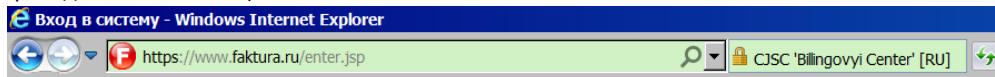


Правила безопасного использования системы «Банк-клиент через Интернет»

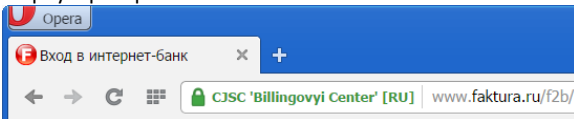
Для повышения безопасности работы в системе «Банк-клиент через Интернет» (далее - Система) и существенного снижения риска использования злоумышленниками ключей для работы в Системе, взлома/заражения компьютера с целью совершения операции без согласия клиента **необходимо выполнять следующее:**

- Незамедлительно обращаться по тел. 8-800-250-3300 для блокировки ключа в случаях:
 - утраты доверия к ключу (доступа неуполномоченных лиц, утраты или оставления ключа без присмотра и проч.);
 - неожиданного выхода из строя или вирусного заражения компьютера;
 - обнаружения признаков работы в Системе без согласия клиента (несанкционированные расходные операции, получение SMS- или e-mail-уведомлений об операциях, которые не совершались, SMS- или e-mail- уведомлений об изменении адреса e-mail или номера мобильного телефона для получения уведомлений, при этом изменения были совершены без Вашего ведома);
 - экстренного прекращения полномочий одного из уполномоченных на доступ в Систему лиц;
 - обнаружения в разделе «Безопасность -> Журнал сеансов работы» фактов проникновения в Систему посторонних лиц (вход в систему с нетипичного IP-адреса либо в нетипичное для Вас время);
 - блокирования телефона, на который приходят SMS сообщения с кодами для подтверждения операций в Системе;
- Ключевой носитель (смарт-карта, токен, флеш-накопитель, дискета и пр.) использовать только лицом, для которого он изготовлен, не передавать его другим лицам, включая других уполномоченных для работы в Системе лиц.
- Хранить Ключевые носители разных уполномоченных лиц отдельно, в защищенном от несанкционированного доступа месте.
- Не устанавливать Ключевые носители в компьютеры, ноутбуки и иные устройства, не используемые для работы в Системе. Не оставлять Ключевые носители установленными в компьютеры после завершения сеанса работы в Системе.
- В случае использования в качестве Ключевого носителя флеш-накопителя, дискеты или прочих не защищенных от копирования носителей — не копировать ключ на жесткий диск, сетевой каталог и прочие совместно используемые ресурсы.
- Устанавливать длинные и сложные пароли для доступа к Ключевому носителю (смарт-карта, токен), содержащие от 6 до 8 символов, или пароли для доступа к Закрытому ключу (флеш-накопитель, дискета), содержащие свыше 6 символов; пароли обязательно должны содержать буквы в верхнем и нижнем регистре (например, «Q» и «q»), цифры и спецсимволы (например, «!;%:?*()_+» и т.п.). Пароль не должен включать в себя повторяющиеся или легко вычисляемые сочетания символов (полные слова; полные слова в транслитерации; полные слова, набранные в другой, противоположной языковой раскладке или обратном порядке; символы, расположенные рядом на клавиатуре; имена; фамилии; памятные даты; адреса; номера телефонов и т.п.). Производить регулярную смену паролей не реже одного раза в месяц. Использовать пароли только соответствующему уполномоченному для работы в Системе лицу. Пароли запрещено записывать, произносить вслух, выводить на экран, кому-либо передавать.
