

ООО «ВАЛИДАТА»

УТВЕРЖДЕН  
ВАМБ.00077-06-ЛУ

**«ВАЛИДАТА КЛИЕНТ» ВЕРСИЯ 4**

ПРОГРАММА TLSPROXY

Руководство по установке и настройке

ВАМБ.00077-06 91 06

2022

## **Аннотация**

Данный документ содержит описание процесса установки и настройки программы TLSProху, входящей в состав программного комплекса ВАНБ.00077-06 «Валидата Клиент» версия 4».

Документ предназначен для администраторов и пользователей как руководство по установке и настройке программы TLSProху.

## Содержание

<b>1 НАЗНАЧЕНИЕ ПРОГРАММЫ TLSPROXY</b>	<b>4</b>
<b>2 УСТАНОВКА ПРОГРАММЫ TLSPROXY</b>	<b>5</b>
2.1 Предварительные действия . . . . .	5
2.2 Установка . . . . .	5
<b>3 НАСТРОЙКА ПРОГРАММЫ TLSPROXY</b>	<b>9</b>
3.1 Требования к сертификатам . . . . .	9
3.2 Настройка конфигурационного файла . . . . .	9
<b>4 ЗАПУСК И УСТАНОВКА СЕРВИСОВ ПРОГРАММЫ TLSPROXY</b>	<b>12</b>
<b>5 УДАЛЕНИЕ ПРОГРАММЫ TLSPROXY</b>	<b>13</b>
<b>6 УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ TLSPROXY БЕЗ ВЫВОДА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА (В «ТИХОМ» РЕЖИМЕ)</b>	<b>14</b>
<b>ПЕРЕЧЕНЬ СОКРАЩЕНИЙ</b>	<b>14</b>
<b>ПЕРЕЧЕНЬ РИСУНКОВ</b>	<b>16</b>
<b>ПЕРЕЧЕНЬ ТАБЛИЦ</b>	<b>17</b>

# **1 НАЗНАЧЕНИЕ ПРОГРАММЫ TLSPROXY**

Программа TLSProxy из состава программного комплекса (ПК) ВАМБ.00077-06 «“Валидата Клиент” версия 4», которая является аналогом программы STunnel, предназначена для защиты данных, передаваемых по TCP соединениям, посредством оборачивания (инкапсуляции) этих данных протоколом TLS. В отличие от программы STunnel, программа TLSProxy работает в режиме сервиса, всегда выполняет двухстороннюю аутентификацию (проверяет цепочку сертификата противоположной стороны), а также имеет возможность фильтровать (блокировать) TLS соединения на основании данных сертификатов противоположной стороны.

## **2 УСТАНОВКА ПРОГРАММЫ TLSPROXY**

### **2.1 Предварительные действия**

Перед установкой программы TLSProxy на ЭВМ необходимо предварительно установить следующие компоненты:

- ПК ВАМБ.00060-06 СКЗИ «Валидата CSP» версия 6» (далее — криптопровайдер) в соответствии с документом ВАМБ.00060-06 91 01 «СКЗИ «Валидата CSP» версия 6. Руководство по установке и настройке»;
- ПК «Справочник сертификатов» из состава ПК ВАМБ.00077-06 «“Валидата Клиент” версия 4» в соответствии с документом ВАМБ.00077-06 91 01 «“Валидата Клиент” версия 4. Руководство по установке и настройке»;
- Microsoft Visual C++ 2015 Redistributable.

Далее необходимо проверить целостность установочного комплекта программы TLSProxy с использованием программы контроля целостности, входящей в состав криптопровайдера.

Описание работы с программой контроля целостности, требования и порядок проведения процедуры контроля целостности описаны в документах ВАМБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности» и ВАМБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя».

### **2.2 Установка**

Установка должна производиться пользователем, имеющим права локального администратора. Установка программы TLSProxy выполнена в стандартном для операционной системы (ОС) Windows формате Windows Installer.

