

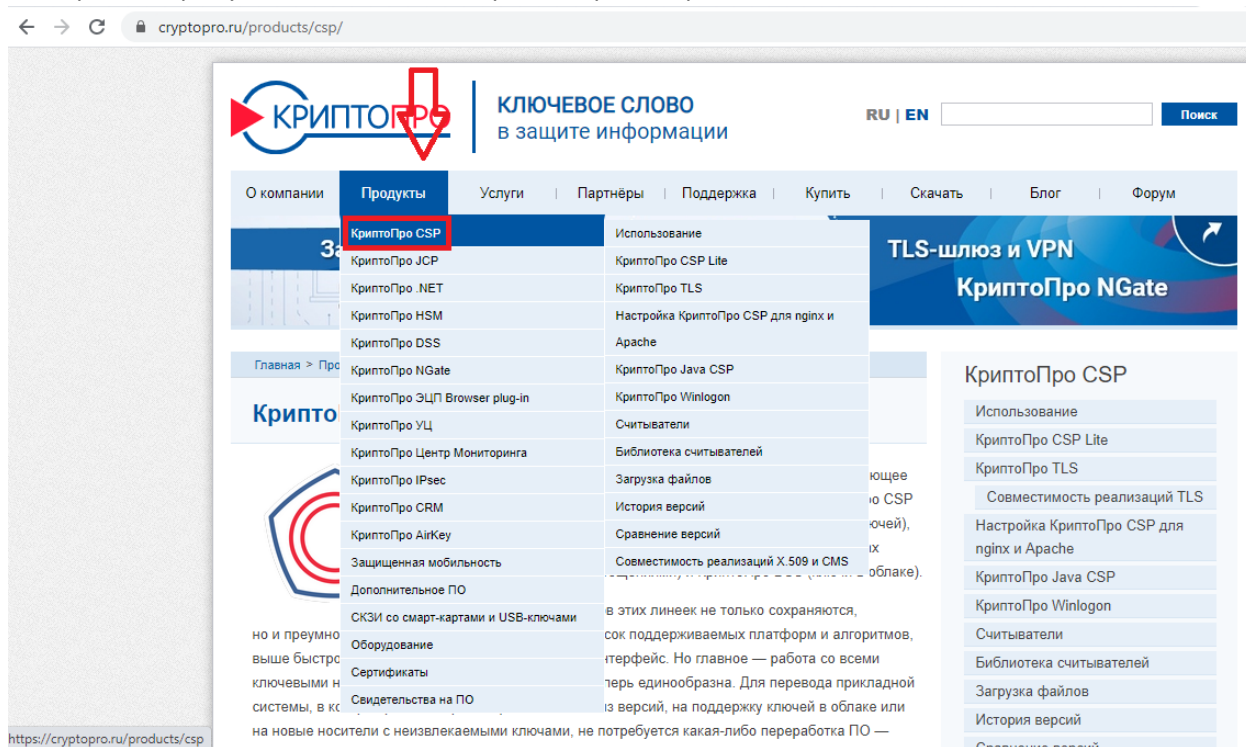
Шифрование заявления сертификатом электронной подписи.

1. Скачать заявление с сайта <http://medcol-ptz.ru/>. Для этого переходим на сайт. Входим во вкладку «Аккредитация специалистов» скачиваем «Заявление» и заполняем.

2. Скачать и установить крипто провайдер, он нам потребуется для подписания заявления.

<https://www.cryptopro.ru/> Потребуется зарегистрироваться на сайте.

Выбираем «Продукты», из меню выбираем «КриптоПро CSP»



3. Нажимаем большую синюю кнопку «Скачать КриптоПро CSP».

КриптоПро CSP



КриптоПро CSP 5.0 — новое поколение криптопровайдера, развивающее три основные продуктовые линейки компании КриптоПро: КриптоПро CSP (классические токены и другие пассивные хранилища секретных ключей), КриптоПро ФКН CSP/Рутокен CSP (неизвлекаемые ключи на токенах с защищенным обменом сообщениями) и КриптоПро DSS (ключи в облаке).

Все преимущества продуктов этих линеек не только сохраняются, но и преумножаются в КриптоПро CSP 5.0: шире список поддерживаемых платформ и алгоритмов, выше быстродействие, удобнее пользовательский интерфейс. Но главное — работа со всеми ключевыми носителями, включая ключи в облаке, теперь единообразна. Для перевода прикладной системы, в которой работал КриптоПро CSP любой из версий, на поддержку ключей в облаке или на новые носители с неизвлекаемыми ключами, не потребуется какая-либо переработка ПО — интерфейс доступа остается единым, и работа с ключом в облаке будет происходить точно таким же образом, как и с классическим ключевым носителем.



Скачать КриптоПро CSP

4. Откроется новая страница сайта с лицензионным соглашением. Чтобы скачать программу нажимаем кнопку «Я согласен с Лицензионным соглашением. Перейти к загрузке».

Контрольная сумма md5 может быть проверена, например, с помощью md5sum (linux) или File Checksum Integrity Verifier (<http://support.microsoft.com/kb/841290>).

Использование программного обеспечения регламентируется приведенным ниже Лицензионным соглашением с ООО "КРИПТО-ПРО":


ВНИМАТЕЛЬНО ОЗНАКОМЬТЕСЬ С ЛИЦЕНЗИОННЫМ СОГЛАШЕНИЕМ НА ИСПОЛЬЗОВАНИЕ ИЗДЕЛИЯ

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ

1. Исключительные права на программу для ЭВМ, включая документацию в электронном виде, (далее – Изделие) принадлежат ООО «КРИПТО-ПРО», далее – Правообладатель.
2. Настоящее соглашение является офертой ООО «КРИПТО-ПРО» к физическому или юридическому лицу, далее – Пользователь.
3. Пользователь в соответствии с настоящим соглашением получает право использовать Изделие на территории Российской Федерации.
4. Установка Изделия в память ЭВМ рассматривается как безусловное согласие Пользователя с условиями настоящего соглашения.
5. В случае несогласия с каким-либо из условий настоящего соглашения Пользователь не имеет права продолжать установку Изделия в память ЭВМ, а в случае установки Изделия в память ЭВМ обязан удалить Изделие из ЭВМ.

Я согласен с Лицензионным соглашением. Перейти к загрузке.

5. Переходим на новую страницу. Где нажимаем кнопку «Скачать для Windows»



КЛЮЧЕВОЕ СЛОВО
в защите информации


RU | EN

Поиск

О компании | Продукты | Услуги | Партнёры | Поддержка | Купить | Скачать | Блог | Форум

Защищённый доступ

к корпоративным ресурсам
через незащищённые сети



TLS-шлюз и VPN

КриптоПро NGate

Главная > Продукты > КриптоПро CSP

КриптоПро CSP - Загрузка файлов

Актуальная версия криптопровайдера

Скачать для Windows

▼

Сертифицированные и другие версии опубликованы ниже

Предварительные несертифицированные версии

КриптоПро CSP 5.0 R2 для Windows, macOS, UNIX и Android (несертифицированный)

КриптоПро CSP 4.0 R5 для Windows, macOS и UNIX (несертифицированный)

КриптоПро CSP

Использование

КриптоПро CSP Lite

КриптоПро TLS

Совместимость реализаций TLS

Настройка КриптоПро CSP для
nginx и Apache

КриптоПро Java CSP

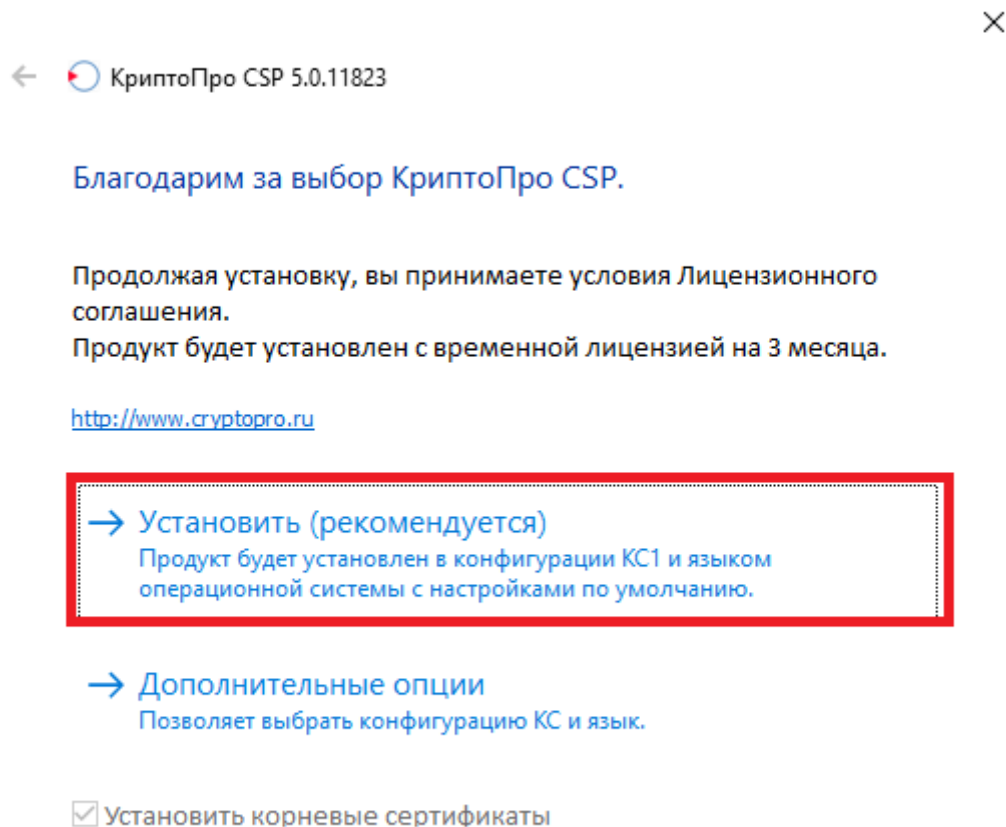
КриптоПро Winlogon

Считыватели

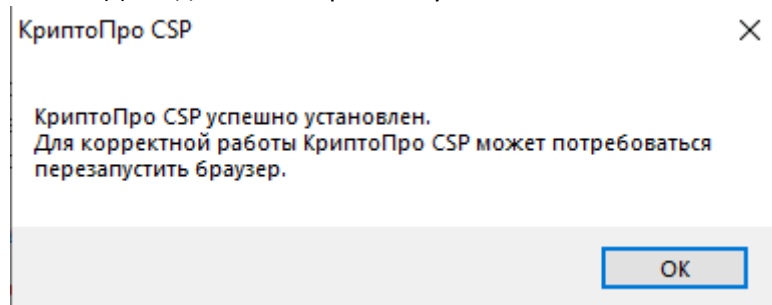
Библиотека считывателей

Загрузка файлов

6. Запускаем скачанную программу. Выбираем «Установить (рекомендуется)»

