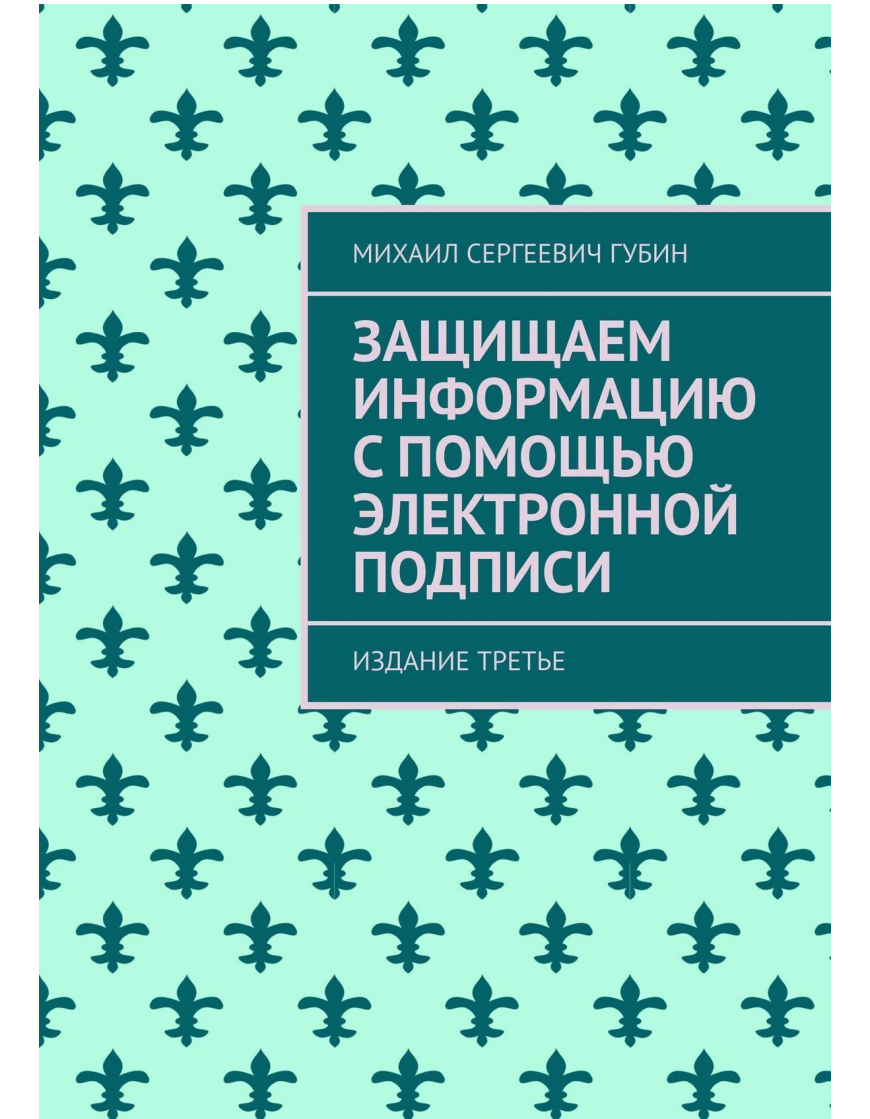




МИХАИЛ СЕРГЕЕВИЧ ГУБИН

ЗАЩИЩАЕМ ИНФОРМАЦИЮ С ПОМОЩЬЮ ЭЛЕКТРОННОЙ ПОДПИСИ

ИЗДАНИЕ ТРЕТЬЕ

Михаил Сергеевич Губин

Защищаем информацию с помощью электронной подписи. Издание третье

http://www.litres.ru/pages/biblio_book/?art=48780677

ISBN 9785005085146

Аннотация

В этой книге речь пойдет о средстве криптографической защиты (СКЗИ) КриптоПро CSP. Данное СКЗИ позволяет управлять практически всеми носителями электронных ключей (токенами), которые известны на сегодня. При этом нельзя путать токены с обычными флешками. Токены – это модули памяти, и в консоли «Компьютер» они не отобразятся, так как устроены на манер оперативной памяти, но сохраняют информацию постоянно.

