1. Инсталляция СКЗИ КриптоПро CSP

Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.

Для установки программного обеспечения вставьте компакт-диск в дисковод.

Рисунок 1. Установка СКЗИ КриптоПро CSP

Выберите удобный для Вас язык установки и дистрибутив, соответствующий используемой операционной системе.

Примечание. также установка может производиться с дистрибутива, полученного с сайта ООО КРИПТО-ПРО. В таком случае пользователю нужно запустить файл дистрибутива CSPSetup.exe.

Перед запуском мастера установки выводится диалоговое окно, в котором доступен выбор уровня защищенности (кнопка **Опции**).

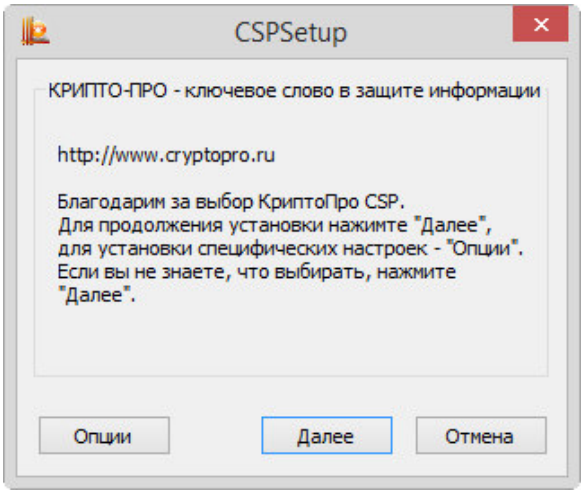

Рисунок 2. Начало установки

В СКЗИ КриптоПро реализованы классы защиты КС1, КС2, КС3 согласно требованиям ФСБ России.

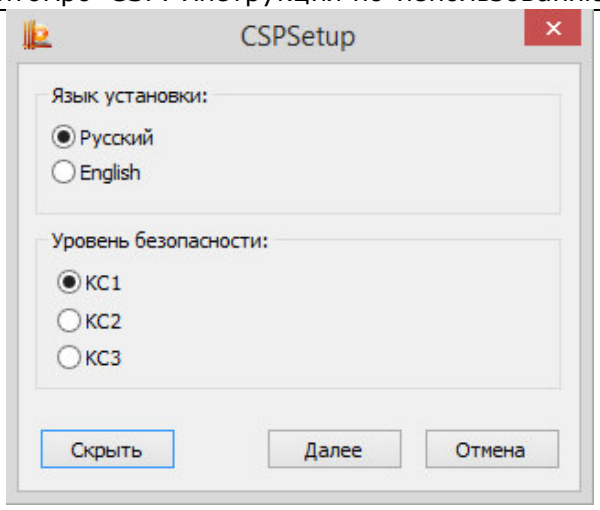

Рисунок 3. Выбор уровня безопасности

Укажите требуемый уровень безопасности, если он отличается от значения по умолчанию. После этого можно переходить к работе с мастером установки.

