

Лабораторная работа № 9

Работа с криптопровайдерами

Цель работы. В данной работе предполагается ознакомление с некоторыми практическими аспектами применения инфраструктуры открытых ключей и инструмента электронной цифровой подписи (работа с сертификатами, подпись документов и защита почты) на примере тестовых удостоверяющих центров.

Для обеспечения крипtosистемы отечественными криптографическими алгоритмами предполагается установка и использование криптопровайдеров фирм КРИПТО-ПРО и Сигнал-КОМ.

Краткие теоретические сведения

Криптопровайдер (CSP – Cryptographic Service Provider) – это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft, управление которым происходит с помощью функций интерфейса Microsoft CryptoAPI.

Криптопровайдер должен экспортировать набор обязательных функций, которые формируют системный программный интерфейс CryptoAPI, а также обеспечивать:

- реализацию стандартного интерфейса криптопровайдера;
- работу с ключами шифрования, предназначенными для обеспечения работы алгоритмов, специфичных для данного криптопровайдера;
- невозможность вмешательства третьих лиц в схемы работы алгоритмов.

Одним из основных объектов, используемых криптопровайдером, является ключевой контейнер. В контейнере может существовать не более одной пары ключей подписи, одной пары ключей обмена и одного симметричного ключа. Если поддерживается несколько алгоритмов симметричного шифрования, то симметричных ключей может быть несколько, по одному ключу для каждого алгоритма.

Пары ключей и симметричные ключи могут находиться только в контейнере. Только открытый ключ пары может находиться вне контейнера.

Закрытые ключи пар ключей экспортируются только в зашифрованном виде. Некоторые криптопровайдеры принципиально не позволяют экспортить закрытые ключи, даже в зашифрованном виде. Симметричные ключи при экспорте также обязательно шифруются на открытом ключе получателя или ключе согласования.

В ОС Microsoft Windows существуют встроенные криптопровайдеры, однако они не поддерживают российских стандартов шифрования, хеширования и подписи, поэтому в данной работе будут использованы сертифицированные ФСБ России криптопровайдеры КриптоPro CSP и Сигнал-КОМ CSP, поддерживающие ГОСТ 28147-89, ГОСТ 34.11-94 и ГОСТ 34.10-2001, а также ГОСТ 34.10-2012 для шифрования, хеширования и цифровой подписи соответственно.

Инфраструктура открытых ключей (англ. PKI – Public Key Infrastructure) – реализация технологии управления механизмами доверия между субъектами информационной системы, основанная на использовании открытых ключей и сертификатов.

Задачи, решаемые инфраструктурой открытых ключей:

- установления доверия (в рамках заданной модели доверия);
- система именования субъектов, обеспечивающая уникальность имени в рамках системы;
- связь имени субъекта и пары ключей (открытый и закрытый) с подтверждением этой связи средствами удостоверяющего центра, которому доверяет субъект, проверяющий правильность связи.

Удостоверяющий центр – организация или подразделение, обеспечивающее взаимное доверие между участниками обмена электронными сообщениями, подписанными электронной цифровой подписью. Именно обеспечение доверия между сторонами является основной задачей удостоверяющего центра, в этом его задача близка к задаче службы нотариата. Только на основании доверия всех участников обмена к удостоверяющему центру строится механизм доверия сторон к электронным цифровым подписям и сведениям, указанным в сертификатах участников обмена.

Для реализации механизма взаимного доверия участников обмена удостоверяющий центр имеет центр сертификации, который:

- изготавливает сертификаты открытых ключей;
- создает ключи по обращению участников информационной системы с гарантией сохранения в тайне закрытого ключа;
- приостанавливает и возобновляет действие сертификатов открытых ключей, а также аннулирует их;
- ведет реестр сертификатов открытых ключей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- проверяет уникальность открытых ключей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- выдает сертификаты открытых ключей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- осуществляет по обращениям пользователей сертификатов открытых ключей подтверждение подлинности электронной подписи в электронном документе в отношении выданных им сертификатов открытых ключей;
- может предоставлять участникам информационных систем иные связанные с использованием электронных подписей услуги.

Сертификат открытого ключа – цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа.

Сертификат содержит в себе информацию о владельце сертификата, сведения об открытом ключе, его назначении и области применения, Удостоверяющем Центре, выдавшем сертификат, сроке действия сертификата и другие данные. Сертификат в электронном виде защищён электронной подписью Удостоверяющего Центра, выдавшего сертификат – это позволяет доверять сведениям, указанным в сертификате, ответственность за них берёт на себя Удостоверяющий Центр.

Сертификат играет роль визитной карточки владельца в информационной среде, а также несёт криптографическую нагрузку как хранилище открытого ключа.

Отдельно можно выделить сертификат корневого Удостоверяющего Центра. Такой

сертификат является самоподписаным – для него нет электронной подписи, позволяющей проверить достоверность сведений, указанных в сертификате. Доверие сертификату корневого Удостоверяющего Центра оказывается априори, подтвердить достоверность указанных в нём сведений некому.

Цепочка сертификатов – набор взаимосвязанных документов, который позволяет удостовериться, что предъявленный сертификат был выдан доверенным удостоверяющим центром. Последним звеном в этой цепочке является предъявленный сертификат, начальным – сертификат корневого доверенного центра сертификации, а промежуточными – сертификаты промежуточных центров сертификации. Особенностью пути доверия является то, что при потере доверия к начальному звену цепочки (корневому центру сертификации) теряется доверие ко всей цепочке, то есть ко всем выданным данным центром сертификатам и к предъявленному в том числе.

Список отзываемых сертификатов (СОС) – особым образом оформленный перечень идентификаторов сертификатов открытых ключей, признанных удостоверяющим центром недействительными по разным причинам. Опубликовывается удостоверяющим центром, доставляется пользователю (например, в виде файла с расширением .crl) и размещается в операционной системе. СОС является частью инфраструктуры открытых ключей и позволяет пользователю не допустить ошибочного доверия к какому-либо сертификату открытого ключа, если удостоверяющий центр в доверии сертификату отказал.

Электронная подпись

Электронная цифровая подпись используется для аутентификации текстов, передаваемых по телекоммуникационным каналам. При таком обмене существенно снижаются затраты на обработку и хранение документов, убыстряется их поиск. Но возникает проблема аутентификации автора электронного документа и самого документа, т. е. установления подлинности автора и отсутствия изменений в полученном электронном документе. Целью аутентификации электронных документов является их защита от возможных видов злоумышленных действий, к которым относятся:

- **активный перехват** – нарушитель, подключившийся к сети, перехватывает документы (файлы) и изменяет их;
- **маскарад** – абонент С посыпает документ абоненту В от имени абонента А;
- **ренегатство** – абонент А заявляет, что не посыпал сообщения абоненту В, хотя на самом деле послал;
- **подмена** – абонент В изменяет или формирует новый документ и заявляет, что получил его от абонента А;
- **повтор** – абонент С повторяет ранее переданный документ, который абонент А посыпал абоненту В.

Эти виды злоумышленных действий могут нанести существенный ущерб банковским и коммерческим структурам, государственным предприятиям и организациям, частным лицам, применяющим в своей деятельности компьютерные ИТ.

Проблему проверки целостности сообщения и подлинности автора сообщения позволяет эффективно решить методология электронной цифровой подписи.

Электронная подпись может применяться в разных областях:

- в качестве аналога собственноручной подписи и/или печати на бумажном документе. В частности, в этой ипостаси электронная подпись используется в системах электронного документооборота разного назначения;
- для подписи программ или отдельных модулей, чтобы пользователь компьютера, загружая эти программы из Интернета, и используя их в работе, мог быть убежден в надежности и корректности их работы и надежности источника получения этих программ;
- установка авторства, так и подтверждение целостности любых данных в электронном виде. Например, полученное вами от, казалось бы, знакомого человека, письмо без электронной подписи может оказаться на самом деле поддельным или содержать искаженную после его отправления информацию. Использование электронной подписи такую возможность исключает. При проверке электронной подписи будет установлено, что документ был изменен после его подписания;
- при ведении деловой переписки канцеляриями или секретарями разных компаний электронная подпись может служить в качестве «конверта» - на одном конце письмо запечатывают с помощью электронной подписи, а на финише получатель «вскрывает» конверт, предварительно убедившись в полной неприкосновенности и подлинности данных;
- с помощью электронной подписи можно согласовывать электронные варианты документов (например, договоров) как между различными службами внутри одной организации, так и между разными организациями. В таком случае текст договора будет защищен от несогласованных изменений, а каждая ответственная инстанция должна будет согласовать документ с помощью собственной электронной подписи.

Разновидности электронной подписи

Существуют различные виды электронной подписи.

Электронная подпись может быть присоединена к подписываемым данным, отсоединена от них или находиться внутри данных. Наиболее часто применяют электронные подписи к данным, хранящимся в файлах, а сама подпись относится ко всему содержимому файла.

Присоединенная электронная подпись

В случае создания присоединенной подписи создается новый файл электронной подписи, в который помещаются данные подписываемого файла. Этот процесс аналогичен помещению документа в конверт и его опечатыванию. Перед извлечением документа следует убедиться в сохранности печати (для электронной подписи ее правильности). К достоинствам присоединенной подписи следует отнести простоту дальнейшего манипулирования с подписанными данными, т.к. все они вместе с подписями содержатся в одном файле. Этот файл можно копировать, пересыпать и т.п. К недостаткам следует отнести то, что без использования средств СКЗИ уже нельзя прочесть и использовать содержимое файла, точно так же, как нельзя извлечь содержимое конверта, не расклейв его.

Отсоединенная электронная подпись

При создании отсоединенной подписи файл подписи создается отдельно от подписываемого файла, а сам подписываемый файл никак не изменяется. Достоинством отсоединенной подписи является то, что подписанный файл можно читать, не прибегая

к СКЗИ. Только для проверки подписи нужно будет использовать и файл с электронной подписью, и подписанный ей файл. Недостаток отсоединенной подписи - необходимость хранения подписанной информации в виде нескольких файлов (подписанного файла и одного или нескольких файлов с подписями). Последнее обстоятельство существенно осложняет применение подписи, так как при любых манипуляциях с подписанными данными требуется копировать и передавать несколько независимых файлов.

Электронная подпись внутри данных

Применение электронной подписи этого вида существенно зависит от приложения, которое их использует, например электронная подпись внутри документа Microsoft Word или Acrobat Reader. Вне приложения, создавшего электронную подпись, без знания структуры его данных проверить подлинность частей данных, подписанных электронной подписью затруднительно.

Ход работы

Загрузка дистрибутивов криптопровайдеров

Загрузка КриптоПро CSP

Зайдите на сайт компании-разработчика данного продукта КРИПТО-ПРО (www.cryptopro.ru). На главной странице (см. рисунок 1) можно ознакомиться как с самой компанией, так и с ее продуктами и услугами.

The screenshot shows the main page of the Cryptopro.ru website. At the top, there's a navigation bar with links for RU | EN, a search bar, and a 'Поиск' button. Below the header, there's a large logo for 'КРИПТОПРО' with the tagline 'КЛЮЧЕВОЕ СЛОВО в защите информации'. The main content area has several sections: 'Клиентам', 'Правовая информация', and 'Разработчикам'. A prominent section for 'КриптоПро CSP' is shown, mentioning it's software for electronic signatures according to the Federal Law No. 63-FZ. It features download links ('Скачать'), purchase links ('Купить лицензию'), and a 'Техподдержка' button. To the right, there's a section for 'КриптоПро для работы с электронной подписью' with a 'Подробнее...' button and an icon of a document with a seal. Further down, there's a 'Новости КриптоПро' section, a 'Итоги 2024 года' section with a publication date of 20 January 2025 at 16:27, and a 'Авторизоваться' section with links for 'Вход', 'Регистрация', and 'Забыли пароль?'. At the bottom, there are social media links for VKontakte and YouTube, and a 'Подписка' section.

Рисунок 1 – Главная страница сайта КРИПТО-ПРО.

Для загрузки дистрибутива, прежде всего, необходима регистрация на сайте, для чего нажмите на соответствующую ссылку. Появится окно регистрации (см. рисунок 2), где Вам необходимо заполнить обязательные поля и нажать на кнопку **Регистрация**. На

указанный Вами во время регистрации почтовый адрес должно прийти письмо для подтверждения регистрации. После этого на сайте можно авторизоваться.

Профиль пользователя

Вход Регистрация Забыли пароль?

Информация об учетной записи

E-mail: *

Актуальный адрес электронной почты. Все почтовые сообщения с сайта и Портала технической поддержки будут приходить на указанный адрес, также он может быть использован для восстановления пароля.

Пароль / Password: *

Повторите пароль / Confirm password: *

Укажите пароль для новой учетной записи в обоих полях.

Личная информация

Имя / Firstname: *

Содержание этого поля является приватным и не предназначено к показу.

Фамилия / Lastname: *

Содержание этого поля является приватным и не предназначено к показу.

Контактный номер телефона / Phone number:

Содержание этого поля является приватным и не предназначено к показу.

Название компании:

Содержание этого поля является приватным и не предназначено к показу.

Правила использования

Соглашаюсь с обработкой своих персональных данных ООО «КРИПТО-ПРО» в электронной форме. [Политика в отношении обработки персональных данных пользователей сайта ООО «КРИПТО-ПРО»](#) *

Я не робот

Нажмите, чтобы продолжить

SmartCaptcha by Yandex Cloud

Регистрация

Продукты компании, обновления и доп. ПО

Услуги технического сопровождения

Информационно-консультационные услуги

Подписка

vkontakte RUTUBE

Новости КриптоПро

Рисунок 2 – Форма регистрации.

Теперь можно приступить к загрузке. Из главной страницы сайта перейдите на вкладку **Продукты → КриптоПро CSP → Загрузка файлов**. Вам будет предложено прочесть лицензионное соглашение (см. рисунок 3-4). Примите его условия нажав на ссылку **Я согласен с Лицензионным соглашением. Перейти к загрузке**, и появится окно со ссылками для загрузки различных версий.

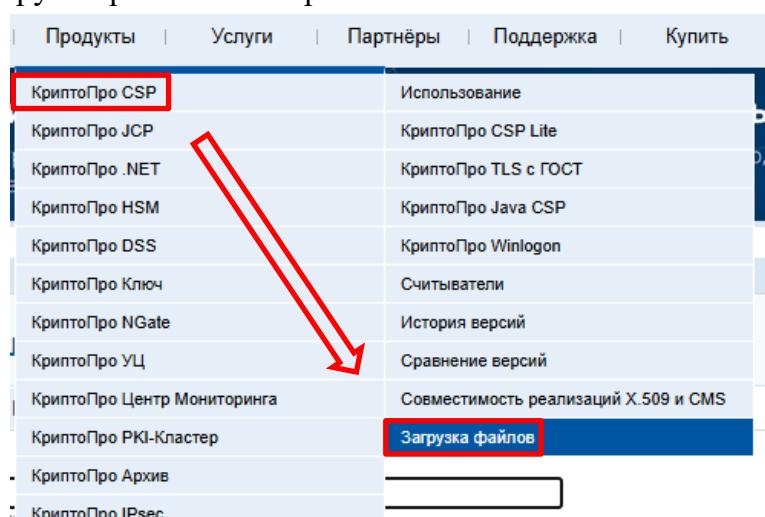


Рисунок 3 – Загрузка КРИПТО-ПРО.



