

OpenSSL

Для работы Axiom Lab и пакета утилит Axiom Software (ContainerTool, TokenTool) может потребоваться установленная и корректно сконфигурированная библиотека OpenSSL с движком ГОСТ.

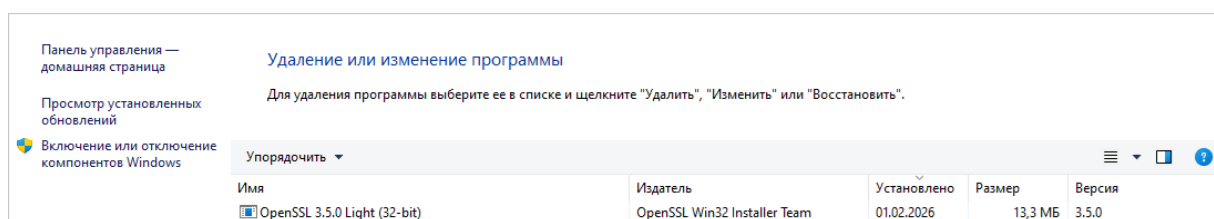
Работоспособность указанного ПО проверялась на сборках OpenSSL версий 1.1.1 и выше (3.3, 3.4, 3.5, 3.6).

Установка OpenSSL может оказать негативное влияние на уже установленное (или устанавливаемое в будущем) ПО сторонних производителей. Опытным путем выяснено, что Saby (СБИС) отказывается работать при наличии в системе OpenSSL 1.1.1 с движком ГОСТ (без движка ГОСТ работоспособность Saby сохраняется), в связи с чем крайне рекомендуется использование актуальных сборок OpenSSL.

Подробная инструкция по установке и настройке OpenSSL, включая движок ГОСТ, приведена [тут](#).

Прежде чем приступить к установке OpenSSL, стоит проверить, быть может, она уже установлена и, даже, настроена.

Явным признаком установленной OpenSSL является наличие соответствующего элемента в списке установленных программ:



Отсутствие OpenSSL в списке установленных программ ни о чем не говорит – может использоваться портативная версия библиотеки. Чтобы проверить наличие сконфигурированной портативной версии OpenSSL, необходимо в командной строке выполнить

```
openssl version
```

и проверить результат:

- «"openssl" не является внутренней или внешней командой, исполняемой программой или пакетным файлом» говорит о том, что OpenSSL не установлена или не настроена, а это, в свою очередь, означает, что ее самостоятельная установка не должна сказаться на системе
- «OpenSSL 3.5.0 8 Apr 2025 (Library: OpenSSL 3.5.0 8 Apr 2025)» (или что-то похожее) говорит о наличии настроенной OpenSSL соответствующей версии

При отсутствии явных признаков OpenSSL в системе можно приступить к ее установке и последующей настройке. При наличии в системе той или иной версии библиотеки можно приступить к ее настройке.