Установка программы TLSProxy производится путем выбора необходимого пакета инсталляции (ztlspoxy\_x86.msi или ztlspoxy\_x64.msi) в зависимости от разрядности ОС и/или требований прикладного программного обеспечения (ПО) и запуска процесса инсталляции двойным щелчком «мыши» по выбранному файлу, находящемуся на инсталляционном диске.

После запуска процесса установки будет отображен начальный диалог (Рисунок 1).

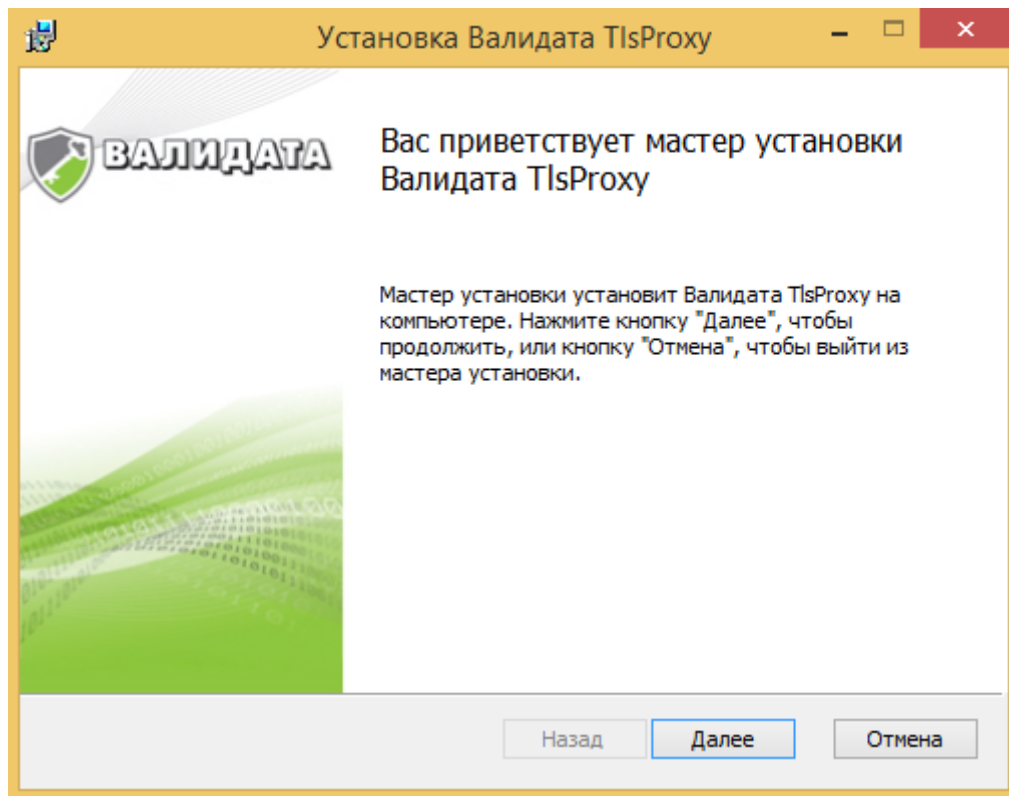


Рисунок 1 – Начальный диалог установки

Нажмите кнопку «Далее». Отображается диалог выбора директории установки (Рисунок 2).

