефона и другие данные, которые легко узнать.
3. **Отключайте, извлекайте носители с ключами ЭП**, если они не используются для работы с Faktura.ru. Не держите носители постоянно подключенными к компьютеру, используйте их только в случае необходимости подписи документов.
4. **При генерации ключа ЭП сохраняйте его исключительно на ключевом носителе, полученном в Банке.**
5. **Ограничьте доступ к компьютерам, используемым для работы с Faktura.ru:**
* исключите доступ к компьютерам персонала, не имеющего отношения к работе с Faktura.ru;
* исключите возможность дистанционного доступа к компьютеру, к которому подключаются хранилища ключей.

**Требования 6-9 распространяется и на ПК для переводов денежных средств и на телефон для приема SMS-паролей для переводов.**

1. **Используйте только лицензионное программное обеспечение.** Необходимо использовать и оперативно обновлять системное и прикладное программное обеспечение только из доверенных источников, гарантирующих отсутствие вредоносных программ. При этом необходимо обеспечить целостность получаемых на носителях или загружаемых из Интернета обновлений.
2. **Исключите посещение Интернет‑сайтов** сомнительного содержания, загрузку и установку нелицензионного ПО и т. п.
3. **Используйте и постоянно обновляйте специализированные лицензионные программные средства безопасности:**
* антивирусное программное обеспечение с актуальными антивирусными базами;
* средства выявления вредоносных программ (Троянов);
* персональные межсетевые экраны (файрволы);
* средства защиты от несанкционированного доступа и пр.
1. **Не открывайте письма и вложения к ним, полученные от неизвестных отправителей**, при работе с электронной почтой, не переходите по содержащимся в таких письмах ссылкам.
2. **В адресной строке браузера должен быть указан адрес:** [**https://www.faktura.ru/f2b/**](https://www.faktura.ru/f2b/)**.**

Особое внимание уделяйте наличию **https** в начале строки адреса, это свидетельствует о наличии защищенного соединения.

1. **Не вводите имена и пароли**, **если окно для ввода отличается от стандартных** окон Faktura.ru или отображается не так, как всегда. При вводе ключа и пароля особое внимание обращайте на правильное отображение названия ключа. Внимательно читайте сообщения, которые появляются на экране.
2. **Извлеките СЕКРЕТНЫЙ КЛЮЧ, выключите компьютер, обратитесь в круглосуточную службу технической поддержки системы Faktura.ru:**
* при недоступности web-сервера системы Faktura.ru;
* при появлении во время работы с системой нестандартных сообщений и окон на экране;
* при зависании компьютера;
* при невозможности подключиться к сети Интернет.
1. **Ознакомьтесь с информацией о последних сеансах работы в системе при входе в Faktura.ru.** 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, незамедлительно поставьте в известность службу технической поддержки БАНКА и заблокируйте ключи ЭП.
2. **Не отвечайте на письма с просьбой выслать СЕКРЕТНЫЙ КЛЮЧ ЭП и пароль.** БАНК никогда не запрашивает у клиентов такую информацию. Такое письмо может быть направлено только злоумышленниками с целью завладеть Вашим ключом.
3. **Не оставляйте без контроля рабочие места системы Faktura.ru.**

При кратковременном отсутствии необходимо:

* сохранить все открытые на редактирование документы;
* средствами операционной системы заблокировать рабочее место.
1. **Выполните следующие настройки на компьютерах, где выполняется работа в Faktura.ru:**
* запретите в свойствах обозревателя Интернета:
* автоматическую загрузку файлов из сети Интернет;
* автоматический запуск файлов из сети Интернет;
* автоматическую загрузку не подписанных элементов ActiveX;
* отключите загрузку c внешних носителей, загрузку по сети, если внутренним регламентом организации не предусмотрено иное;
* вход в BIOS рабочих мест системы Faktura.ru защитите паролем, который должен быть известен только системному администратору, если иное не предусмотрено внутренним регламентом организации;
* отключите учетную запись для гостевого входа (Guest);
* не используйте права администратора в повседневной практике при отсутствии необходимости;
* исключите использование режима автоматического входа пользователя в операционную систему при ее загрузке;
* отключите режимы отображения окна всех зарегистрированных на ПЭВМ пользователей и быстрого переключения пользователей;
* включите системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривайте журнал и реагируйте на ошибки;
* запретите в межсетевом экране соединение с интернет по протоколам FTP, SMTP, кроме соединения SMTP только с конкретными почтовыми серверами, на которых зарегистрированы ваши электронные почтовые ящики;
* не давайте разрешения неизвестным программам выходить в Интернет.
1. **Исключите возможность несанкционированного изменения аппаратной части рабочего места с системой Faktura.ru.** При каждом включении проверяйте возможные изменения.
2. Не храните пароли и логины
3. **Обеспечьте контроль действий обслуживающего компьютер персонала, в т.ч.:**
* исключите обслуживание компьютеров, используемых для работы с Faktura.ru, нелояльными сотрудниками;
* никогда не передавайте ключи ЭП кому-либо для проверки работы Faktura.ru, проверки настроек взаимодействия с банком, и т.п. При необходимости таких проверок только лично владелец ключа ЭП должен подключить носитель к компьютеру, убедиться, что пароль доступа к ключу вводится в интерфейс клиентского АРМ Faktura.ru, и лично ввести пароль, исключая его подсматривание.
1. **Позвоните в БАНК и заблокируйте ключ ЭП:**
* при увольнении ответственного сотрудника, имевшего прямой, или технический доступ к СЕКРЕТНОМУ КЛЮЧУ ЭП;
* при возникновении любых подозрений на компрометацию (копирование) СЕКРЕТНЫХ КЛЮЧЕЙ ЭП или компрометацию среды исполнения (наличие незарегистрированных программ, нарушения целостности операционной системы, либо выявления факта повреждения печатей на системных блоках);
* при утере, краже, использовании посторонними лицами мобильного телефона, или SIM-карты, с номером для SMS-паролей и уведомлений связанных с платежами.

**Ответственность за конфиденциальность Ваших СЕКРЕТНЫХ КЛЮЧЕЙ ЭП полностью лежит на Вас, как единственных владельцах СЕКРЕТНЫХ КЛЮЧЕЙ ЭП.**

ПАО «САРОВБИЗНЕСБАНК» не имеет доступа к Вашим СЕКРЕТНЫМ КЛЮЧАМ и возможности подписания документов электронной цифровой подписью от имени владельца СЕКРЕТНОГО КЛЮЧА.

БАНК не несет ответственность за сохранность ключевой информации, находящейся у Вас, а также за возможный ущерб, который можете понести Вы или Ваша организация в случае исполнения БАНКОМ платежных документов, инициированных неуполномоченными лицами, но подписанным с использованием Вашего СЕКРЕТНОГО КЛЮЧА. Ответственность за это полностью лежит на Вас, так как только Вы является единственным владельцем своей ключевой информации.