Общество с ограниченной ответственностью «АСП Лабс»

Программное обеспечение
автоматизированного рабочего места оператора информационной безопасности
программного комплекса «Аркан»
(ПО АРМ ИБ ПК «Аркан»)

Руководство администратора

СТРЦ.501540.001-01 РА 01

Листов 29

2018

Содержание

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ	–	автоматизированное рабочее место
МЭ	–	межсетевой экран
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
СВТ	–	средство вычислительной техники
СОВ	–	система обнаружения вторжений
СФ	–	среда функционирования
УЗ	–	устройство защиты

Аннотация

Данный документ представляет собой руководство для администратора системы ПК «Аркан».

Руководство администратора предназначено для следующих целей:

- установка и запуск ПО (название);
- поддержание работоспособности системы;
- резервное копирование и восстановление базы данных;
- добавление/удаление/изменение системных пользователей;
- выявление неисправностей.

1 Требования к среде функционирования

Минимальный состав используемых аппаратных (технических) средств представлен в таблице 1.

Таблица 1 – Технические характеристики СВТ

Наименование СВТ	**Технические характеристики**
Автоматизированное рабочее место (АРМ) оператора	– процессор - Intel Atom 1500 МГц и выше; – оперативной памяти - 1 Гб или больше; – жесткий диск - 60 Гб или больше, SATA/SCSI; – сетевое оборудование – наличие не менее одного сетевого интерфейса 100/1000 Base-T; – ОС Windows 8 и новее; – ОС Ubuntu 16.04 и новее.
Сервер	– процессор - Intel Core i5 2400 МГц и выше; – оперативной памяти - 8 Гб или больше; – жесткий диск - 60 Гб или больше, SATA/SCSI; – сетевое оборудование – наличие не менее одного сетевого интерфейса 100/1000 Base-T; – ОС Debian 9; – PostgreSQL 9.6; – Nginx 1.10.3-1 с пакетом обновлений deb9u1; – Redis-server 3:3.2.6-1 с пакетом обновлений deb8u5; – Django 1.11.10; – Uwsgi 2.0.15; – Amqp 1.4.9.
Устройство защиты	– процессор - Intel Core i5 2400 МГц и выше; – оперативной памяти - 8 Гб или больше; – жесткий диск - 60 Гб или больше, SATA/SCSI; – сетевое оборудование – наличие не менее 3-х сетевых интерфейсов 100/1000 Base-T; – ОС Debian 9; – Tshark 1.12.1 с пакетами обновлений g01b65bf-4 и deb8u13;

Список зависимостей среды функционирования ПО «Аркан» представлен ниже:

– tshark

– bridge-utils
– rsync
– screen
– python3
– python3-pip
– python3-netifaces
– python3-requests
– python3-simplejson
– python3-systemd
– libcurl3-gnutls
– libboost-random1.55.0
– libboost-system1.55.0
– libpugixml1
– libpcap0.8
– python
– python-dev
– python-virtualenv
– python-pip
– build-essential
– libpq-dev
– curl
– wget
– sshpass
– libssl-dev
– postgresql
– nginx
– redis-server
– websocket-client версии 0.40
– sysv-ipc версии 0.7.0
– json-cfg версии 0.4.2
– Django версии 1.11.4
– django-celery версии 3.2.2
– djangorestframework==3.6.3
– django-rest-swagger версии 2.0.5
– django-websocket-redis версии 0.5.0
– django-filter версии 1.0.4
– drf-nested-routers версии 0.11.0

- numpy версии 1.11.2
- psycopg2 версии 2.6.1
- rest_condition версии 1.0.2
- xmltodict версии 0.10.2
- jinja2 версии 2.9.6
- cefevent версии 0.4.8
- uwsgi версии 2.0.15
- amqp-1.4.9-py2.py3-none-any
- anyjson-0.3.3
- billiard-3.3.0.23
- kombu-3.0.37-py2.py3-none-any
- pytz-2018.3-py2.py3-none-any

2 Установка ПО «Аркан» устройства защиты

Установка ПО «Аркан» устройства защиты осуществляется из пакетов, предоставленных на съемном носителе.

Для установки ПО «Аркан» устройства защиты необходимо наличие активного интернет-соединения на СВТ, на которое будет производиться установка.

Для того, чтобы установить ПО «Аркан» устройства защиты необходимо выполнить следующие шаги:

1. Перенести пакеты с съемного носителя на устройство защиты.
2. Добавить путь до данной директории в `/etc/apt/sources.list` (в самый верх файла). Пример для `/home/ttyadmin/bins:`

```
deb [trusted=yes] file:///home/ttyadmin/bins ./
```

3. Установить пакеты и их зависимости, выполнив следующие команды:

```
sudo apt-get update
sudo apt-get install asap-shield
```

3 Установка ПО «Аркан» сервера

Для того, чтобы установить ПО «Аркан» сервера необходимо выполнить подготовительные работы, а затем саму установку.

Установка ПО «Аркан» сервера осуществляется из каталогов, предоставленных на съемном носителе.

Для установки ПО «Аркан» сервера необходимо наличие активного интернет-соединения на СВТ, на которое будет производиться установка.

Установка ПО «Аркан» сервера осуществляется только с помощью ОС семейства Linux.