Лицензионное соглашение

[Главная](#)

КриптоПро CSP

Срок использования демонстрационной версии КриптоПро CSP ограничен 90 днями с момента установки.

Передача прав на использование программного обеспечения производства ООО "КРИПТО-ПРО" осуществляется на основании Лицензионного соглашения.

Лицензии на использование продукта необходимо приобретать в ООО "КРИПТО-ПРО" или у официального дилера.

Предупреждение.

Для штатной эксплуатации средств криптографической защиты информации (СКЗИ) они должны быть установлены с дистрибутива.

Дистрибутив может быть:

1. Приобретен у производителя или у официального дилера производителя на материальном носителе.
2. Получен с сайта производителя или официального дилера.

Рисунок 4 – Лицензионное соглашение.

Прокрутите вниз до ссылки **КриптоПро CSP 5.0 R3 для Windows (x86/x64)** (новейшая сертифицированная версия на момент написания) и кликните по ней. Загрузка должна начаться автоматически, если нет, то выберите место куда будет сохранен установщик. Рекомендуется создать папку **КриптоПро** на Рабочем столе и в нее сохранять все файлы.

Инсталляция СКЗИ КриптоПро CSP

Для установки программного обеспечения запустите на выполнение файл установки **CSPSetup-5.0.13000.exe**, расположенный в папке **КриптоПро** на Рабочем столе. В появившемся окне (см. рисунок 5-б) нажмите **Дополнительные опции** для выбора языка установки, а также есть возможность выбрать уровень защищенности (по умолчанию выбран КС1, который нам подходит, т.к. в работе не используются аппаратные датчики случайных чисел, аутентификаторы и ключевые носители).

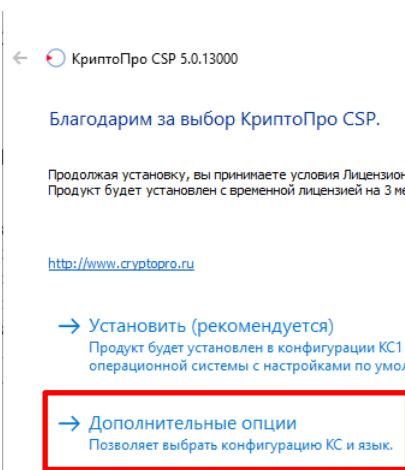


Рисунок 5 – Стартовое окно установки.

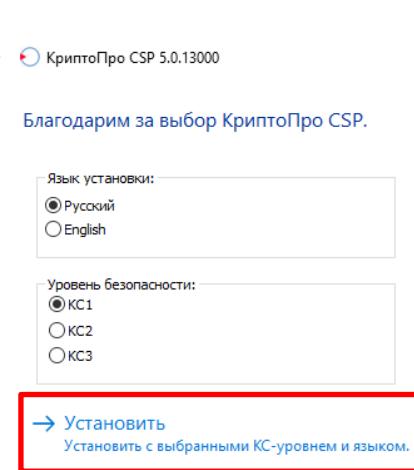


Рисунок 6 – Окно выбора языка и уровня безопасности.

Нажмите **Установить**, после чего следуйте инструкциям мастера установки. При установке не нужно вводить лицензионный ключ (см. рисунок 7), т.к. пробная версия не имеет функциональных ограничений, вид установки – **Обычная** (в работе достаточно стандартных компонентов). (см. рисунок 8).

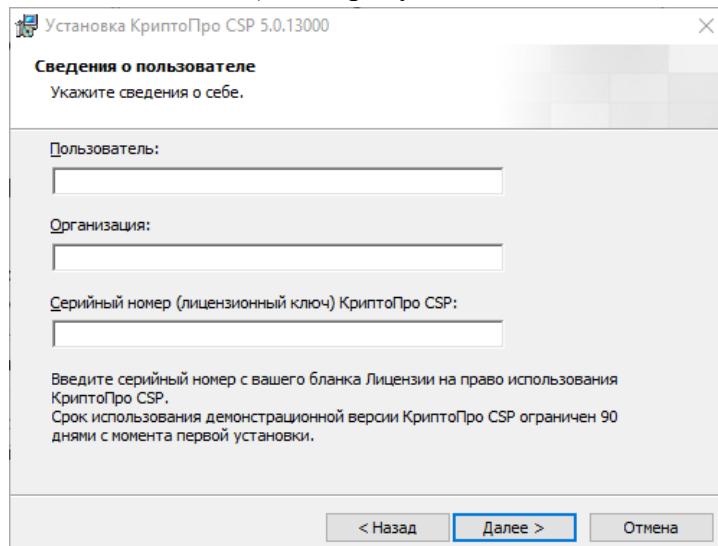


Рисунок 7 – Окно ввода лицензионного ключа.

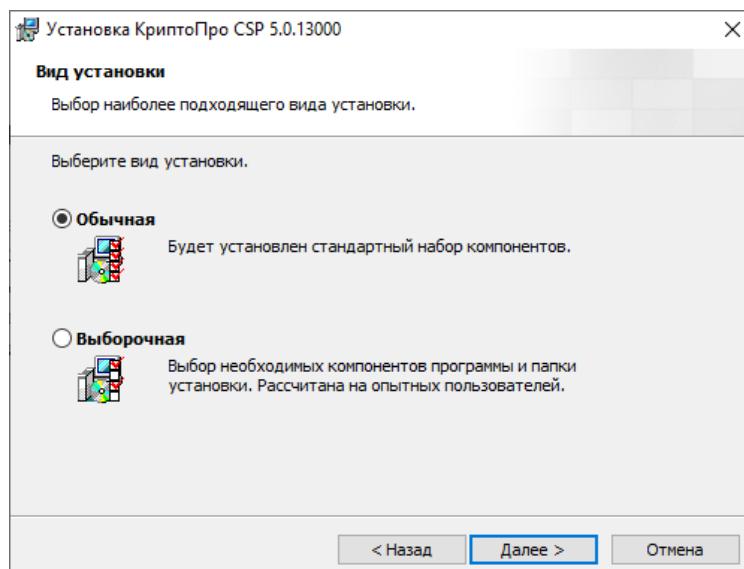


Рисунок 8 – Окно выбора установки.

Криптопровайдер КриптоPro успешно установлен.

Запрос и установка сертификата КриптоПро CSP

Внесите в адресную строку браузера Microsoft Edge (или любого другого браузера) адрес сайта тестового УЦ компании КРИПТО-ПРО: <https://www.cryptopro.ru/certsrv> (см. рисунок 9).

The screenshot shows the homepage of the Cryptopro Test Certification Center. At the top, there is a logo for 'КРИПТОПРО' and a link to the English version. The main heading is 'Тестовый Удостоверяющий Центр ОOO "КРИПТО-ПРО"'. Below it, a welcome message reads 'Добро пожаловать на сайт тестового Удостоверяющего Центра ОOO "КРИПТО-ПРО"'. A list of requirements follows:

- Вы можете использовать тестовый центр сертификации для того, чтобы получить сертификат ключа проверки электронной подписи (сертификат открытого ключа).
- Для получения сертификата вы должны будете сформировать закрытый и открытый ключи и ввести данные, которые используются для связывания открытого ключа и владельца сертификата.

A section titled 'Требования' (Requirements) contains the following text:

- Для проверки подписи тестового центра сертификации необходим криптопровайдер с поддержкой алгоритмов ГОСТ - КриптоПро CSP или аналогичный. Криптопровайдер можно загрузить [здесь](#).
- Центр реализован на основе службы сертификации, входящей в состав операционной системы Microsoft Windows Server 2012 R2.
- Если вы используете веб-браузер, отличный от Microsoft Internet Explorer, то для получения сертификата нужно дополнительно установить [КриптоПро ЭЦП Browser plug-in](#).

Below the requirements, there is a yellow box containing three informational messages:

- Центр предназначен только для целей **тестирования** и не должен использоваться для других целей.
- Центр не проверяет информацию, указанную в запросах на сертификат. Не следует доверять сертификатам, выданным тестовым Удостоверяющим Центром.
- Узнать об услугах действующего Удостоверяющего Центра ОOO "КРИПТО-ПРО" можно [здесь](#).

A section titled 'Получить сертификат' (Get Certificate) contains the text: 'Выберите нужное действие:' (Select the required action) followed by a list of actions:

- Сформировать ключи и отправить запрос на сертификат
- Отправить готовый запрос PKCS#10 или PKCS#7 в кодировке Base64
- Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов

Рисунок 9 – Сайт тестового УЦ.

Если вы используете веб-браузер, отличный от Microsoft Internet Explorer, то для получения сертификата нужно дополнительно установить **КриптоПро ЭЦП Browser plug-in**. Найдите на странице советующую ссылку и нажмите на нее. В окне КриптоПро ЭЦП Browser plug-in нажмите скачать **Сертифицированный** криптопровайдер и плагин. Сохраните установщик в папке **КриптоПро**. (см. рисунок 10).

Требования

- Для проверки подписи тестового центра сертификации необходим криптопровайдер с поддержкой алгоритмов ГОСТ - КриптоПро CSP или аналогичный. Криптопровайдер можно загрузить [здесь](#).
- Центр реализован на основе службы сертификации, входящей в состав операционной системы Microsoft Windows Server 2012 R2.
- Если вы используете веб-браузер, отличный от Microsoft Internet Explorer, то для получения сертификата нужно дополнительно установить [КриптоПро ЭЦП Browser plug-in](#).

Рисунок 10 – Ссылка на скачивание КриптоПро ЭЦП Browser plug in.

Для установки программного обеспечения запустите на выполнение файл установки **CryptoPro-5.0.13000.exe**, расположенный в папке **КриптоПро** на Рабочем столе, после чего после чего следуйте инструкциям мастера установки. Установщик в конце попросит перезагрузить компьютер для применения изменений. Перезагружаемся. (см. рисунок 11).

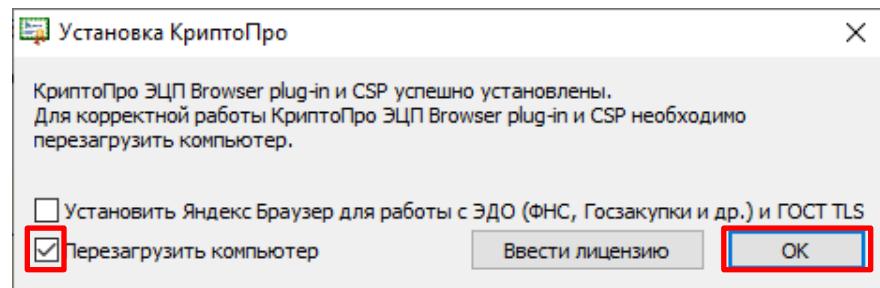


Рисунок 11 – Успешная установка КриптоПро ЭЦП Browser plug in.

После перезагрузки необходимо открыть браузер и в настройках браузера найти пункт **Расширения** и проверить чтобы расширение от КриптоПро было **включено**. (см. рисунок 12).

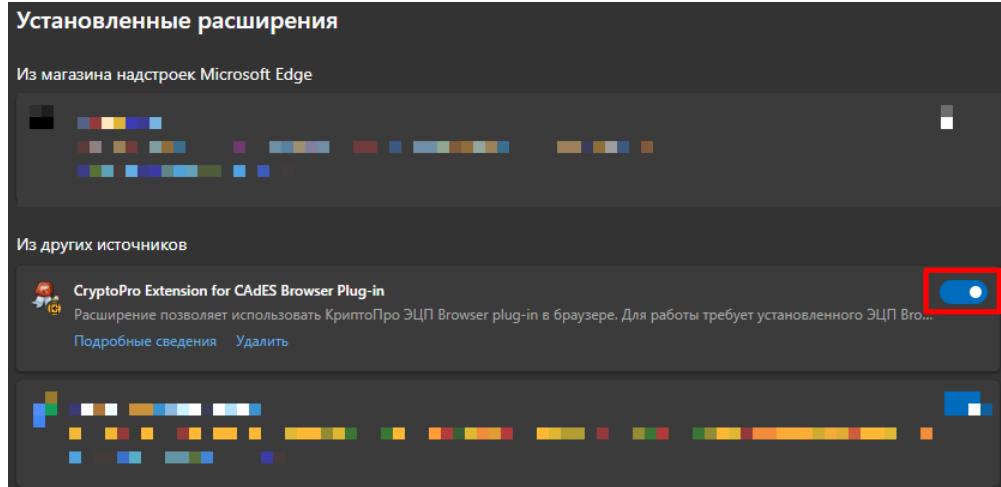


Рисунок 12 – Проверка включенного расширения.

Перед заказом личного сертификата необходимо установить сертификат самого УЦ. Выберите пункт **Получить сертификат Удостоверяющего Центра или действующий список отозванных сертификатов** и нажмите **Загрузка сертификата ЦС**. Метод шифрования выберите **DER**. (см. рисунок 13). Сохраните скачанный сертификат в папке **КриптоПро**.

The screenshot shows the 'Службы сертификации Active Directory (Microsoft) – CRYPTO-PRO Test Center 2' interface. At the top, there is a green bar with the title and a 'Home' link. Below it, a section titled 'Загрузка сертификата ЦС, цепочки сертификатов или CRL' (Load certificate CS, certificate chains or CRL) is shown. A note says: 'Чтобы доверять сертификатам, выданным этим центром сертификации, установите эту цепочку сертификатов ЦС.' (To trust certificates issued by this certification center, install this certificate chain). Another note says: 'Чтобы загрузить сертификат ЦС, цепочку сертификатов или список отзыва сертификатов (CRL), выберите этот сертификат и метод шифрования.' (To load a certificate CS, certificate chain or certificate revocation list (CRL), select this certificate and encryption method). A dropdown menu for 'Сертификат ЦС:' (Certificate CS:) shows 'Текущий [CRYPTO-PRO Test Center 2(2)]'. Below it, a 'Метод шифрования:' (Encryption method:) dropdown has 'DER' selected, indicated by a red arrow. At the bottom, there is a 'Загрузка сертификата ЦС' (Load certificate CS) button, and below it, options for 'Base 64' and 'Загрузка цепочки сертификатов ЦС' (Load certificate chain CS).

Рисунок 13 – Загрузка сертификата ЦС.

В папке **КриптоПро** нажмите на файл **certnew.cer** двойным щелчком мыши и нажмите Открыть. (см. рисунок 14).



Вы хотите открыть этот файл?



Имя: C:\Users\Downloads\certnew (1).cer

Издатель: Неизвестный издатель

Тип: Сертификат безопасности

Из: C:\Users\Downloads\certnew (1).cer

 Всегда спрашивать при открытии этого файла

Файлы из Интернета могут быть полезны, но этот тип файла может повредить компьютер. Если вы не доверяете источнику, не открывайте этот файл. [Факторы риска](#)

Рисунок 14 – Окно с предупреждением системы безопасности.

