УДК 378.147

ТЕХНОЛОГИЯ ПОДПИСИ ДОКУМЕНТОВ MS OFFICE ПРОСТОЙ ЦИФРОВОЙ ПОДПИСЬЮ

Кутьин М.К.

Военная академия Республики Беларусь, г. Минск, Беларусь, kutin1957@mail.ru

Аннотация. Рассматривается технология подписи документов MS Word с использованием цифровой подписи, созданной в приложении Adobe Acrobat Pro, с целью перевода учебно-методических материалов и учебно-программной документации в безбумажную среду

Ключевые слова. Цифровое удостоверение, цифровой сертификат открытого ключа, цифровая подпись.

В законодательстве Российской Федерации [1] предусматривается понятие простой электронной подписи (ПЭП). Принципиальным отличием ПЭП от электронной цифровой подписи (ЭЦП), предусмотренной в законодательстве Республики Беларусь [2], является то, что она создается без привлечения удостоверяющих центров.

Анализ свойств ПЭП показывает, что при придании такой подписи правового статуса она может использоваться для подписи электронных учебно-методических и других электронных документов, циркулирующих в рамках образовательного процесса ВУЗа.

Примером простой электронной подписи является цифровая подпись, создаваемая, например, в приложении Adobe Acrobat Pro. Создаваемое в данном приложении цифровое удостоверение может использоваться только при работе с документами pdf-формата. Однако при разработке учебно-методических материалов (УММ) и учебно-программных документов, как правило используется приложение MS Word.

В приложении MS Word создать цифровое удостоверение по аналогии с приложением Adobe Acrobat Pro не представляется возможным. В тоже время, использовать ЭЦП в классическом исполнении при работе с УММ не целесообразно.

Существует возможность использования созданного в Adobe Acrobat Pro самоподписанного цифрового удостоверения для подписи документов, разрабатываемых в приложениях MS Office. Для этого необходимо произвести импорт цифрового удостоверения из файлов приложения Adobe Acrobat Pro, где оно по умолчанию сохраняется, в хранилище сертификатов пользователя операционной системы Windows.

Данная задача решается в следующей последовательности.

Предположим, что в приложении Adobe Acrobat Pro было создано цифровое удостоверение пользователем Ivan Ivanov.

По адресу C:\Users\kmk\AppData\Roaming\Adobe\Acrobat\9.0\Security находится файл обмена личной информацией IvanIvanov.pfx (рисунок 1). В данном файле хранится цифровое удостоверение, включающее закрытый ключ цифровой подписи и сертификат открытого ключа. Необходимо отметить, что в приложении Adobe Acrobat Pro понятие простой электронной подписи трактуется как цифровая подпись (ЦП). Двойной клик по файлу вызывает открытие диалогового окна Мастер импорта сертификатов (рисунок 2).

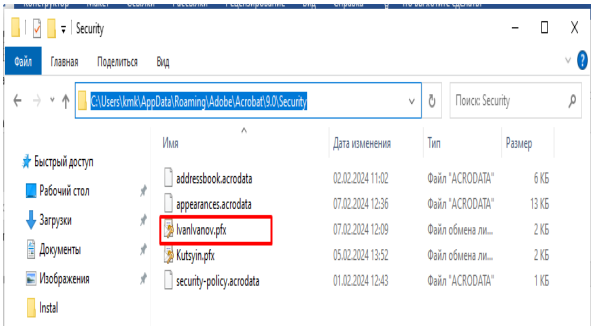

Рисунок 1 – Файл обмена личной информацией *IvanIvanov.pfx*

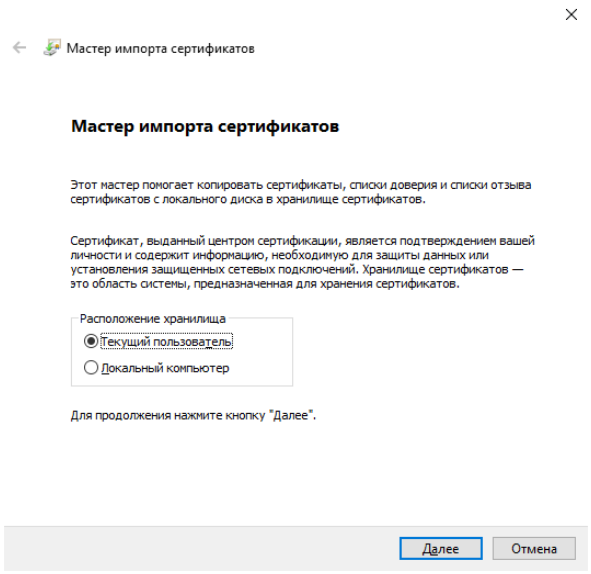

Рисунок 2 – Диалоговое окно Мастер импорта сертификатов

Учитывая, что цифровое удостоверение является личной информацией пользователя, переключатель Расположение хранилища устанавливаем в положение Текущий пользователь и нажимаем кнопку Далее.

