

Инструкция по проверке электронной подписи инсталляционного файла компонента системы КТБ-Онлайн и контролю его целостности

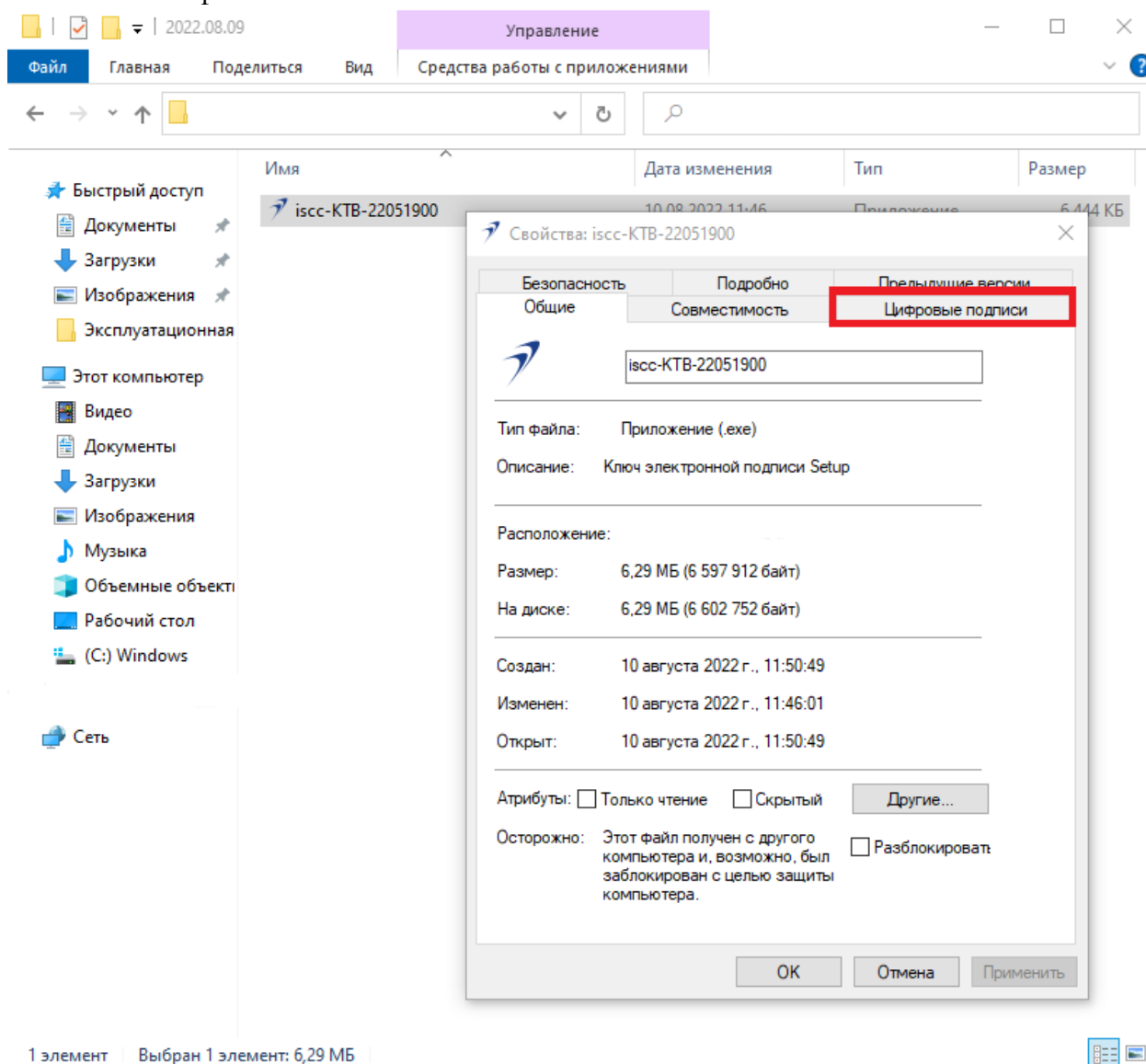
I. Проверка электронной подписи

В качестве дополнительной защиты от фишинга АО «Кубаньторгбанк» рекомендует проверить электронную подпись инсталляционного файла компонента системы КТБ-Онлайн (для Windows OS). Для проверки подлинности достаточно посмотреть на наличие электронной подписи у загруженного инсталляционного файла.