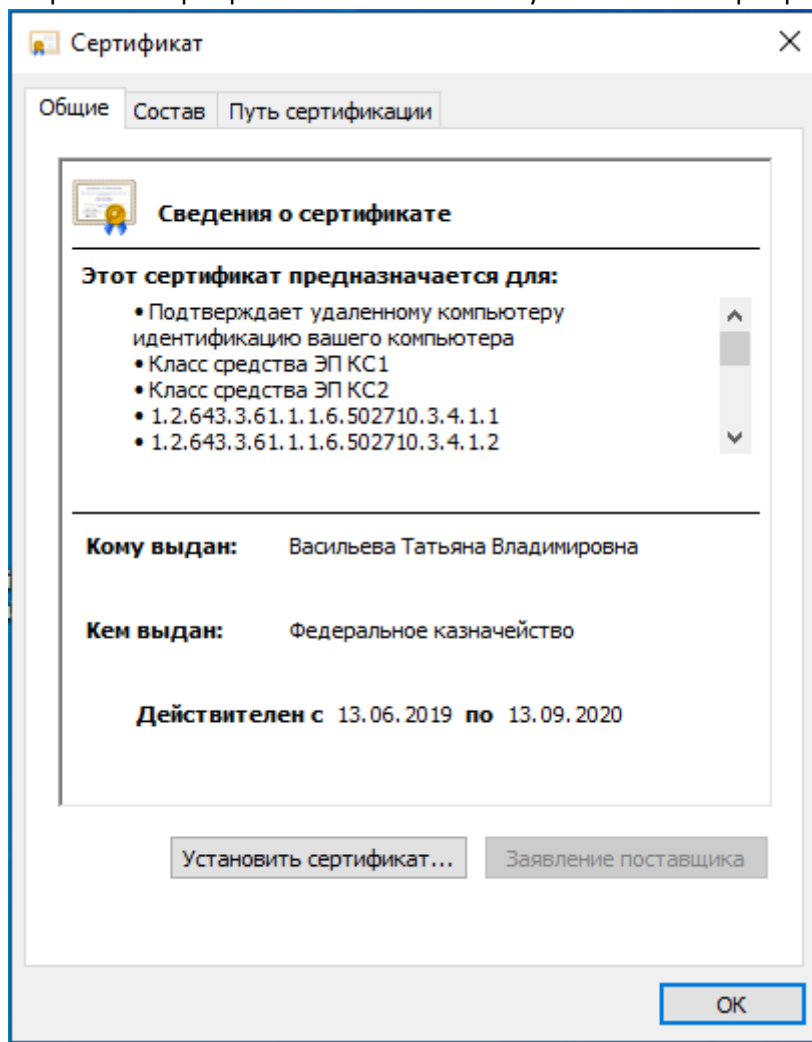


7. Дожидаемся завершения установки и нажимаем «ОК»

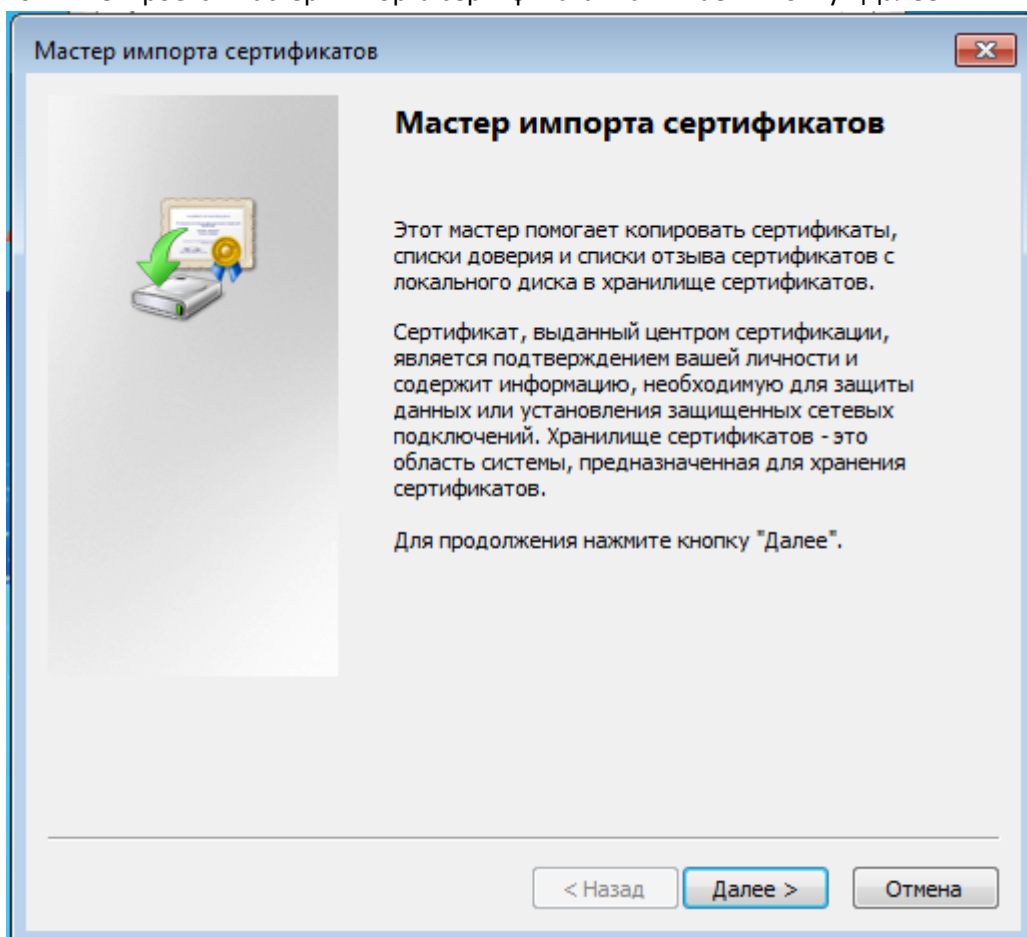


8. Скачиваем с сайта Коледжа сертификат электронной подписи по [ссылке](#). На этом сертификате будем подписывать документы для поступления.

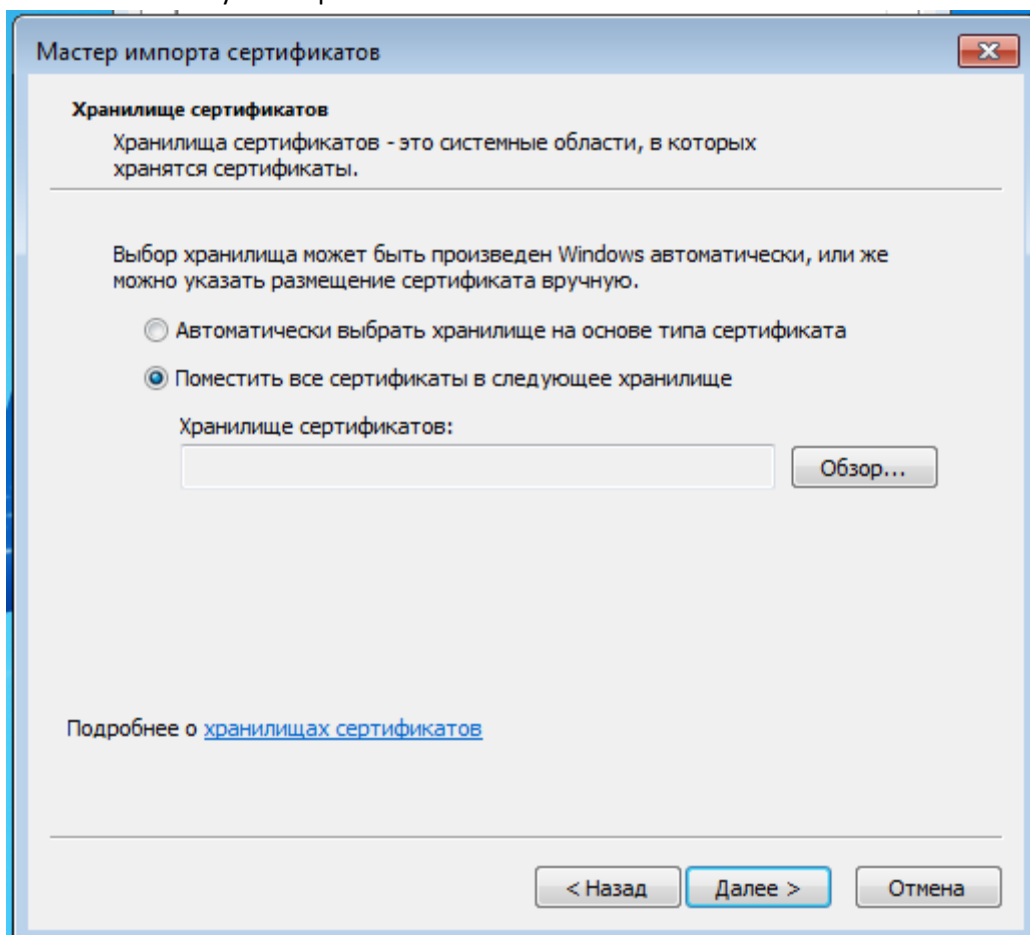
9. Устанавливаем сертификат в хранилище личных сертификатов. Для этого двойным кликом открываем сертификат. Нажимаем кнопку «Установить сертификат».