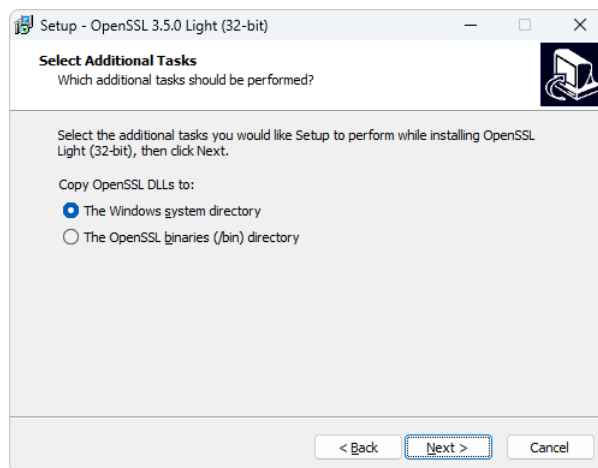
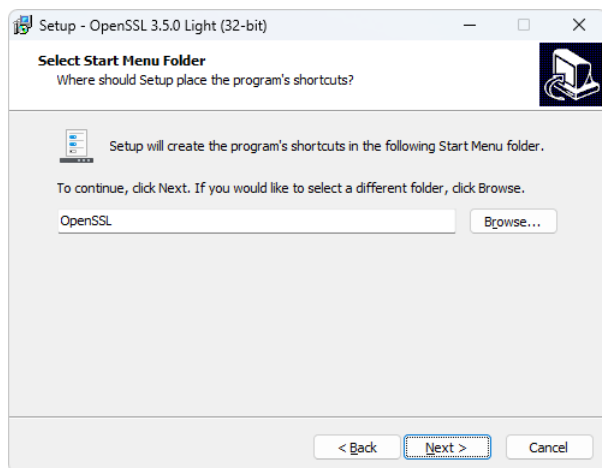
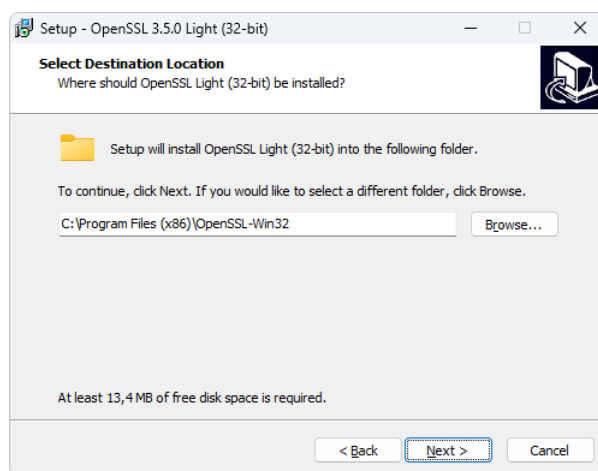
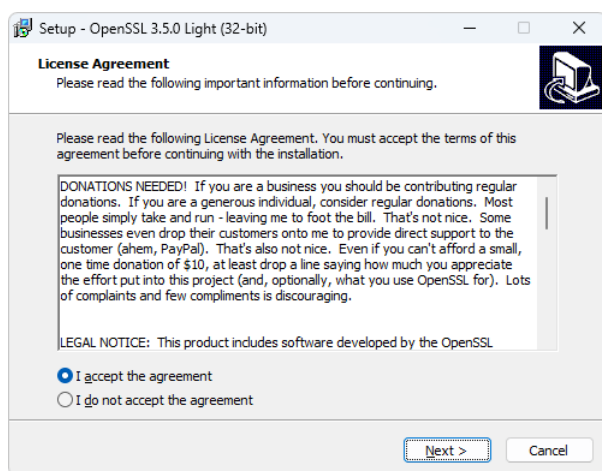
Установка OpenSSL

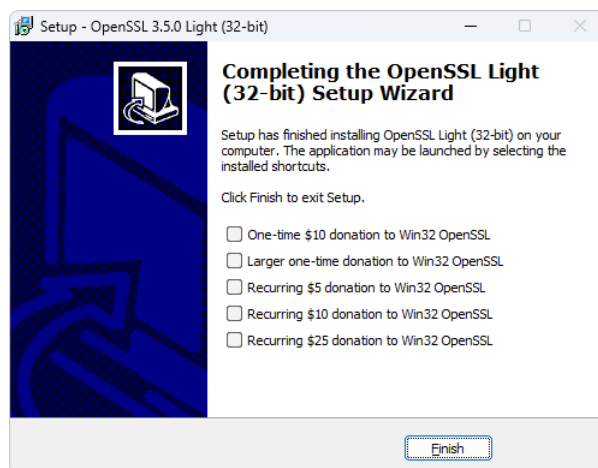
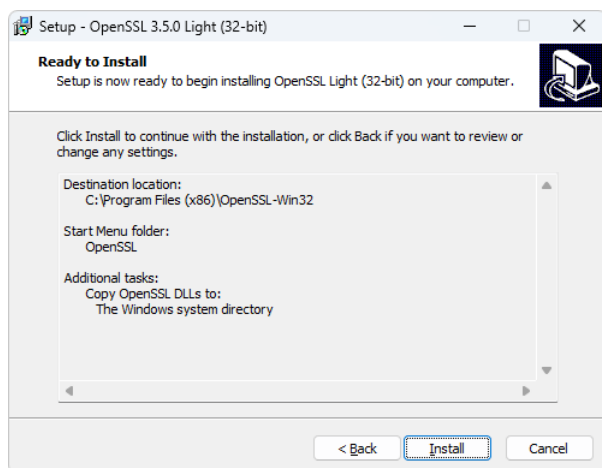
Примерный порядок установки OpenSSL 3.5 (LTS согласно [релизной стратегии](#)) выглядит следующим образом:

1. Скачать дистрибутив OpenSSL 3.5. Можно использовать лайт-версию. В любом случае необходимо скачивать 32-х битный дистрибутив

Неплохой ресурс с различными версиями OpenSSL располагается [здесь](#), однако его доступность без использования VPN может вызывать вопросы. На текущий момент данный ресурс полноценно открывается через [вэб-архив](#).