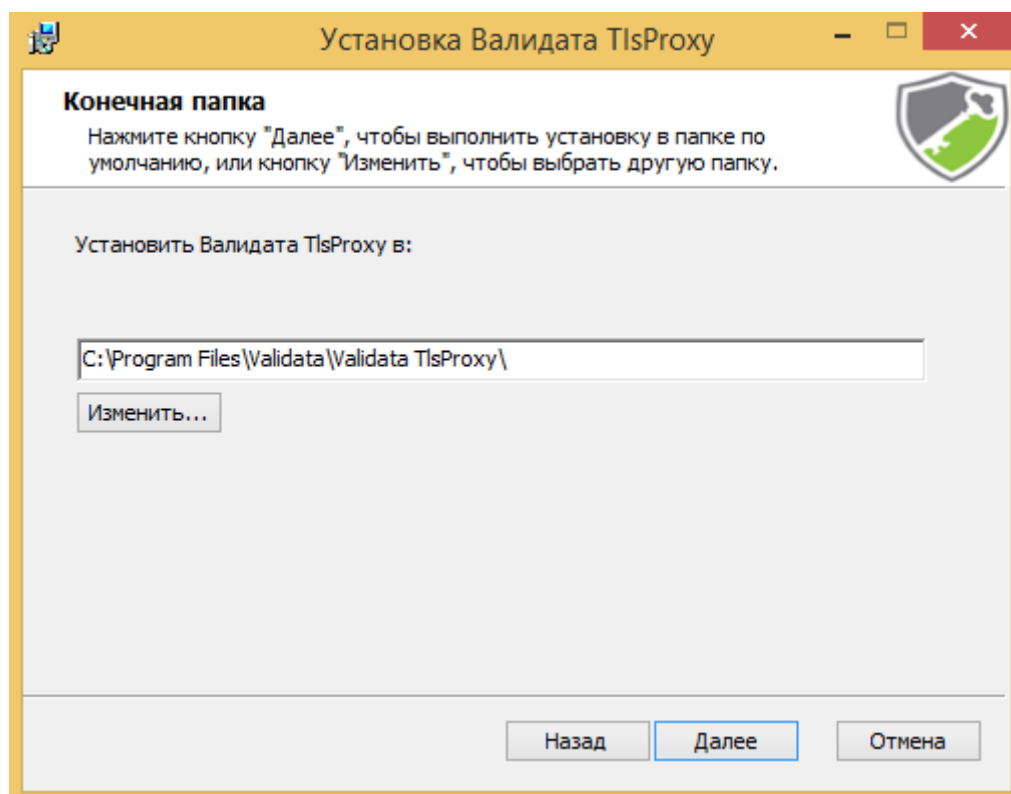


Рисунок 2 – Диалог выбора директории установки

Для продолжения установки необходимо нажать «Далее» и «Установить», после чего появится диалог о готовности к установке (Рисунок 3).