Содержание

Глава 1. Программа КриптоПро и электронные подписи	5
Глава 2. Система ЕИС и авторизация на торговых порталах	7
Глава 3. ГОСТы электронных подписей	10
Глава 4. Цепочки сертификатов. Корневые удостоверяющие центры	14
Глава 5. Случаи мошенничества с электронной подписью	17
Глава 6. Как корректно переустановить КриптоПро	19
Глава 7. Электронный документооборот	24
Конец ознакомительного фрагмента.	25

Защищаем информацию с помощью электронной подписи Издание третье

Михаил Сергеевич Губин

© Михаил Сергеевич Губин, 2020

ISBN 978-5-0050-8514-6

Создано в интеллектуальной издательской системе Ridero

В этой книге речь пойдет о средстве криптографической защиты (СКЗИ) КриптоПро CSP. Данное СКЗИ позволяет управлять практически всеми носителями электронных ключей (токенами), которые известны на сегодня. При этом, нельзя путать токены с обычными флешками. Токены – это модули памяти, и в консоли «Компьютер» они не отобразятся, так как устроены на манер оперативной памяти, но сохраняют информацию постоянно. Перезаписать электронные ключи можно только с помощью программ КриптоПро CSP или VipNet CSP.

Глава 1. Программа КристоПро и электронные подписи

Электронная подпись, известная также как электронный ключ – это не монолитная структура. Она состоит из двух частей. Первая часть называется **контейнером**. Она представляет собой логическое пространство на накопителе или в памяти компьютера, содержащее в себе **сертификаты** – ваши электронные идентификаторы. Сертификаты, в свою очередь, хранятся логически в оснастке «Сертификаты пользователя», а физически – в реестре системы, а также в контейнерах электронного ключа.

Электронные ключи выпускаются специализированными организациями – удостоверяющими центрами (УЦ). В свою очередь, удостоверяющие центры проходят обязательную сертификацию ФСБ России. Можно привести в пример такие УЦ, как БТП, СКБ «Контур», ИжТендер, или ITCom. У каждого из удостоверяющих центров имеются свои особенности по выпуску электронных подписей. Например, БТП и ИжТендер позволяют выпускать электронные ключи без записи на физический носитель.

КристоПро CSP – не бесплатная программа. Ее стои-

мость определяет компания-разработчик. На тот момент, когда писалась эта книга, стоимость лицензии начиналась от 1000 рублей за рабочее место. К тому же, ключ можно приобрести как у удостоверяющего центра, так и у самой компании КriptoПро.

Самих электронных подписей существует несколько разновидностей.

– **Простая электронная подпись (ЭП)** является логином пользователя, либо его e-mail'ом. Она употребляется в случае, если необходимо заключить договор на сервисе как услуге. Такая подпись подтверждает акцепт документа, но не может выполнять иные функции.

– **Квалифицированная электронная подпись (КЭП)** применяется в сфере торгов, налоговой службе, ФАС, а также многих других отраслях. Она поставляется на защищенном носителе (токене) и является основной электронной подписью, применяемой во многих сферах.

– **Усиленная квалифицированная электронная подпись (УКЭП)** является модификацией КЭП, и является самой юридически значимой среди подписей. Она применяется, например, на государственном уровне.

Глава 2. Система ЕИС и авторизация на торговых порталах

ЕИС (Единая Информационная Система) – это часть глобальной машины по авторизации. Она базируется на портале gosuslugi.ru и помогает быстро распространить информацию о участнике торгов на электронных площадках. ЕИС имеет собственный адрес – портал zakupki.gov.ru. Система автоматически подгружает полную информацию о юридическом лице или индивидуальном предпринимателе из системы gosuslugi.ru, а также загружает выписку с портала nalog.ru о текущем состоянии юридического лица либо индивидуального предпринимателя. ЕИС имеет огромное значение, так как ранее, до ее введения, приходилось вручную регистрироваться на каждом торговом портале.

На настоящий момент имеется девять торговых площадок:

- Сбербанк АСТ.
- ЗаказРФ (или Общероссийская система электронной торговли ОСЭТ).
- Росэлторг (или Единая электронная торговая площадка ЕЭТП).

- Национальная электронная площадка (бывшая ММВБ-Госзакупки).
- РТС-Тендер.
- Российский аукционный дом (РАД).
- ТЭК-Торг.
- ЭТП ГПБ (Газпромбанк) – Секция «Государственные закупки».
- АСТ ГОЗ (для проведения закрытых торгов оборонного заказа).

Каждая из перечисленных торговых площадок по-своему уникальна, имеет собственные правила торгов, а также список участников закупок и заблокированных за какие-либо нарушения организаций и индивидуальных предпринимателей.

ЕИС действует на торговых порталах не сама по себе, а через площадку под названием ЕРУЗ (Единый Реестр Участников Закупок). ЕРУЗ выполняет роль простой электронной подписи, а также собирает и хранит в себе информацию об участниках закупок и поставщиках, поступившую из ЕИС.

