R301 ФОРОС USB, смарт-карта ФОРОС для Windows
Руководство пользователя

ООО СмартПарк
2021

Оглавление

1 Общее описание

Носитель R301 ФОРОС USB/смарт-карта ФОРОС для Windows (далее - Форос-Windows) предназначен для применения в качестве персонального электронного идентификатора в ОС Windows (7, 8.1, 10) в рамках информационной технологии компании Microsoft.

Аутентификация при помощи Форос-Windows позволяет кардинально повысить безопасность системы, снижает риск несанкционированного доступа. Использование Форос-Windows позволяет внедрить двухфакторную аутентификацию в следующие сценарии использования:

- аутентификация при входе в ОС Windows (winlogon);
- аутентификация в VPN-соединениях;
- аутентификация при доступе к удаленному рабочему столу по протоколу RDP;
- аутентификация при доступе к интернет ресурсам.

Также Форос-Windows можно использовать для:

- защиты электронной почты в Microsoft Outlook;
- подписи документов Microsoft Office;
- подписи pdf документов;
- шифрования отдельных файлов и целиком разделов жестких дисков (EFS, BitLocker).

Форос-Windows обеспечивает неизвлекаемость ключевой информации из носителя. Неизвлекаемость означает, что ключ применяется исключительно внутри микроконтроллера Форос-Windows и не может попасть на жёсткий диск компьютера или в оперативную память. При этом для применения Форос-Windows требуется знание ПИН-кода пользователя. Для защиты от подбора значения ПИН-кода присутствует механизм блокировки ПИН-кода. При 5 неверных попытках подряд ввести ПИН-код он заблокируется.

Для всех применений Форос-Windows, кроме шифрования EFS, требуется, чтобы компьютер, на котором применяется Форос-Windows, был членом домена. Соответственно должен быть сервер являющийся контроллером домена и сервер являющийся центром сертификации.

2 Перед применением

Процедура установки драйверов Форос-Windows описана в Руководстве администратора (раздел 2).

Перед непосредственным применением пользователем Форос-Windows

его необходимо персонализировать, то есть записать ключ и сертификат. Данная процедура описана в Руководстве администратора.

Для обеспечения безопасности пользователь должен сменить транспортное значение ПИН пользователя Форос-Windows на рабочее. Для этого надо либо использовать административную утилиту UnblockForosWindows (её описание приведено в Руководстве администратора), либо это можно выполнить средствами Windows после установки драйверов Форос-Windows. Для этого необходимо подключить Форос-Windows к компьютеру, нажать сочетание клавиш Ctrl+Alt+Delete и выбрать опцию «Изменить пароль». После чего будет предложено ввести старый и новый ПИН-код. Минимальная длина ПИН-кода 4 символа, максимальная – 8 символов. ПИН-код может состоять из любых печатных символов.

Транспортное значение ПИН-код Пользователя, устанавливаемое производителем Форос-Windows: «11111111».

3 Вход в учетную запись Windows

Форос-Windows обеспечивает двухфакторную аутентификацию при входе в учетную запись Windows (физическое наличие носителя у Пользователя и знание Пользователем ПИН-кода пользователя). Для этого персонализированный Форос-Windows подключите к компьютеру, состоящему в том же домене, что и центр сертификации. Загрузите ОС. Выберите «Параметры входа» («Sign-in options») и затем выберите иконку смарт-карты.

ОС считает данные с Форос-Windows и выведет на экран имя пользователя. Введите ПИН-код.

При следующем входе в ОС опция использования Форос-Windows будет активна по умолчанию.

Таким образом, для входа в учетную запись пользователя необходимо наличие Форос-Windows и знание ПИН-кода.

4 Подпись и шифрования почты в Outlook

Используя Форос-Windows, на который записан сертификат и ключевая пара, пользователь может защитить свою электронную почту – подписать и зашифровать электронное сообщение.

Цифровая подпись сообщений позволяет подтвердить:

- личность отправителя
- что содержимое сообщения не было изменено после подписания

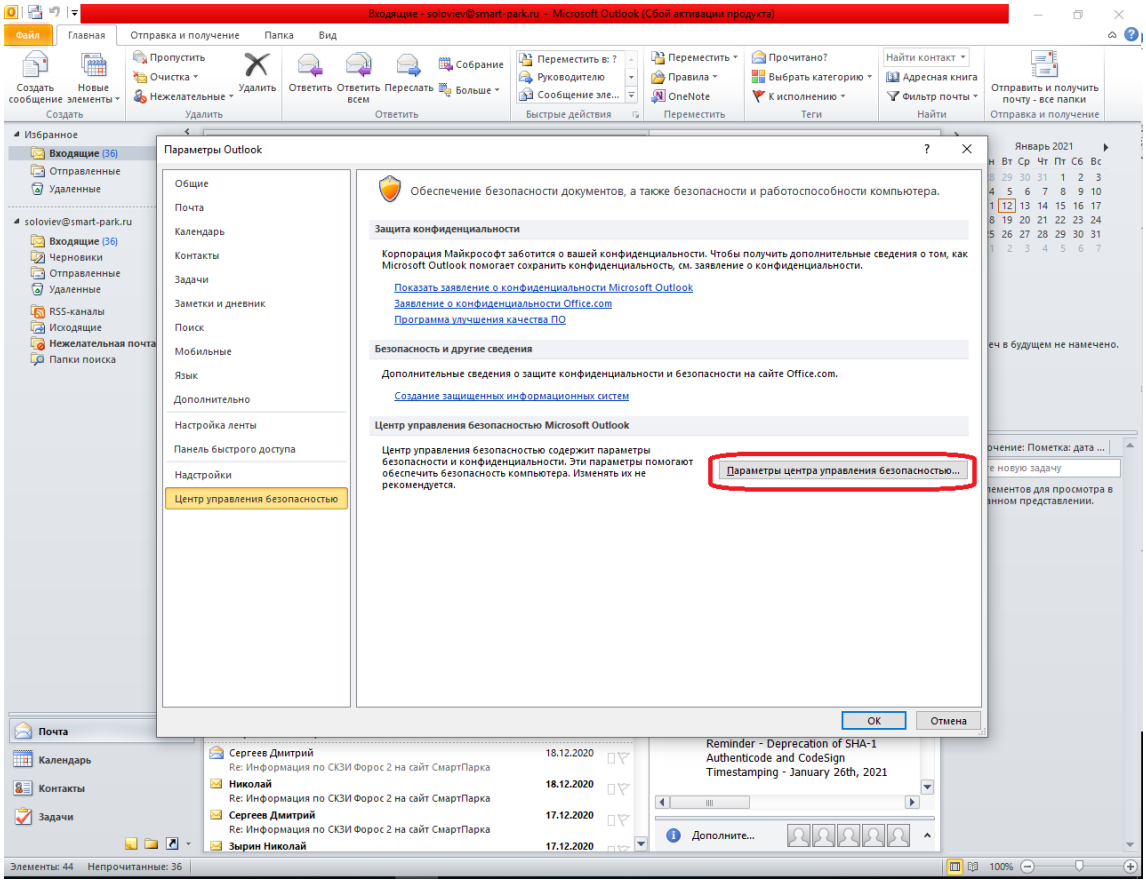
Цифровая подпись почтовых сообщений производится отправителем сообщения с использованием своего закрытого ключа. Получатель сообщения