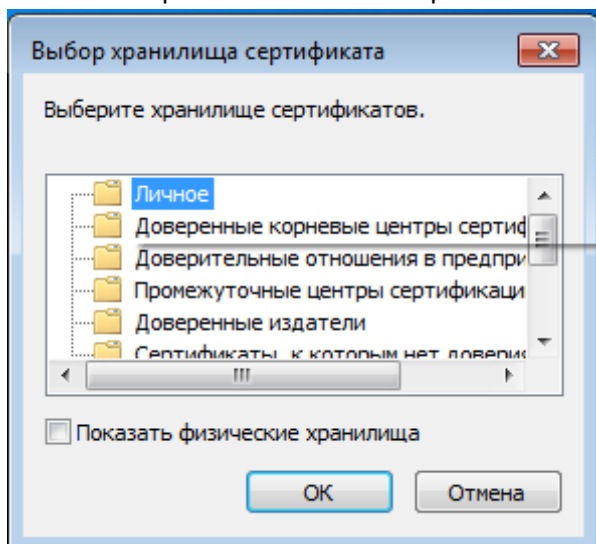
10. Откроется мастер импорта сертификата. Нажимаем кнопку «Далее».



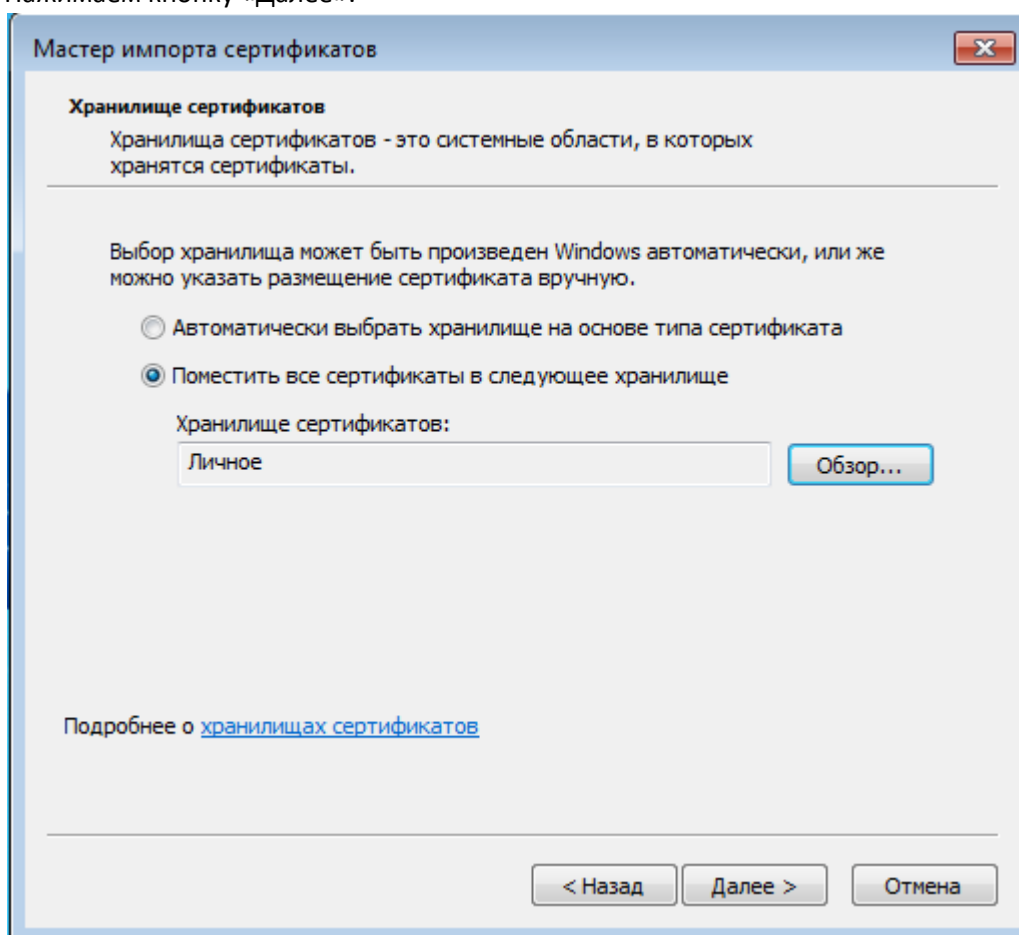
11. В следующем окне выбираем «Поместить все сертификаты в следующее хранилище». Нажимаем кнопку «Обзор».



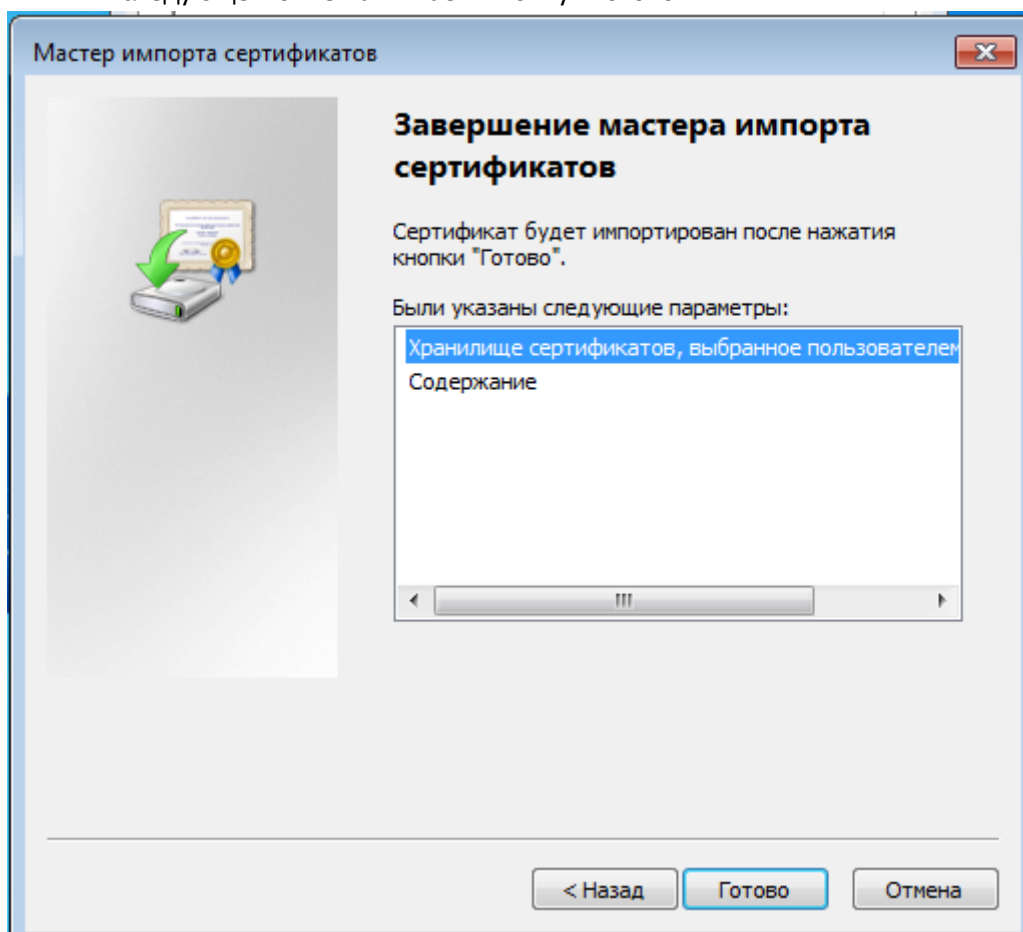
12. В открывшемся окне выбираем «Личное». Нажимаем кнопку «ОК».



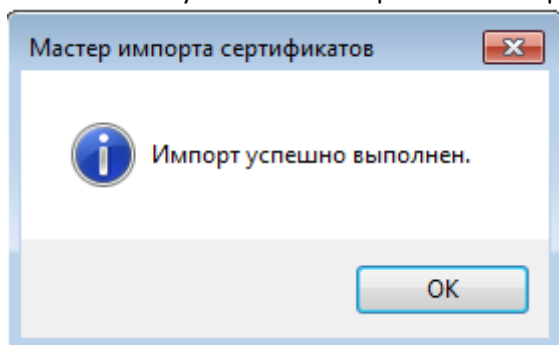
13. Убеждаемся что в поле «Хранилище сертификатов» появилась надпись «Личное». Нажимаем кнопку «Далее».



14. В следующем окне нажимаем кнопку «Готово».