На следующем шаге подтверждается тип выбранного файла обмена личной информацией (рисунок 3).

Поскольку цифровое удостоверение включает закрытый ключ, который должен быть недоступен другим пользователям, мастер импорта сертификатов предлагает произвести выбор варианта защиты закрытого ключа с помощью пароля. В диалоговом окне в перечне параметров Параметры импорта необходимо выставить флажки напротив выбранных параметров (рисунок 4).

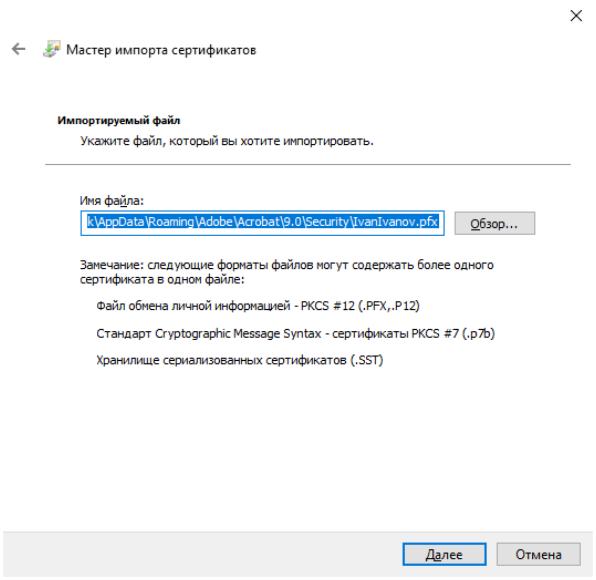

Рисунок 3 – Выбор типа импортируемого файла с личной информацией

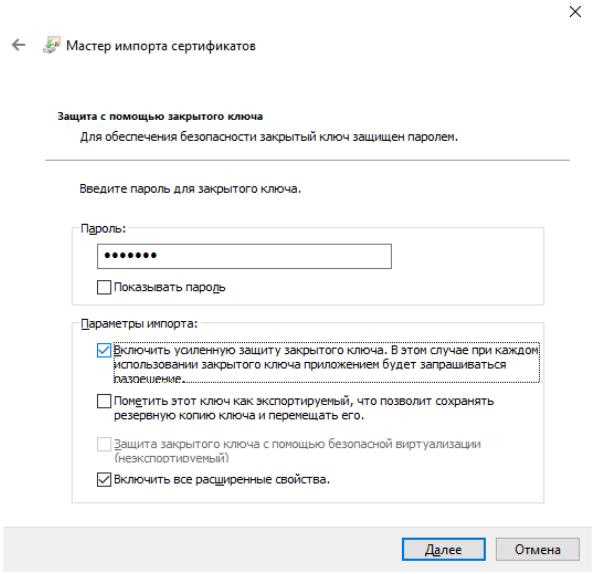

Рисунок 4 – Выбор вариантов защиты закрытого ключа с помощью пароля

Далее Мастер импорта сертификатов предлагает выбрать хранилище, в которое необходимо импортировать цифровое удостоверение. При установке переключателя в положение Автоматически выбрать хранилище на основе типа сертификата (рисунок 5) в качестве хранилища будет выбрано хранилище сертификатов пользователей.

На следующем шаге производится проверка параметров импорта сертификата и нажатием кнопки Готово завершается процесс импорта (рисунок 6).

После завершения импорта цифрового удостоверения производится проверка уровня безопасности хранения закрытого ключа. Для этого автоматически открывается диалоговое окно Импорт нового закрытого ключа обмена (рисунок 7), которое предлагает установить уровень защиты закрытого ключа – средний или высокий. При выборе среднего уровня (предлагается по умолчанию) пользователь нажимает кнопку Ok и на этом установка уровня защиты закрытого ключа завершается. Для повышения уровня защиты необходимо нажать на кнопку Уровень безопасности, в результате чего откроется диалоговое окно Выбор уровня безопасности (рисунок 8).