при помощи открытого ключа может проверить цифровую подпись. Открытый ключ передаётся внутри сертификата, который прикладывается к подписанному сообщению. С помощью сертификата получатель также посмотреть информацию об отправителе.

Зашифрование электронного сообщения производится на открытом ключе получателя. Получатель расшифровывает полученное сообщение на своём закрытом ключе. Поэтому прежде чем шифровать сообщение, получатель и отправитель должны обменяться открытыми ключами. Обмен открытыми ключами производится путём отправки сообщения с электронной подписью и сертификатом.

Описание применения Форос-Windows приведено на примере Outlook 2010. В других версиях действия аналогичные. Пункты 1-5 касаются настройки Outlook. Их можно доверить администратору. Непосредственно описание применения Форос-Windows для подписи и шифрования сообщений начинается с пункта 6.

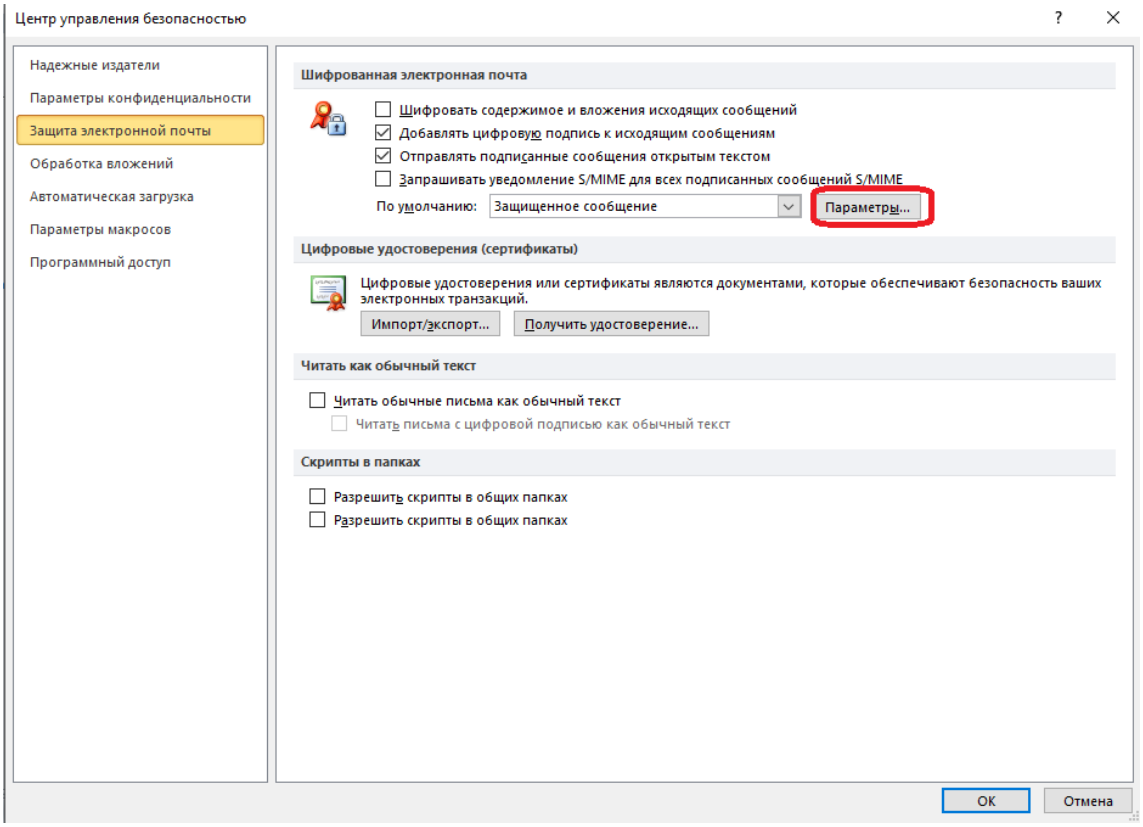
1. Выберите Файл->Параметры. В отобразившемся окне, в левом меню выберите «Центр управления безопасностью» и справа нажмите «Параметры центра управления безопасностью».



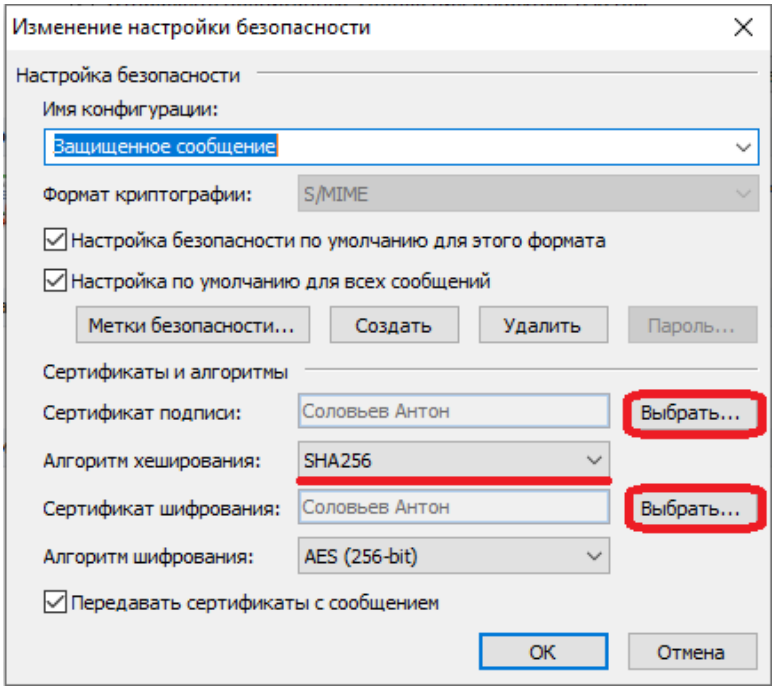
2. В окне Центр управления безопасностью выберите «Защита