2. Установить OpenSSL из скаченного дистрибутива в режиме "далее-далее-далее", т.е. оставив все параметры без изменений:

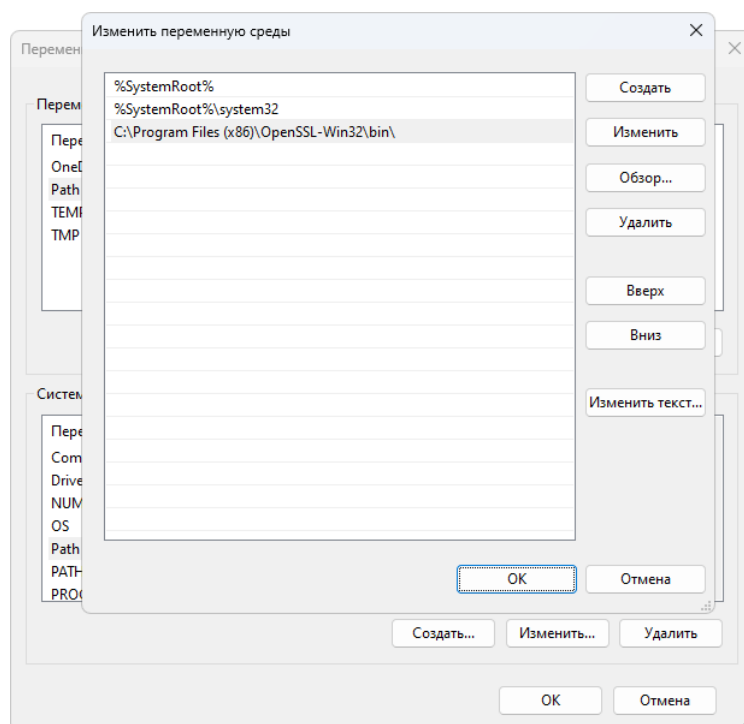




Далее считаем, что OpenSSL была установлена в директорию "C:\Program Files (x86)\OpenSSL-Win32", а основные dll библиотеки установлены в системной директории Windows ("C:\Windows\SysWOW64").

Настройка OpenSSL

Директория бинарных файлов OpenSSL ("C:\Program Files (x86)\OpenSSL-Win32\bin") содержит исполняемый файл "openssl.exe", служащий интерпретатором команд OpenSSL (например, openssl version) через командную строку. Для того чтобы командный интерпретатор OpenSSL стал доступным не только из директории бинарных файлов OpenSSL, необходимо добавить в системную переменную среды "Path" (не путать с переменными среды текущего пользователя) путь к этой директории:



Движок ГОСТ

Движок ГОСТ необходим для работы с закрытыми ключами сертификатов ГОСТ Р 34.11-2012 (2001). Без него Axiom Lab не сможет подписывать данные с использованием сертификатов, хранящихся в файлах (JKS, PEM, PFX), а ContainerTool не сможет экспортировать сертификаты и ключи.

Для установки движка ГОСТ требуется

1. Скачать 32-х битную библиотеку "[gost.dll](#)" (в случае с OpenSSL 3.X еще и "[gostprov.dll](#)"). Ссылку на скачивание можно найти [ТУТ](#)
2. Поместить скаченные библиотеки в системную директорию Windows ("[C:\Windows\SysWOW64](#)")

Если при установке OpenSSL на шаге №4 ("Select Additional Tasks") был выбран пункт "The OpenSSL binaries (/bin) directory", скаченные библиотеки следует помещать в директорию бинарных файлов OpenSSL ("[C:\Program Files \(x86\)\OpenSSL-Win32\bin](#)").

3. Отредактировать файл конфигурации "[C:\Program Files \(x86\)\Common Files\SSL\openssl.cnf](#)":

a) Определить имя секции с конфигурацией OpenSSL:

```
# This definition stops the following lines choking if HOME isn't
# defined.
HOME = .

openssl_conf = openssl_conf
```

b) Добавить в конец файла следующие строки:

```
[openssl_conf]
engines = engine_section

[engine_section]
gost = gost_section

[gost_section]
engine_id = gost
dynamic_path = ./gost.dll
default_algorithms = ALL
CRYPTO_PARAMS = id-Gost28147-89-CryptoPro-A-ParamSet
GOST_PK_FORMAT = LEGACY_PK_WRAP
```

4. Убедиться в работоспособности OpenSSL и движка ГОСТ. Для этого в командной строке выполнить
`openssl engine`
и убедиться в том, что в выведенном списке движков присутствует движок ГОСТ (GOST)
(rdrand) Intel RDRAND engine
(dynamic) Dynamic engine loading support
(gost) Reference implementation of GOST engine