- Осуществлять работу в Системе в помещениях с малой проходимостью или ограниченным доступом во избежание хищения Ключевых носителей. Для обеспечения сохранности пароля ограничить возможность визуального наблюдения за его экраном и клавиатурой, в том числе с использованием системы видеонаблюдения и через оконные проемы.
- Использовать для работы в Системе технически исправный компьютер с установленной лицензионной операционной системой, лицензионным антивирусным программным обеспечением от ведущих производителей и иным лицензионным программным обеспечением, используемым в работе с Системой. Устанавливать критичные обновления и обновления безопасности операционной системы и используемого программного обеспечения, не реже раза в сутки производить обновление антивирусных баз, не реже раза в неделю производить полное антивирусное сканирование компьютера. На компьютере должна быть установлена только одна операционная система.
- Не использовать операционную систему, антивирусное и иное программное обеспечение, для которых прекращен предусмотренный разработчиком выпуск обновлений безопасности, антивирусных баз (например, Windows XP, Windows Server 2003).
- Осуществлять работу на компьютере с правами пользователя, доступ к учетным записям администраторов защищать надежным паролем.
- Исключить удаленное управление компьютером, с которого осуществляется доступ в Систему, без явного подтверждения каждого подключения уполномоченным на доступ в Систему лицом.
- Максимально ограничить работу с флэш-накопителями, дискетами, дисками и т.п. за исключением Ключевых носителей, перед использованием первых осуществлять их полное сканирование антивирусным программным обеспечением.
- В случае использования мобильного телефона с операционной системой Android для получения SMS-уведомлений Системы установить лицензионное антивирусное программное обеспечение от ведущих производителей и только из официального источника (Google Play), не реже раза в сутки производить обновление антивирусных баз, не реже раза в неделю производить полное антивирусное сканирование мобильного телефона. Не устанавливать на телефон приложения, обладающие полномочиями работы с SMS-сообщениями.
- Незамедлительно заблокировать SIM-карту в случае утраты мобильного телефона, используемого для получения сообщений при работе с Системой, включая SMS-сообщения с разовыми паролями.
- Прежде, чем подтверждать платеж в Системе, внимательно проверить в полученном SMS-сообщении с разовым паролем информацию о сумме и получателе платежа.
- По запросу подтверждать подлинность платежных операций с использованием одноразового пароля, высылаемого на номер телефона, либо иным способом, предусмотренным Регламентом, в целях снижения риска совершения мошеннических операций. Незамедлительно направлять в Банк новые номера телефонов в случае их изменения.
- Для предотвращения ввода пароля на мошеннических сайтах, имитирующих работу в Системе, до ввода пароля проверять в адресной строке Интернет-браузера наименование сайта [https://www.faktura.ru/...](https://www.faktura.ru/), на котором осуществляется работа в Системе, и состояние сертификата, обеспечивающего безопасный доступ к сайту www.faktura.ru. Корректное отображение наименования сайта в браузере