электронных писем». Если необходимо включить подпись ко всем письмам по умолчанию, то отметьте пункт «Добавлять цифровую подпись к исходящим сообщениям».

3. Нажмите «Параметры».



4. В открывшемся окне выберите сертификат подписи и алгоритм хэширования. Если планируется использовать шифрование, то выберите алгоритм шифрования.



5. После нажатия на кнопку «Выбрать…» в открывшемся окне необходимо выбрать нужный сертификат. Нажмите ОК.

6. Создайте новое письмо. Заполните необходимые данные для отправки.

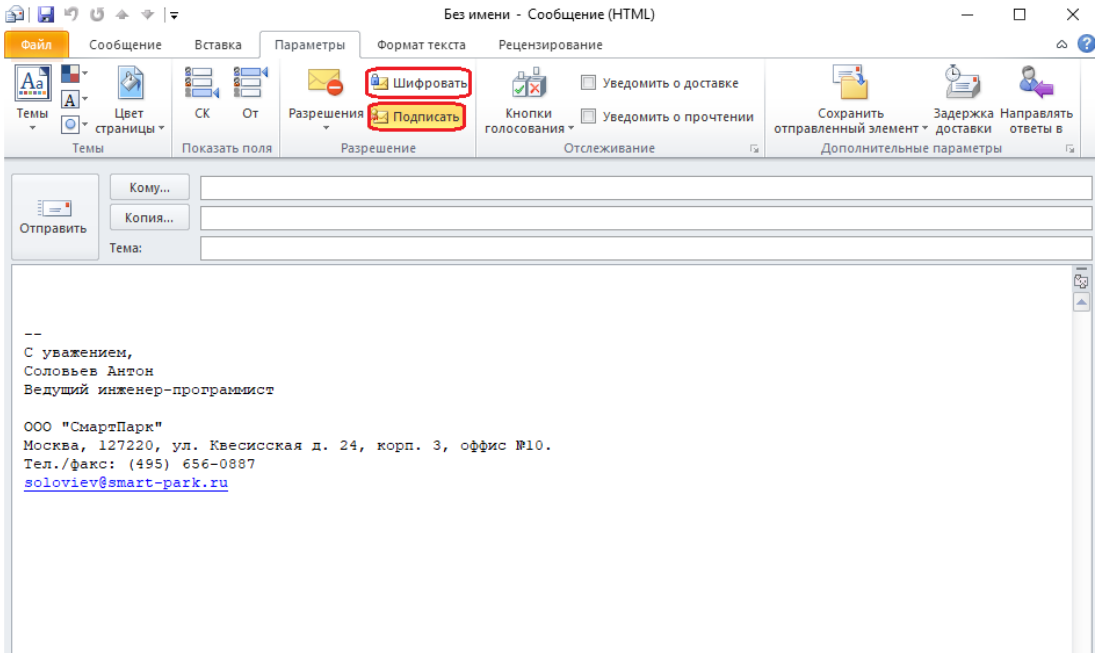
7. Выберите в верхнем меню «Параметры».

8. На открывшемся меню доступны две кнопки «Подписать» и «Шифровать». Если ранее был выбран пункт «Добавлять цифровую подпись к исходящим сообщениям», то кнопка «Подписать» уже будет активна. Соответственно на данном шаге можно включить/отключить подпись и шифрование сообщения.

9. Если настройки по умолчанию корректны и их менять не надо, то пункт 8 можно пропустить.

10. Убедитесь, что к компьютеру подключён Форос-Windows.

11. Нажмите кнопку «Отправить», появится окно ввода ПИН-кода. Введите ПИН-код и нажмите «ОК».



12. Подписанные письма будут отмечены специальным значком.

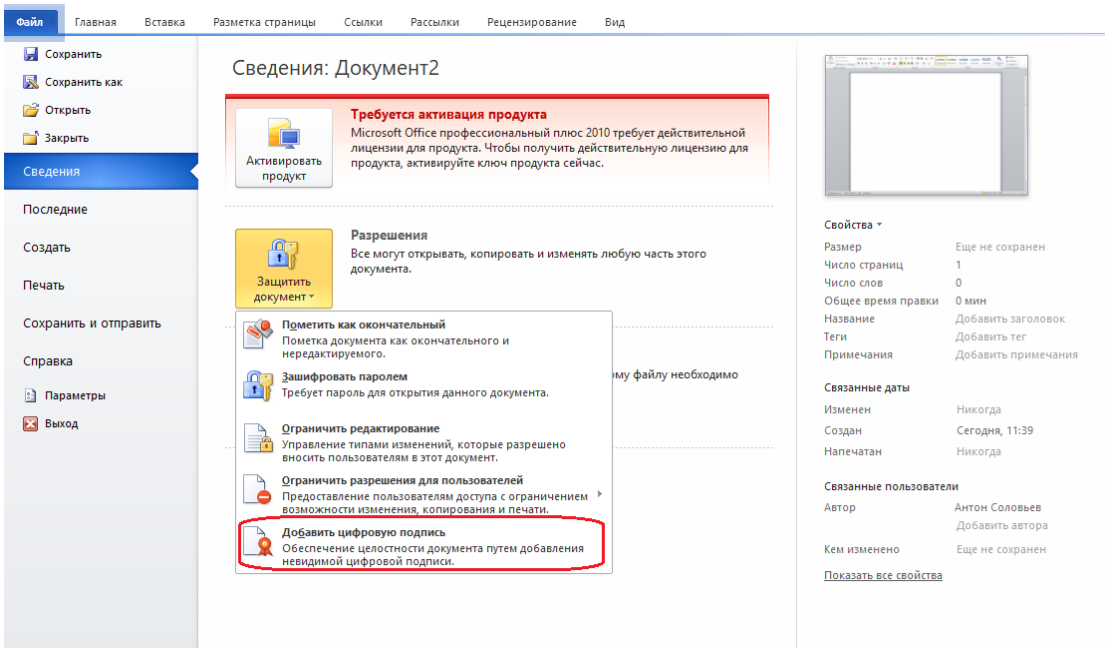
5 Цифровая подпись в Microsoft Office: Word, Excel, Power Point

К документам, созданным посредством программ Microsoft Office можно добавлять цифровую подпись.