Порядок действий:

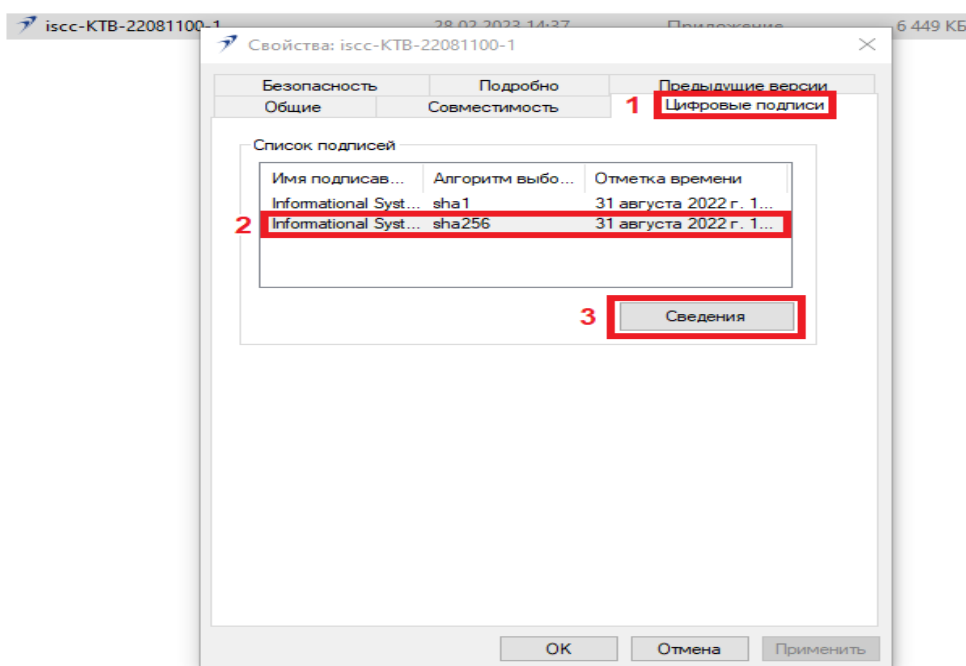
1. Скачайте инсталляционный файл компонента системы КТБ-Онлайн с официального сайта АО «Кубаньторгбанк»: <http://bktb.ru/%d0%b2%d1%85%d0%be%d0%b4>

2. Найдите загруженный установочный файл на вашем компьютере, далее щёлкните его правым щелчком мыши и выберете в меню пункт «Свойства». Откроется окно со свойствами файла.