После окончания загрузки будет показано окно свойств сертификата (см. рисунок 15). Можете подробно ознакомиться со всеми свойствами сертификата на вкладке **Состав**. Нажмите на кнопку **Установить сертификат**. В появившемся окне нажмите **Далее**. Затем необходимо выбрать место хранения сертификата в хранилище. Выберите **Доверенные корневые центры сертификации** (см. рисунок 16) и нажмите **Далее**. Далее необходимо подтвердить, что Вы доверяете данному ЦС (см. рисунок 17). Сертификат центра установлен. Теперь система доверяет всем сертификатам, выданным данным ЦС.

The screenshot shows two windows side-by-side. On the left is the 'Сертификат' (Certificate) properties dialog box. It has tabs for 'Общие' (General), 'Состав' (Details), and 'Путь сертификации' (Certification Path). The 'Состав' tab is selected, showing details like 'Этот сертификат предназначен для:' (This certificate is intended for: All issuance policies, All application policies), 'Кому выдан:' (Issued to: CRYPTO-PRO Test Center 2), 'Кем выдан:' (Issued by: CRYPTO-PRO Test Center 2), and 'Действителен с 14.05.2024 по 14.05.2025' (Valid from 14.05.2024 to 14.05.2025). A red box highlights the 'Установить сертификат...' (Install certificate...) button at the bottom-left. Another red box highlights the 'OK' button at the bottom-right.

On the right is the 'Мастер импорта сертификатов' (Import Certificate Wizard) dialog box. It has tabs for 'Хранилище сертификатов' (Certificate store) and 'Хранилище сертификатов' (Certificate store). The second tab is selected, showing options for where to store the certificate. It includes radio buttons for 'Автоматически выбрать хранилище на основе типа сертификата' (Automatically choose the store based on certificate type) and 'Поместить все сертификаты в следующее хранилище' (Place all certificates in the following store). A red arrow points to the second option. A red box highlights the 'Доверенные корневые центры сертификации' (Trusted Root Certificate Authorities) button in the 'Хранилище сертификатов' section. Another red box highlights the 'Обзор...' (Browse...) button next to it. At the bottom are 'Далее' (Next) and 'Отмена' (Cancel) buttons.

Рисунок 15 – Свойство сертификата УЦ.

Рисунок 16 – Указание места хранения сертификата.

Предупреждение системы безопасности

×



Будет установлен сертификат от центра сертификации (ЦС), представляющий:

CRYPTO-PRO Test Center 2

Windows не удастся проверить, что сертификат действительно получен от "CRYPTO-PRO Test Center 2".
Обратитесь к "CRYPTO-PRO Test Center 2" для подтверждения происхождения сертификата. В ходе этого процесса вам пригодится следующее значение:

Отпечаток (sha1) : 17D4ABC6 EA4BA263 D7D75AE2 757C5A10
B9F9B0FA

Предупреждение:

Если вы установите этот корневой сертификат, Windows будет автоматически доверять любому сертификату, выданному этим ЦС. Установка сертификата с неподтвержденным отпечатком представляет риск для безопасности. Если вы нажмете кнопку "Да", вы принимаете на себя этот риск.

Вы хотите установить этот сертификат?

Да

Нет

Рисунок 17 – Подтверждение доверенного статуса центра.

Теперь можно загрузить и установить личный сертификат. Для этого вернитесь на главную страницу УЦ (см. рисунок 9), выберите **Сформировать ключи и отправить запрос на сертификат**. На запрос разрешения (см. рисунок 18) ответьте Да. Загрузится страница расширенного запроса (см. рисунок 19). Заполните поля **Имя** и **Электронная почта**. Обратите внимание, что для дальнейшей работы нужно указать действующий почтовый ящик, который вы указывали при регистрации. (см. рисунок 2). В поле **Страна, регион** напишите **RU**. В поле **Тип требуемого сертификата** выберите **Сертификат защиты электронной почты**. В поле **SCP** выберете **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**. В поле **Размер ключа** укажите **512**. В поле **Алгоритм хеширования** выберите **ГОСТ Р 34.11-2012 256 бит** и нажмите **Выдать**.

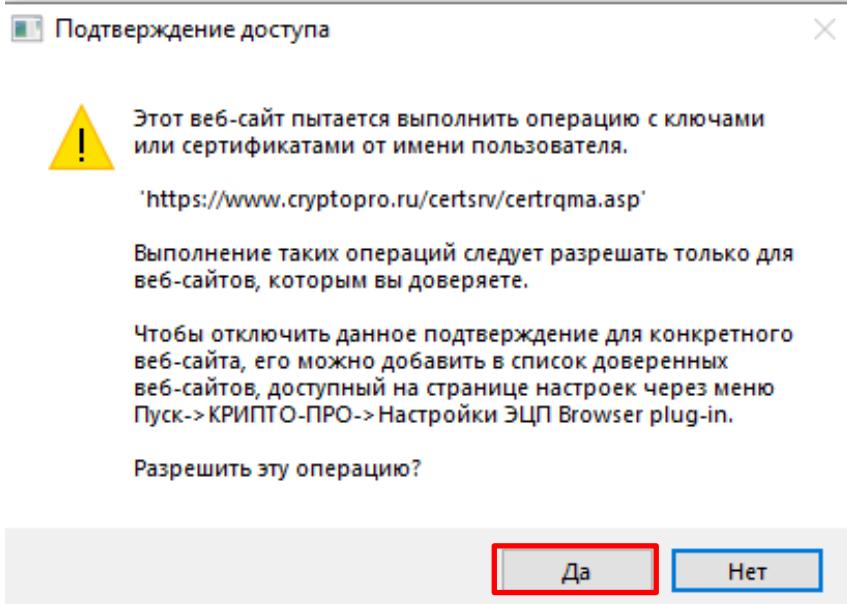


Рисунок 18 – Запрос на разрешение.

Расширенный запрос сертификата**Идентифицирующие сведения:**

Имя:	<input type="text"/>
Электронная почта:	<input type="text"/>
Организация:	<input type="text"/>
Подразделение:	<input type="text"/>
Город:	<input type="text"/>
Область, штат:	<input type="text"/>
Страна, регион:	<input type="text"/>

Тип требуемого сертификата:

Параметры ключа:

Создать новый набор ключей Использовать существующий набор ключей

CSP:

Использование ключей: Ключ подписи и обмена Ключ подписи

Размер ключа: Минимальный:512 Максимальный:512 (стандартные размеры ключей: [512](#))

Автоматическое имя контейнера ключа Заданное пользователем имя контейнера ключа

Пометить ключ как экспортируемый

Использовать локальное хранилище компьютера для сертификата
 Сохраняет сертификат в локальном хранилище
 вместо пользовательского хранилища сертификатов.
 Не устанавливает корневой сертификат ЦС.
 Необходимо быть администратором, чтобы создать
 локальное хранилище.

Дополнительные параметры:

Формат запроса: CMC PKCS10

Алгоритм хэширования:

Используется только для подписания запроса.

Сохранить запрос

Атрибуты:

Понятное имя:

Выдать >

Рисунок 19 – Страница расширенного запроса сертификата.

Сначала появится окно выбором носителя для создания контейнера. В учебно-лабораторных целях сохраните его в директории, далее появится окно инициализации ДСЧ (см. рисунок 20). Нажимайте клавиши и двигайте мышью, пока не заполнится полоса прогресса. Затем потребуется задать пароль на доступ к ключевому контейнеру (см. рисунок 21). Задайте пароль, подтвердите его и нажмите **OK**. Нажмите на ссылку **Установить этот сертификат** (см. рисунок 22), подтвердите доступ нажмите **Да**, после чего появится окно ввода пароля (см. рисунок 23). Введите пароль к контейнеру, заданный ранее, и нажмите **Ок**. А также рекомендуется установить галочки напротив пунктов **Сохранить пароль в приложении** и **Сохранить пароль в системе** чтобы постоянно не вводить пароль.

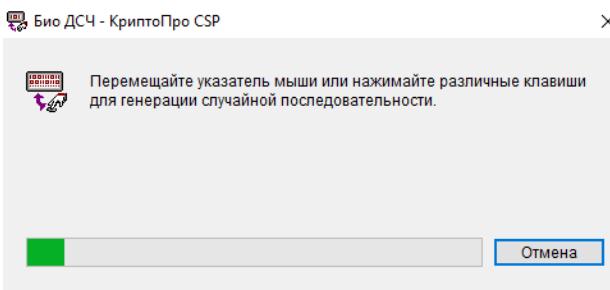


Рисунок 20 – Инициализация ДСЧ.

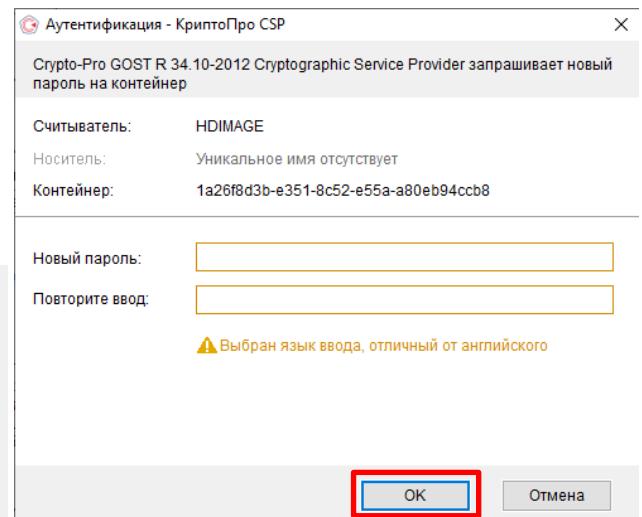


Рисунок 21 – Задание пароля на контейнеру.

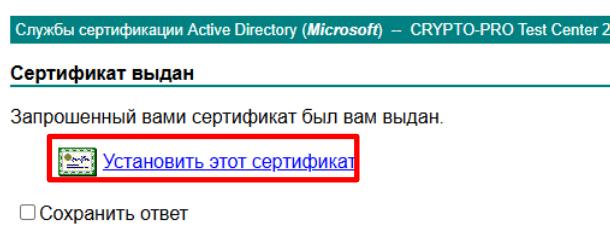


Рисунок 22 – Установка сертификата.

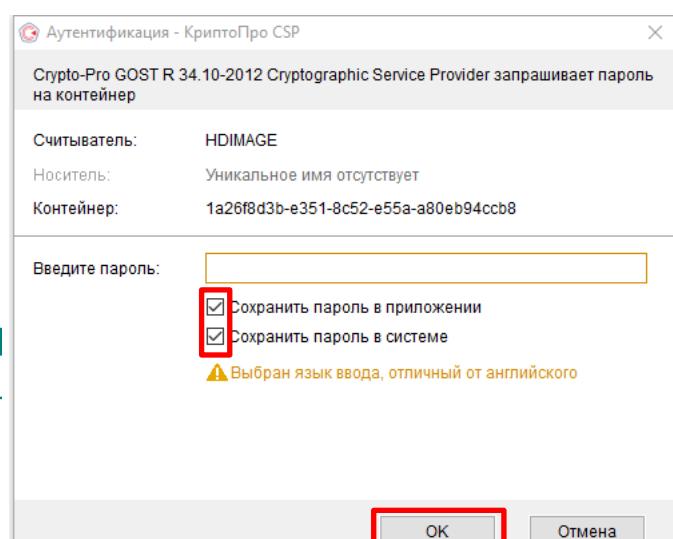


Рисунок 23 – Ввод пароля к контейнеру.

Если пароль введен правильно то **Сертификат** будет успешно **установлен**.

Создание и проверка ЭЦП в MS Office Word 2024 Установка КриптоPro Office Signature

Для создания ЭЦП документа в **Microsoft Office Word/Excel 2024** необходимо наличие плагина **КриптоPro Office Signature**. Для загрузки дистрибутива зайдите на сайт компании КРИПТО-ПРО и перейдите на вкладку **Дополнительное ПО → КриптоPro Office Signature** (см. рисунок 24). На появившейся странице (см. рисунок 25) приведено краткое описание данного продукта, а также взаимодействие подписи, созданной при помощи данного плагина, с различными версиями MS Office. Пролистайте вниз и перейдите по ссылке **КриптоPro Office Signature – Загрузка файлов** и выберите плагин для 64-битных версий. Запустите файл установщика и следуйте указаниям мастера установки. Лицензионный ключ при установке вводить не нужно. Вид установки – **Полная**. Дождитесь завершения установки и нажмите **Готово**.

Продукты	Услуги	Партнёры	Поддержка	Купить
КриптоPro CSP				электронной подписи для работы с электронной подписью 63-ФЗ «Об электронной подписи»
КриптоPro JCP				
КриптоPro .NET				
КриптоPro HSM				
КриптоPro DSS				
КриптоPro Ключ				
КриптоPro NGate				
КриптоPro УЦ				
КриптоPro Центр Мониторинга				
КриптоPro PKI-Кластер				
КриптоPro Архив				
КриптоPro IPsec				
КриптоPro ЭЦП Browser plug-in				
Дополнительное ПО				
СКЗИ со смарт-картами и USB-ключами				
Оборудование			КриптоPro Office Signature	
Сертификаты			КриптоPro PDF	
Свидетельства на ПО			Защищенная мобильность	

Рисунок 24 – КриптоPro Office signature.

Реализуемые алгоритмы:

- ГОСТ Р 34.11/34.10-2001
- ГОСТ Р 34.11-2012/34.10-2012

Системные требования:

- Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, Microsoft Office 2016, Microsoft Office 2019 или Microsoft Office 2021 (32 или 64 бит);
- КриптоPro CSP в соответствии с версией ОС (2.0 и выше).

Преимущества:

Добавляет возможность создания и проверки электронной подписи по ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012 в стандартный интерфейс Microsoft Office Word и Excel.

Страница загрузки:

[КриптоPro Office Signature - Загрузка файлов](#)

Документация:

- [Инструкция по установке и использованию \(версия 2.0\)](#)
- [Инструкция по установке и использованию \(версия 1.0\)](#)

 Страница для печати

Рисунок 25 – Загрузка КриптоPro Office signature.

Создание ЭЦП

В папке **КриптоПро** создайте новый документ Microsoft Word, наполните его произвольным текстом и сохраните. После завершения редактирования и сохранения документа можно добавить к нему ЭЦП. Подписанный документ будет доступен только для чтения. Если в подписанный документ нужно внести изменения, то все созданные ЭЦП следует удалить из документа.

На вкладке **Файл** в разделе **Сведения** нажмите кнопку **Добавить электронную подпись (КРИПТО-ПРО)**. (см. рисунок 26).