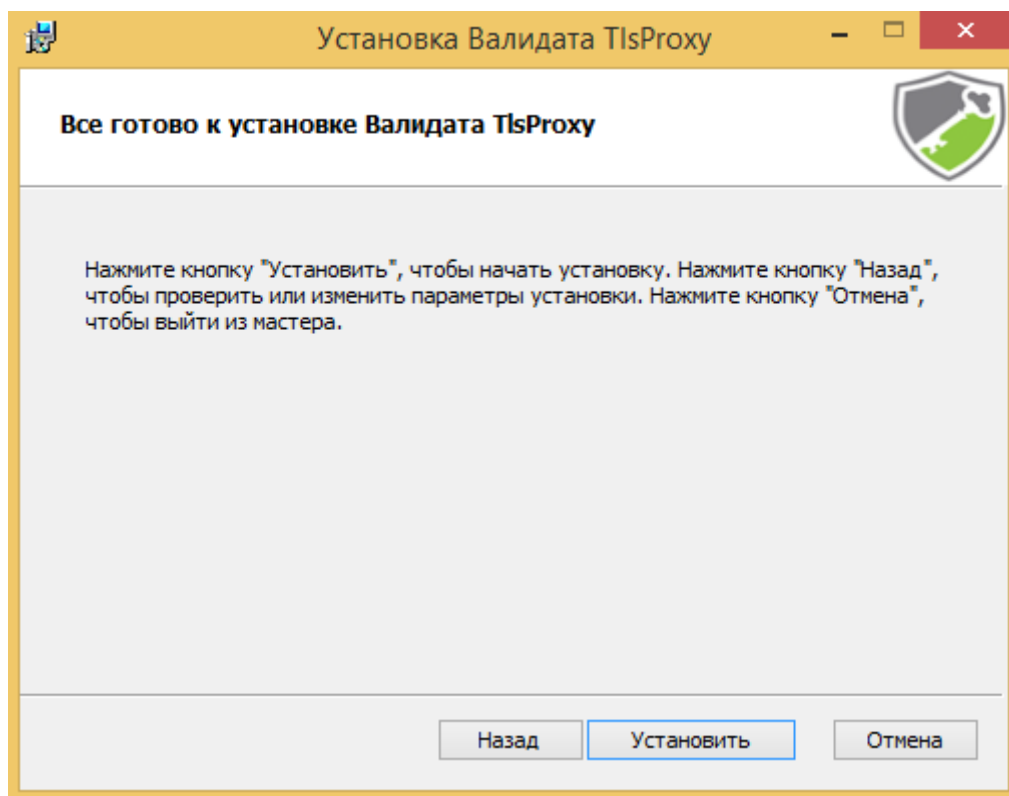


Рисунок 3 – Диалог готовности к установке

После отображения диалога о готовности к установке необходимо нажать кнопку «Далее» для проведения установки с указанными параметрами. По завершении процесса установки будет выдан диалог о завершении процесса установки (Рисунок 4).

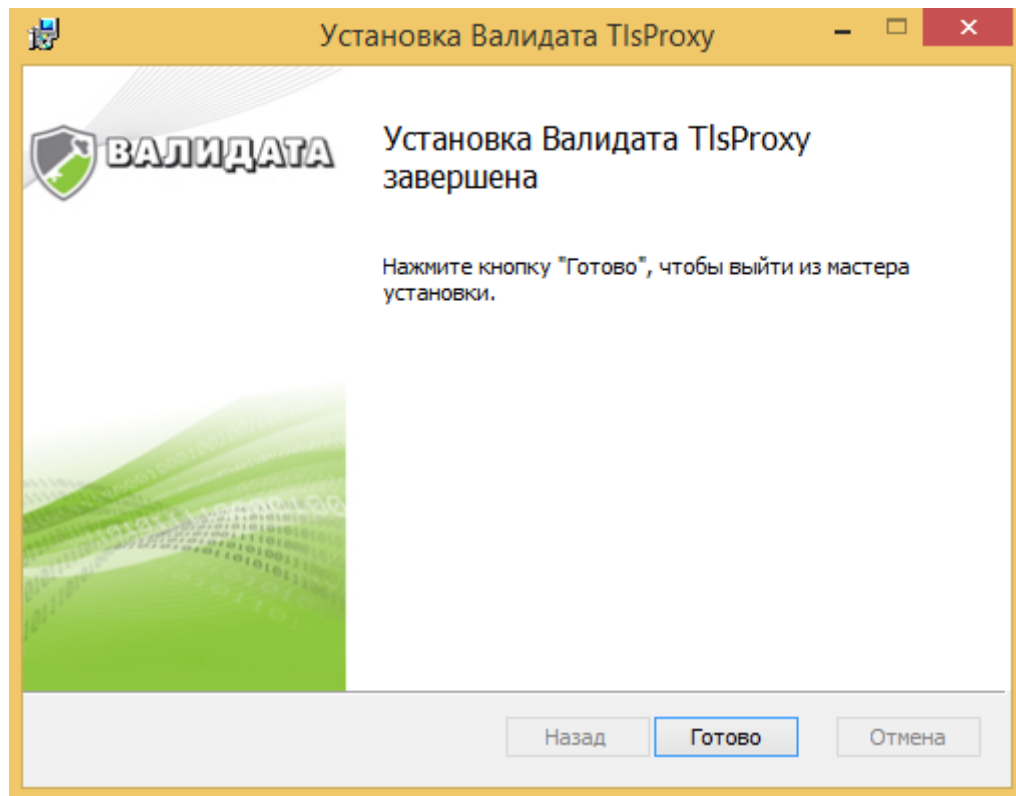


Рисунок 4 – Диалог завершения установки

Необходимо нажать кнопку «Готово» для завершения установки.