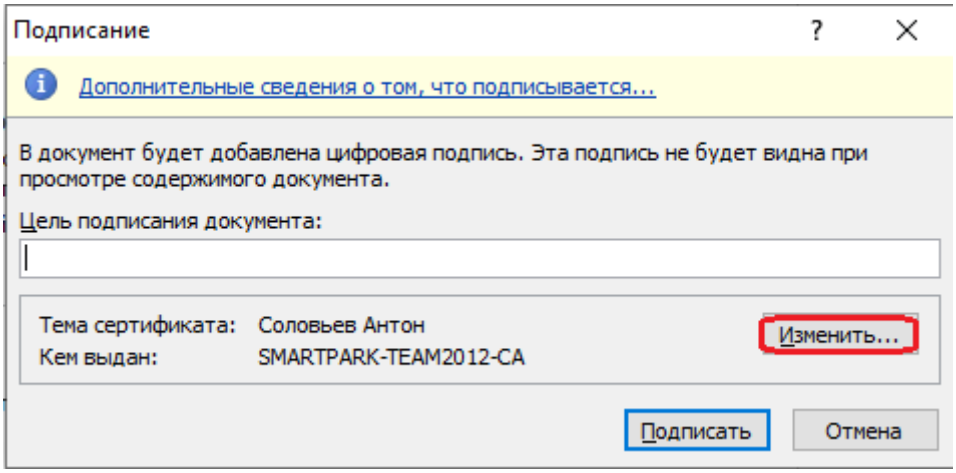
Цифровая подпись электронных документов позволяет убедиться, что содержимое данных документов не было изменено после процедуры подписания.

Описанный ниже пример дан на основе Word 2010, в остальных продуктах и версиях Microsoft Office цифровая подпись делается аналогично.

1. Откройте необходимый документ Microsoft Word.
2. Выберете меню «Файл->Сведения->Защитить документ->Добавить цифровую подпись»

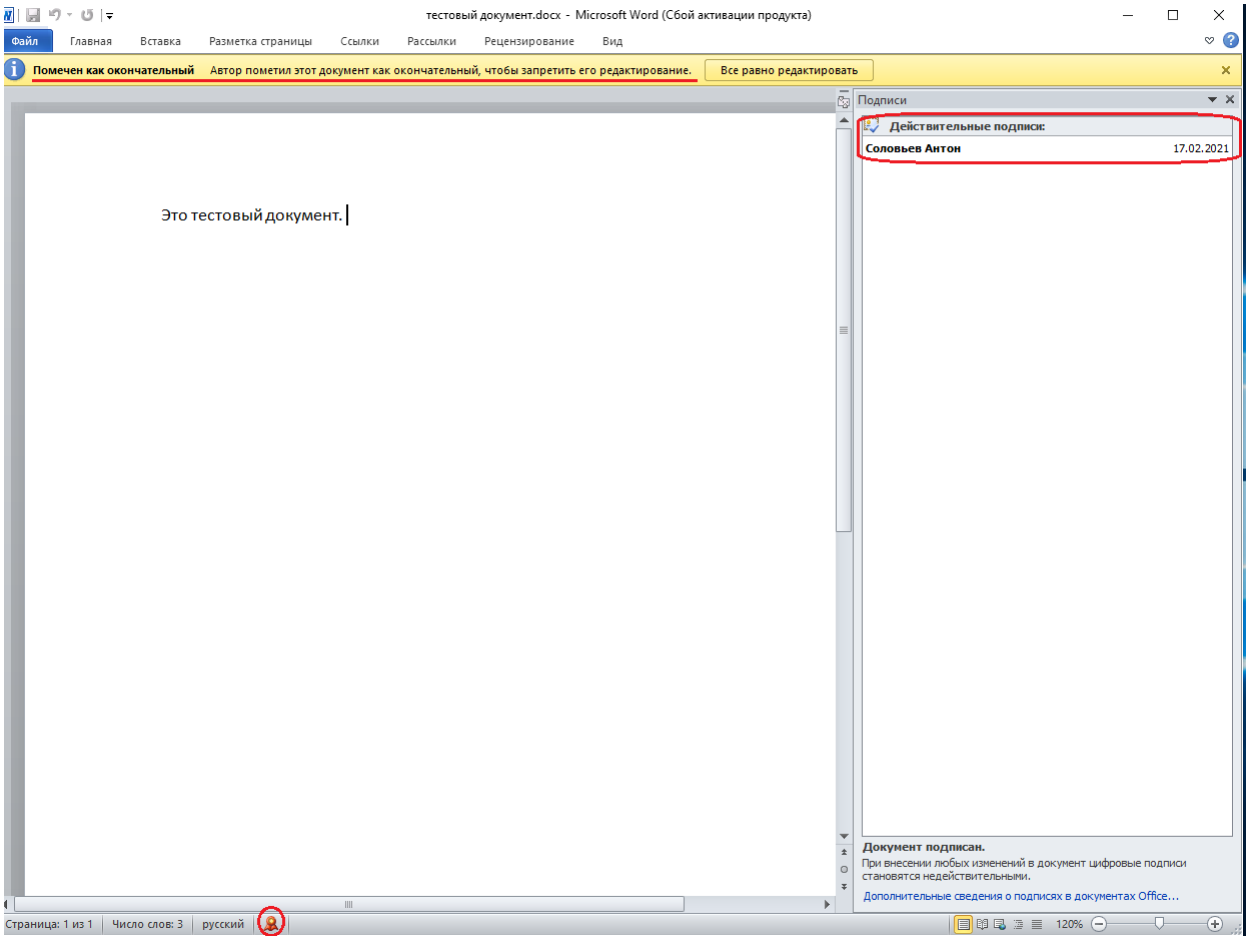


3. Появится окно «Подписание». С помощью кнопки «Изменить» можно выбрать сертификат, используемый для подписи документа.