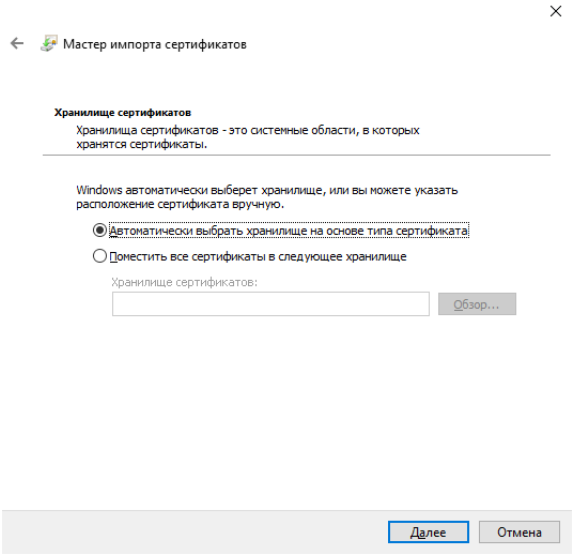

Рисунок 5 – Выбор хранилище, в которое необходимо импортировать цифровое удостоверение

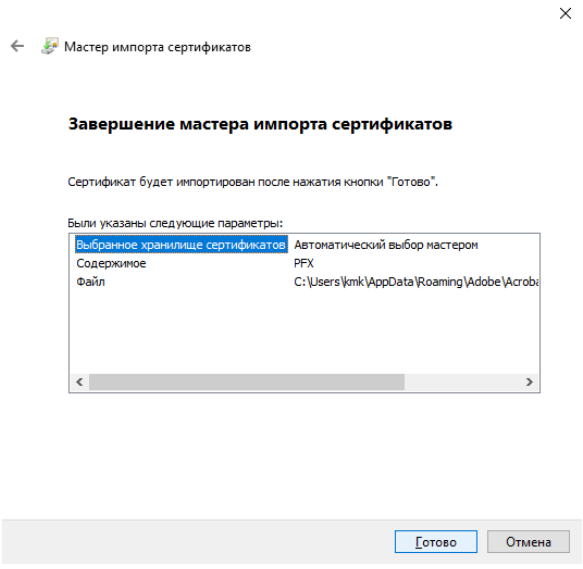

Рисунок 6 – Проверка параметров и завершение импорта цифрового удостоверения

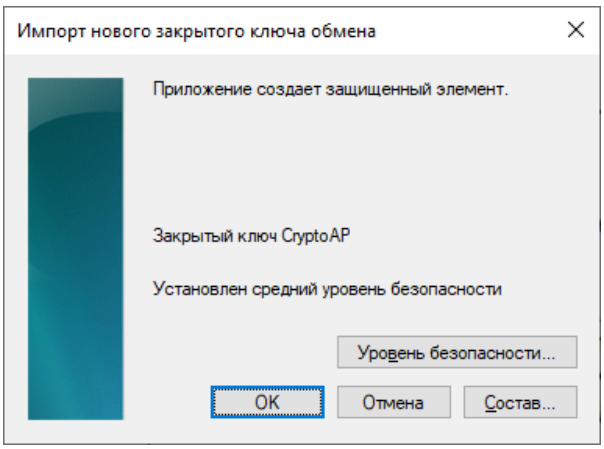

Рисунок 7 – Выбор уровня безопасности закрытого ключа

На следующем шаге создается пароль для доступа к закрытому ключу и подтверждается сделанный выбор защиты (рисунки 9, 10).