В случае ошибки при установке можно посмотреть протокол выполнения установки, который получается с помощью запуска программы установки со следующими параметрами: **msiexec /I\*v tlsproxy.log /I ztlsproxy\_x86.msi (или ztlsproxy\_x64.msi).**

После завершения процесса установки программы TLSProху должны быть выполнены действия, необходимые для осуществления регулярного контроля установленного ПО (см. документы ВАНБ.00060-06 93 02 «СКЗИ «Валидата CSP» версия 6. Контроль целостности. Руководство администратора информационной безопасности», ВАНБ.00060-06 92 01 «СКЗИ «Валидата CSP» версия 6. Программа контроля целостности. Руководство пользователя» и ВАНБ.00077-06 93 01 ««Валидата Клиент» версия 4. Руководство администратора информационной безопасности»).



## 3 НАСТРОЙКА ПРОГРАММЫ TLSPROXY

### 3.1 Требования к сертификатам

Для работы программы TLSProxy необходимо получить в удостоверяющем центре ключи ЭП и сертификаты ключей проверки ЭП, удовлетворяющие следующим требованиям:

- для клиентской ЭВМ: в сертификате должен присутствовать OID расширенного использования ключа (Extended Key Usage) **Проверка подлинности клиента** (1.3.6.1.5.5.7.3.2), а также должно быть указано разрешённое использование ключа ЭП (Key Usage) для выполнения ЭП;

- для серверной ЭВМ: в сертификате должен присутствовать OID расширенного использования ключа (Extended Key Usage) **Проверка подлинности сервера** (1.3.6.1.5.5.7.3.1), а также должно быть указано разрешённое использование ключа ЭП (Key Usage) для выполнения ЭП и шифрования. Дополнительно, DNS-имя сервера должно быть прописано в атрибуте CN X.500-имени владельца (Subject Name) и в альтернативном имени владельца (Subject Alternative Name) сертификата сервера.

### 3.2 Настройка конфигурационного файла

Настройка программы TLSProxy заключается в редактировании текстового конфигурационного файла программы *tlsproxy.conf*.

Пример конфигурационного файла *tlsproxy.conf*:

```
PSE=pse://signed/C:\\stores\\user\\local.pse
local=file://C:\\stores\\user\\local.gdbm
```

```
clientport=10101,192.168.1.1:4433
port=4433,80
```

```
log_path=C:\\logs\\
log_level=warning
```

```
timeout=60
```

```
aia_cdp=yes
```

```
crl_interval=3600
crl_crit=no
```

```
keep_alive=yes
```

Конфигурационный файл *tlsproxy.conf* состоит из списка параметров с присвоенными им значениями. Для присвоения заданного значения определённому параметру используется выражение вида **Параметр = Значение**. Символ '#' используется для обозначения комментария (комментарием считается весь текст, находящийся за символом '#' и до конца текущей строки).

В конфигурационном файле могут использоваться следующие параметры (Таблица 1).