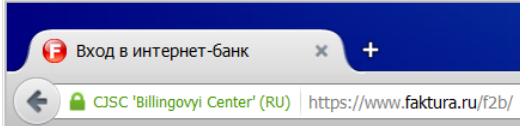
Internet Explorer выглядит следующим образом (при использовании разных версий браузеров изображение может отличаться от приведенных в памятке):



– в браузере Opera:




– в браузере Mozilla Firefox:



– в браузере Google Chrome:



- Проходить процедуру входа в Систему с использованием только ключевого носителя и пароля, в случае использования разовых SMS-паролей на вход в Систему — также использовать присылаемый разовый пароль. Не использовать иную информацию для входа в систему, включая: номер мобильного телефона, номер банковской карты, CVV2/CVC2 коды, расположенные на обратной стороне банковской карты, разовые пароли для подтверждения платежей и прочее. Не сообщать никому, включая сотрудников банка: номер мобильного телефона, номер банковской карты, CVV2/CVC2 коды банковской карты, разовые пароли для подтверждения платежей и прочую конфиденциальную информацию, исключая случаи, предусмотренные Регламентом. Не вводить разовые пароли вне Системы.
- Регулярно контролировать состояние счетов путем просмотра выписки.
- Посредством Системы регулярно проверять список IP-адресов, с которых осуществлялись подключения к Системе (на первой странице после входа), дату и время последних сеансов работы («Безопасность -> Журнал сеансов работы»).
- Руководствоваться информацией сайта www.faktura.ru о безопасном использовании и настройках Системы. Внимательно просматривать все информационные сообщения в Системе и на странице входа в Систему, точно следовать содержащимся в них рекомендациям по безопасности.
- Не оставлять без контроля компьютер при активной сессии работы в Системе. При оставлении компьютера необходимо осуществлять выход из Системы, используя соответствующие кнопки Системы «Выйти» или «Завершить», после чего закрыть окно Интернет-браузера, извлечь Ключевой носитель и произвести блокировку компьютера одновременным нажатием на клавиатуре  и L. Возобновление работы на компьютере производить с использованием пароля доступа. По окончании рабочего дня производить выключение компьютера.
- Об ошибках в работе Системы уведомлять Службу технической поддержки по телефонам 8 (495) 725-59-53, 8 (8442) 99-50-32, 8(8443) 24-10-52, 8 (84457) 2-33-15, 8-800-250-3300.

Для существенного повышения безопасности работы в Системе рекомендуется:

- Устанавливать длинные и сложные пароли для доступа к учетным записям компьютера, используемого для работы в Системе. Установить пароль на вход в BIOS компьютера. Настроить в BIOS возможность загрузки операционной системы только с основного жесткого диска и пароль на загрузку компьютера.
- Настроить правила доступа компьютера в сеть Интернет.
- Настроить аудит (протоколирование) событий в операционной системе и программах, установленных на компьютере, периодически просматривать журналы аудита, реагировать на ошибки и попытки несанкционированного доступа.
- Компьютеры, применяемые для работы в Системе, не использовать в других целях, в том числе рабочих; ограничить посещение Интернета сайтами www.faktura.ru, authority.ru; не посещать сайты социальных сетей, развлекательные и игровые сайты, сайты знакомств, сайты, распространяющие программное обеспечение, музыку, фильмы и т.п. в целях предотвращения заражения компьютера. Новые модификации вирусов, описания которых еще не включены в антивирусные базы, успешно преодолевают антивирусное программное обеспечение и могут быть использованы злоумышленниками для хищения денежных средств.
- Использовать возможности SMS-уведомления о входе в Систему и разовых SMS-паролей на вход в Систему, информирования по электронной почте о расходных операциях по Счету, дополнительной услуги SMS-информирования. Для дополнительного контроля рекомендуется подключить SMS-информирование лицу, не осуществляющему отправку платежей.
- Ограничить диапазон IP-адресов, с которых возможен вход в Систему.
- Не открывать письма электронной почты или сообщения интернет-мессенджеров (ICQ, Viber, WhatsUp, Facebook messenger и проч.) от неизвестных отправителей, сразу удалять их, не открывать вложенные файлы, не переходить по содержащимся в таких письмах ссылкам.
- На компьютере запретить выполнение службы удаленных рабочих столов.
- Все работы, связанные с поддержкой и обслуживанием компьютера, осуществлять под контролем лица, уполномоченного для работы в Системе.
- В случае непоступления одноразового пароля по SMS (на вход в Систему или подтверждение платежей) обратиться по тел. 8-800-250-3300. Если Банк не подтверждает проблем с доставкой SMS, рекомендуется сообщить о блокировке ключа в соответствии с Регламентом.

Будьте бдительны. Если к Вам обращаются с просьбой отправить платежный документ для того, чтобы «вернуть ошибочно перечисленные средства» – позвоните в Банк по известному Вам телефону (Вашему менеджеру) и подтвердите легитимность запроса.

Знайте, что Банк ни при каких обстоятельствах не будет отправлять программное обеспечение или какие-либо обновления посредством электронной почты.

Помните, что при работе со своими счетами в Системе следует быть настолько же внимательными и бдительными, как при обращении с наличными деньгами в Вашем кошельке!