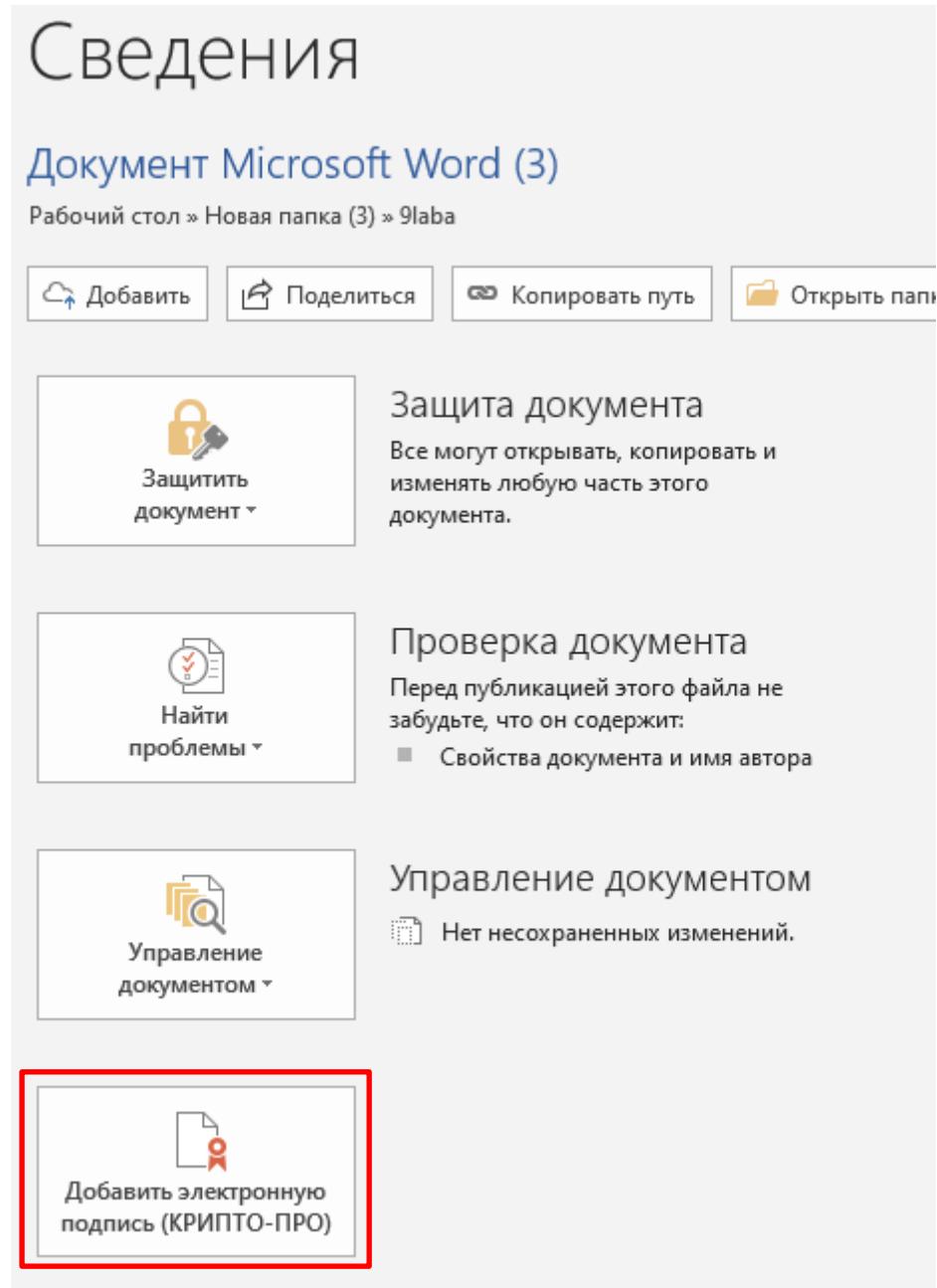


Рисунок 26 – Добавление ЭЦП.

Затем появится окно выбора сертификата (см. рисунок 27). Это окно позволяет пользователю указать свой личный сертификат, который будет использоваться для формирования ЭЦП. Один из сертификатов будет выбран автоматически. Если нужно выбрать другой сертификат - нажмите кнопку **Изменить**. В появившемся окне (см. рисунок 28) представлен список сертификатов пользователя, установленных на компьютере. Выберите сертификат и нажмите **OK**. Для доступа к ключевому контейнеру требуется ввести пароль, но если вы поставили галочки для сохранения

пароля, то пароль вводить повторно не нужно. (см. рисунок 23). При успешном вводе пароля появится окно о статусе подписания документа (см. рисунок 29). Для удобства работы можно установить флажок **Больше не показывать это сообщение**.

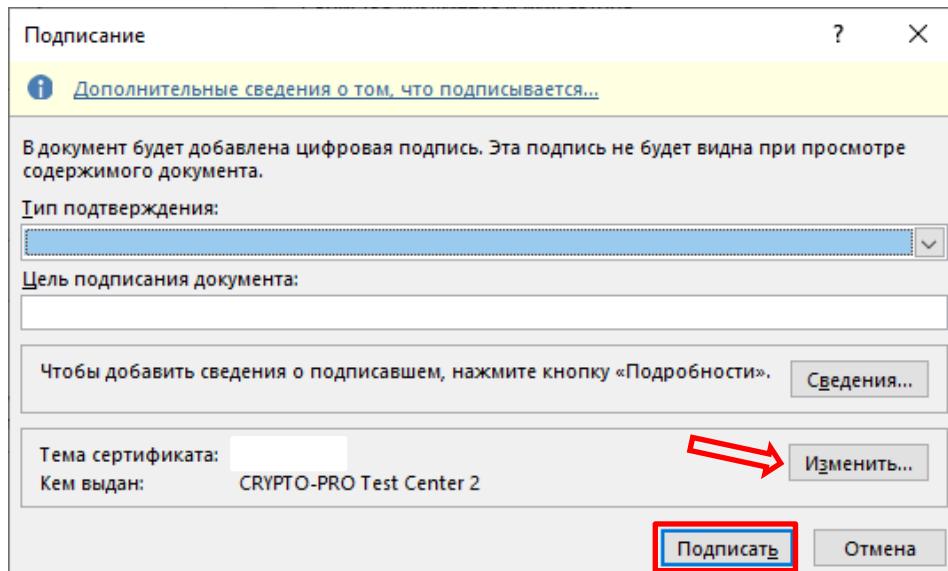


Рисунок 27 – Подписание документа.

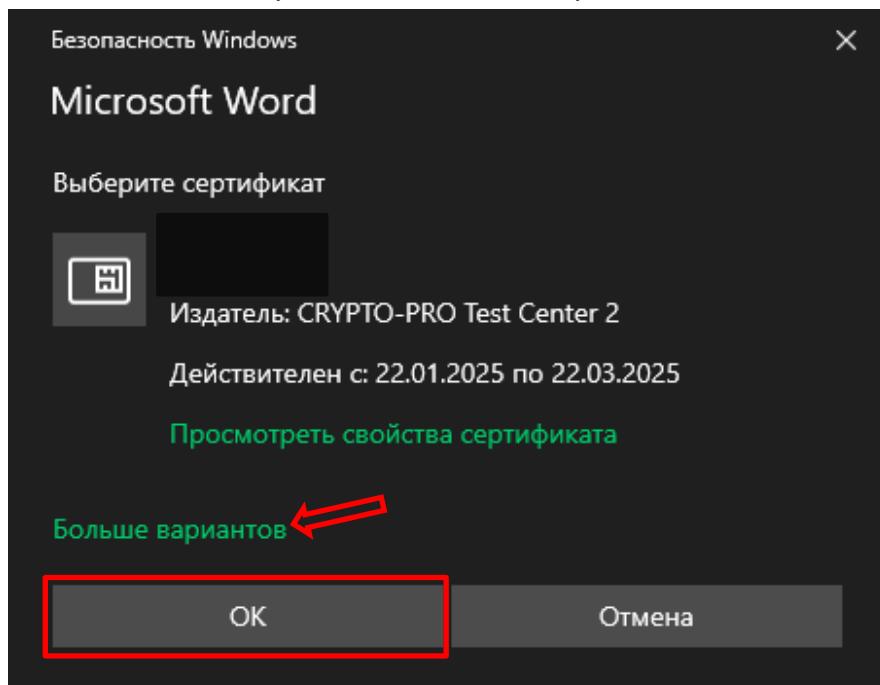


Рисунок 28 – Выбор сертификата.

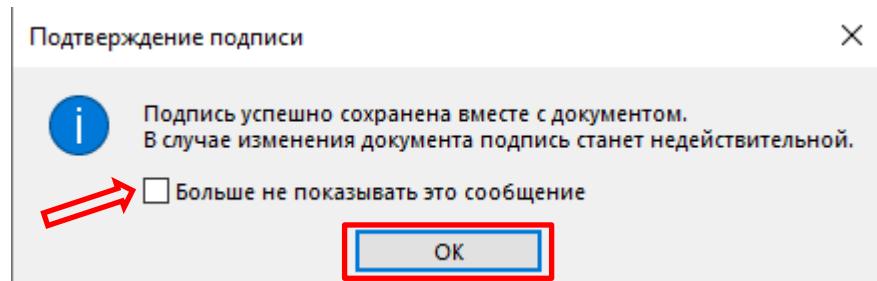


Рисунок 29 – Статус подписание документа.

После подписи документа, в строке состояния окна документа (см. рисунок 30) появится значок, свидетельствующий о том, что данный документ имеет ЭЦП. Также при попытке изменения его содержания (например, печатания текста) с документом ничего не будет происходить. Только в строке состояния появится сообщение о невозможности

изменения.

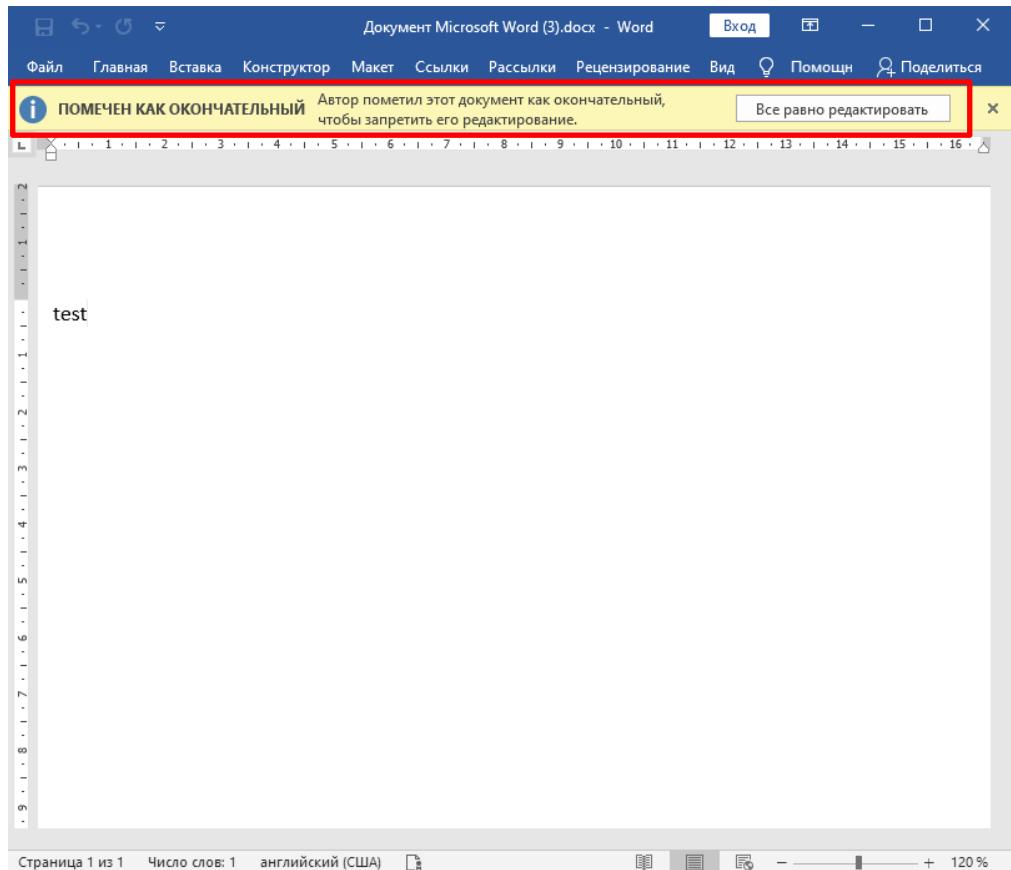


Рисунок 30 – Подписанный документ.

Проверка статуса подписи

Для проверки статуса подписи, нажмите **Сведения** → **Просмотр подписей**, и справа появится вкладка **Подписи**, в которой указан статус подписи (см. рисунок 31). Для просмотра состава подписи щелкните правой кнопкой мыши на строке подписи и выберите пункт **Состав подписи**. Появится более детальное сообщение о составе подписи (см. рисунок 32).

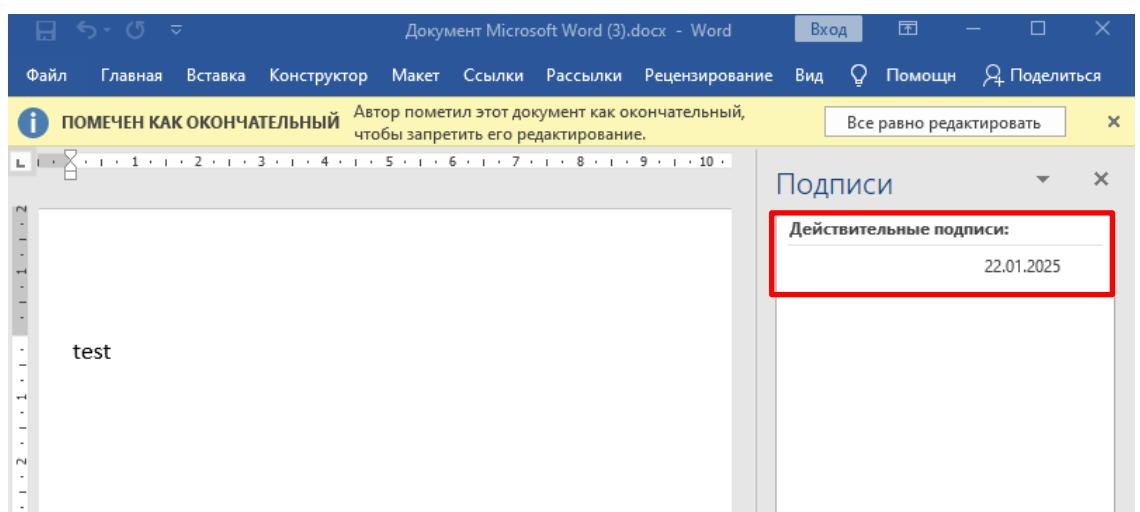


Рисунок 31 – Вкладка Подписи.