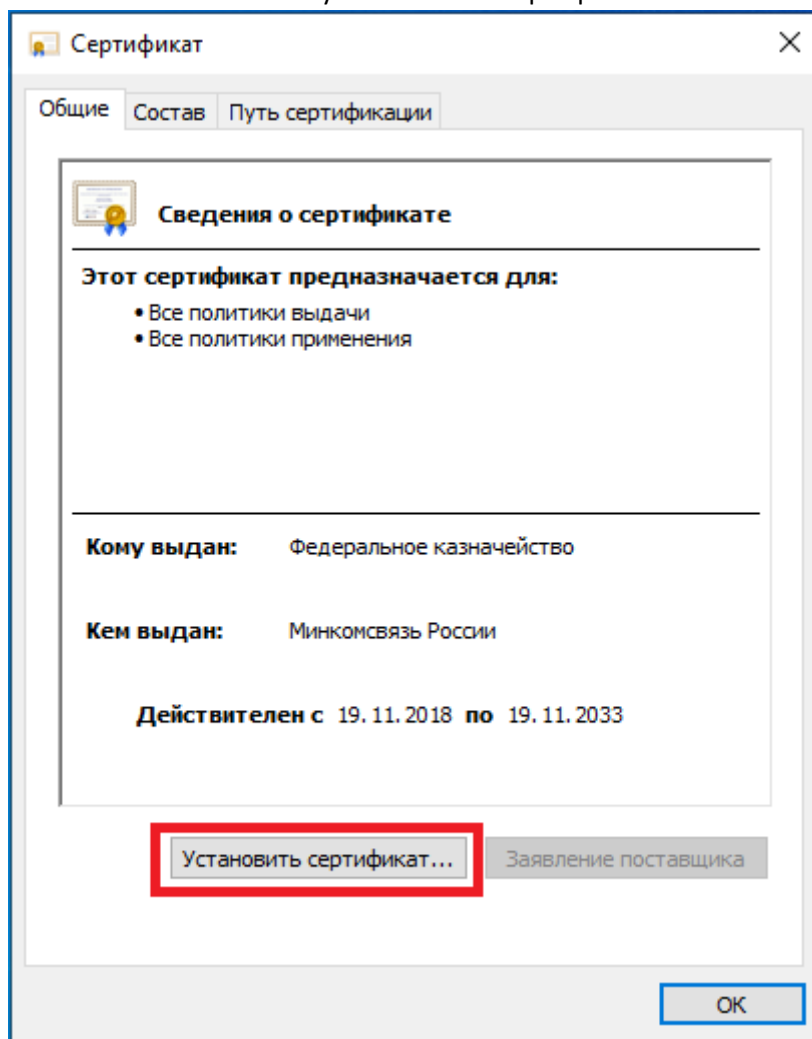


15. После успешного завершения импорта сертификата появится окно. Нажимаем «Ок».



16. Скачиваем сертификат для «Федерального казначейства» [ссылка](#) и повторим процедуру установки с небольшими изменениями.

17. Нажимаем кнопку «Установить сертификат...»



18. Убеждаемся что выбран «Текущий пользователь» и нажимаем кнопку «Далее».



←  Мастер импорта сертификатов

Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

☒ Текущий пользователь

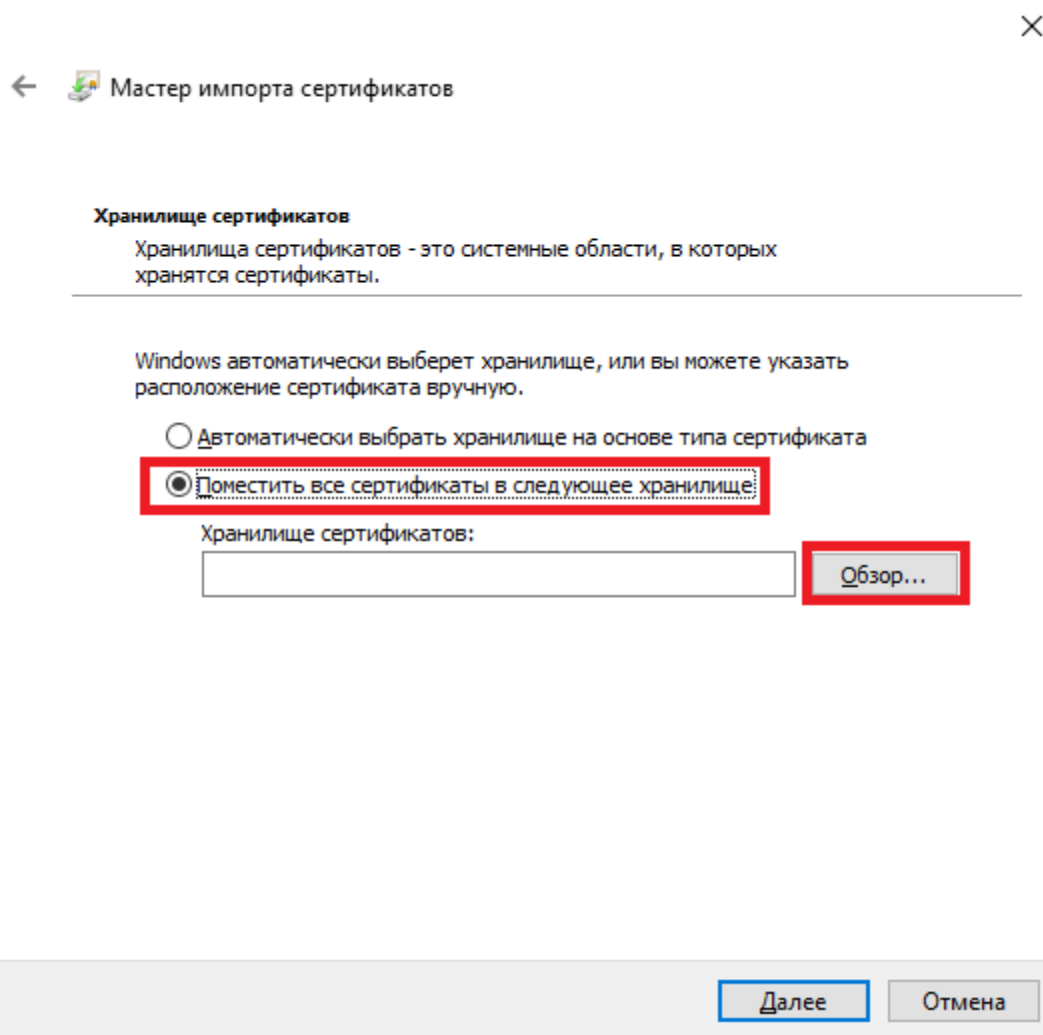
☐ Локальный компьютер

Для продолжения нажмите кнопку "Далее".

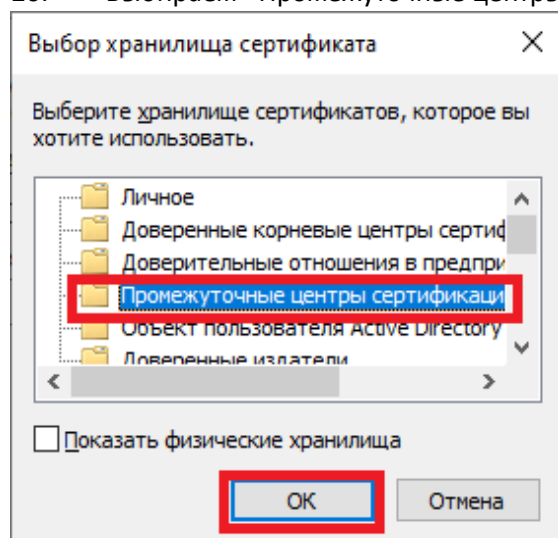
Далее

Отмена

19. Выбираем «Поместить все сертификаты в следующее хранилище». Нажимаем кнопку «Обзор»



20. Выбираем «Промежуточные центры сертификации» и нажимаем кнопку «ОК».



21. Убеждаемся что в поле появилась надпись: «Промежуточные центры сертификации». Нажимаем кнопку «Далее».

←  Мастер импорта сертификатов



Хранилище сертификатов

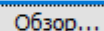
Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

- ☐ Автоматически выбрать хранилище на основе типа сертификата
- ☒ Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

Промежуточные центры сертификации

 Обзор...

Далее

Отмена

22. Нажимаем готово.



←  Мастер импорта сертификатов

Завершение мастера импорта сертификатов

Сертификат будет импортирован после нажатия кнопки "Готово".

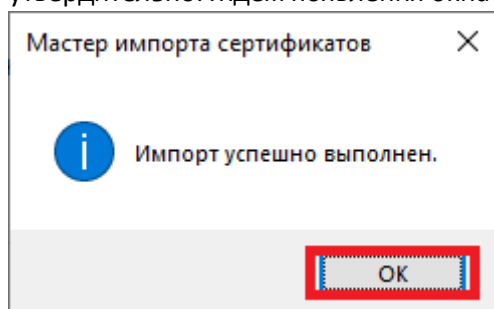
Были указаны следующие параметры:

Хранилище сертификатов, выбранное пользователем	Промежуточные центры сер
Содержимое	Сертификат