С 1 января 2019 года регистрация в ЕРУЗ является обязательной для всех участников закупок, будь то физическое лицо, индивидуальный предприниматель либо юридическое лицо. Система ЕРУЗ также извещает участников закупок

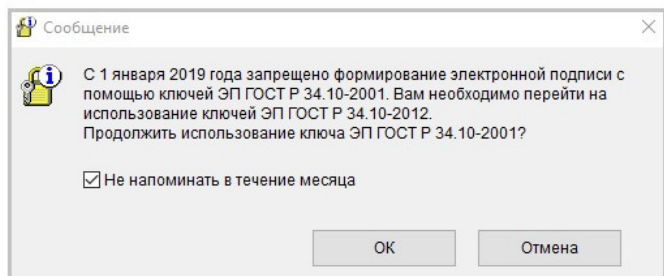
от входа по электронной подписи на физическом носителе, как как авторизация производится через портал gosuslugi.ru и информация берется из профиля организации на Госуслугах.

Глава 3. ГОСТы электронных подписей

ГОСТ (Государственный Стандарт) – это система норм, описывающая ту или иную электронную подпись в действии. В настоящее время на все без исключения электронные подписи действует ГОСТ Р 34.11 2012 (кратко ГОСТ 2012), введенный в действие приказом Федерального агентства по техническому регулированию и метрологии №215-ст от 7 августа 2012 года в качестве национального стандарта Российской Федерации с 1 января 2013 года.

Также работает ГОСТ 34.11—2018 (кратко ГОСТ 2018), являющийся межгосударственным и который был принят Межгосударственным советом по метрологии, стандартизации и сертификации (протокол №54 от 29 ноября 2018 года). Приказом Федерального агентства по техническому регулированию и метрологии №1059-ст от 4 декабря 2018 г. введен в действие в качестве национального стандарта Российской Федерации с 1 июня 2019 года. Электронные подписи любят давать сюрпризы пользователям. Не успеешь привыкнуть к одному ГОСТу, как на его смену приходит другой. Такой вот круговорот стандартов.

Ранее пользователи использовали устаревший ГОСТ Р 34.10—2001 (кратко ГОСТ 2001), принятый постановлением Госстандарта России №380-ст от 12 сентября 2001 года. Но время идет, требуются все более мощные способы защиты информации, и ГОСТ 2012 начал потихоньку вытеснять ГОСТ 2001 с персональных компьютеров пользователей. Фактически, ГОСТ 2001 уже запрещен, выпуск электронных подписей по нему не производится, а сам ГОСТ 2001 не работает с 1 января 2020 года. Пользователям, которые его использовали в 2019 году, выводилась вот такая табличка:



Действующий ГОСТ 2012 можно изобразить в виде небольшой блок-схемы.

Исходные данные:
(цифровая подпись ζ ,
полученное
сообщение M и ключ
проверки подписи Q)

Процесс проверки
подписи

Шаг 1 – вычисление r и s по полученной
подписи ζ

Нет
Подпись неверна

Да

$0 < r < q$
 $0 < s < q$

Шаг 2 – вычисление хэш-функции
полученного сообщения M

Шаг 3 – вычисление α и определение e

Шаг 4 – вычисление v

Шаг 5 – вычисление z_1 и z_2

Шаг 6 – вычисление точки эллиптической
кривой $C = z_1P + z_2Q$ и определение R

Нет
Подпись неверна

Да

$R =$

На самом деле, схема очень проста. Для проверки подписи необходимо прочесть контрольную сумму, сформированную ранее при процессе подписи документов электронной подписью. Такую подпись формирует, например, программа КриптоАРМ и сам плагин, через который браузеры работают с КриптоПро CSP.

Глава 4. Цепочки сертификатов.