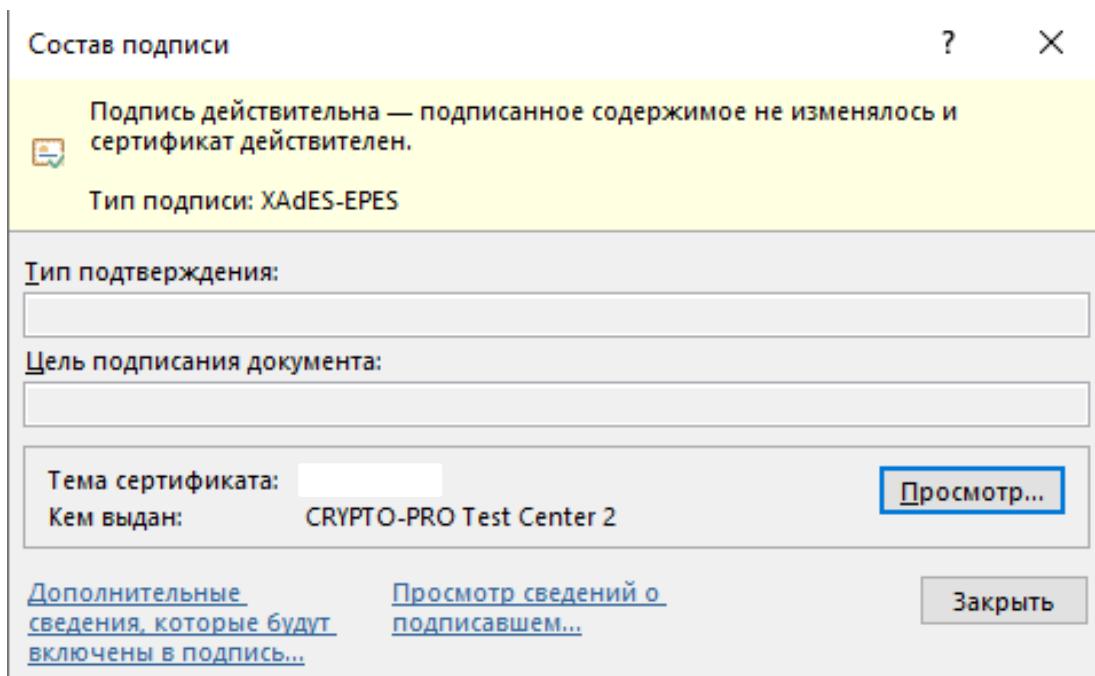


Рисунок 32 – Окно состава подписи.

Теперь откройте подписанный документ и нажмите на кнопку **Все равно редактировать** на желтой панели (см. рисунок 30). Появится предупреждение (см. рисунок 33) о том, что перед редактированием все подписи будут удалены. Нажмите, **Да** и документ снова можно будет редактировать, но значок подписи исчезнет из состояния (см. рисунок 34), а сама **подпись будет удалена**.

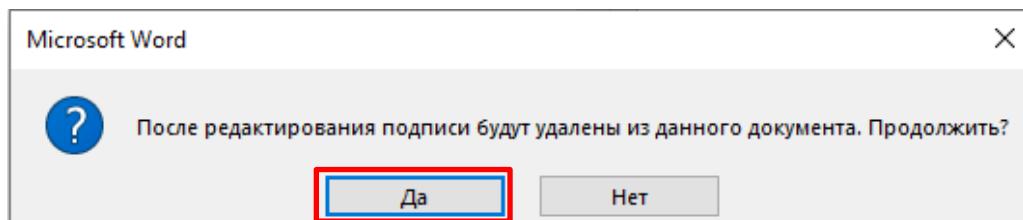


Рисунок 33 – Окно с предупреждением.

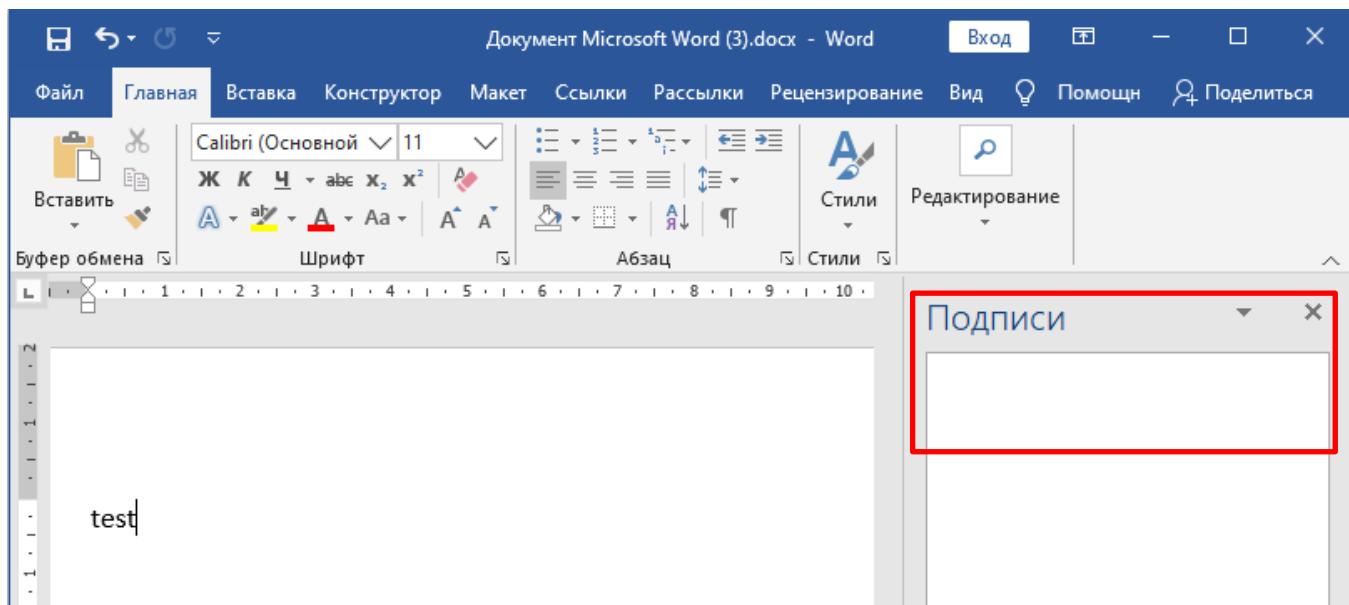


Рисунок 34 – Редактирование документа.

Снова сохраните и подпишите документ. После этого попробуйте сохранить его под другим именем (**Файл → Сохранить как**). Появится окно с предупреждением (см.

рисунок 35). Нажмите Да, после чего откроется только что созданная копия документа.

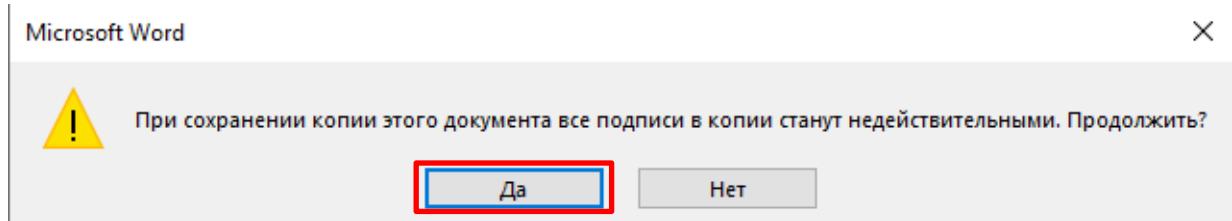


Рисунок 35 – Окно с предупреждением.

Подписание документа, содержащего цифровую подпись

Если документ уже содержит цифровую подпись, его можно подписать еще раз. Для добавления новой ЭЦП в MS Office Word 2024 на вкладке **Файл** в разделе **Сведения** нажмите кнопку **Добавить цифровую подпись (КРИПТО-ПРО)**. Дальнейшие действия аналогичны созданию первой подписи. В результате на вкладке **Подписи** появится еще одна действительная подпись (см. рисунок 36). Для просмотра состава подписи щелкните правой кнопкой мыши на строке нужной подписи и выберите пункт **Состав подписи**.

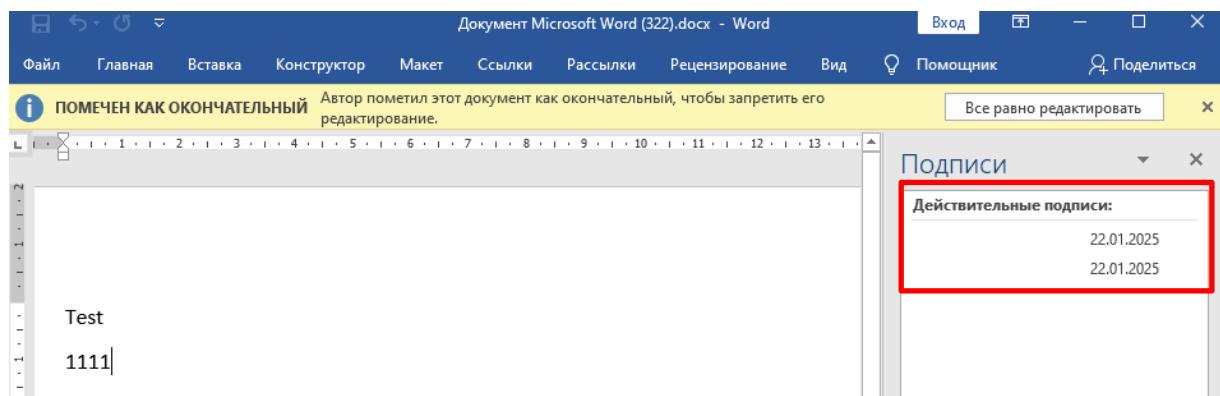


Рисунок 36 – Несколько подписей.

Видимые строки подписи

Видимая строка подписи представляет собой аналог рукописной подписи.

Добавление строки подписи

На вкладке **Вставка** в группе **Текст** нажмите на стрелку рядом с кнопкой **Строка подписи** и в появившемся меню выберите **Строка подписи (КРИПТО-ПРО)**.

Появится диалоговое окно **Настройка подписи** (см. рисунок 37). В нём можно ввести информацию о лице, которое будет добавлять подпись:

- в поле **Предложенный подписывающий** вводится ФИО, подписывающего;
- в поле **Должность предложенного подписывающего** — название должности подписывающего;
- в поле **Адрес электронной почты предложенного подписывающего** — адрес электронной почты подписывающего.

Эти сведения будут отображены в строке подписи в документе. Заполнять все пункты необязательно.

В поле **Инструкции для подписывающего** можно ввести рекомендации или требования для подписывающего. Эти инструкции отображаются в диалоговом окне **Подпись**, в котором подписывающий будет ставить подпись. Для разрешения самому подписывающему добавления комментариев в процессе создания подписи установите

флажок **Разрешить подписывающему добавлять примечания в окне подписи**. Для отображения даты подписания документа, установите флажок **Показывать дату подписи в строке подписи**. Нажмите кнопку **OK**.

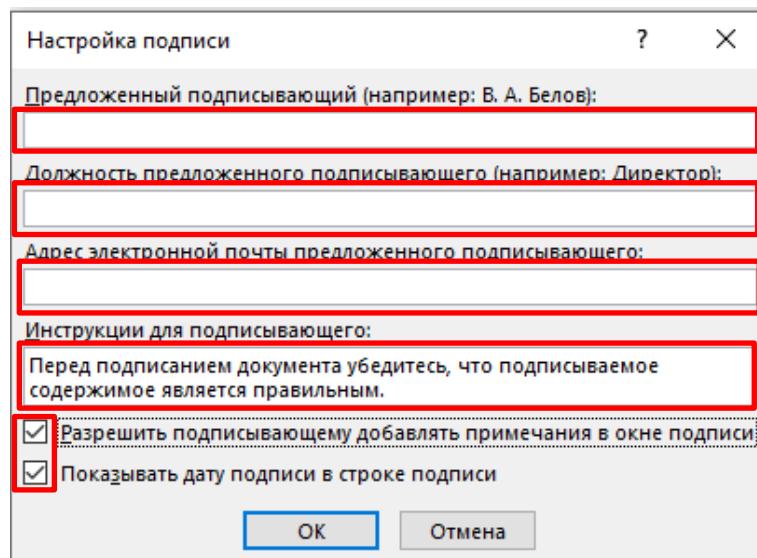


Рисунок 37 – Настройка подписи.

Созданная строка подписи представляет собой графический объект, который можно переместить на любое место в тексте документа (см. рисунок 38). При необходимости можно повторить добавление видимой строки подписи в случае, если документ подписывается разными людьми.

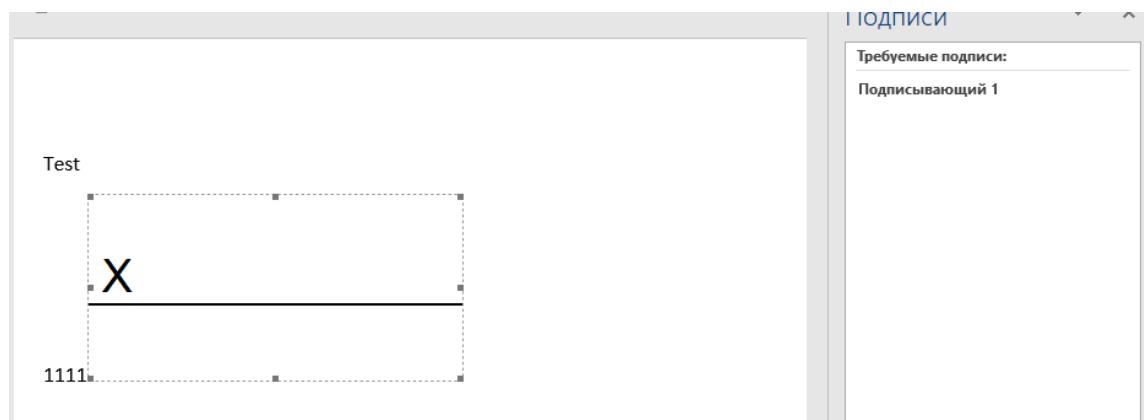


Рисунок 38 – Видимая строка подписи.

Добавление подписи в строку подписания

Дважды щелкните мышью в документе по строке подписи, в которую требуется ввести подпись. Появится диалоговое окно **Подписание** (см. рисунок 39). В верхней части окна можно просмотреть дополнительные сведения о создаваемой подписи, нажав ссылку **Сведения**. При нажатии ссылки **Выбрать рисунок** можно добавить изображение, например, своей рукописной подписи. Один из имеющихся на компьютере сертификатов будет выбран автоматически.

Для выбора другого цифрового сертификата для подписи нажмите кнопку **Изменить** и в окне **Выбор сертификата** выберите необходимый сертификат. В окне **Подписание** нажмите кнопку **Подписать**. Созданная подпись будет отображена в документе. Одновременно будет отображена вкладка **Подписи**, в которой приведен список подписей в документе. Созданная подпись будет находиться в разделе **Действительные подписи**.