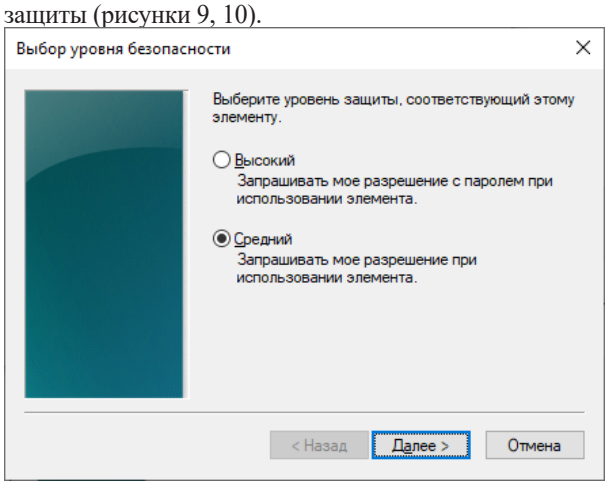

Рисунок 8 – Диалоговое окно Выбор уровня безопасности

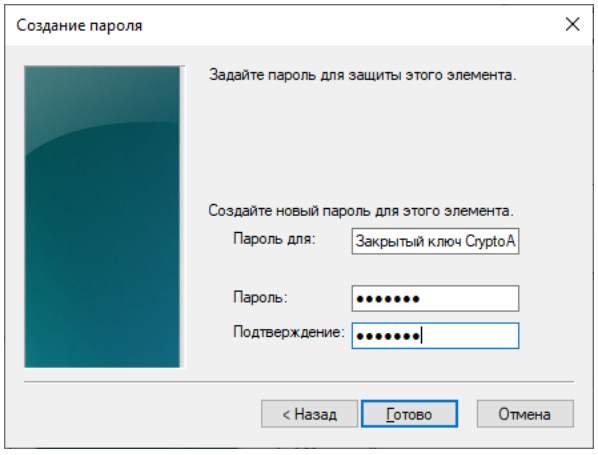

Рисунок 9 – Диалоговое окно создания нового пароля для защиты закрытого ключа

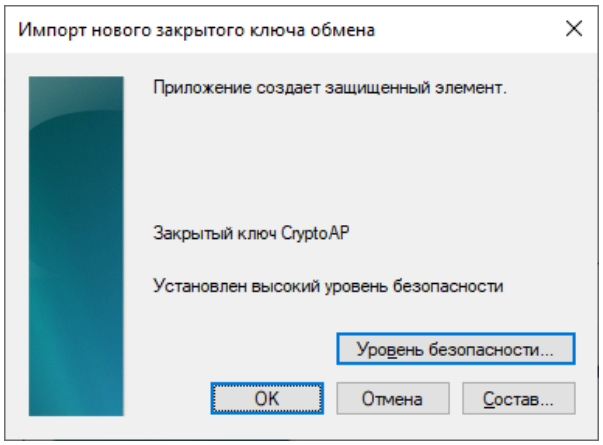

Рисунок 10 – Диалоговое окно завершения выбора уровня защиты закрытого ключа

В результате открывается диалоговое окно Мастер импорта сертификатов (рисунок 11) с сообщением о том, что импорт успешно выполнен.

Для проверки успешного завершения импорта сертификата из хранилища приложения Adobe Acrobat Pro в хранилище сертификатов пользователей операционной системы Windows можно открыть менеджер сертификатов пользователей (рисунок 12) и проверить вложенную папку Личное → Сертификаты.

Как видно из рисисунка 12, в хранилище сертификатов личных пользователей имеется сертификат Ivan Ivanov.

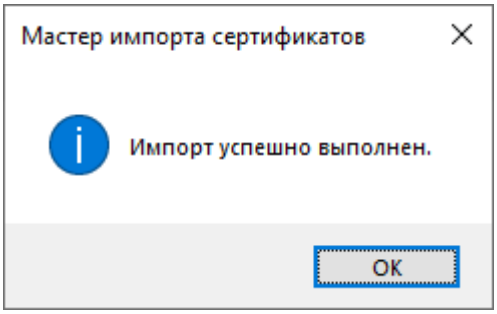

Рисунок 11 – Сообщение Импорт успешно выполнен

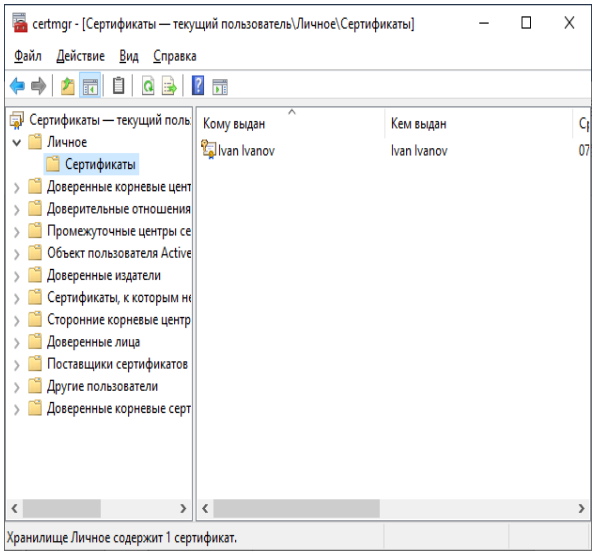

Рисунок 12 – Менеджер сертификатов пользователей

Для получения подробной информации о данном сертификате необходимо его открыть через контекстное меню. В диалоговом окне Сертификат (рисунок 13) имеются три вкладки Общие, Состав и Путь сертификации.

На вкладке Общие (рисунок 13) отображаются сведения о том, кому выдан сертификат, кем выдан, сроки действия и сведения о наличии закрытого ключа. Кроме того, указываются сведения о доверии к сертификату.