Корневые удостоверяющие центры

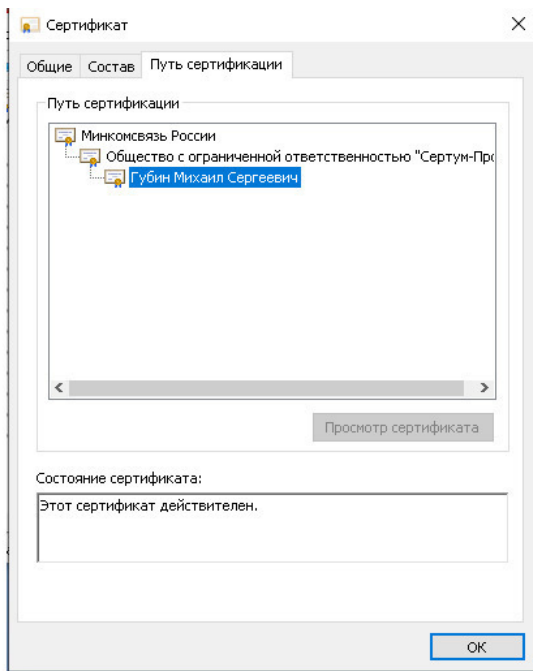
Цепочка сертификатов – это логический элемент, с помощью которого выявляется связь между удостоверяющим центром и конечным пользователем. Кроме того, цепочка сертификатов принимает непосредственное участие в процедуре отзыва сертификатов пользователей. Отзыв сертификата производится в том случае, если пользователь не оплатил электронную подпись, либо ее отозвал самостоятельно по какой либо причине.

Цепочку сертификатов можно установить самостоятельно, но рекомендуется это делать с помощью специализированной программы, которая имеется у каждого удостоверяющего центра. Эта программа автоматически устанавливает необходимую цепочку сертификатов, но есть и универсальные программы, позволяющие установить цепочки всех удостоверяющих центров сразу. Такая программа имеется, например, у удостоверяющего центра ИжТендер.

Также, цепочка сертификатов является самой важной в работе электронной подписи. Без нее не будет работать ни один сертификат электронной подписи, а значит, нельзя бу-

дет подписать никакие данные. Вот почему очень важно следить за корректностью цепочки сертификатов и устанавливать ее недостающие звенья.

Какие элементы имеет цепочка сертификатов? Давайте рассмотрим ее на примере цепочки из моей электронной подписи.



Как мы видим, цепочка сертификатов построена не абы

как. Самым верхним является сертификат Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь) России, поскольку именно Минкомсвязь вместе с ФСБ России разрешает всем без исключения удостоверяющим центрам вести свою деятельность. После сертификата Минкомсвязи идет сертификат текущего удостоверяющего центра – это общество с ограниченной ответственностью «Сертум-Про», входящее в состав компании СКБ «Контур». Самым последним в цепочке выступает мой сертификат. У вас цепочки сертификатов будут иметь похожую структуру, причем Минкомсвязь будет обязательным элементом, а удостоверяющий центр и название компании либо физического лица будут уже вашими.

Глава 5. Случаи мошенничества с электронной подписью

Не все удостоверяющие центры бывают честными. Случаются и такие инциденты, когда владелец электронной подписи лишается квартиры, бизнеса, имущества, на него «вешается» кредит, который он не брал, а также происходят иные незаконные манипуляции с персональными данными владельца подписи.

Так, один 37-летний москвич в 2018 году случайно узнал, что мошенники с помощью его личных данных и электронной подписи после попытки взлома портала Госуслуг. При этом мошенники не удалили его профиля, но скопировали паспортные и иные данные. В ходе разбирательства удалось установить, что вместе с мошенниками принимал участие в «деле» и работник удостоверяющего центра, где москвич заказывал электронную подпись.

Обезопаситься от такого вида мошенничества очень просто, так как достаточно подать в ведомство заявление о невозможности проведения сделок с принадлежащей им недвижимостью без их личного участия. После этого ни одна сделка с недвижимостью не сможет быть произведена без

вашего прямого участия.

Обезопаситься от кражи личных данных элементарно, достаточно не хранить их в открытом доступе, не загружать на подозрительные сайты, а также сменить стандартный PIN код электронной подписи на собственный – тогда базовая часть безопасности будет выполнена. Особенно тщательно необходимо относиться к паспортным и иным личным данным.

Глава 6. Как корректно переустановить КriptoПро

У всех бывают ситуации, когда программа не работает. В случае КriptoПро при некорректной работе (например, при блокировке параметров браузера Internet Explorer) помогает только переустановка. Некорректной работой мы тут не будем называть случаи, когда неверно выставлены, например, параметры протоколов SSL и TLS и в браузере, либо отключена возможность использовать старые комбинации шифров (Cipher Suite).