Таблица 1 – Описание конфигурационного файла программы TLSProxy

Конфигурационный параметр	Возможные значения и описание применения
<b>PSE</b>	Значение единого указателя ресурса (Uniform Resource Locator, URI) персонального справочника пользователя (ПСП). Данный параметр является обязательным
<b>local</b>	Значение URI локального справочника пользователя (ЛСП). Данный параметр является обязательным
<b>pin</b>	Значение ПИН-кода для "тихой" загрузки ключа ЭП, если последний находится в ФКН «Валидата vdToken» версия 2.0
<b>clientport port</b>	<p>Значения правил перенаправления клиентских (<b>clientport</b>) и серверных (<b>port</b>) подключений. Хотя-бы одно из данных правил должно присутствовать в конфигурации. В качестве значений правил принимаются два адреса входящего и исходящего подключений вида ( <b>Адрес1, Адрес2</b> ), разделенные символом <b>','</b>. Каждый из адресов представляет собой пару вида ( <b>DNS-имя или IP-адрес : TCP-порт</b> ), разделенную символом <b>':'</b>, или только <b>TCP-порт</b> (в этом случае исходящие подключения производятся к узлу <b>localhost</b>).</p> <p><b>Адрес1</b> правила используется для входящих подключений, <b>Адрес2</b> - для исходящих. Для клиентских (<b>clientport</b>) правил входящее подключение защищено протоколом TLS, для серверных (<b>port</b>) правил - исходящее подключение защищено протоколом TLS.</p>
<b>rule</b>	<p>Значения правил фильтрации сертификатов противоположной стороны TLS соединения. Каждое правило задается набором операторов присваивания вида <b>Параметр=Значение</b>, разделенных символом <b>','</b>. Для соответствия с правилом сертификат должен удовлетворять всем операторам присваивания данного правила. Проверка сертификата выполняется в соответствии с последовательностью правил, до первого совпадения. Если проверяемый сертификат соответствует правилу из белого списка, то соединение устанавливается. Если проверяемый сертификат соответствует правилу из черного списка, то соединение разрывается. Если проверяемый сертификат не соответствует ни одному правилу, то соединение разрывается.</p> <p>Ниже описаны возможные значения параметров правил фильтрации:</p> <ul style="list-style-type: none"> <li>– <b>pattern</b> - фильтрация по имени владельца сертификата. Разрешено использовать специальные символы <b>'*'</b> и <b>'?'</b> для обозначение последовательности любых символов и строго одного любого символа соответственно;</li> <li>– <b>policy</b> - фильтрация по регламенту сертификата - объектному идентификатору (OID);</li> <li>– <b>eku</b> - фильтрация по расширенному использованию ключа сертификата - объектному идентификатору (OID);</li> <li>– <b>type</b> - задает принадлежность правила к белому или черному списку - число <b>0</b> обозначает белый список (по умолчанию), число <b>1</b> обозначает черный список</li> </ul>
<b>log_path</b>	Значение пути к каталогу для записи файлов протоколов (по умолчанию используется текущий каталог процесса)
<b>log_level</b>	Значение требуемого уровня протоколирования: <b>error</b> - сообщения об ошибках, <b>warning</b> - предупреждения, <b>info</b> - информационные сообщения, <b>debug</b> - отладочные сообщения (по умолчанию)
<b>timeout</b>	Значение таймаута ожидания соединения или передачи данных в секундах (по умолчанию равно <b>5</b> )
<b>min_thread</b>	Значение минимального количества свободных потоков, ожидающих входящих соединений (по умолчанию равно <b>10</b> )
<b>aia_cdp</b>	Значение, указывающее разрешен ли доступ к точкам доступа к Центру (AIA) и точкам распространения CAC (CDP) при построении и проверке цепочек сертификатов. Принимает значения <b>yes</b> и <b>no</b> (по умолчанию)
<b>silent</b>	Значение, указывающее разрешено ли отображение пользовательского интерфейса. Принимает значения <b>yes</b> и <b>no</b> (по умолчанию)
<b>crl_interval</b>	Значение интервала автоматического обновления CAC в секундах (по умолчанию равно <b>3600</b> )
<b>crl_crit</b>	Значение, указывающее критичность автоматического обновления CAC. Принимает значения <b>yes</b> (в этом случае ошибки обновления CAC протоколируются) и <b>no</b> (по умолчанию)

Конфигурационный параметр	Возможные значения и описание применения
<b>keep_alive</b>	Значение, отключающее применение интервала <b>timeout</b> для разрыва уже установленных, но при этом неактивных соединений. Принимает значения <b>yes</b> (по умолчанию) и <b>no</b>
<b>no_delay</b>	Значение, выключающее использование задержки передачи данных (алгоритм Нейгла, RFC 896) для локального и удаленного TCP сокетов. Принимает значения <b>yes</b> (по умолчанию) и <b>no</b>
<b>tls12</b>	Значение, принудительно включающее использование протокола TLS версия 1.2 для клиентских правил. Принимает значения <b>yes</b> и <b>no</b> (по умолчанию, используется протокол TLS версия 1.0)