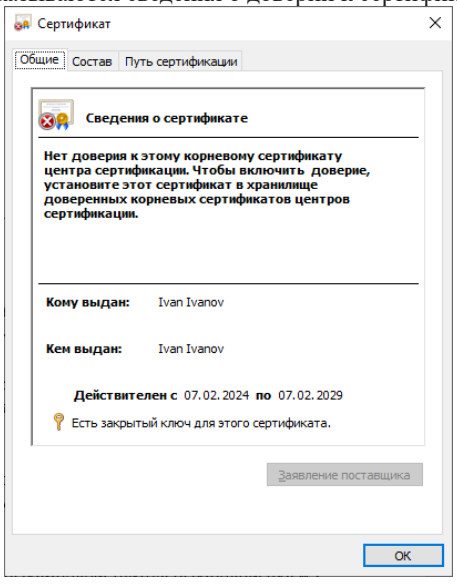

Рисунок 13 – Сертификат, вкладка Общие

На вкладке Состав (рисунок 14) отображаются версия, серийный номер, алгоритм подписи, хэш-алгоритм подписи, сведения об издателе, сроки действия, длина открытого ключа и другая информация о сертификате.

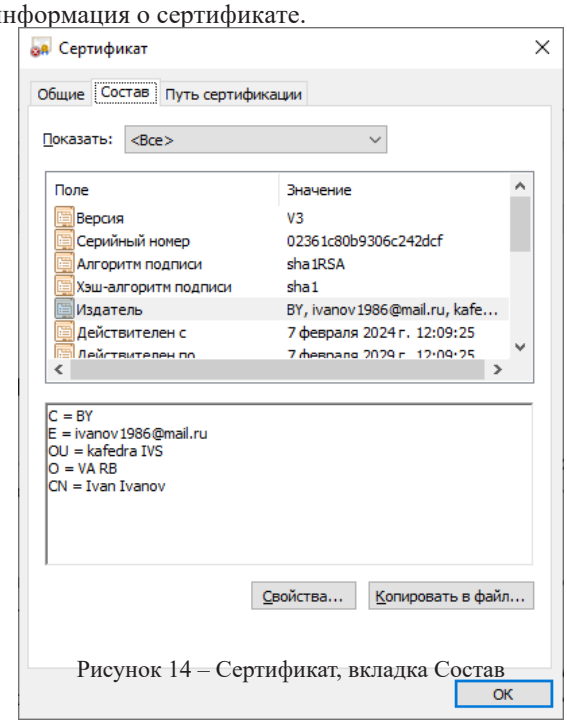

Рисунок 14 – Сертификат, вкладка Состав

В связи с тем, что данный сертификат был издан пользователем и не проходил через удостоверяющий центр, хранилище сертификатов позиционирует данный сертификат с комментарием «нет доверия к этому корневому сертификату центра сертификации. Чтобы включить доверие, установите этот сертификат в хранилище доверенных корневых сертификатов центров сертификации». После установки сертификата в хранилище доверенных корневых сертификатов комментарий к сертификату преобразуется – «Все политики выдачи. Все политики применения» (рисунок 15).

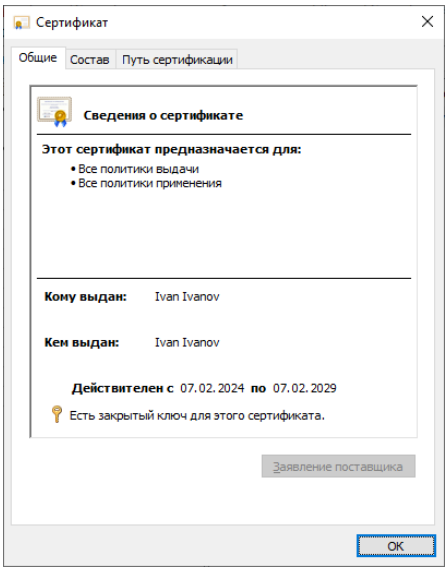

Рисунок 15 – Сертификат, вкладка Общие *после установки сертификата в хранилище доверенных корневых сертификатов*

Данная характеристика политик выдачи и политик применения говорит о том, что сертификат можно применять для решения различных криптографических задач с обеспечением высоких гарантий безопасности.

После перемещения цифрового удостоверения в хранилище сертификатов пользователей операционной системы Windows закрытый ключ можно использовать для цифровой подписи документов приложения MS Word, а сертификат открытого ключа для проверки подписи.