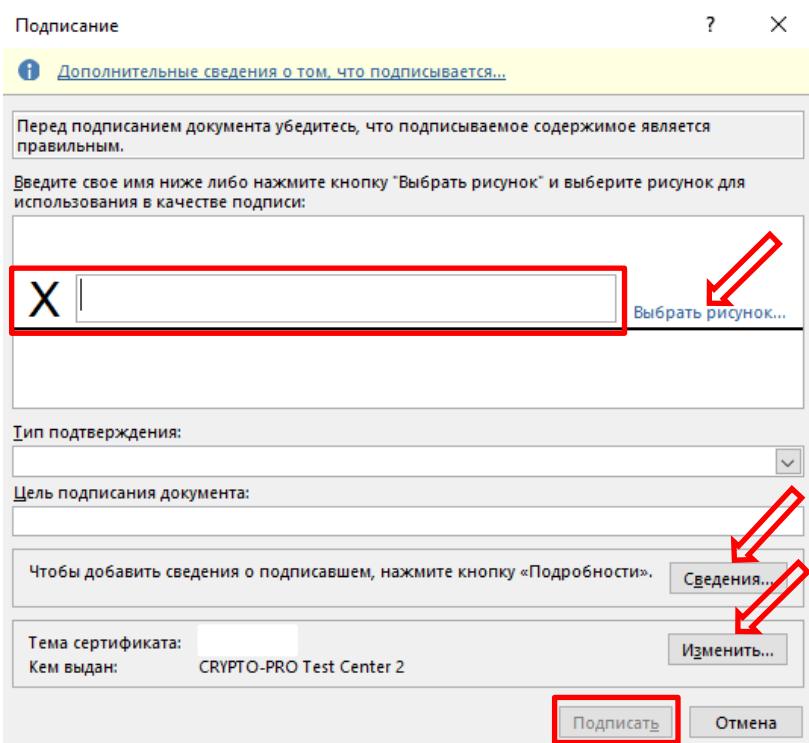


Рисунок 39 – Подписание строки видимой подписи.

Если документ содержит одну или несколько незаполненных строк подписи, то все они будут находиться на вкладке **Подписи** в разделе **Требуемые подписи**. После того, как в документе появилась первая (или единственная) цифровая подпись, она автоматически помечается как окончательный и доступен только для чтения.

Просмотр свойств подписи

В окне документа в панели **Подписи** щелкните по стрелке подписи и выберите команду **Состав подписи**. Можно также дважды щелкнуть мышью по строке подписи в тексте документа. Свойства подписи будут отображены в соответствующем окне (см. рисунок 40). Для просмотра сертификата, использовавшегося при создании подписи, нажмите кнопку **Просмотр**.

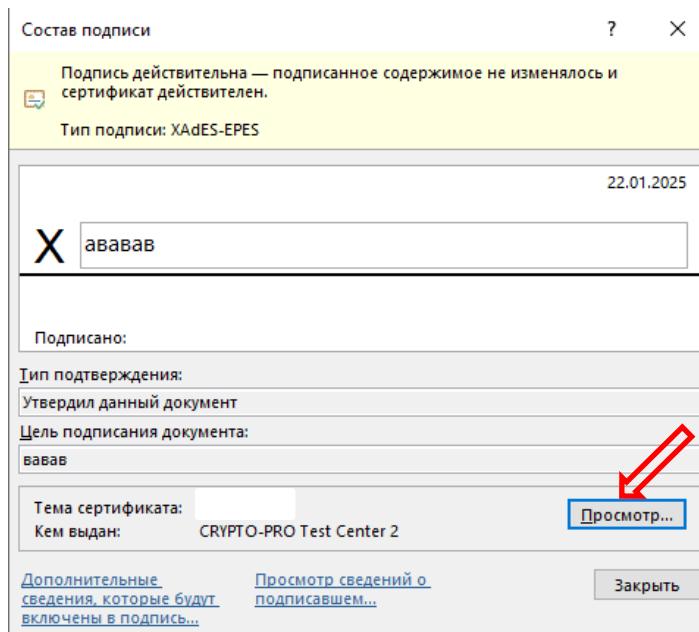


Рисунок 40 – Свойства подписи.

Создайте новый документ Microsoft Word и попытайтесь осуществить следующие операции:

- копирование текста из подписанного документа в новый;
- копирование строки подписи, содержащей действительную подпись, в новый документ.

Проанализируйте результат. Сохраните документ, содержащий строку видимой подписи, под другим именем. В окне с предупреждением (см. рисунок 35) нажмите Да. Посмотрите, как изменилась строка подписи, когда сама подпись стала недействительной. Документ, содержащий недействительную подпись, можно подписать повторно. Для этого на вкладке **Подписи** щелкните по стрелке недействительной подписи и выберите команду **Подписать еще раз**. Можно также щелкнуть правой кнопкой мыши по строке подписи в тексте документа и в контекстном меню выбрать команду **Подписать еще раз**. Заново заполните окно **Подписание** и нажмите кнопку **Подписать**.

Работа с почтовым клиентом The Bat!

Создание почтового ящика

Скачайте установщик с официального сайта ([The Bat! - Главная](#)). Сохраните файл thebat_64_11-4-1.msi (актуальная версия на момент написания) в папке **КриптоПро**. Запустите инсталлятор и следуйте указаниям **Мастера установки**. Далее необходимо создать собственный почтовый ящик. Для этого выберите пункт меню **Ящик → Новый почтовый ящик** (см. рисунок 41).

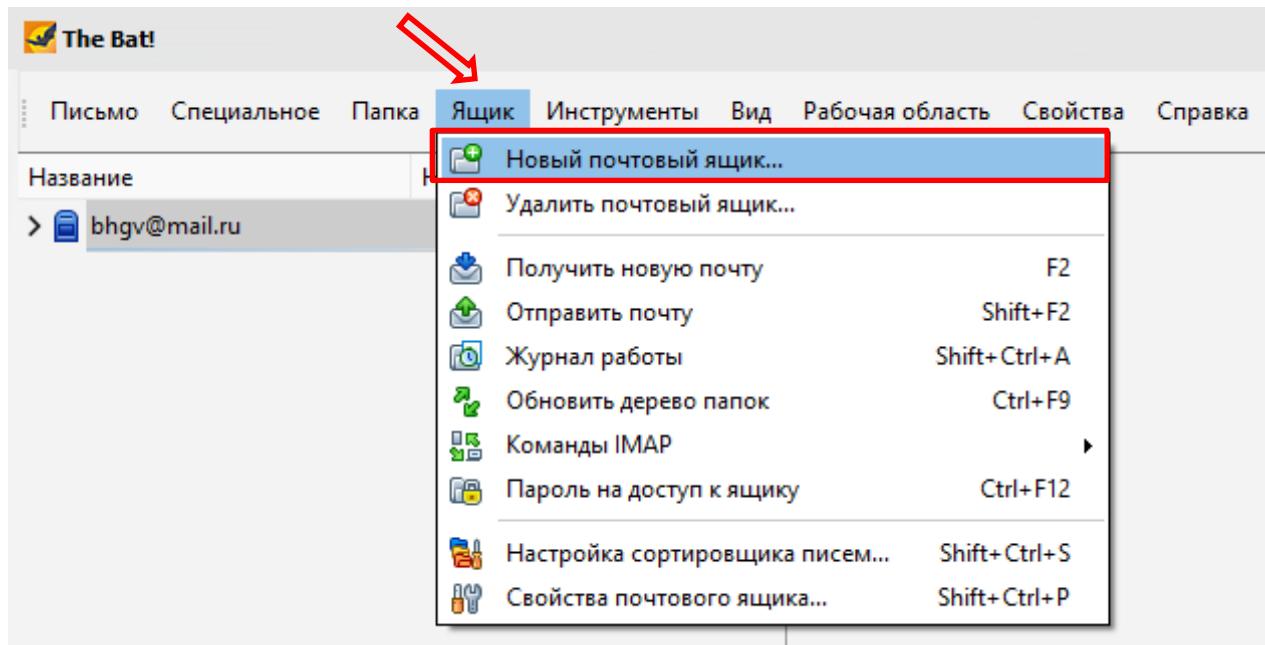


Рисунок 41 – Создание почтового ящика.

В появившемся окне задайте название создаваемого ящика, в строке Электронный адрес введите существующую почту, которую вы указывали при заказе личного сертификата, в строке Пароль введите Пароль для внешнего приложения (например, из почты Mail.ru). (см. рисунок 48). Для этого зайдите на свою почту → Под своим профилем → Пароль и безопасность → Пароли для внешних приложений → Создать. Далее придумываете название и вам необходимо выбрать Настройки доступа.

Рекомендую выбирать **Полный доступ к почте**. После проверки что вы не робот появляется ваш пароль, который и необходимо ввести в поле приложения The Bat!!! **Без этой настройки The bat работать не будет.** **Важно:** пароль будет виден **ТОЛЬКО ОДИН РАЗ ПОЭТОМУ СКОПИРУЙТЕ ЕГО ИЛИ ЗАПОМНИТЕ!!!!** (см. рисунок 42-49). И только в конце всех настроек необходимо нажать **Далее**.

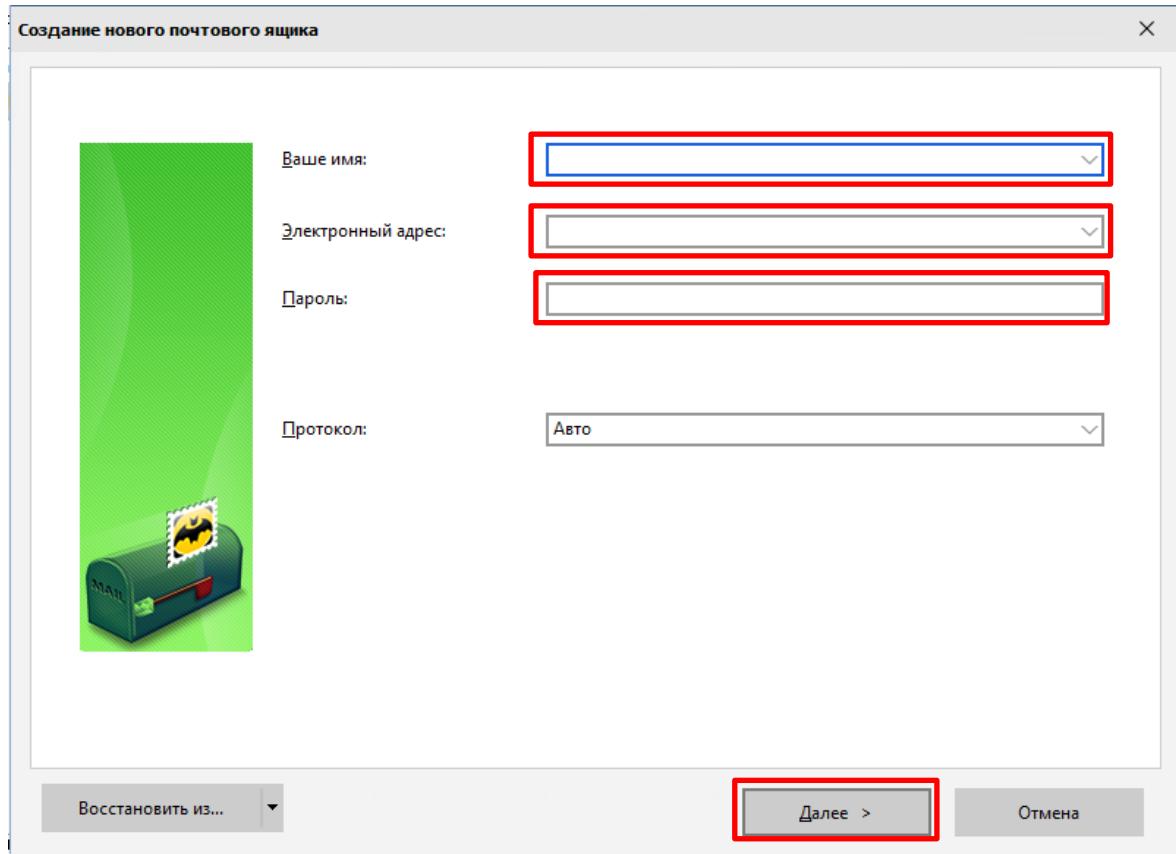


Рисунок 42 – Настройка почтового ящика.

Войти в аккаунт ×

@ mail Яндекс Другой

Имя аккаунта @mail.ru

Войти > запомнить

Другие способы входа VK VK ID Gmail Gmail

[Восстановить доступ](#) [Создать аккаунт](#)

 [Быстрый вход по QR-коду](#)
Наведите камеру телефона
[Подробнее](#)

Занято 440 МБ из 8 ГБ ⋮

● Почта 440 МБ ● Облако 0 байт

Увеличить место

👤 [Личные данные](#)

🔒 Пароль и безопасность

☰ [Вход в приложение по QR-коду](#)

➡ [Выйти](#)

Рисунок 43 – Вход в почту Mail.

Рисунок 44 – Настройка почты Mail.

Способы входа

The screenshot shows a list of login methods:

- Пароль** (Password): A key icon. Description: Use random letters, numbers, and symbols to make the password harder to crack. [Подробнее](#) (More details). A blue 'Изменить' (Change) button is to the right.
- Электронные ключи** (Electronic Keys): A key fob icon. Description: Login without a password using fingerprint, face, or external device scanning. [Подробнее](#). A blue arrow icon is to the right.
- Двухфакторная аутентификация** (Two-factor authentication): A lock icon. Description: Two-step login: after a password, verify via SMS sent to your phone number. [Подробнее](#). A blue arrow icon is to the right.
- Пароли для внешних приложений** (Passwords for external applications): A grid icon. Description: Special passwords for logging into third-party apps like Microsoft Outlook, The Bat!, etc. [Подробнее](#). This item is highlighted with a red rectangle.

Рисунок 45 – Настройка способа входа.

Настройка доступа (Access Settings)

Выберите тип протокола, чтобы приложение получило доступ только к нужным данным в Почте, Облаке или Календаре. Или предоставьте полный доступ. [Подробнее](#)

Полный доступ к Почте
SMTP, IMAP, POP3

Только чтение и удаление писем в Почте
IMAP, POP3

Только отправка писем в Почте
SMTP

Полный доступ к Облаку
WebDAV

Полный доступ к Календарю
CalDAV

Полный доступ к Почте, Облаку, Календарю
Все протоколы

Пароли для внешних приложений (Passwords for external applications)

Создавайте специальные пароли, чтобы входить в аккаунт в сторонних приложениях: Microsoft Outlook, The Bat! и др. [Подробнее](#)

Пароль для внешнего приложения

Рисунок 46 – Создание пароля.

Рисунок 47 – Выбор типа протокола.

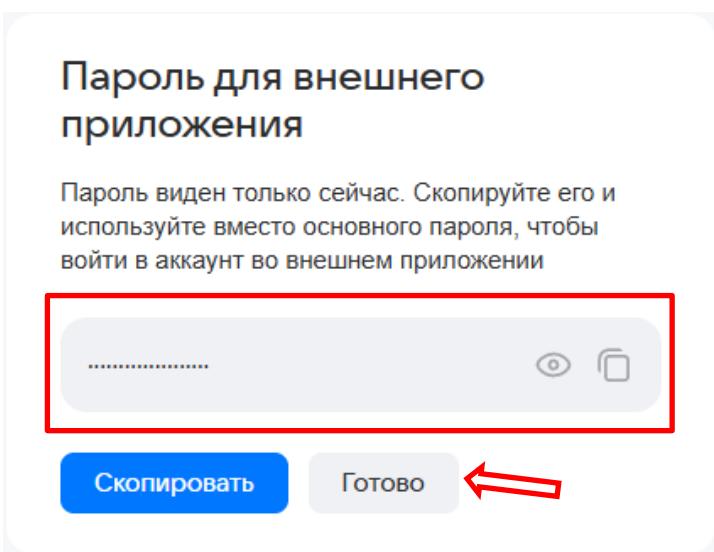


Рисунок 48 – Пароль для TheBat.