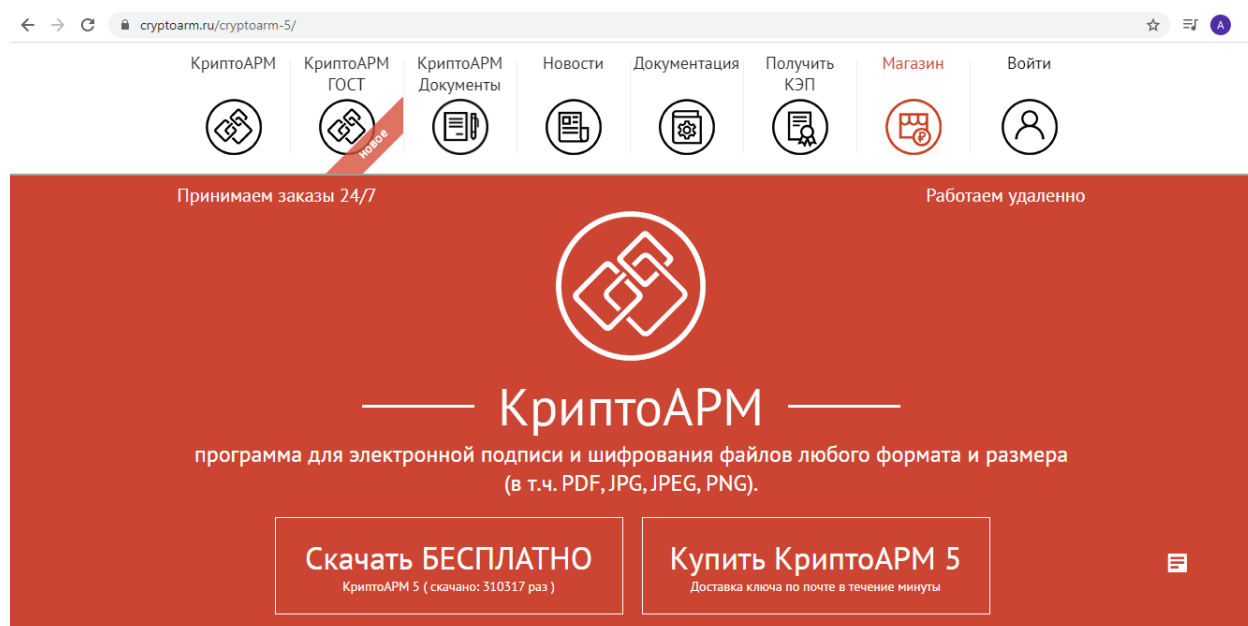
Готово

Отмена

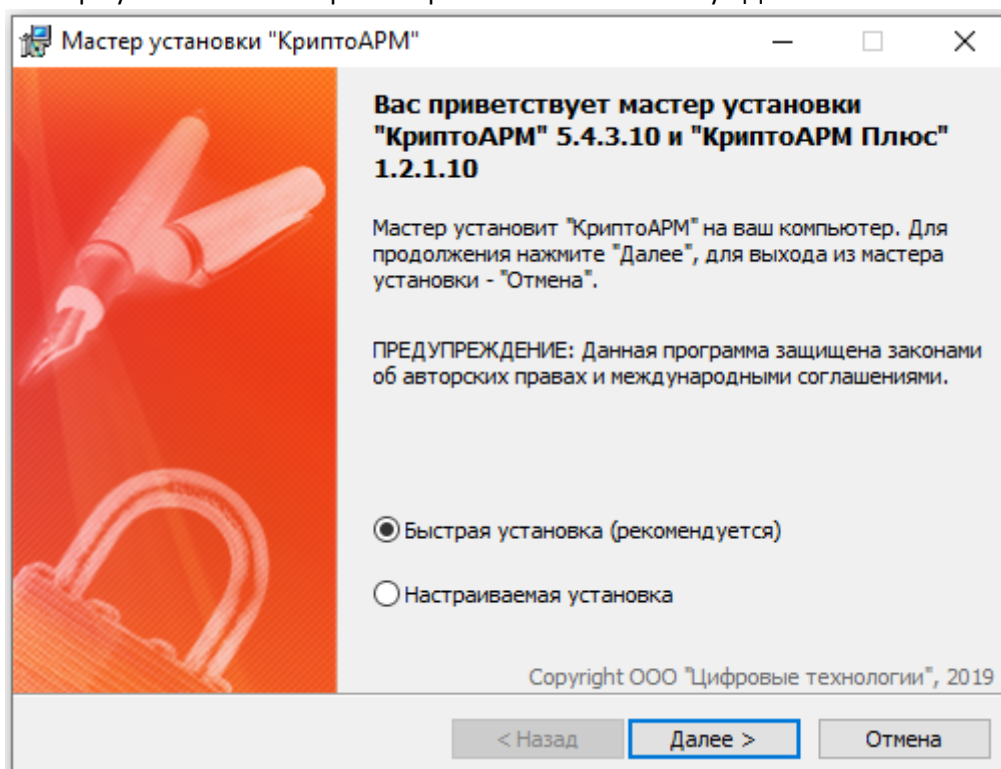
23. Ждем окончания добавления сертификата на все всплывающие окна отвечаем утвердительно. Ждем появления окна и нажимаем «ОК».



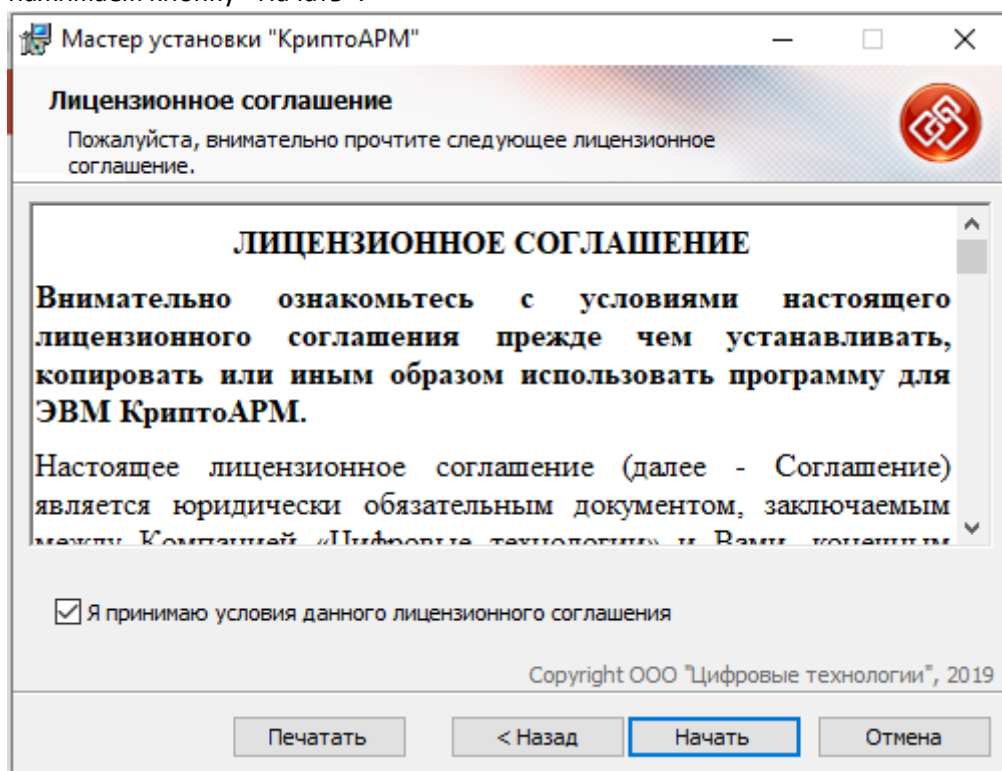
24. Скачать программу <https://cryptoarm.ru/>, выбираем для скачивания бесплатную версию. Программа будет работать 14 дней.



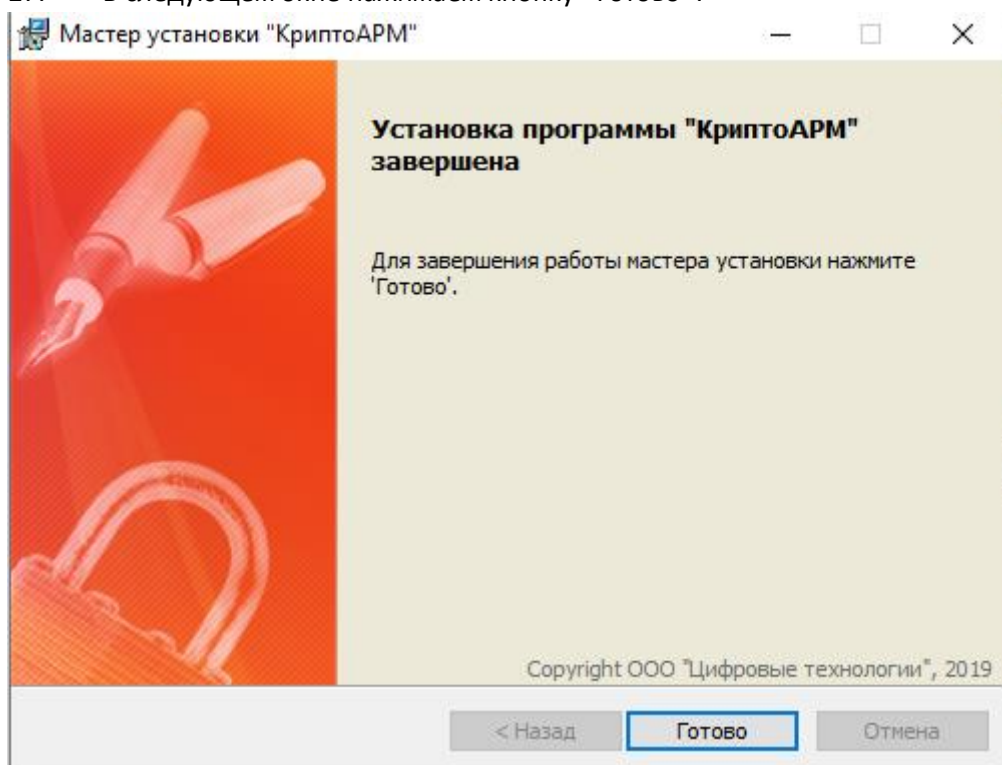
25. Устанавливаем программу. Для этого запускаем скачанную программу, следуем указаниям мастера установки. На первом экране нажимаем кнопку «Далее».



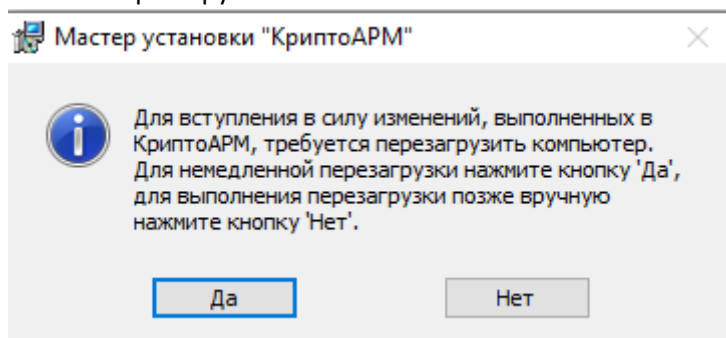
26. На следующей ставим галку «Я принимаю условия данного лицензионного соглашения». И нажимаем кнопку «Начать».