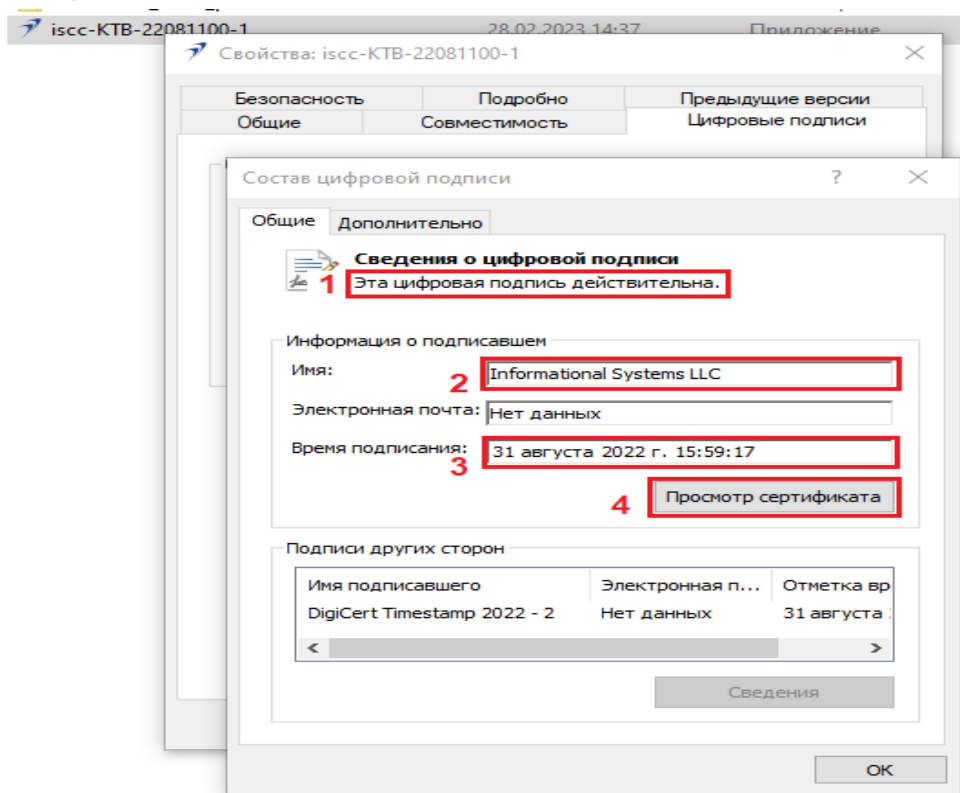


ВНИМАНИЕ!!! Если в окне «Свойства» нет вкладки «Цифровые подписи», то подпись нарушена. В таком случае устанавливать программу не рекомендуется.

3. Перейдите во вкладку «Цифровые подписи», далее в блоке «Список подписей» щёлкните «Informational Systems LLC» и нажмите кнопку «Сведения».