Рассмотрим технологию цифровой подписи документа Word на примере документа *ПЦП Иванова.docx (рисунок 16).*

Профессор кафедры
информационно-вычислительных систем
И.И. Иванов

Рис. 16. Документ Word *ПЦП Иванова.docx, предназначенный для ЦП*

Для ЦП документа воспользуемся командой Строки подписи в группе команд Текст вкладки Вставка (рисунок 17). В выпадающем списке команды выбираем вкладку *Строка подписи Microsoft Office. В результате открывается диалоговое окно Настройка подписи с полями, которые необходимо заполнить (рисунок 18).*

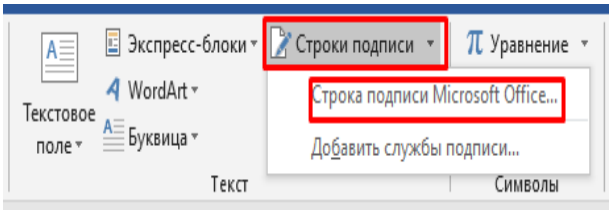

Рисунок 17 – Команда *Строки подписи в группе команд Текст вкладки Вставка*

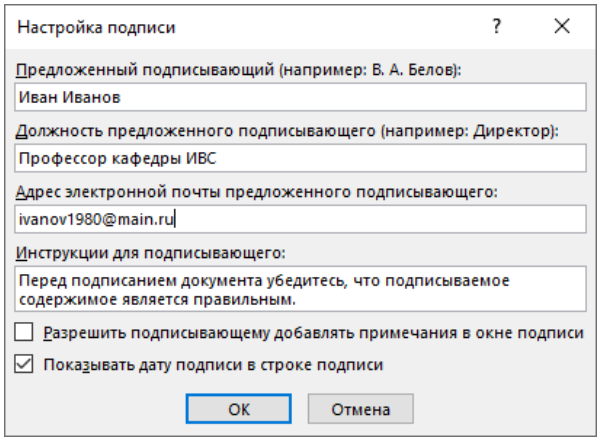

Рисунок 18 – Диалоговое окно *Настройка подписи*

После настройки подписи в месте расположения курсора формируется строка подписи (рисунок 19). Для завершения подписи в контекстном меню строки подписи выбирается вкладка *Подписать, в результате чего открывается диалоговое окно Подписание (рисунок 20).*

Диалоговое окно Подписание предлагает завершить оформление строки подписи. Так, в строку подписи мож-

но вставить либо текстуальные данные подписывающего документ, либо графическое изображение. Для вставки графического изображения предлагается нажать кнопку Выбрать рисунок и произвести выбор рисунка через диалоговое окно Вставка изображений (рисунок 21).

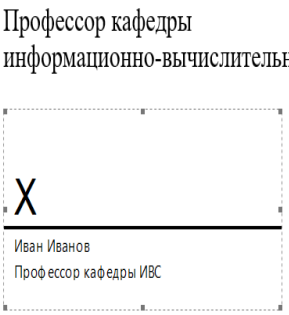

Рисунок 19 – Формируемые строки подписи после настройки

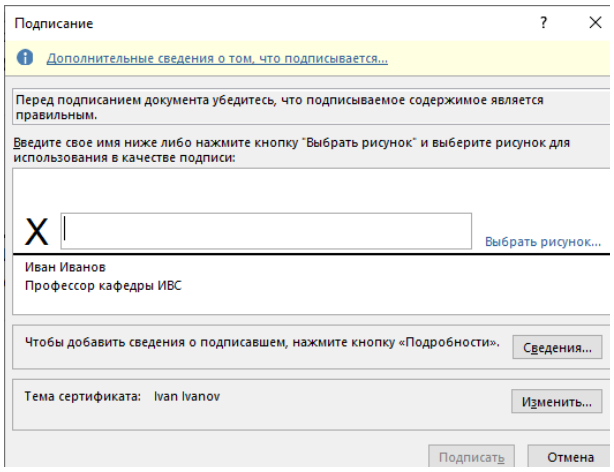

Рисунок 20 – Диалоговое окно Подписание

Кроме того, диалоговое окно *Подписание предлагает добавить сведения о подписавшем. После внесения дополнительных сведений данная информация отображается в диалоговом окне Подписание (рисунок 22).*