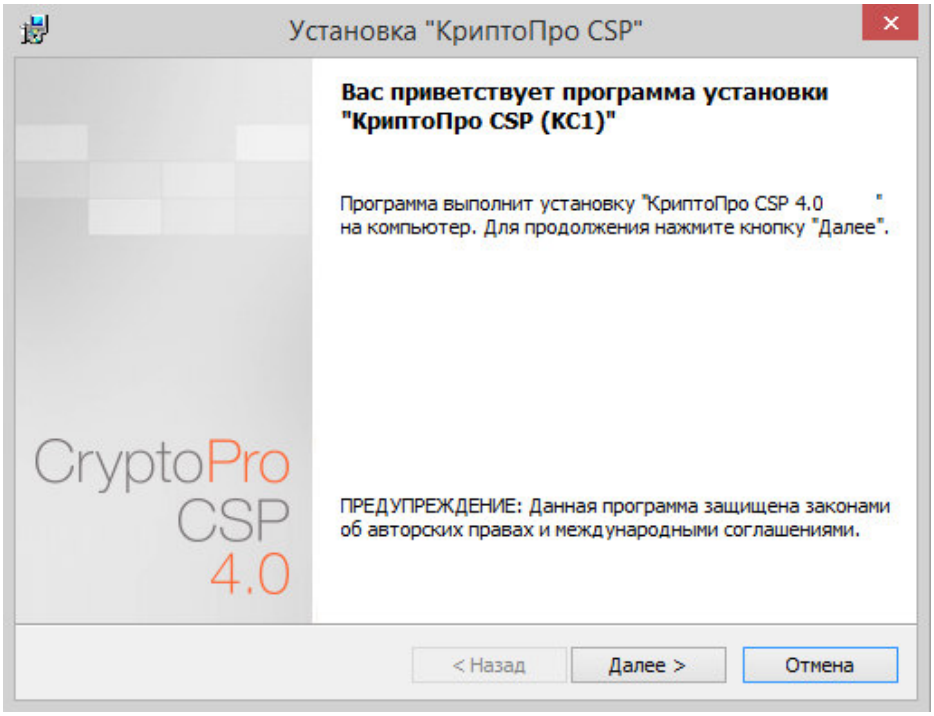

Рисунок 4. Приветственное окно мастера установки

Если на машине была установлена более ранняя версия СКЗИ КриптоПро CSP, то в окне появится информация об обновляемой версии:

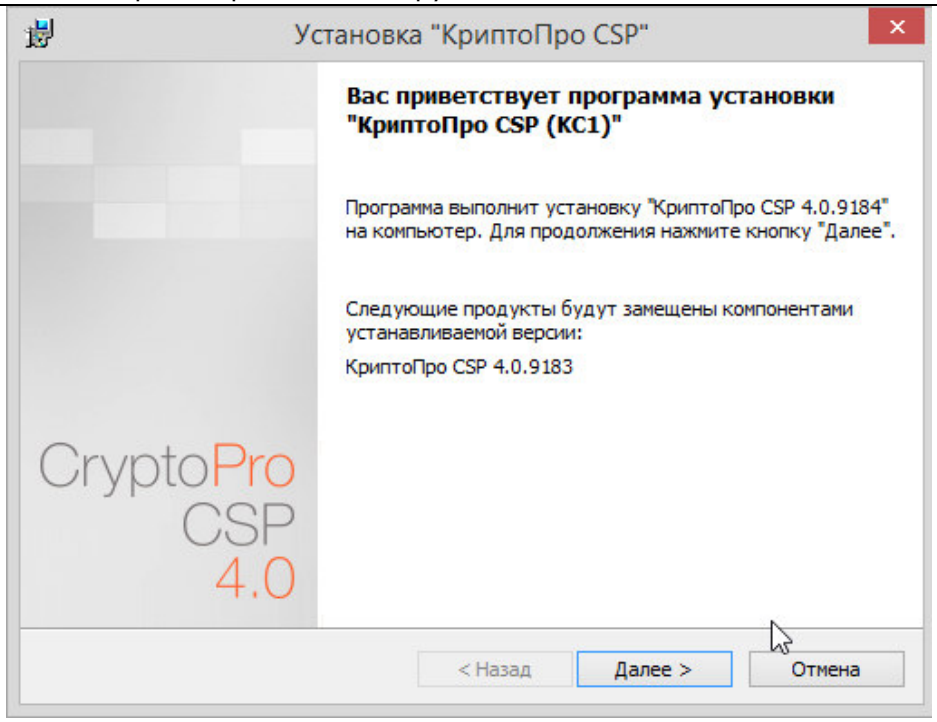

Рисунок 5. Установка с замещением компонентов

Для продолжения установки КриптоПро CSP нажмите **Далее**.

Внимательно прочитайте лицензионное соглашение, которое выводится при первой установке.

Дальнейшая установка производится в соответствии с сообщениями, выдаваемыми мастером.

В процессе установки может быть предложено:

- ввести серийный номер лицензии криптопровайдера;
- зарегистрировать дополнительные считыватели ключевой информации;
- настроить дополнительные датчики случайных чисел (для уровней КС2 и КС3);
- настроить криптопровайдер на использование службы хранения ключей (для уровня КС1).

Эти параметры можно изменить после завершения установки через панель свойств КриптоПро CSP.

Для корректной работы КриптоПро CSP после завершения установки необходимо перезагрузить компьютер в случае, если пользователю предлагается перезагрузка.

В процессе установки мастером может быть предложен выбор наиболее подходящего вида установки.