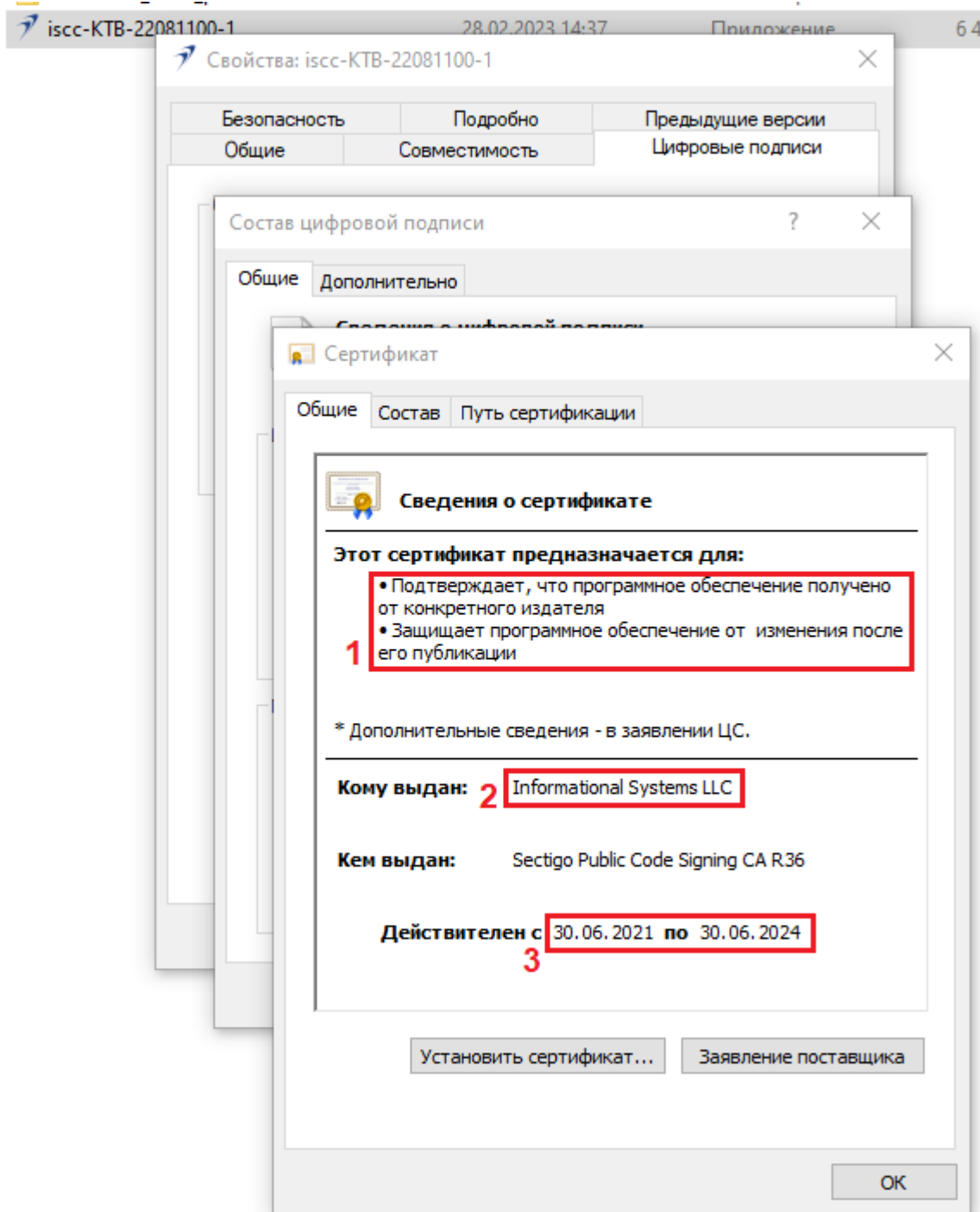


4. Откроется окно «Состав цифровой подписи». В этом окне на вкладке «Общие», убедитесь, что эта цифровая подпись действительна, имя подписавшего «Informational Systems LLC», указано время подписания и далее нажмите кнопку «Просмотр сертификата».



ВНИМАНИЕ!!! Если подпись недействительна, то содержимое программы было изменено после публикации злоумышленниками. В таком случае программу устанавливать не рекомендуется.

5. В сведениях о сертификате проверьте его предназначение, кому выдан, а также срок действия сертификата.



6. Сертификат электронной подписи разработчика программного обеспечения ООО «Информационные системы» (Informational Systems LLC), которым был подписан установочный файл, действителен определенное время с момента подписи. Срок действия сертификата может истечь, но при этом подпись будет считаться действительной, если она была установлена, когда сертификат ещё действовал.

7. Если проверка электронной подписи инсталляционного файла компонента системы КТБ-Онлайн завершена успешно, то можно приступить установке программы.

II. Контроль целостности

1. В качестве дополнительной защиты от фишинга АО «Кубаньторгбанк» рекомендует после получения файла компонента системы КТБ-Онлайн выполнить его проверку на целостность. Проверка осуществляется с помощью утилиты `cpverify.exe` (далее – Утилита).

2. Утилиту допускается использовать для вычисления Хэша¹ любого файла при использовании ГОСТ Р 34.11-2012, скачать ее можно на официальном сайте КриптоПро по адресу в Интернете: <https://www.cryptopro.ru/sites/default/files/public/cpverify/cpverify.exe>

3. Проверка целостности проходит путём выполнения процедуры контроля целостности файла средствами Утилиты и последующего визуального сравнения полученной контрольной суммы, с контрольной суммой Хэш-кода² рассчитанной по алгоритму вычисления хэш-функции в соответствии с ГОСТ Р 34.11-2012. Контрольная сумма Хэш-кода установочного файла компонента системы КТБ-Онлайн размещена на официальном сайте АО «Кубаньторгбанк» по адресу в Интернете: <http://bktb.ru/>

4. Порядок действий:

4.1. Скачайте Утилиту и поместите ее в папку с проверяемым файлом.

4.2. Запускать ее можно из командной строки `cmd`.

4.3. Для ГОСТ Р 34.11-2012 с длиной 256 бит: `cpverify.exe -mk -alg GR3411_2012_256 имя_файла`, где `имя_файла` – полный путь и название файла, например, `d:\iscc-КТВ-2023.exe`

4.4. Если в пути к файлу или в названии файла есть пробел – то всё имя нужно заключить в кавычки, например: `cpverify.exe -mk -alg GR3411_2012_256 "c:\Users\Folder 2023\iscc-КТВ-2023.exe"`

4.5. Если нужно значение хэша сохранить в файл, то в конце нужно добавить значок перенаправления и имя файла для записи значения Хэша, например: `cpverify.exe -mk -alg GR3411_2012_256 "c:\Users\Folder 2023\iscc-КТВ-2023.exe" > "c:\Users\Folder 2023\iscc-КТВ-2023.exe.hsh"`

5. Если проверка контроля целостности установочного файла компонента системы КТБ-Онлайн завершена успешно, то можно приступить к установке программы.

ВНИМАНИЕ!!! В случае отрицательного результата контроля целостности установочного файла компонента системы КТБ-Онлайн, устанавливать программу не рекомендуется.

¹ Хэш, Хэш-функция (англ. hash function от hash — «превращать в фарш», «мешанина»), или функция свёртки — функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом. Преобразование, производимое хэш-функцией, называется хешированием. Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования называется «хешем»,

² Примерный вид опубликованной контрольной суммы:

№	Алгоритм хэширования	Контрольная сумма файла
1	ГОСТ Р 34.11-2012 с длиной 256 бит	A6155D19CFC35213859040C66E34FEBDED36D1ECD633B2E9587850938FFE564D