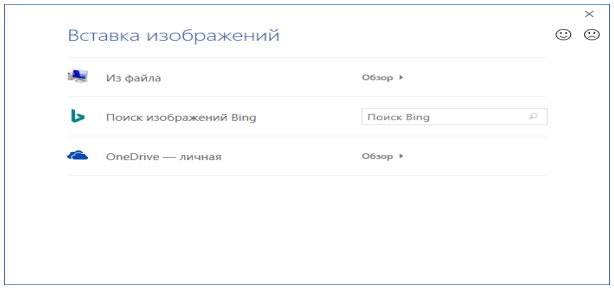

Рисунок 21 – Диалоговое окно Вставка изображений

После заполнения полей в диалоговом окне Подписание становится активной кнопка Подписать. Нажатие кнопки Подписать требует подтверждения в диалоговом окне Подтверждение подписи (рисунок 23). В диалоговом окне *Подтверждение подписи приводится сообщение о том, что «Подпись успешно сохранена вместе с документом. В случае изменения документа подпись станет недействительной». Данное свойство ЦП при подписании или утверждении документа на практике дает возможность на переработку УММ с повторным подписанием либо утверждением.*

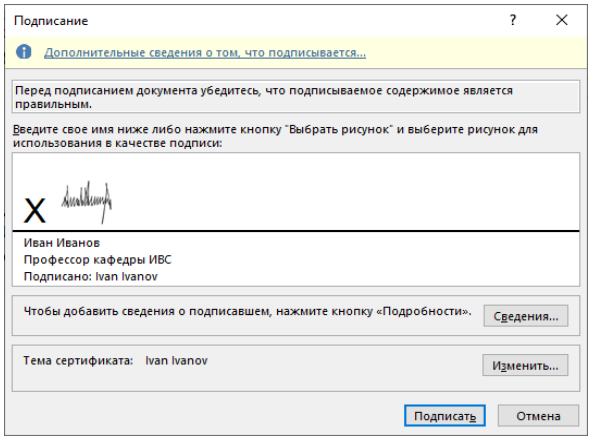

Рисунок 22 – Диалоговое окно Подписание с дополнительными сведениями о подписавшем

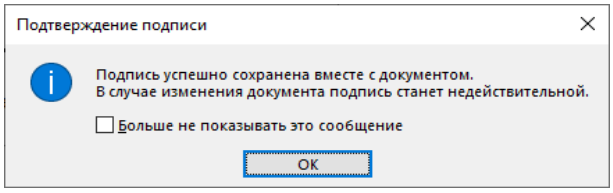

Рисунок 23 – Диалоговое окно Подтверждение подписи

Один из вариантов ЦП приведен на рисунке 24. В качестве графического изображения на ЦП приведено факсимиле.

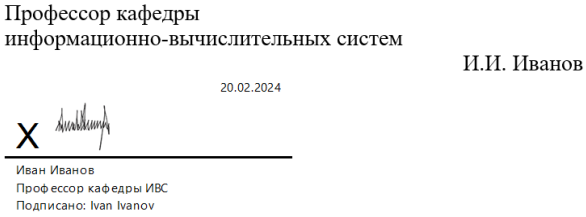

Рисунок 24 – Диалоговое окно Подтверждение подписи

При необходимости посмотреть сведения о подписавшем и сертификате ключа, необходимо войти в контекстное меню ЦП и выбрать вкладку Состав подписи. В результате откроется диалоговое окно Состав подписи, из которого можно получить всю необходимую информацию (рисунки 25– 27).