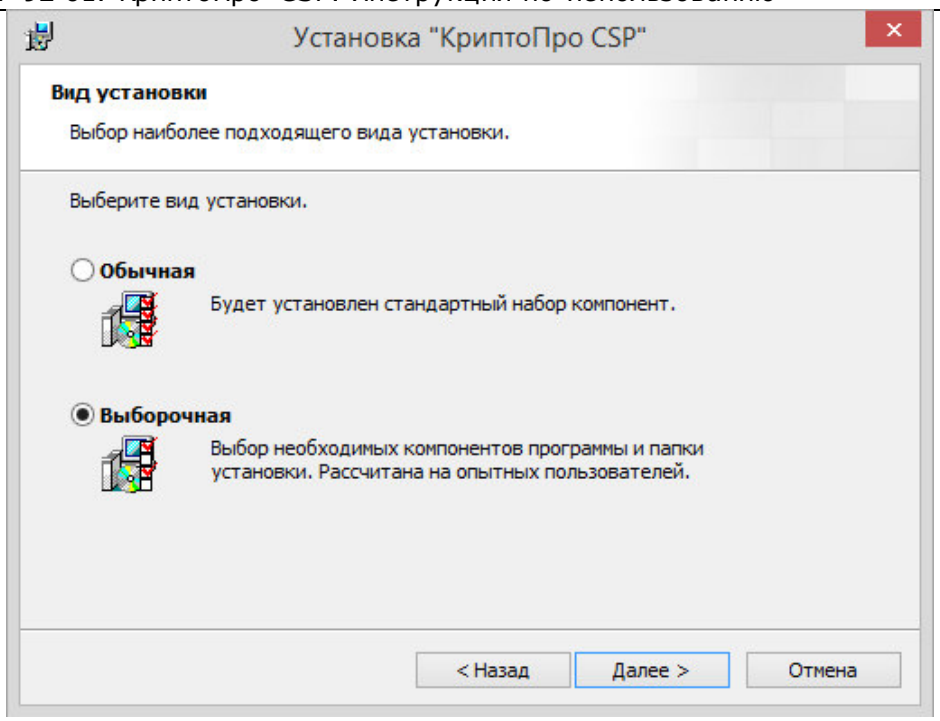

Рисунок 6. Выбор вида установки

По умолчанию (вид установки «Обычная») устанавливаются только основные файлы для работы СКЗИ (для Windows Server 2008 по умолчанию также устанавливается «Драйверная библиотека CSP»). При необходимости можно изменить набор компонентов для установки:

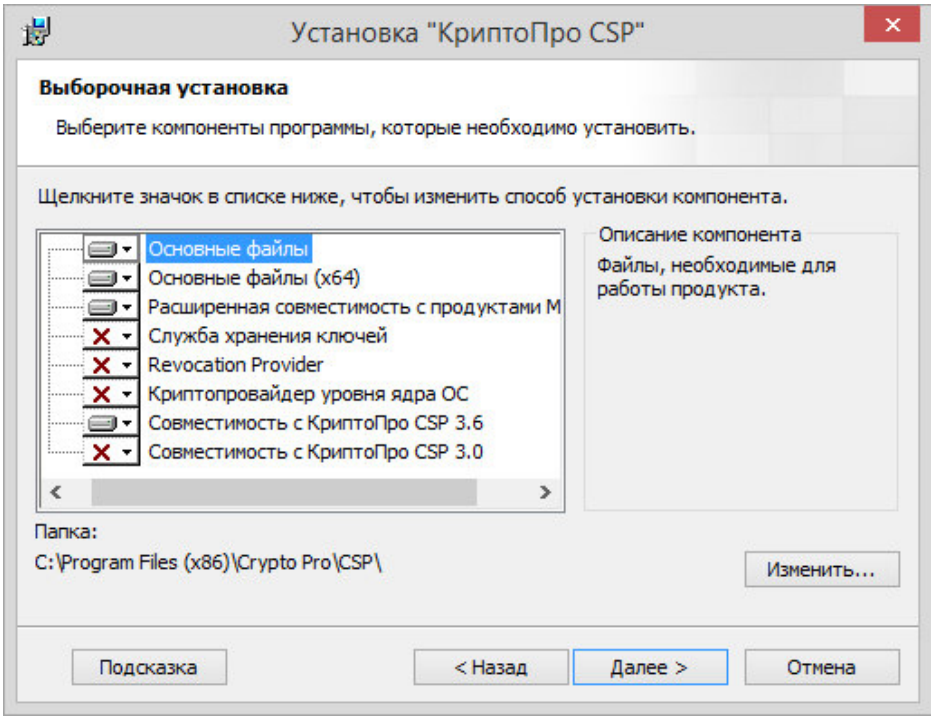

Рисунок 7. Выборочная установка

Расширенная совместимость с продуктами Microsoft – Обеспечивает совместимость с такими приложениями, как Microsoft Office, Outlook Express. Необходима для входа в систему по смарт-картам.