4. Появится окно ввода ПИН-кода. Введите ПИН-код и нажмите «ОК».

5. В документе будет отображена информация, что он подписан и является окончательным. Можно посмотреть, кто подписал документ, сертификат подписавшего. Для этого необходимо выбрать «Файл->Сведения->Просмотр подписей» или кликнуть на иконку подписи внизу документа.



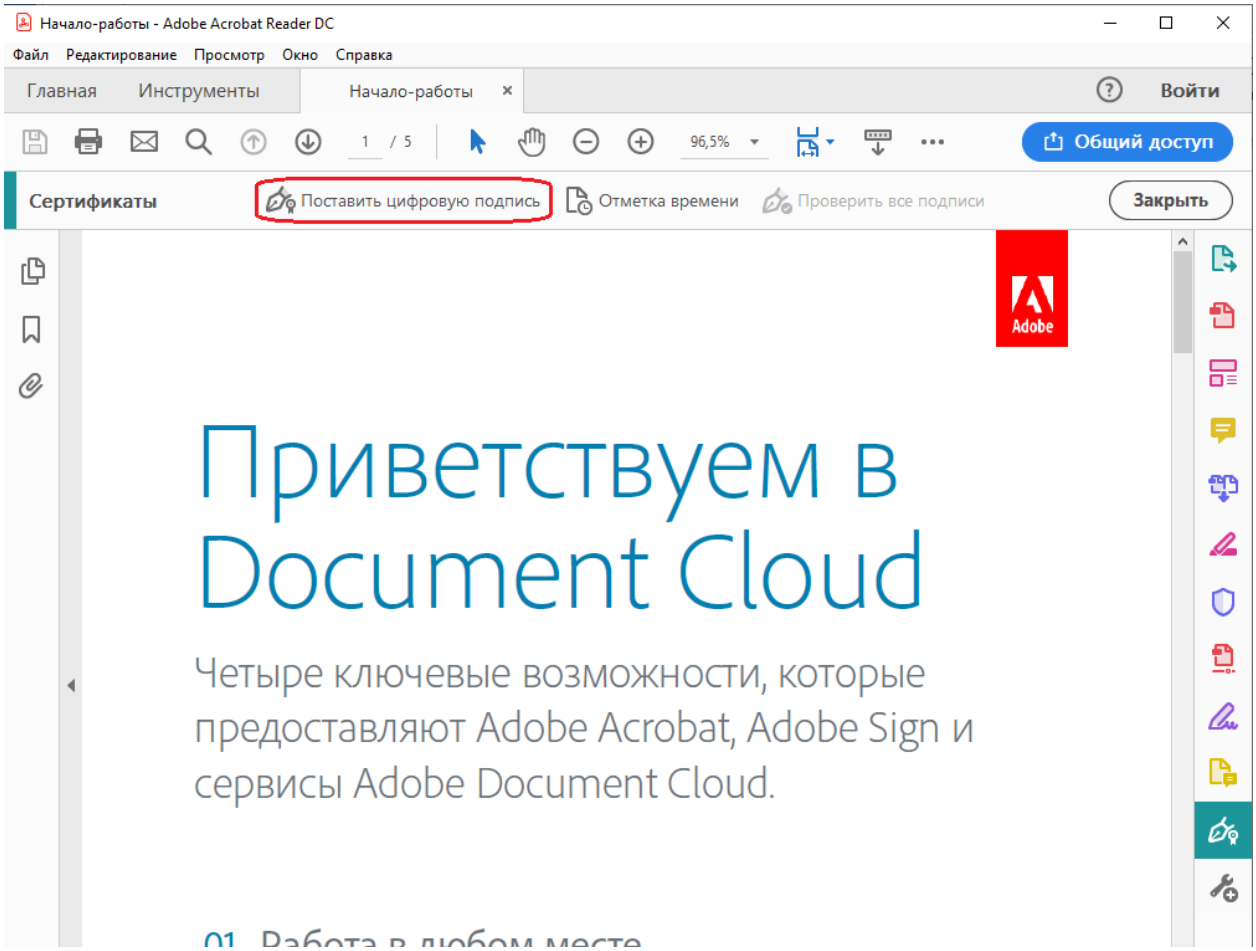
6 Цифровая подпись в Adobe Reader

К документам, созданным посредством программ Adobe Acrobat или Adobe Reader можно добавлять цифровую подпись.