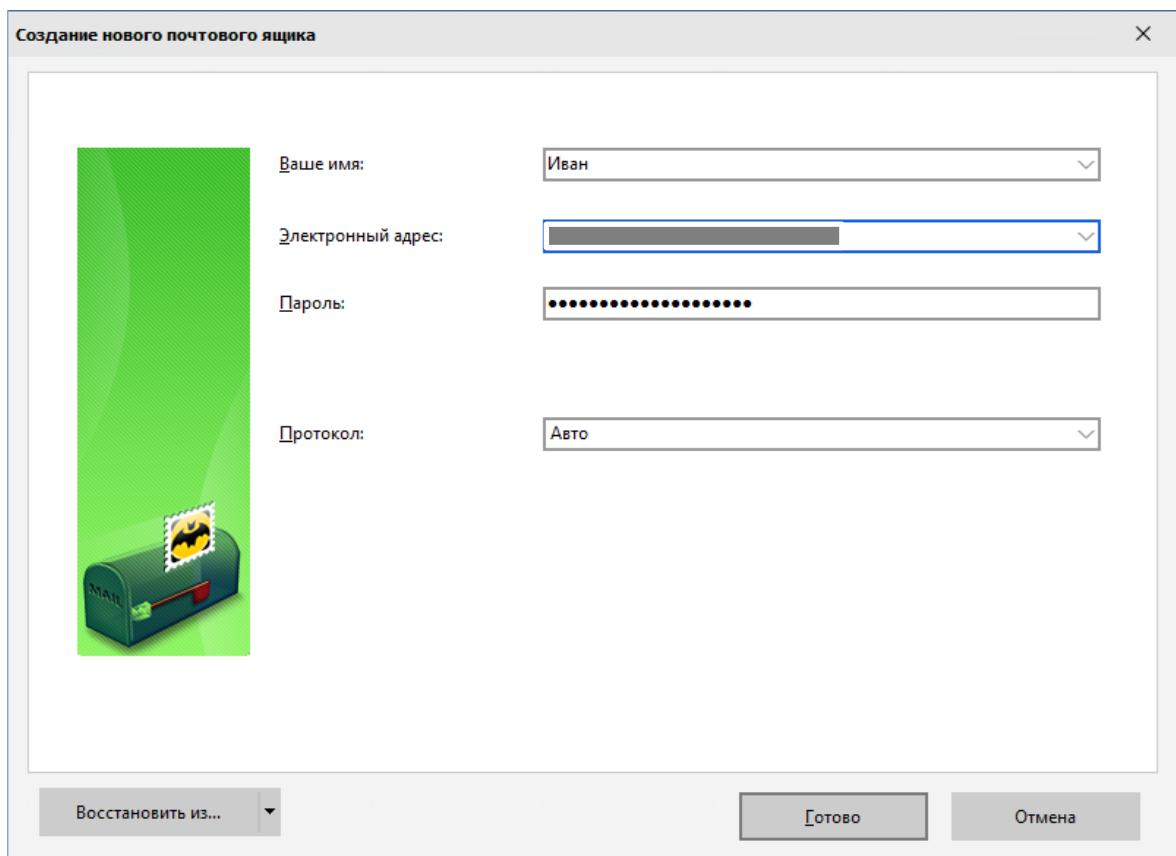


Рисунок 49 – Заполненные строки TheBat.

Готово. Если все сделано правильно, то все сообщения на вашем основном аккаунте будут отображены в TheBat.

Настройка почтового клиента

Для использования протокола S/MIME в почтовой программе The Bat! необходимо настроить параметры.

Для этого выполните следующие действия:

1. Выберите пункт меню **Свойства → Параметры S/MIME** (см. рисунок 50);

2. В появившемся окне (см. рисунок 51) настройки выберите следующие параметры:
Реализация S/MIME и сертификаты TLS → Microsoft CryptoAPI;

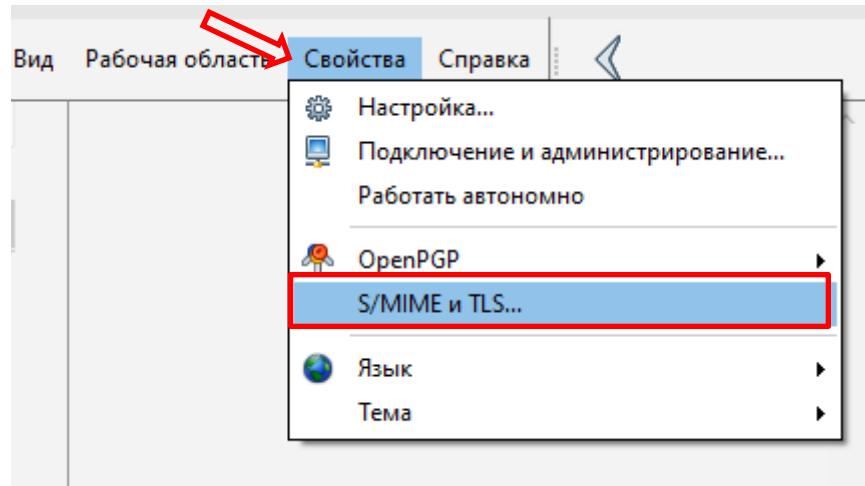


Рисунок 50 – Параметры S/MIME и TLS.

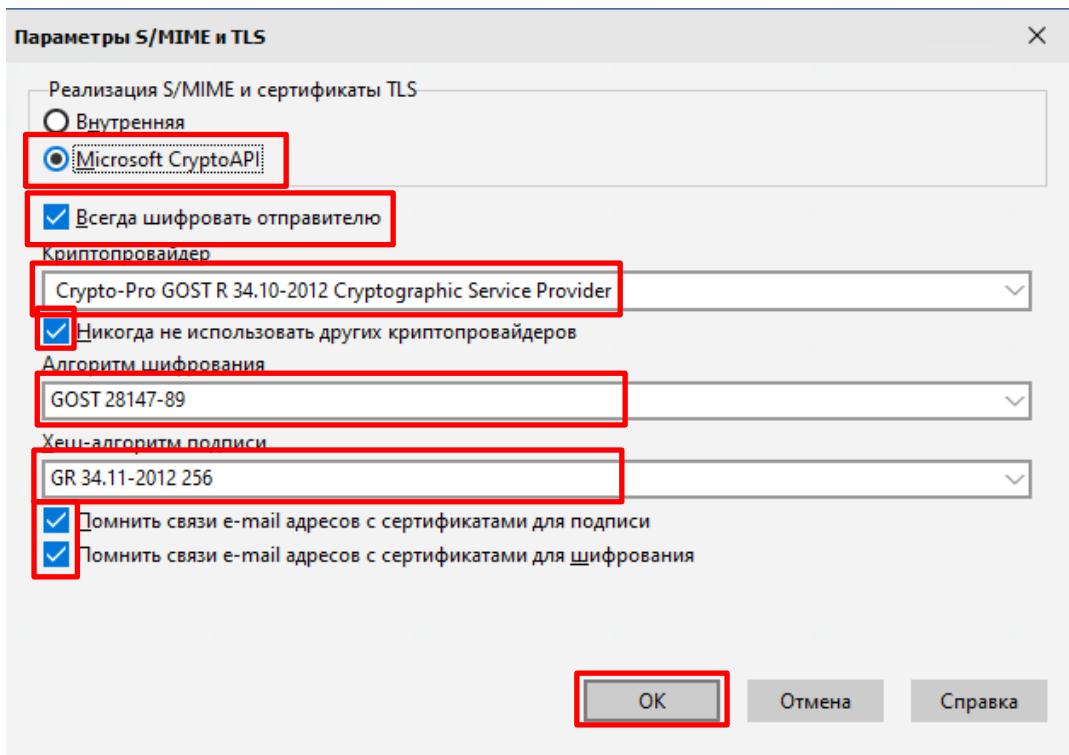


Рисунок 51 – Настройка параметров S/MIME и TLS.

Если Вы хотите, чтобы все письма перед отправкой шифровались на открытом ключе получателя, отметьте пункт **Всегда шифровать отправителю**. **Криптопровайдеры** → **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**. Если Вы не хотите использовать сертификаты и ключевые пары на других криптопровайдерах, пометьте пункт **Никогда не использовать других криптопровайдеров**. **Алгоритм шифрования** → **GOST 28147-89**. **Хеш-алгоритм подписи** → **GR 34.11-2012 256**. Включите опции **Помнить связь e-mail адресов с сертификатами для подписи** и **Помнить связь e-mail адресов с сертификатами для шифрования**. Это избавит Вас от необходимости каждый раз выбирать нужный сертификат из списка.

3. Выберите пункт меню **Ящик** → **Свойства почтового ящика** (см. рисунок 52);
4. В дереве настроек **Свойства почтового ящика** (см. рисунок 53) выберите вкладку **Параметры**;

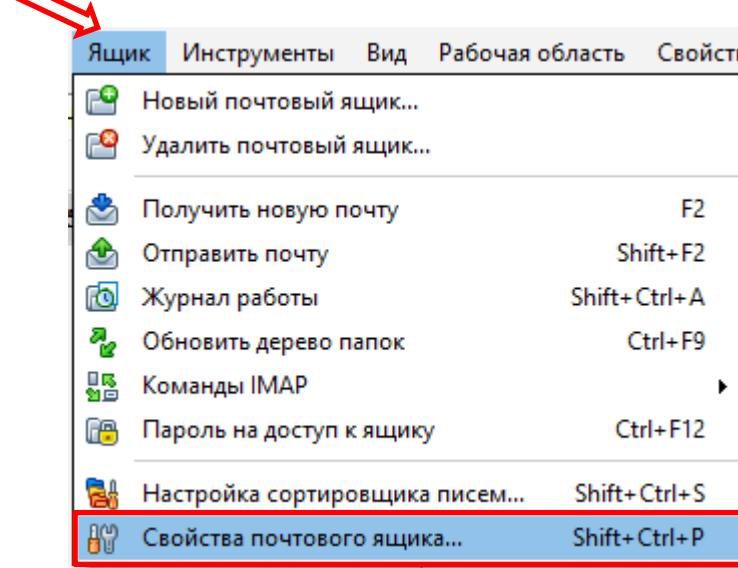


Рисунок 52 – Свойства почтового ящика.

В области **Редактор писем** можно выбрать опцию **Подписать перед отправкой** и **Зашифровать перед отправкой**. Это позволит автоматически при отправке подписывать и зашифровывать сообщения. Обязательно должна быть отмечена опция **Авто – S/MIME**.

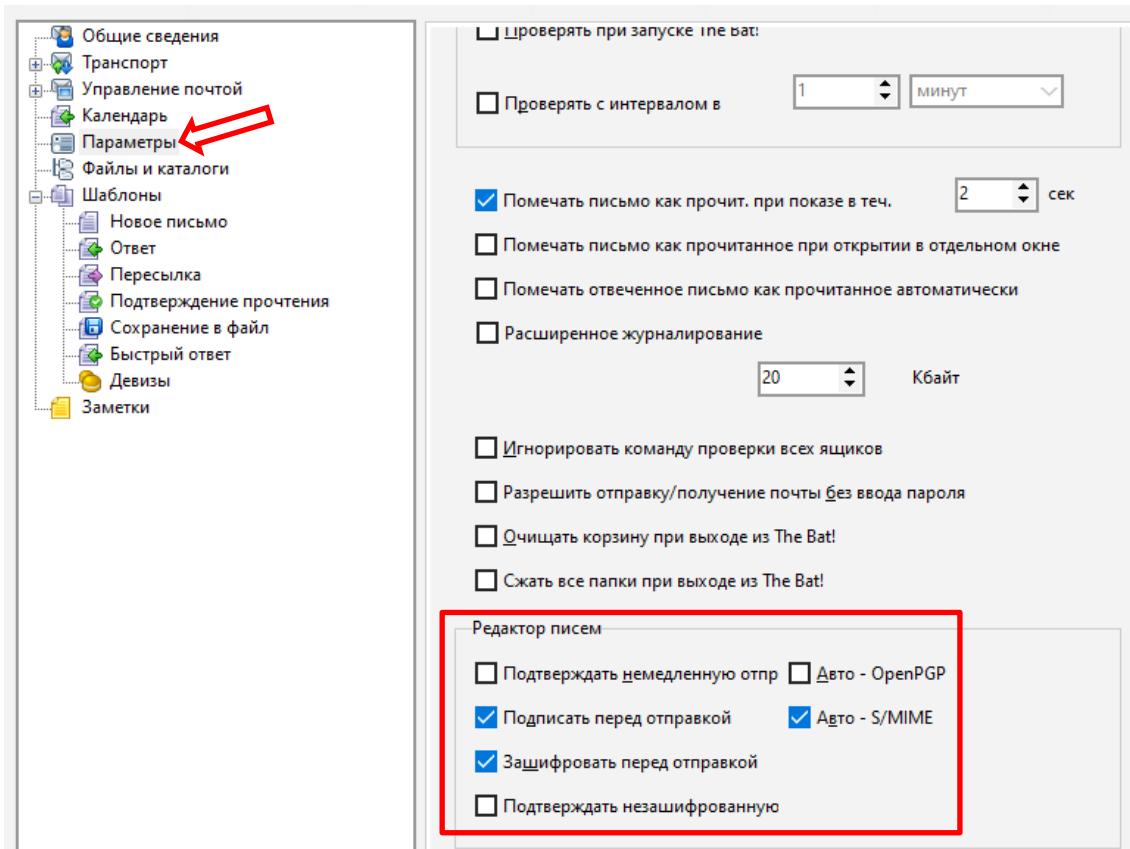


Рисунок 53 – Параметры почтового ящика.

5. В дереве настроек выберите вкладку **Транспорт** (см. рисунок 54).

В областях **Отправка почты** и **Получение почты** установите в полях **Соединение** значение **Безопасное на станд. порт (STARTTLS)**. Остальные настройки в этом пункте лучше не трогать!!!