Служба хранения ключей – Обеспечивает хранение, использование и кэширование ключей в отдельном сервисе ОС. По умолчанию включена для уровня безопасности КС2 и КС3 (подробно описана в разделе Установка параметров безопасности).

Revocation Provider - Механизм проверки текущего статуса сертификата с использованием OCSP. Является дополнением к стандартному механизму Windows проверки статуса сертификата на основе списка отозванных сертификатов (COC, CRL). Кроме этого предоставляет возможность использования COC, выпущенных по правилам, описанным в RFC 3280.

Криптопровайдер уровня ядра ОС– Необходим для работы криптопровайдера в службах и ядре Windows (TLS-сервер, EFS, IPsec).

Совместимость с КриптоПро CSP 3.6 - Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.6. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.6.

Совместимость с КриптоПро CSP 3.0 - Регистрирует имена провайдеров, совместимые с КриптоПро CSP 3.0. Необходимо только при наличии в хранилище «Личные» сертификатов, установленных с КриптоПро CSP 3.0.

Примечание. В состав КриптоПро CSP SDK, входит описание параметров командной строки установщика Windows (**\CHM\msi-readme.txt**), которые удобно использовать для автоматического развертывания дистрибутива.

После нажатия на **Далее** мастером установки предлагается запланировать или отменить установку библиотек поддержки считывателей, а также принять решение о включении функционала накопления информации об использованных съёмных ключевых носителях. Помимо этого, также необходимо включить режим усиленного контроля использования ключей. Данный режим осуществляет контроль срока действия долговременных ключей электронной подписи и ключевого обмена, контроль доверенности ключей проверки электронной подписи и контроль корректного использования программного датчика случайных чисел. Использование СКЗИ КриптоПро CSP 4.0 без включения режима усиленного контроля использования ключей разрешается только в тестовых целях.