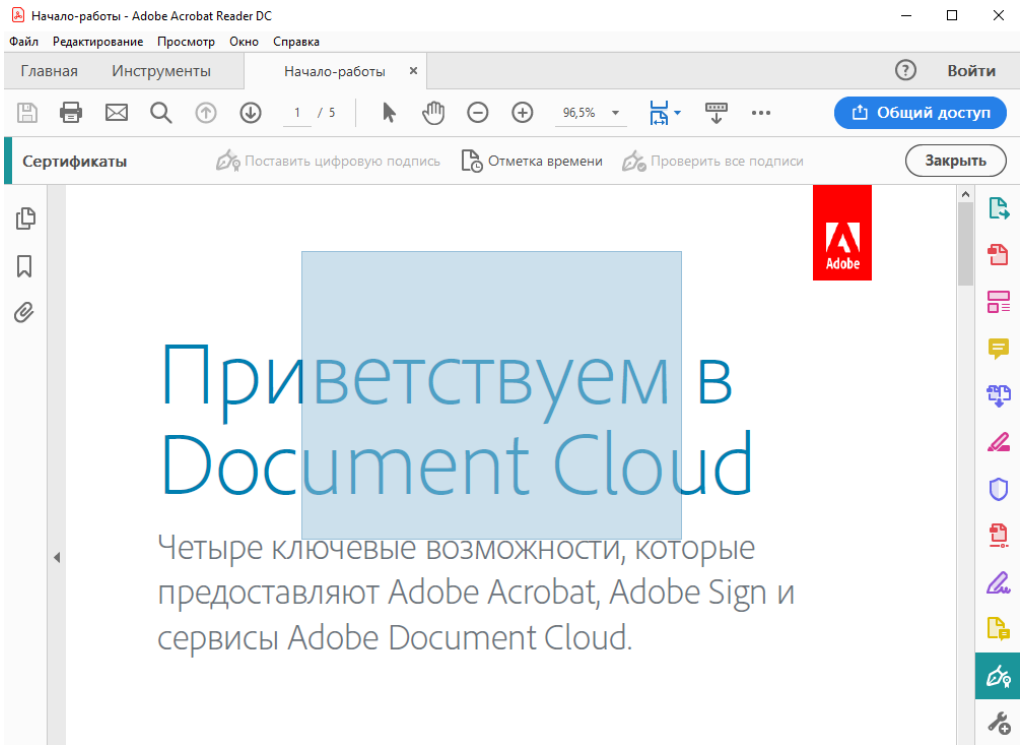
Подпись на основе сертификата, как и обычная подпись шариковой ручкой, идентифицирует лицо, подписавшее документ. В отличие от рукописной, такую подпись очень сложно подделать, так как она содержит зашифрованную, уникальную для подписывающего информацию. Получатели документа могут легко проверить подпись, а также определить, был ли документ изменен после того, как был подписан.

Описанный ниже пример дан на основе Adobe Acrobat Reader DC.

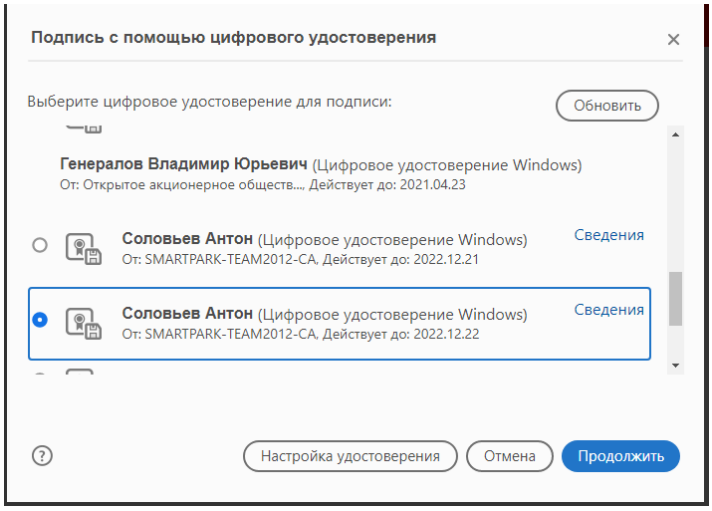
1. Откройте pdf документ, который необходимо подписать.
2. Выберите «Инструменты->Сертификаты».
3. Выберите меню «Поставить цифровую подпись»



4. Выделите область в подписываемом документе, где будет отображаться подпись.



5. Выберете необходимый сертификат для подписи. Нажмите «Продолжить»



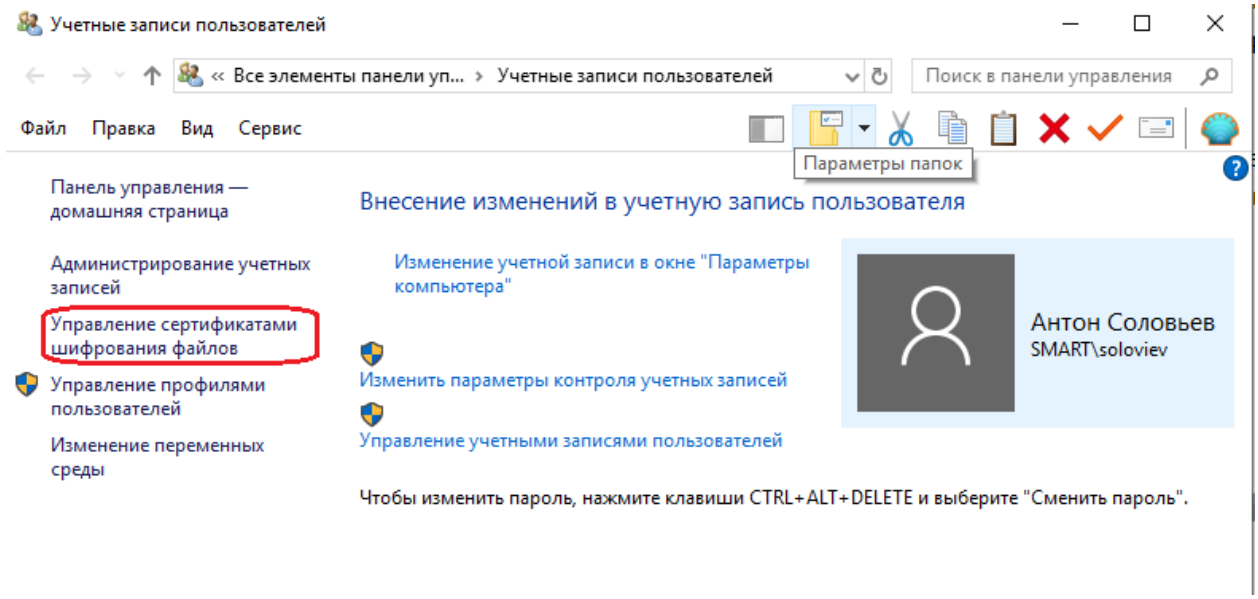
6. Настройте оформление подписи и завершите процесс подписи, введите ПИН-код.