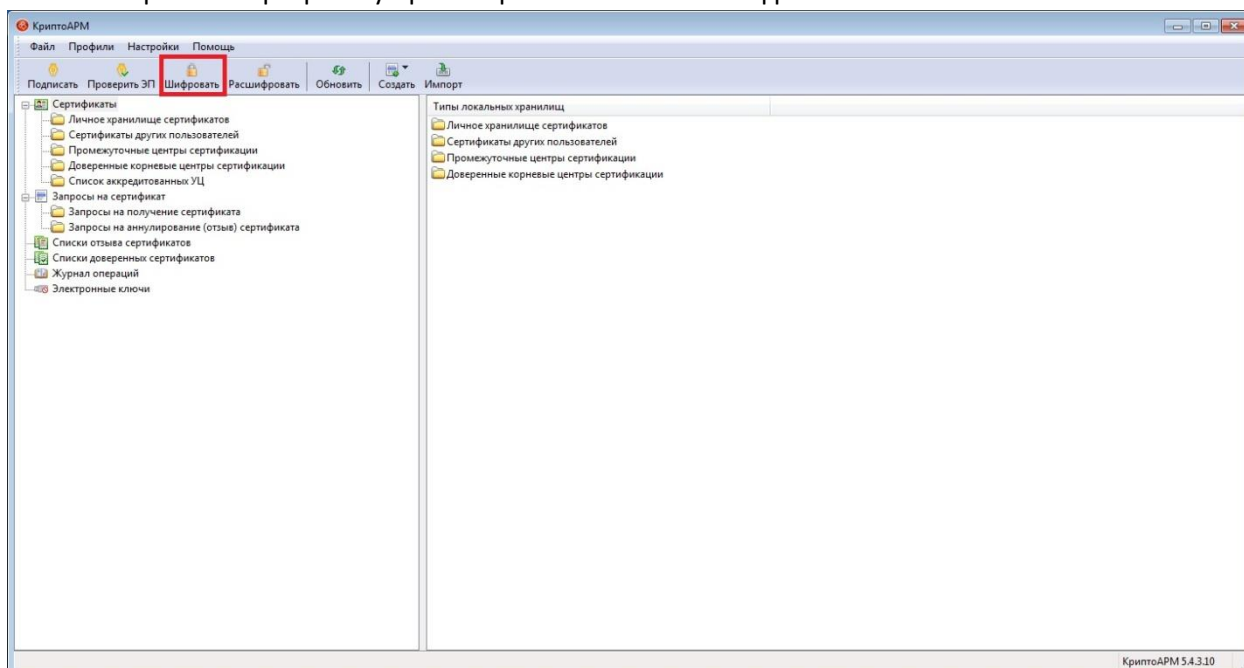
27. В следующем окне нажимаем кнопку «Готово».



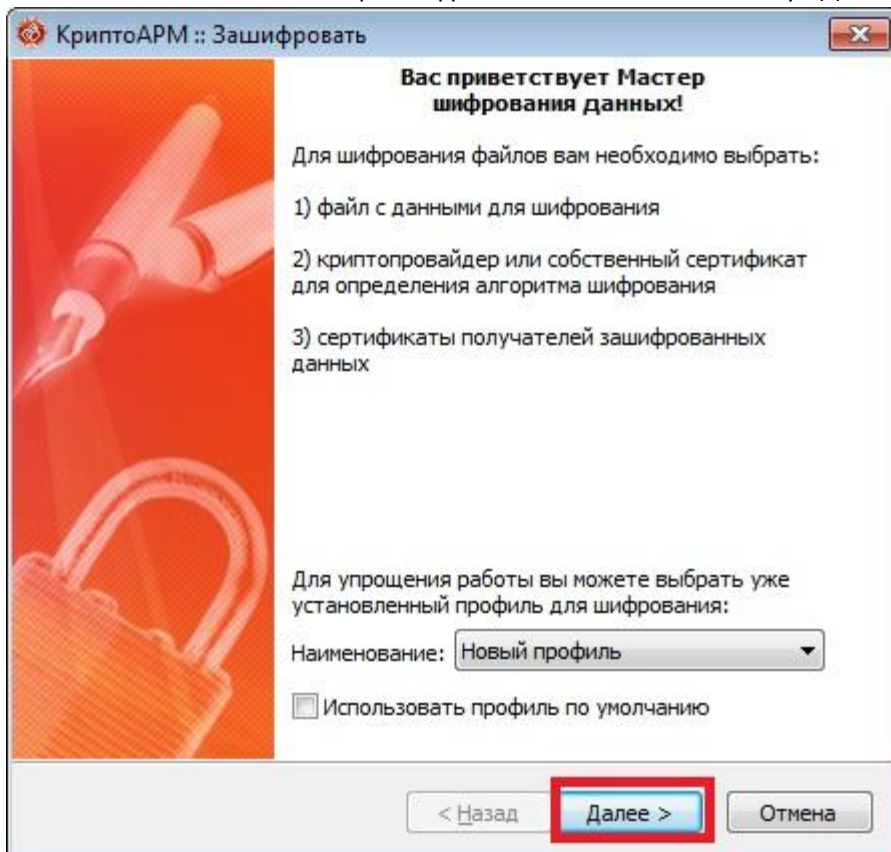
28. Ждем окончания установки и нажимаем кнопку «Да». После этого компьютер перезагрузится.



29. Открываем программу КриптоАрм. Нажимаем зашифровать.

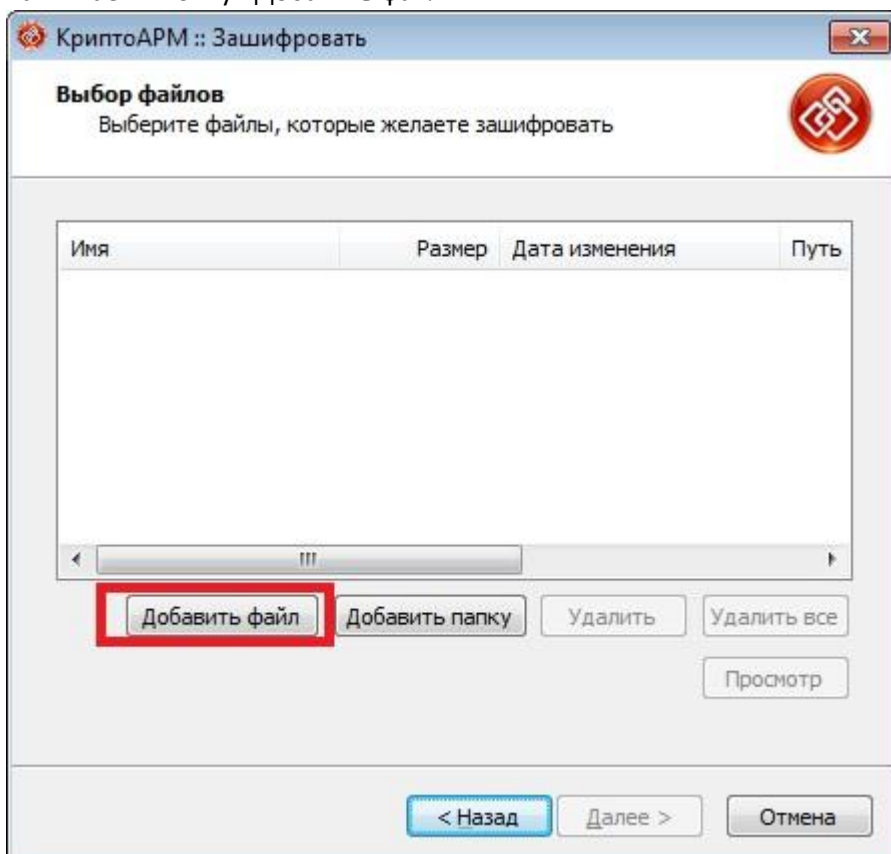


30. Появится окно мастера шифрования. Нажимаем кнопку «Далее».

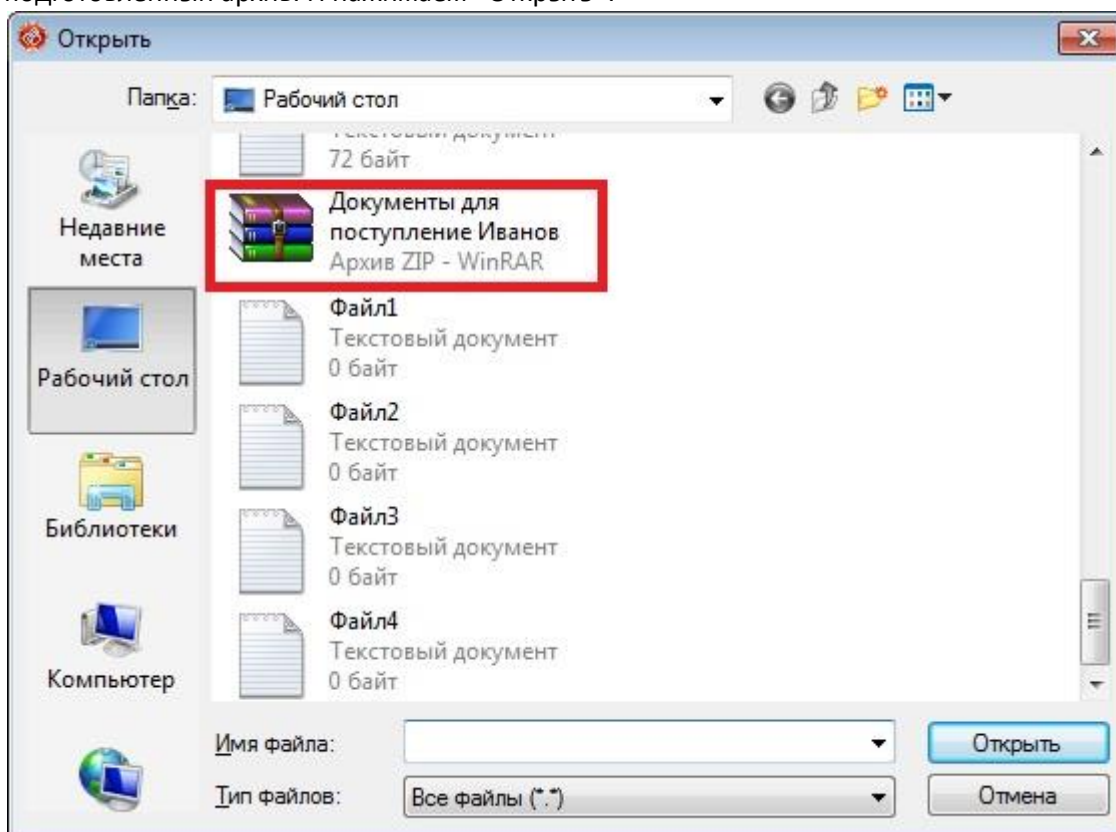


31. Мастер попросит добавить ваши файлы, которые вы подготовили для поступления. Заполните все необходимые заявления и сделайте сканы документов. Добавьте их в файл архива без сжатия.