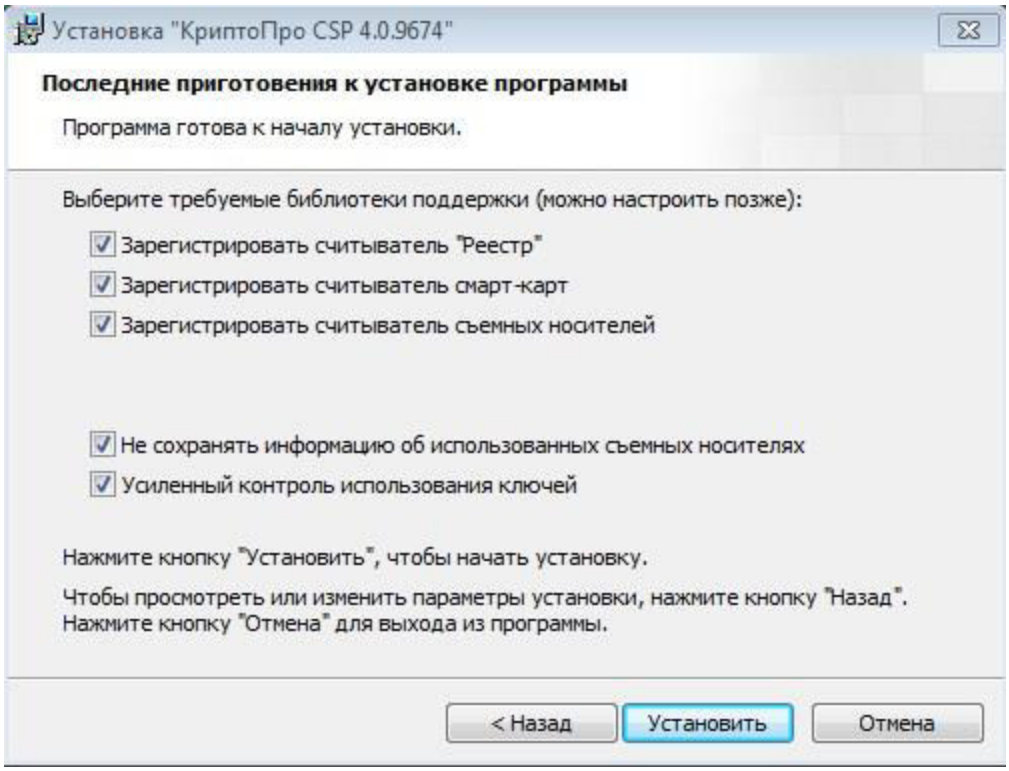

Рисунок 8. Установка усиленного контроля использования ключей

При установке СКЗИ с включением режима усиленного контроля использования ключей будут запрошены данные с датчика случайных чисел. В случае ошибки получения данных будет отображено окно, пример которого приведён на Рисунок 9. В этом случае при начале работы пользователя в системе с установленным СКЗИ КриптоПро CSP 4.0 необходимо проверить, что зарегистрирован хотя бы один физический датчик случайных чисел (например, биологический ДСЧ, внешняя гамма или аппаратный ДСЧ), и выполнить команду:

csptest.exe -keyset -verifycontext -hard_rng.

После завершения установки СКЗИ с включённым режимом усиленного контроля использования ключей **необходимо в обязательном порядке** установить доверенные корневые сертификаты в хранилище сертификатов локального компьютера CryptoProTrustedStore («Доверенные корневые сертификаты КриптоПро CSP», «CryptoPro CSP Trusted Roots») с помощью оснастки Сертификаты либо с помощью утилиты certmgr.exe:

certmgr.exe -inst -cert -silent -store mCryptoProTrustedStore -file ca.cer

После этого следует осуществить перезагрузку компьютера.

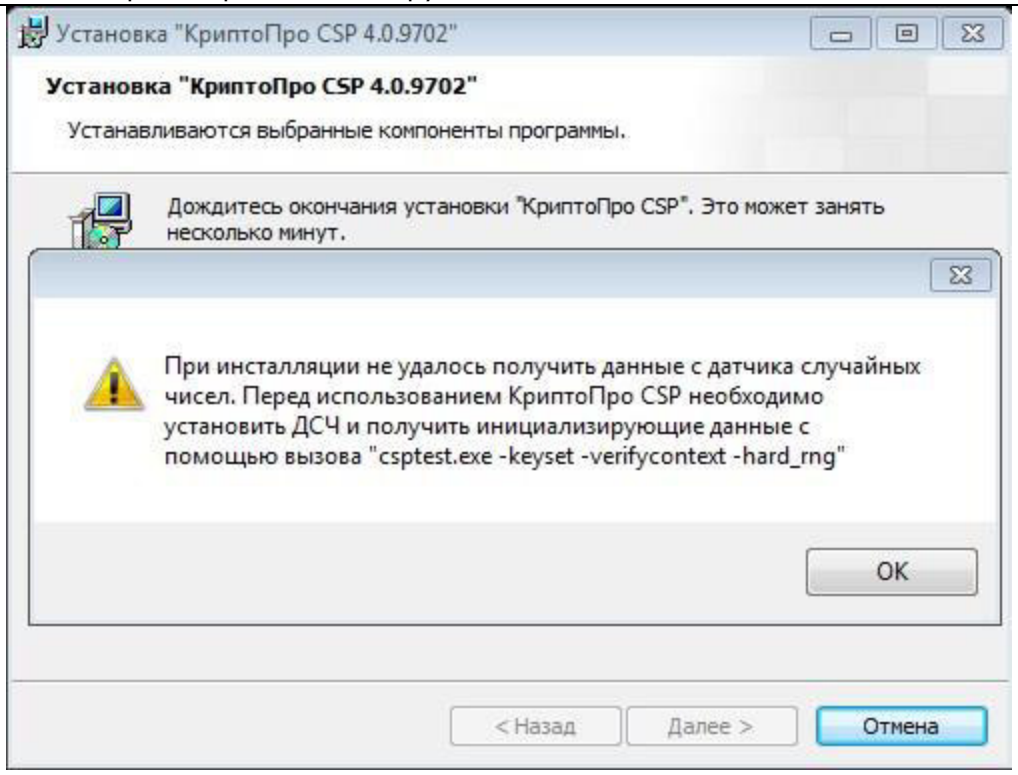

Рисунок 9. Окно ошибки получения данных с датчика случайных чисел при инсталляции СКЗИ.