7 Шифрование данных EFS

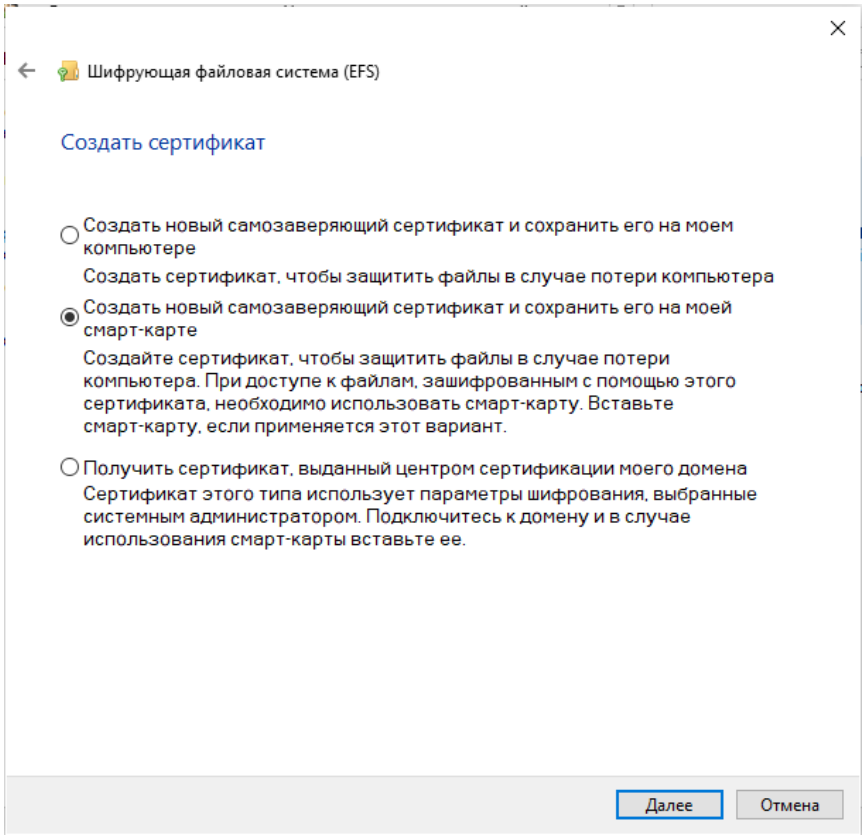
В Windows существует встроенная технология шифрования данных EFS. Эта технология позволяет шифровать каждый файл по отдельности. Помимо этого особенностью данной технологии является локальная работа, то есть пользователь сам создает ключ на Форос-Windows и никак не привязан к домену.

Данные, зашифрованные с помощью EFS, могут быть расшифрованы только с помощью той же самой учётной записи Windows, из-под которой было выполнено шифрование. Также для расшифровки будет необходимо подключить к компьютеру Форос-Windows и ввести ПИН-код.

1. Сначала необходимо выпустить и записать сертификат и закрытый ключ в Форос-Windows. Выберите «Пуск->Панель управления->Учетные записи пользователя». В открывшемся окне выберите «Управление сертификатами шифрования файлов».



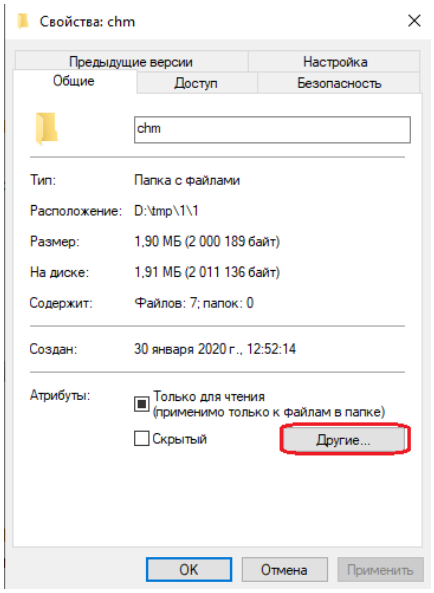
2. Если в Форос-Windows уже есть сертификат, то для дальнейшей работы можно использовать его. Необходимо нажать «Выбрать сертификат» и выбрать соответствующий. Можно создать новый сертификат на Форос-Windows. Для этого необходимо выбирать «Создать новый сертификат» и нажать «Далее». В окне «Создать сертификат» выберите самозаверяемый сертификат с сохранением его на смарт-карте и нажмите «Далее».



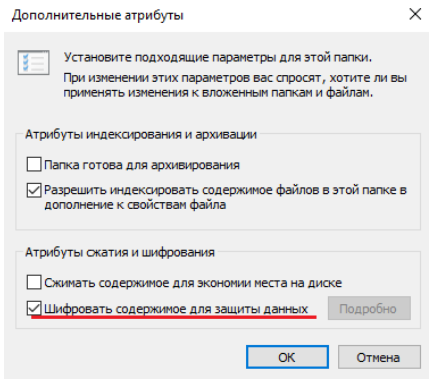
3. Введите ПИН-код смарт-карты.

4. В дальнейших окнах можно обновить ранее зашифрованные файлы, данную опцию в примере пропускаем.

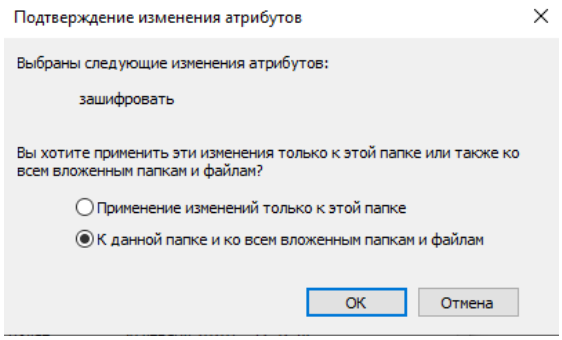
5. Далее необходимо указать файл или директорию, которая будет зашифрована со всем содержимым, можно зашифровать весь диск со всеми вложенными директориями. Щёлкните правой кнопкой по директории и выберите «Свойства». Затем нажмите «Другие».



6. В открывшемся окне выберите «Шифровать содержимое для защиты данных» и нажмите «ОК».



7. Затем нажмите «Применить». В открывшемся окне выберите «К данной папке и ко всем вложенным папкам и файлам». И нажмите «ОК».



8. Чтобы проверить корректную работу шифрования файлов, выйдете из системы и войдите без Форос-Windows. Перейдите в зашифрованную

директорию и попробуйте открыть какой-либо файл. Если все настройки сделаны верно, отобразится предложение вставить смарт карту.