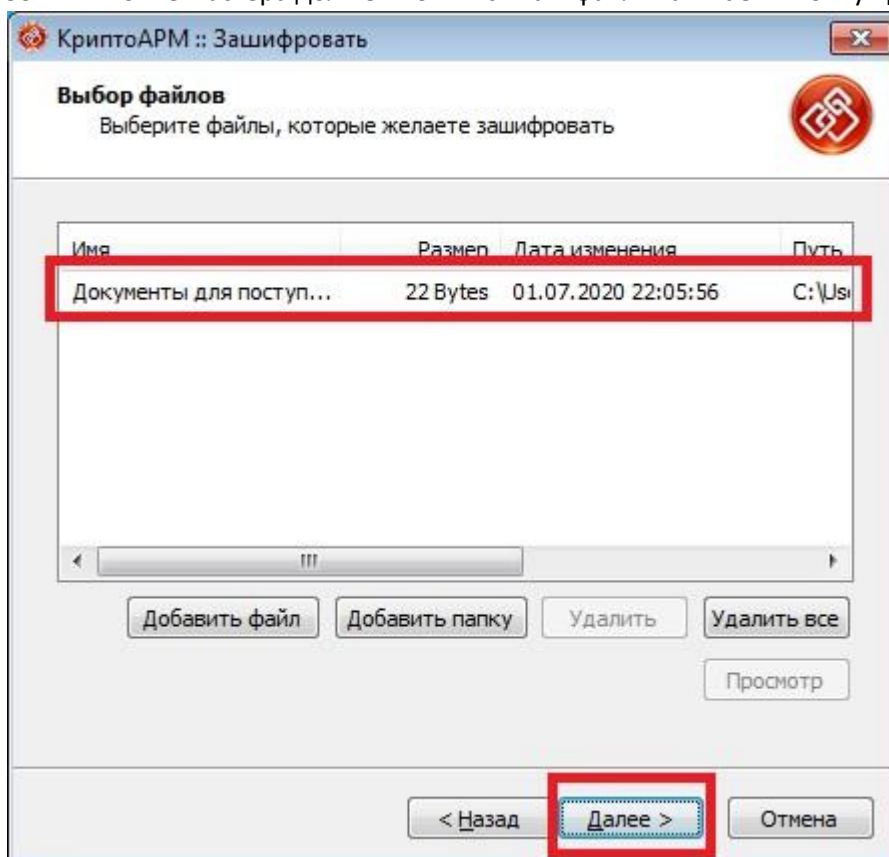
Нажимаем кнопку «Добавить файл».



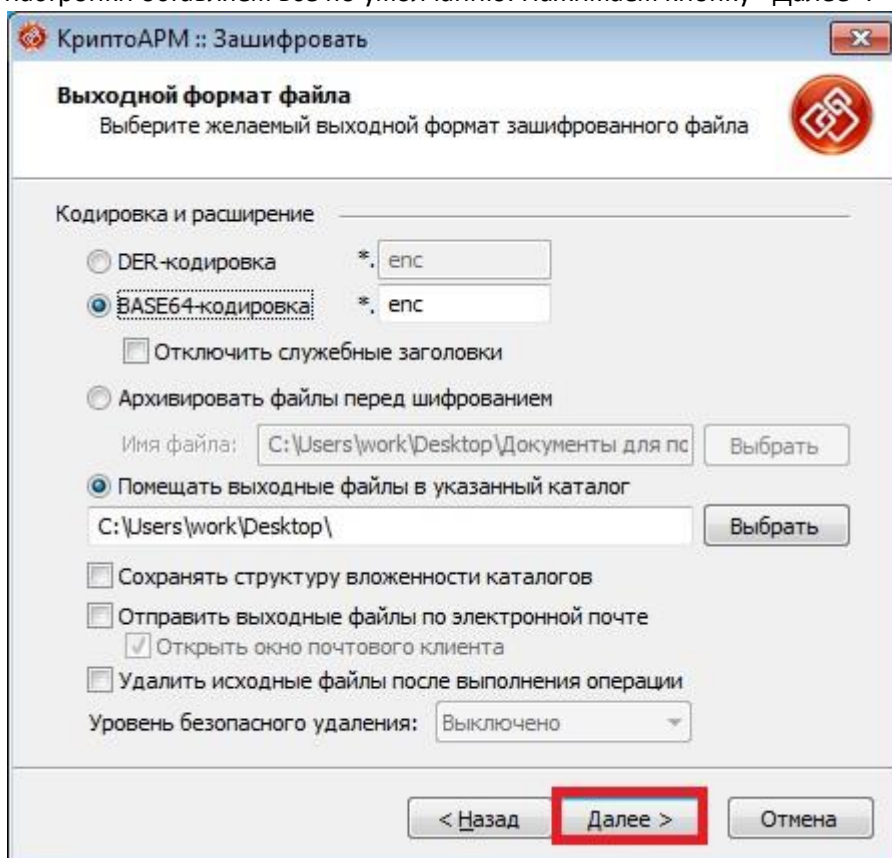
32. После нажатия кнопки «Добавить файл» появится окно. В появившемся окне выбираем подготовленный архив. И нажимаем «Открыть».



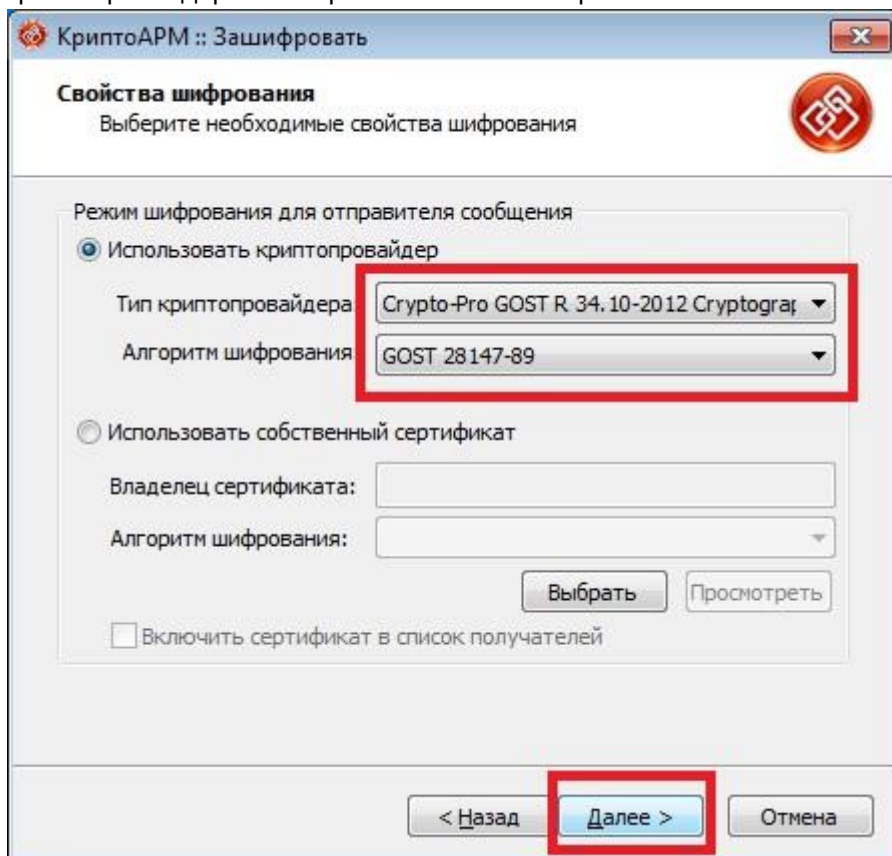
33. В окне мастера должен появиться ваш файл. Нажмаем кнопку «Далее»



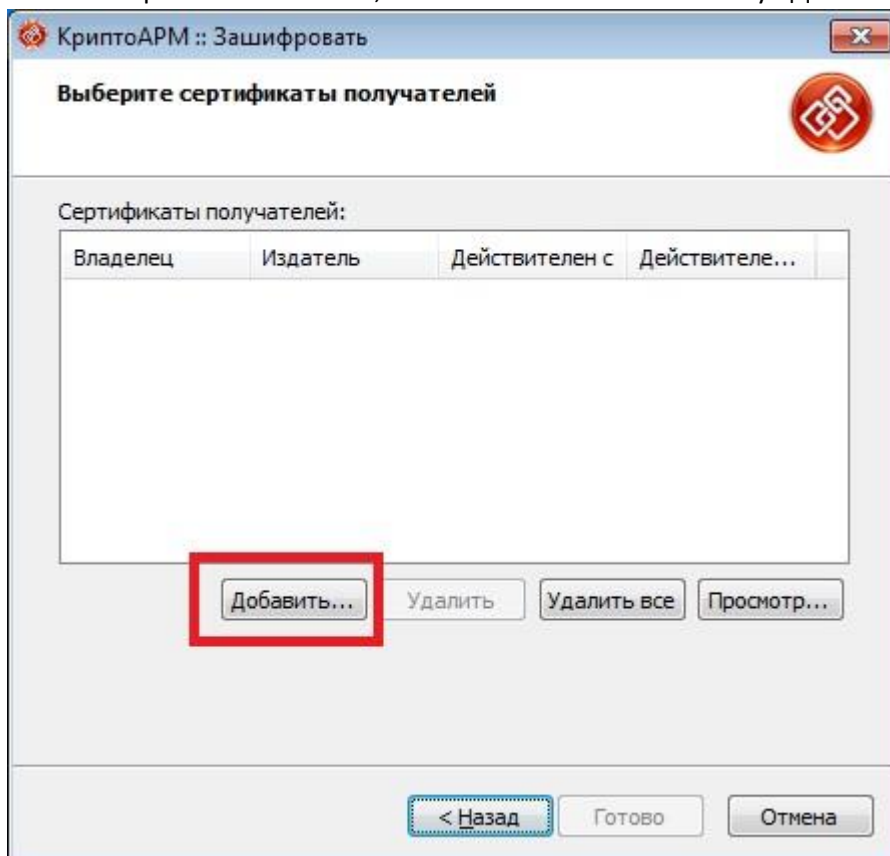
34. В следующем окне выбираем куда будет помещен зашифрованный файл. Остальные настройки оставляем все по умолчанию. Нажимаем кнопку «Далее».