## 4 ЗАПУСК И УСТАНОВКА СЕРВИСОВ ПРОГРАММЫ TLSPROXY

При успешной установке программы TLSProxy в системе устанавливается сервис с именем ***tlsproxy***, который можно запустить стандартными средствами ОС Windows (например, с помощью оснастки «Службы»). Данный сервис использует в качестве конфигурационного файла ***tlsproxy.conf*** из директории установки. Также поддерживаются следующие команды:

– ***tlsproxy debug [имя/путь файла]*** — запуск в режиме отладки с указанным конфигурационным файлом или файлом ***tlsproxy.conf*** из директории установки;

– ***tlsproxy install <имя сервиса> <имя/путь файла>*** — установка нового сервиса с заданными именем и файлом конфигурации.

*Примечание — путь до файлов конфигурации указывается либо абсолютно, либо относительно директории установки программы TLSProxy.*

## 5 УДАЛЕНИЕ ПРОГРАММЫ TLSPROXY

Перед запуском процедуры удаления ПО необходимо зарегистрироваться на компьютере с правами локального администратора.

Для удаления используйте пункт системного меню ОС Windows «**Пуск**», «**Настройка**», «**Панель управления**», «**Удаление программ**».

Выберите пункт «**Валидата TLSProxy**» и нажмите кнопку «**Добавить/Удалить**». В окне инсталлятора выберите пункт «**Удалить**» и нажмите кнопку «**Да**» (Рисунок 5).

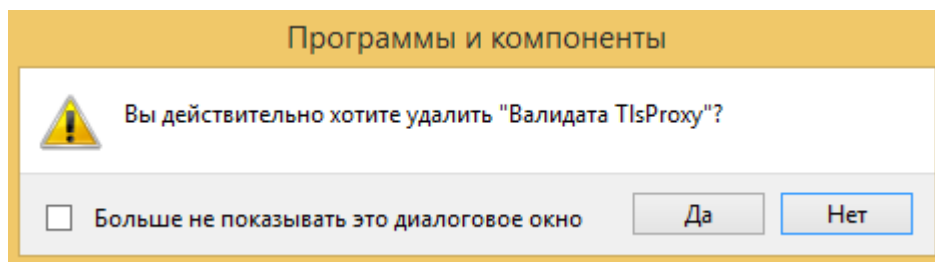


Рисунок 5 – Диалог подтверждения удаления программы TLSProxy

При удалении программы TLSProxy автоматически будет удален только сервис с именем **tlspoxy**. Остальные сервисы (при их наличии) необходимо удалить с использованием команды **sc delete [имя сервиса]**.

## 6 УСТАНОВКА И УДАЛЕНИЕ ПРОГРАММЫ TLSPROXY БЕЗ ВЫВОДА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА (В «ТИХОМ» РЕЖИМЕ)

Установка и удаление ПО выполняется утилитой ***msiexec.exe***, входящей в состав ОС Windows. Имя установочного файла (пакета ***MSI***) передается утилите ***msiexec.exe*** в командной строке сразу после ключа ***/i***. Имя удаляемого файла (пакета ***MSI***) передается утилите ***msiexec.exe*** в командной строке сразу после ключа ***/x***.

Для установки и удаления ПО без вывода пользовательского интерфейса утилите ***msiexec.exe*** необходимо в командной строке передать ключ ***/qn***.

Пример установки программы TLSProxy:

***msiexec.exe /qn /i ztlsproxy\_x64.msi***

Пример удаления программы TLSProxy:

***msiexec.exe /qn /x ztlsproxy\_x64.msi***

## **ПЕРЕЧЕНЬ СОКРАЩЕНИЙ**

ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение

## ПЕРЕЧЕНЬ РИСУНКОВ

1	Начальный диалог установки . . . . .	6
2	Диалог выбора директории установки . . . . .	6
3	Диалог готовности к установке . . . . .	7
4	Диалог завершения установки . . . . .	8
5	Диалог подтверждения удаления программы TLSProxy . . . . .	13



**ПЕРЕЧЕНЬ ТАБЛИЦ**

1	Описание конфигурационного файла программы TLSProху . . . . .	10
---	---	----

[illegible][illegible]