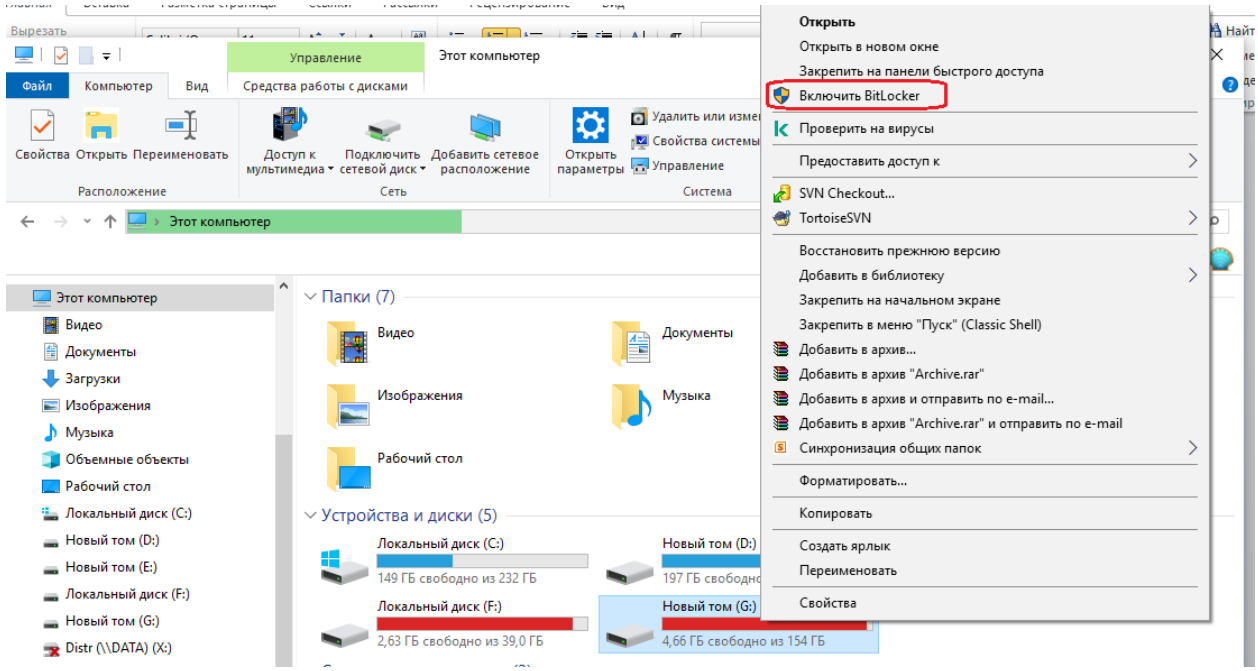
8 Шифрование данных BitLocker

Во всех операционных системах Microsoft Windows существует встроенная технология шифрования разделов жёстких дисков — BitLocker. Данная технология предназначена для шифрования разделов жесткого диска целиком. Есть возможность зашифровать целиком внешний носитель.

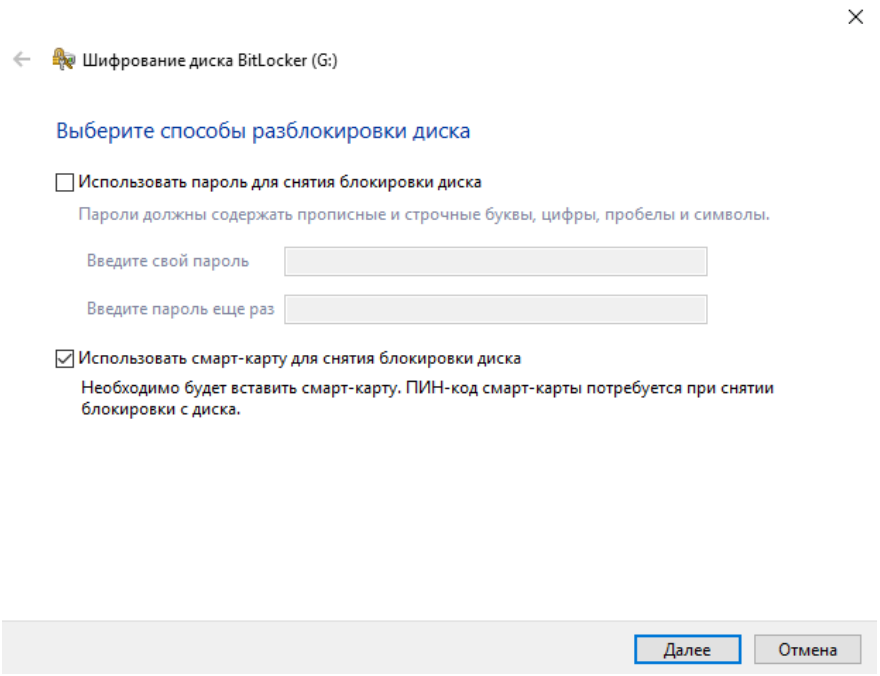
Шифрование производится посредством алгоритма AES. Ключ шифрования можно безопасно хранить на Форос-Windows.

BitLocker в отличии от EFS-шифрования работает только в рамках домена. Требуется наличие сервера и локальная работа технологии невозможна.

1. Откройте Проводник. Выберите диск, который необходимо зашифровать.
2. Щёлкните правой кнопкой диск, в отобразившемся меню выберите «Включить BitLocker».



3. Отметьте «Использовать смарт-карту для снятия блокировки диска», нажмите «Далее».



4. В появившемся окне выберите способ сохранить ключ восстановления, в файл или отправить на печать. Этот ключ можно будет использовать для разблокировки диска в случае утери Форос-Windows.
5. Следующим шагом укажите, какую часть диска требуется зашифровать. Шифровать только занятое место на диске или весь диск.
6. Нажмите «Начать шифрование».
7. Будет отображаться трока состояния шифрования диска.
8. Когда процесс шифрования завершиться, будет выведено соответствующее сообщение и появится кнопка «Закрыть».
9. Перезагрузите компьютер. После перезагрузки подключите Форос-Windows к компьютеру. Откройте проводник.
10. Около зашифрованного диска должен появится значок замка. Щёлкните на данный диск и выберите вариант разблокировки «смарт-карта». Введите ПИН-код.
11. Содержимое диска должно открыться, в значок диска должен измениться на открытый замок.