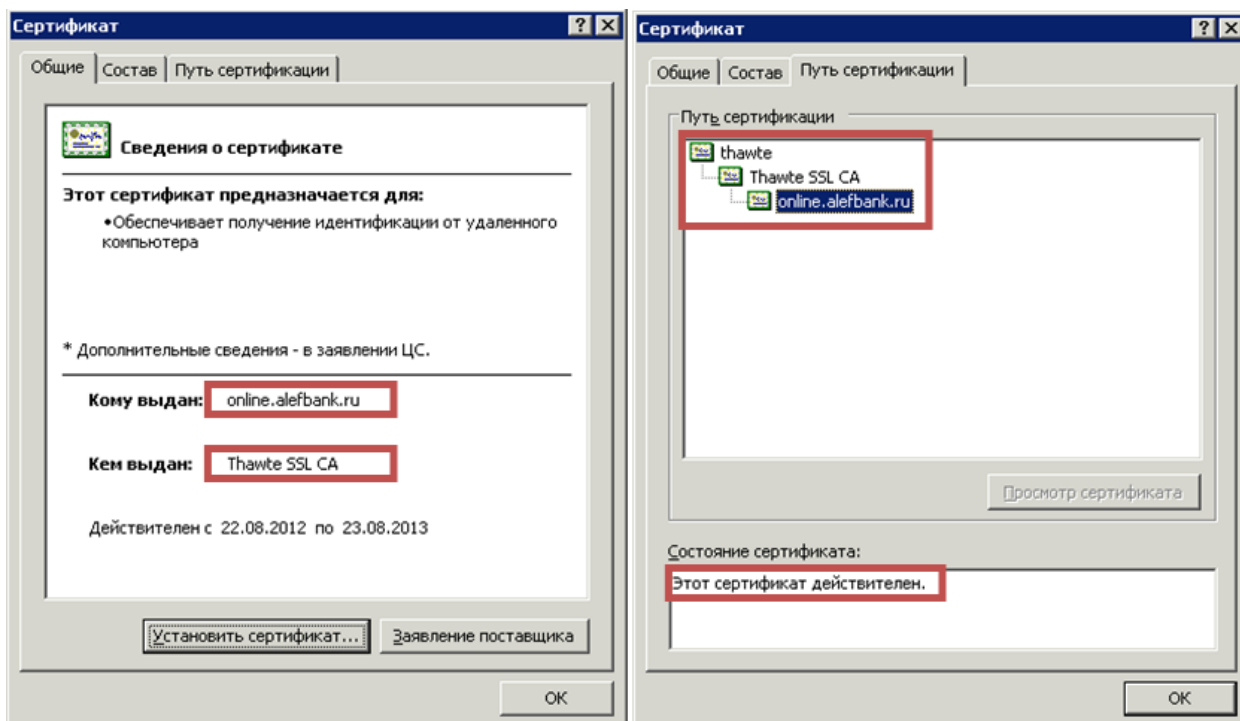


## РЕКОМЕНДАЦИИ КЛИЕНТАМ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПРИ РАБОТЕ С СИСТЕМОЙ «АЛЕФ-БАНК ONLINE» ЧЕРЕЗ ИНТЕРНЕТ

В целях снижения рисков неправомерного доступа и использования услуг дистанционного банковского обслуживания в результате похищения злоумышленниками идентификаторов, используемых для работы с Системой «Алеф-Банк Online», Клиентам рекомендуется соблюдать перечисленные ниже основные правила работы с Системой «Алеф-Банк Online», а также правила обращения с компьютером, который используется для работы в Системе «Алеф-Банк Online».

### Общие правила работы с Системой «Алеф-Банк Online»

1. Не вводите конфиденциальные данные, если окно для ввода отличается от стандартных окон Системы «Алеф-Банк Online» (логотип другого банка, другие надписи, шрифт и тому подобное).
2. При работе с Системой «Алеф-Банк Online» адрес сайта должен начинаться с <https://online.alefbank.ru>. Обращайте внимание на аббревиатуру **https** в начале адреса, которая свидетельствует о наличии защищенного соединения с использованием действительного сертификата. Убедитесь, что сертификат содержит все необходимые реквизиты, которые отображены на рисунке ниже.



3. Незамедлительно сообщайте в Банк о факте невозможности получения доступа к Системе «Алеф-Банк Online» по причине несовпадения пароля на вход в систему. Обычной практикой злоумышленников является смена пароля для

маскировки своих действий и получения дополнительного времени для успешного выполнения операций от имени Клиента.

4. Не храните пароль для входа в систему «Алеф-Банк Online» в файле на локальном диске, либо в любом другом легкодоступном месте.
5. Периодически меняйте пароль для входа в Систему «Алеф-Банк Online» (не реже одного раза в два месяца).
6. После завершения работы в Системе «Алеф-Банк Online» необходимо обязательно нажать кнопку «Выйти из системы» или закрыть окно браузера. Выходите из Системы «Алеф-Банк Online», даже если необходимо отойти на непродолжительное время.
7. По возможности не используйте компьютер, с которого осуществляется работа в Системе «Алеф-Банк Online», для развлечений и посещений сайтов сомнительного содержания.
8. Если заметите подозрительную активность на компьютере с запущенной Системой «Алеф-Банк Online» (самопроизвольные движения мышью, открытие/закрытие окон, набор текста) - немедленно выключите компьютер и сообщите в Банк о возможной попытке несанкционированного доступа к системе.
9. Соблюдайте осторожность при обращении с одноразовыми паролями Системы «Алеф-Банк Online». Одноразовые пароли необходимы для заверения в Системе «Алеф-Банк Online» от Вашего имени финансовых документов и передачи их на исполнение в Банк. Банк предлагает два способа получения одноразовых паролей: в виде SMS на номер мобильного телефона, указанного при оформлении договора и (или) в виде пароля, отображаемого на экране специализированного брелока eToken PASS.

***Внимание: В случае утраты (утери) брелока eToken PASS или номера мобильного телефона, указанного при оформлении договора и зарегистрированного для получения сеансовых ключей в виде SMS, немедленно сообщайте в Банк для их блокировки в Системе «Алеф-Банк Online»***

### **Общие правила работы с компьютером, который используется для работы в Системе «Алеф-Банк Online»**

1. Используйте в работе только лицензионные версии операционных систем и прикладного программного обеспечения.
2. Ежемесячно вручную (или в автоматическом режиме) устанавливайте обновления безопасности операционной системы.
3. Используйте и постоянно (ежедневно) обновляйте персональные средства защиты, такие как:

- a. Антивирусное программное обеспечение и другие средства выявления вредоносных программ (троянов);
  - b. Персональные межсетевые экраны (файрволы);
  - c. Средства защиты от несанкционированного доступа.
4. Не устанавливайте и не сохраняйте подозрительные файлы, полученные из ненадежных источников или скачанные с неизвестных web-сайтов.
  5. Обращайте особое внимание на отправителя почтовой корреспонденции при работе с электронной почтой.

***Внимание: Банк не осуществляет рассылку в адрес Клиентов электронных писем с просьбой ознакомиться с новыми услугами Банка или предоставить конфиденциальную информацию***