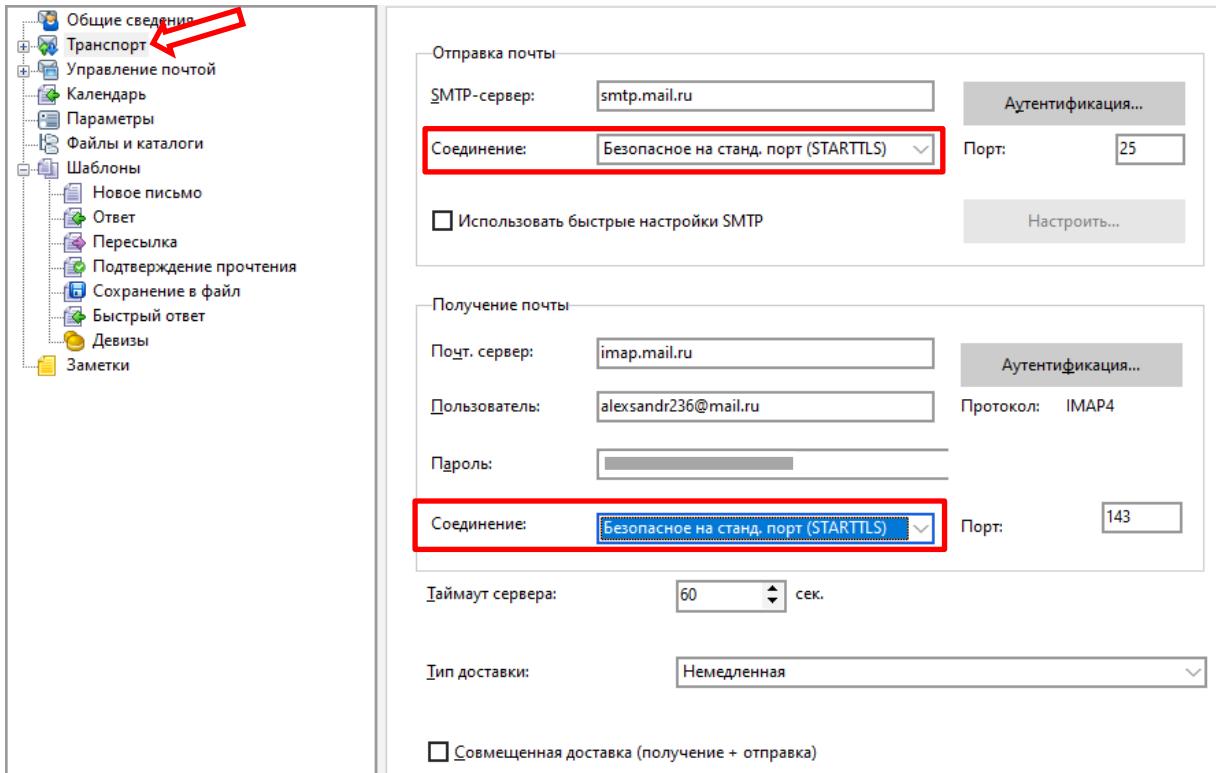


Рисунок 54 – Параметры меню Транспорт.

Отправка и получение писем

Выберите пункт меню **Письмо → Создать**. В появившемся окне (см. рисунок 55) внесите в поле **Кому** электронный адрес данного ящика (письмо будет отправлено себе). Т.к. это первое письмо данному адресату, шифровать его не нужно (уберите опцию **Зашифровать перед отправкой**). Заполните поле **Тема**, напишите некоторый текст в письме и отправьте его (**Письмо → Отправить сейчас**). Появится окно выбора сертификата для подписи (см. рисунок 56). Выберите свой сертификат и нажмите **OK**.

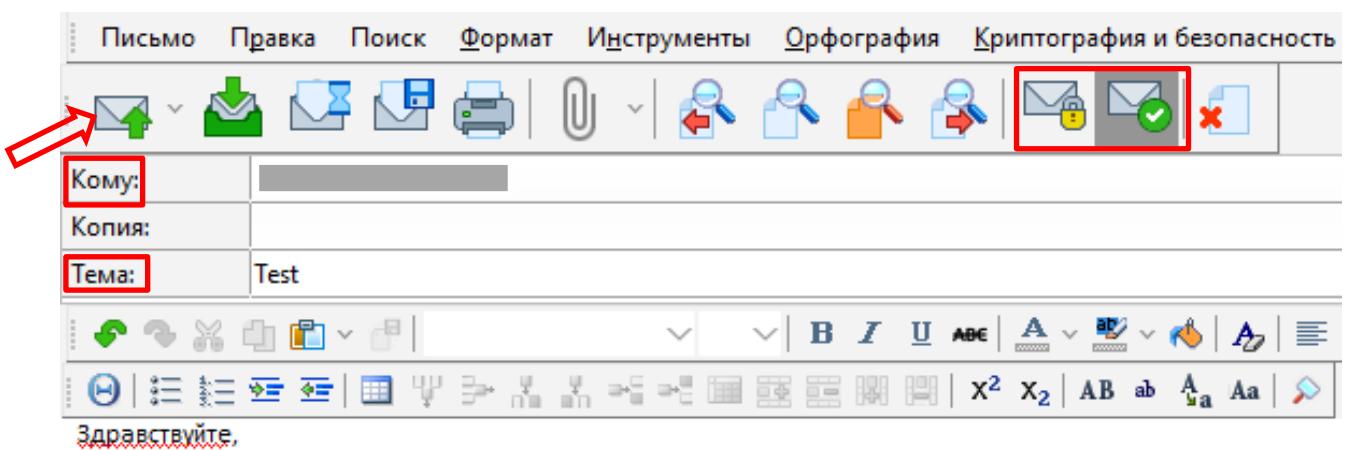


Рисунок 55 – Создание письма.

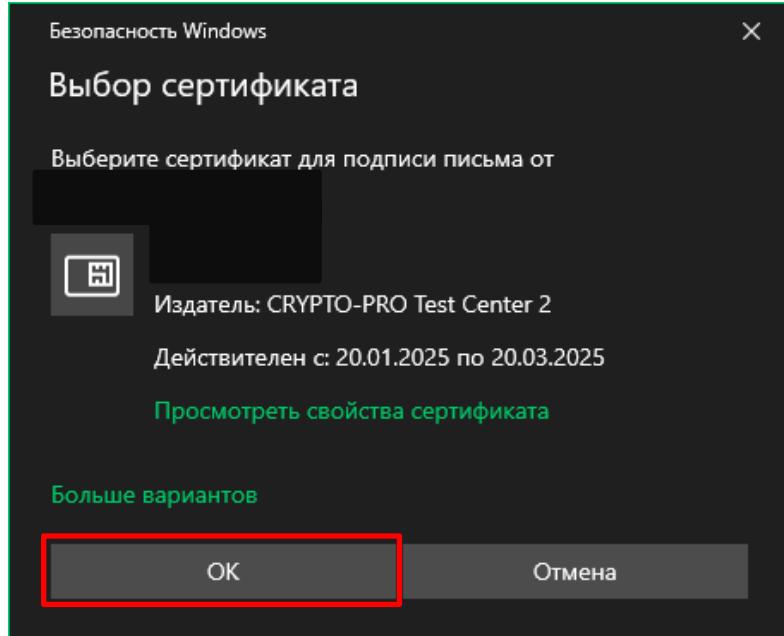


Рисунок 56 – Выбор сертификата.

Подождите некоторое время (1-2 минуты) а затем щелкните правой кнопкой мыши по своему почтовому ящику и в открывшемся контекстном меню выберите пункт **Получить новую почту** (см. рисунок 57). Если письмо не пришло, повторите процедуру позднее. Как получите письмо, выделите его и нажмите (**Ctrl + W**) для добавления отправителя в адресную книгу. В появившемся окне (см. рисунок 58) заполните необходимые поля и нажмите **OK**. Теперь у Вас в адресной книге есть данный адресат с его сертификатом и ему можно отправлять ему зашифрованные сообщения.

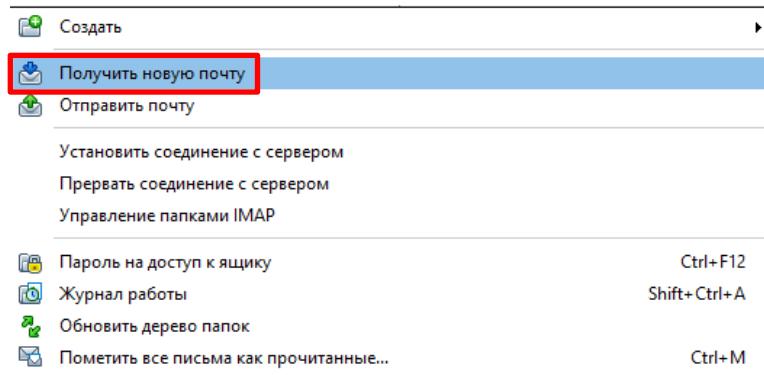


Рисунок 57 – Проверка почты.

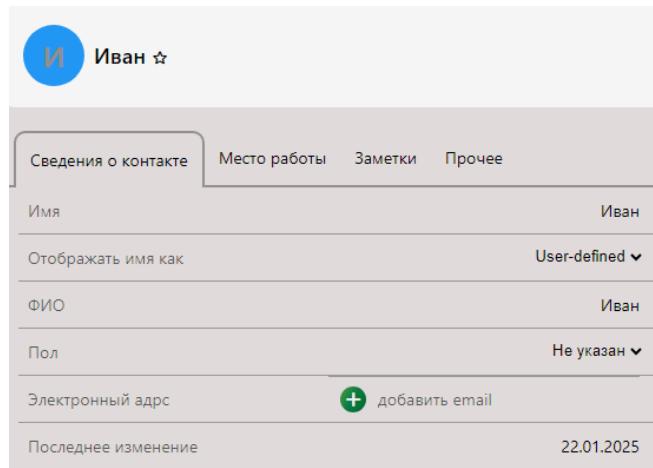


Рисунок 58 – Добавления адресата.

После этого откройте письмо двойным щелчком. Для проверки подписи зайдите в письмо и нажмите на зеленый щит с галочкой. Если во время доставки письмо не было изменено или повреждено, то появится окно (см. рисунок 59) с данными о подписавшем. Если бы письмо было от другого человека, то можно было бы установить данный сертификат (но только если Вы доверяете отправителю). Нажмите **OK**.

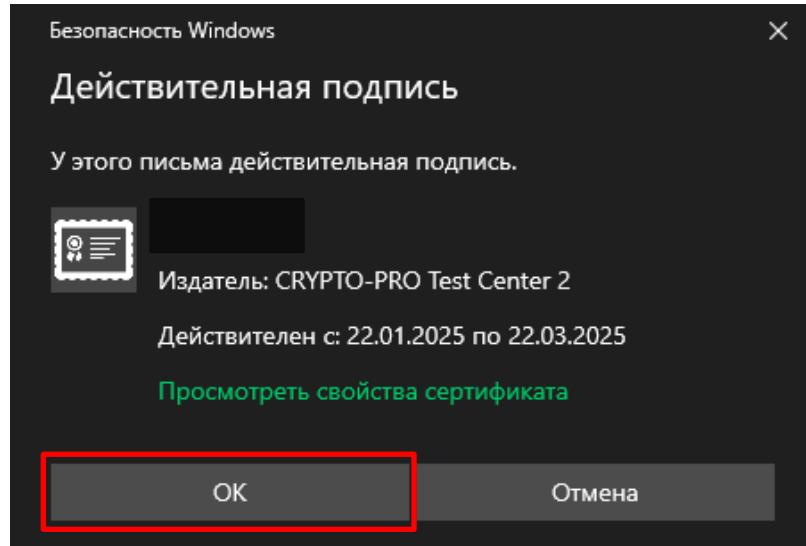


Рисунок 59 – Сведение о подписи.

Создайте новое сообщение. при выборе адресата воспользуйтесь адресной книгой (самая правая иконка в поле **Кому**, см. рисунок 55). Заполните тему и текст письма. В этот раз не убирайте опцию **Зашифровать перед отправкой** (см. рисунок 60).

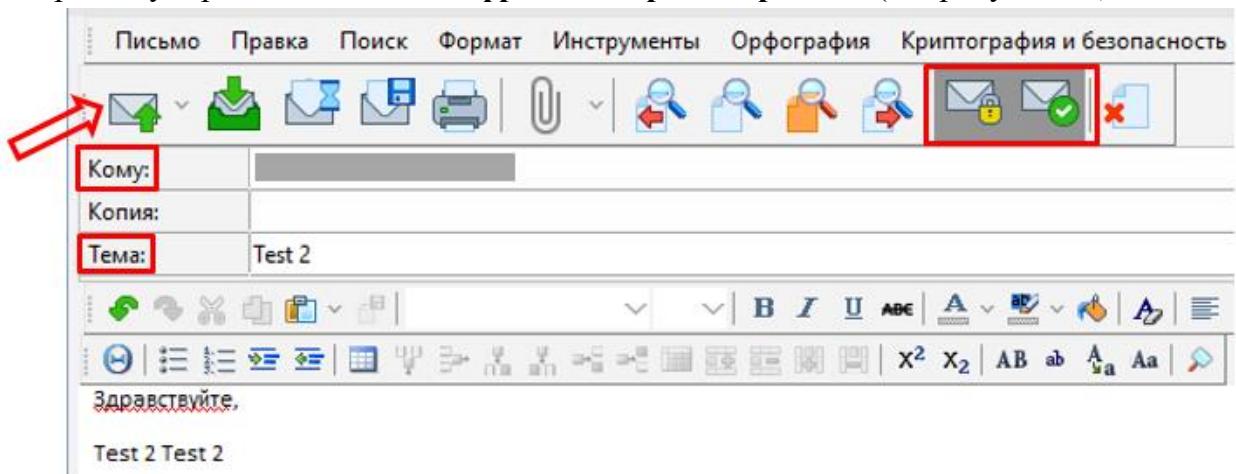


Рисунок 60 – Отправка зашифрованного письма.

Отправьте данное сообщение. После этого выберите сертификат получателя (в данном случае тот же самый), на открытом ключе которого будет выполняться зашифрование. Периодически проверяйте почту, пока не получите письмо. Откройте его двойным нажатием. После этого в письме нажмите на зеленый открытый замочек. Во всплывающем окне будет написано: **это письмо было зашифровано отправителем и расшифровано The Bat!** Работа с криптопровайдером КриптоPro CSP завершена!!!

Контрольные вопросы

- 1. Что представляет собой электронная подпись?**
- 2. Для чего служит электронная подпись? От каких видов злоумышленных действий она может защитить?**
- 3. Какие существуют разновидности электронной подписи?**
- 4. Что такое инфраструктура открытых ключей? Какие основные задачи она решает?**
- 5. Что такое удостоверяющий центр? Каковы функции центра сертификации?**
- 6. Какими удостоверяющими центрами Вы пользовались во время практической работы? Можно ли пользоваться их услугами для реальных, а не учебных задач? Почему?**
- 7. Какова иерархия центров сертификации? Что такое цепочки сертификатов?**
- 8. Что такое сертификат открытого ключа? Какие обязательные компоненты входят в состав сертификата?**
- 9. Для чего нужен список отзываемых сертификатов? Приведите примеры.**
- 10. Что представляет собой криптопровайдер? Какие функции он выполняет?**
- 11. Какие алгоритмы шифрования, хеширования, подписи реализуют криптопровайдеры КриптоПро CSP, Сигнал-КОМ CSP?**
- 12. Что такое ключевой контейнер? Для чего он нужен?**