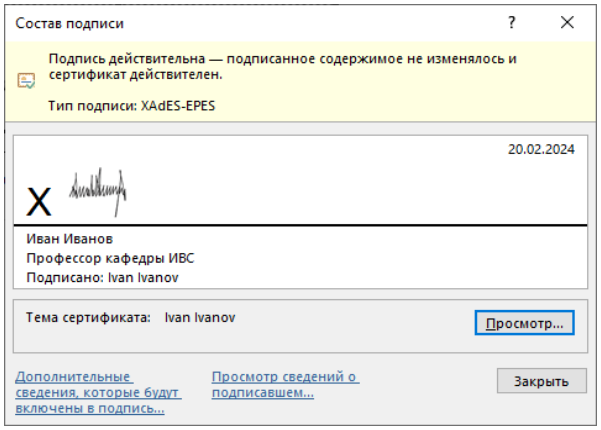

Рисунок 25 – Диалоговое окно Подтверждение

подписи

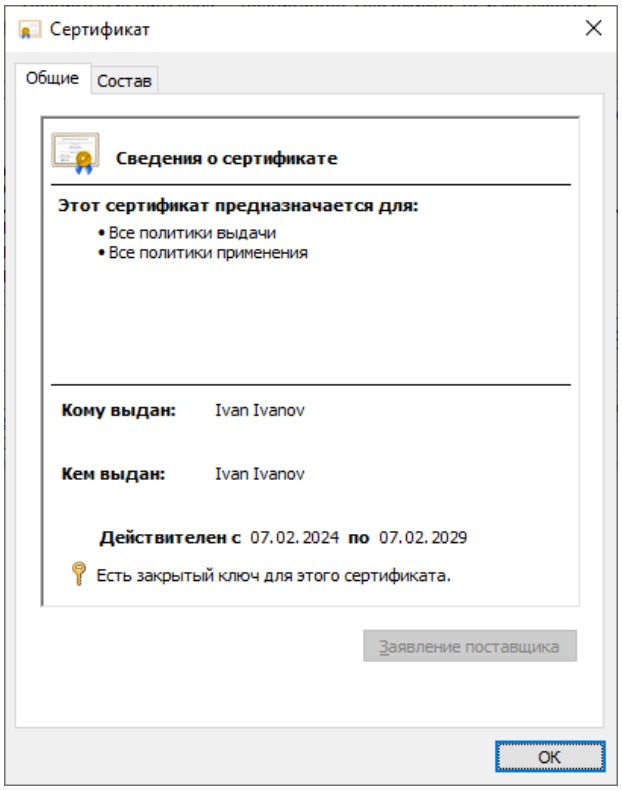

Рисунок 26 – Диалоговое окно Сертификат

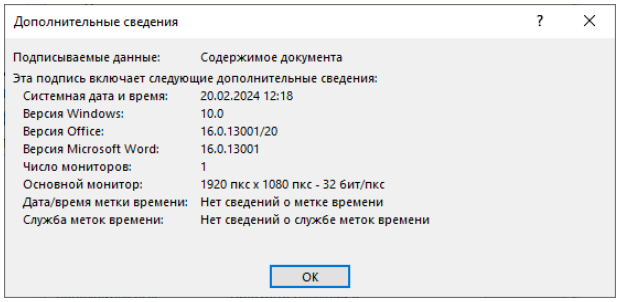

Рисунок 27 – Диалоговое окно Дополнительные сведения

Таким образом, после постановки ЦП на документе отображается видимая цифровая подпись с соответствующей информацией, подтверждающей что документ подписан или утвержден и после подписания не изменялся.

Кроме того, в сведениях о документе, подписанном с помощью ЦП, приводится специфическая информация (рисунок 28). Сведения сообщают, что «документ подписан и помечен как окончательный. В случае изменения этого документа кем-либо подписи станут недействительными».

При необходимости продолжить редактирование документа необходимо выбрать команду *Все равно редактировать, которая отображается снизу под лентой. После выбора этой команды все сведения о ЦП и сама видимая ЦП из документа удаляются.*

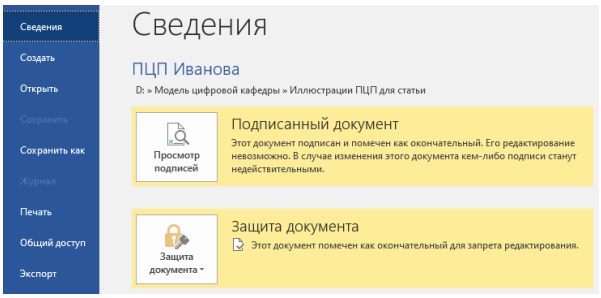

Рисунок 28 – Сведения о документе, подписанном ЦП

Таким образом, на пути перевода учебно-методических материалов и учебно-программной документации в безбумажную среду такой формальный момент, как подпись и утверждение документов, может быть реализован с помощью простой цифровой подписи. Простая цифровая подпись может создаваться в таком, например, приложении как Adobe Acrobar Pro, область ее применения без особых сложностей может быть распространена на документы MS Office. Кроме того, должен быть определен правовой статус простой цифровой подписи.

Литература

1. Федеральный закон Российская Федерация от 6 апреля 2011 года № 63-ФЗ. Об электронной подписи.

2. Закон Республики Беларусь от 28 декабря 2009 г. № 113-З. Об электронном документе и электронной цифровой подписи.

MS OFFICE DOCUMENT SIGNING TECHNOLOGY SIMPLE DIGITAL SIGNATURE

M.K. Kutsyin

Military Academy of the Republic of Belarus, Minsk, Belarus, kutin1957@mail.ru

Annotation. The technology of signing MS Word documents using a digital signature created in the Adobe Acrobat Pro application is considered in order to transfer educational materials and educational program documentation to a paperless environment.

Keywords. Digital ID, digital public key certificate, digital signature.