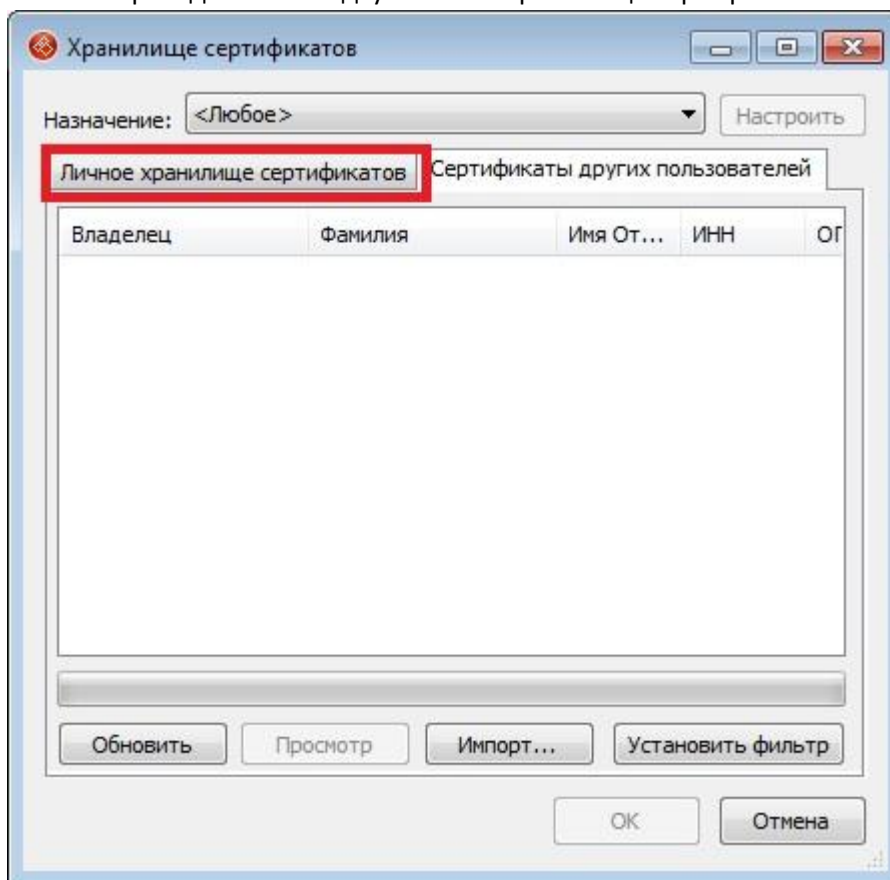
35. Устанавливаем точку в поле «Использовать Криптопровайдер». В поле «Тип криптопровайдера» выбираем поле как на картинке. И нажимаем кнопку «Далее».



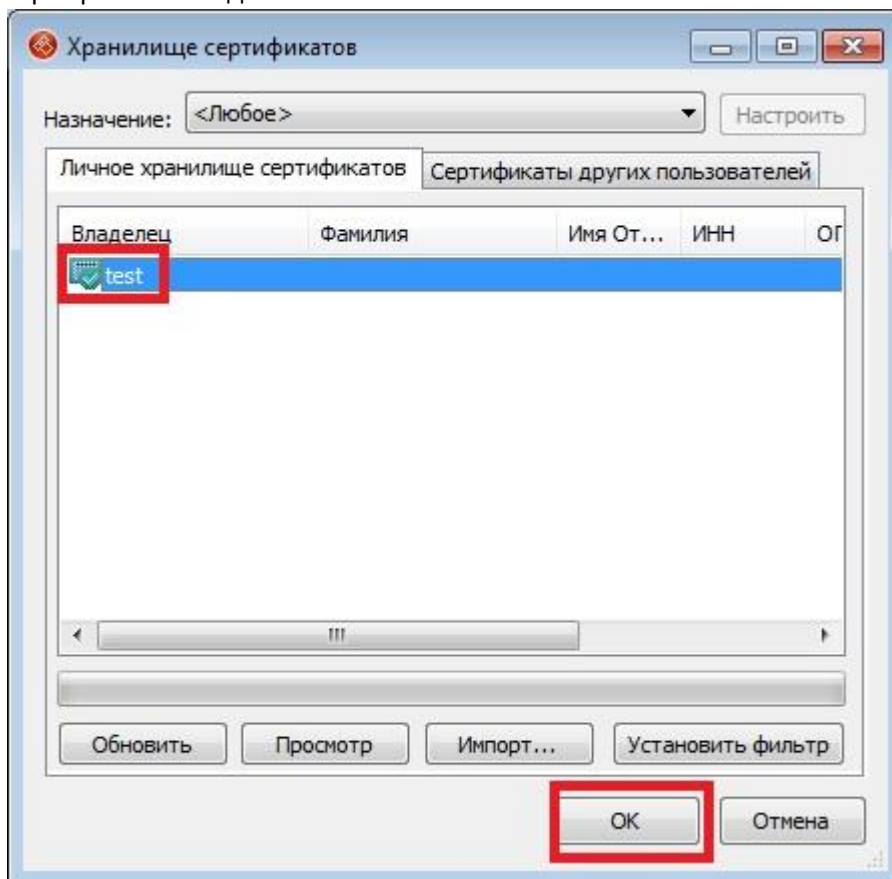
36. Откроется новое окно, в этом окне нажимаем кнопку «Добавить».



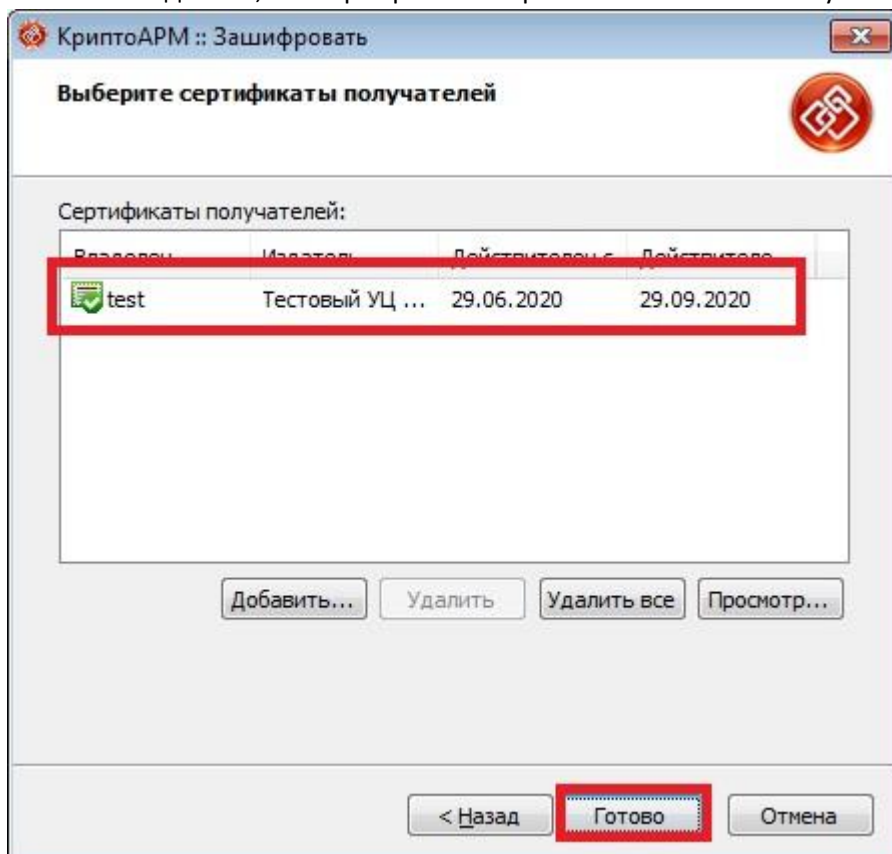
37. Переходим на вкладку «Личное хранилище сертификатов»



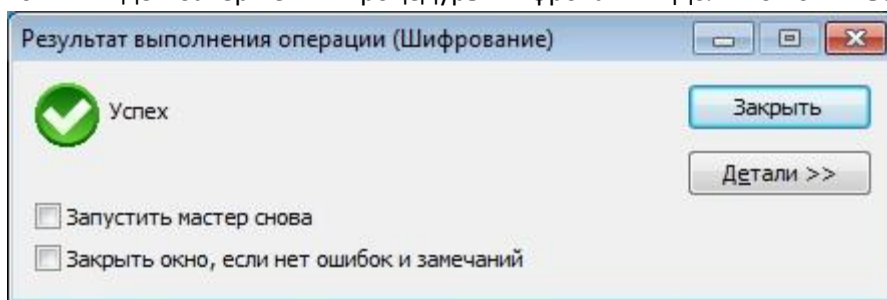
38. На вкладке «Личное хранилище сертификатов» выбираем установленный нами сертификат колледжа. Нажимаем «Ок».



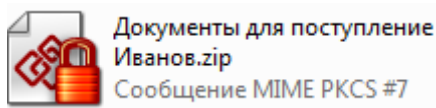
39. Убеждаемся, что сертификат выбран. Нажимаем кнопку «Готово».



40. Ждем завершения процедуры шифрования. Должно появиться соответствующее окно.



41. После удачного завершения процедуры появится файл следующего вида.



42. Этот файл надо отправить на почту учебного заведения.