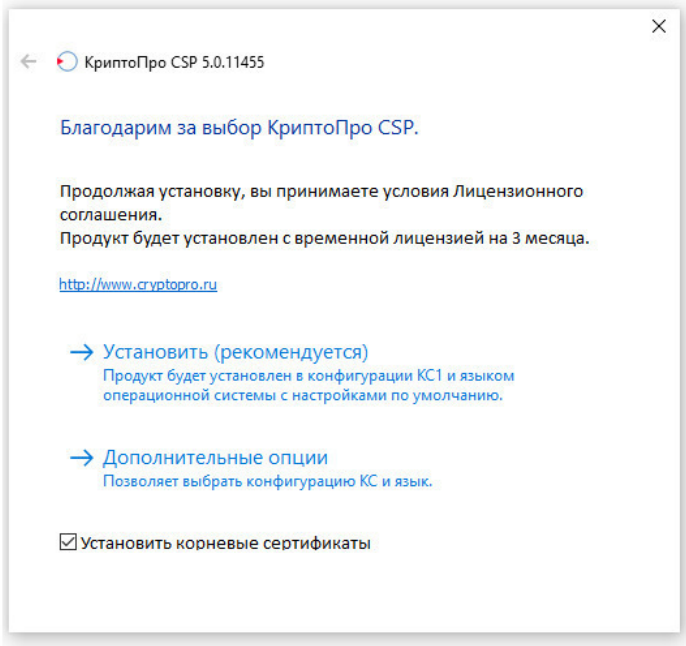
Нам потребуются следующие составляющие.

- Программа **cspclean.exe** для очистки конфигурации КriptoПро. Ее можно использовать для полного удаления КriptoПро из системы. Программа поможет и тогда, когда вы решили избавиться от КriptoПро полностью.
- Установочный файл КriptoПро CSP. Его можно скачать с официального сайта (cryptopro.ru). Я рекомендую КriptoПро версии не ниже 4.0 R5 или 5.0.
- Установочный файл КriptoПро Browser Plug-in. Его также можно скачать с официального сайта КriptoПро.
- Установочный файл плагина Госуслуг. Можно найти через поисковик Google или Yandex по словам «плагин госус-

луги».

Для службы подписи файлов ESEP (ЕСЭП – Единая Система Электронной Подписи) (используется, например, на mos.ru и подписи некоторых документах на портале Госуслуги) потребуется также плагин с сайта rul.mos.ru из раздела «Документы», называющийся prcruso_esep.exe – это криптографический компонент для подписи файлов.

Для начала установки нужно запустить файл CSPSetup.exe или CSPSetup-5.0-xxxx, где xxxx – версия скачанного КриптоПро. Важно знать, что для установки **обязательно** требуются права администратора. У вас появится вот такое окно, которое будет приглашать вас к установке.



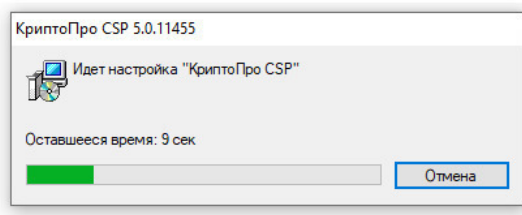
Окно приглашения одинаково для всех версий КриптоПро, вне зависимости от того, какую версию вы устанавливаете.

Нам нужно выбрать первый пункт, где написано «Установить (рекомендуется)».

При выборе пункта запусится установка КриптоПро. Устанавливаться программа будет с помощью сер-

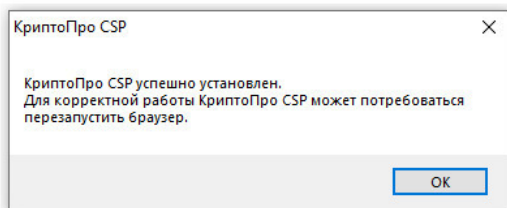
виса под названием Windows Installer, который включен по умолчанию во все версии Microsoft Windows, начиная с Windows NT.

Сам процесс установки выглядит вот таким образом.



Установка может продолжаться до 10 минут, в зависимости от быстродействия вашего компьютера. На современных компьютерах установка завершается за минуту или полторы.

По завершении установки КриптоПро вам будет выдан диалог подтверждения, показывающий, что КриптоПро успешно установлен в систему.



Установка плагина КриптоПро и плагина Госуслуг для браузеров совершается подобным образом. Единственный момент – в браузерах Google Chrome, Yandex, Спутник придется активировать расширения для плагинов КриптоПро и Госуслуг руками.

Глава 7. Электронный документооборот

Электронный документооборот (ЭДО) – это система обмена документами с помощью их подтверждения через электронную подпись. Он является юридически значимым действием – таким же, если бы вы сами обменивались бумажными документами с собственноручной подписью и печатью.

ЭДО совершается не сам по себе, а через специальных операторов. В качестве примера можно привести сервисы Синердокс и Диадок. Сама концепция обмена документами с помощью ЭДО проста как апельсин.

- Имеется два контрагента.
- Первый и второй контрагент регистрируются в сервисе обмена документами.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.