3.1 Подготовительные работы

Подготовительные работы включают в себя следующие шаги:

1. Необходимо скопировать директорию «server» с накопителя в директорию на компьютере, с которого будет происходить установка.
2. Перейти в скопированный каталог.
3. Для установки начальных зависимостей выполнить команды:

```
sudo apt-get install python-dev
sudo apt-get install python-pip
```

4. Для установки утилиты virtualenv выполнить команды (не обязательно):

```
sudo apt-get install python-virtualenv
sudo apt-get install libpq-dev
```

5. Создать виртуальное окружение (если устанавливали virtualenv):

```
cd server
virtualenv -p /usr/bin/python2.7 venv
```

6. Активировать виртуальное окружение, то есть перейти в это окружение (если устанавливали virtualenv):

```
source venv/bin/activate
```

7. Установить все требуемые для сервера утилиты. Для этого необходимо перейти в директорию с проектом и выполнить следующие команды:

```
pip install --upgrade setuptools
cd requirements
pip2 install -r fab.txt
```

Примечание – все команды, начинающиеся с fab выполняются из корня скопированной директории установки сервера.

3.2 Установка серверной части

Для установки сервера ПО «Аркан» необходимо выполнить следующие шаги:

1. Подключиться к серверу: ssh <USERNAME>@<IP_ADDRESS>, где <USERNAME> - имя пользователя для подключения, <IP_ADDRESS> - адрес IP для удаленного подключения.

2. Набрать su и ввести пароль пользователя root.

3. Если нет sudo, установить:

```
apt-get install sudo
```

4. Создать пользователя server, если отсутствует (указав пароль):

```
adduser server
adduser server sudo
```

5. Выполнить команду fab deploy из директории server на СВТ, с которой производится установка ПО сервера.

6. Which server use? Выбрать номер, соответствующий необходимому адресу, либо выбрать пункт Custom server и ввести адрес СВТ, на которое будет устанавливаться ПО сервера.

7. При выборе Custom server необходимо ввести адрес устройства, на которое будет разворачиваться серверная часть, имя пользователя (server) и пароль к нему:

```
Please, enter host: 192.168.1.50
Please, enter username for hosts: server
[192.168.1.50] Login password for 'server':
```

8. Сгенерировать SSL-ключи:

```
Use default ssl template[y/n]? y
[192.168.1.50] out: Enter pass phrase for server.key:
[192.168.1.50] out: Verifying - Enter pass phrase for
server.key:
Enter your domain. For example: www.example.org:
[192.168.1.50] out: Enter pass phrase for server.key:
```

```
[192.168.1.50] out: Enter pass phrase for server.key:
Please, enter password for PKCS#12 certificate:
```

9. По умолчанию создается учетная запись администратора для api: adminapi - KillerBean@1401

10. После завершения установки и конфигурации сервера, его необходимо перевести в prod конфигурацию, вызвав команду fab finish_deploy.

11. Для перехода обратно в dev (debug) версию – fab enable_debug_mode.

12. Для получения ключей SSL для подключения ПО АРМ ПК «Аркан» необходимо выполнить команду fab get_ssl_crts и ввести данные для подключения к серверу. После выполнения операции в каталоге server/ssl/ будет создан подкаталог, в котором будут находиться необходимые для подключения ключи SSL.

4 Установка графического интерфейса ПО АРМ ИБ ПК «Аркан»

Для установки графического интерфейса необходимо выполнить следующие шаги:

1. Предварительно отредактировать файл «C:\Windows\System32\drivers\etc\hosts», добавив в конец файла строку: 10.10.10.122 asp-server-cert.io, где 10.10.10.122 – адрес СВТ сервера с ПК «Аркан».
2. Подключить FLASH-накопитель либо вставить CD-диск с ПО в дисковод компьютера.
3. Запустить установщик графического интерфейса и выполнить установку. Шаги установки представлены на рисунках 1 – 6.

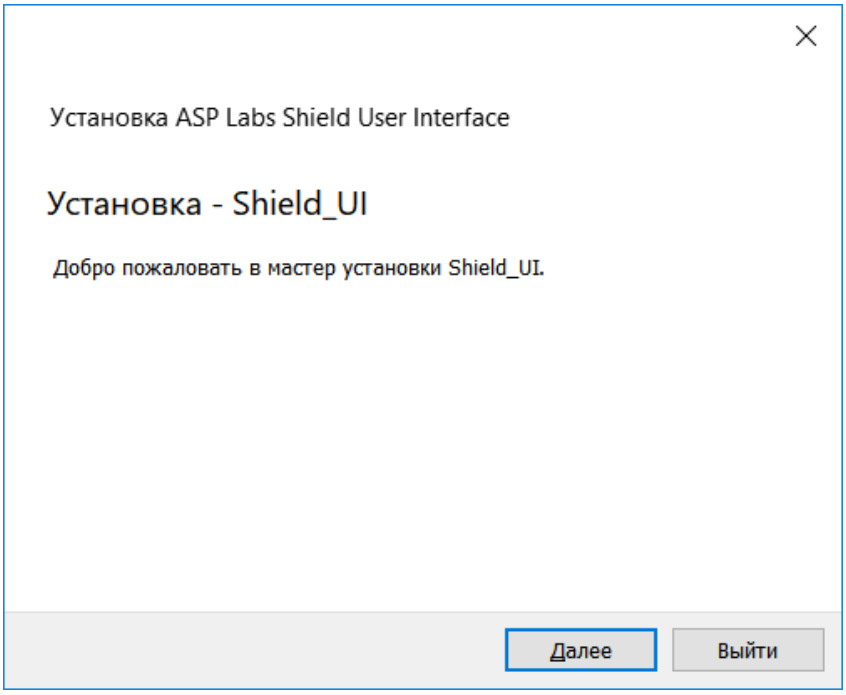

Рисунок 1 – Запуск установщика

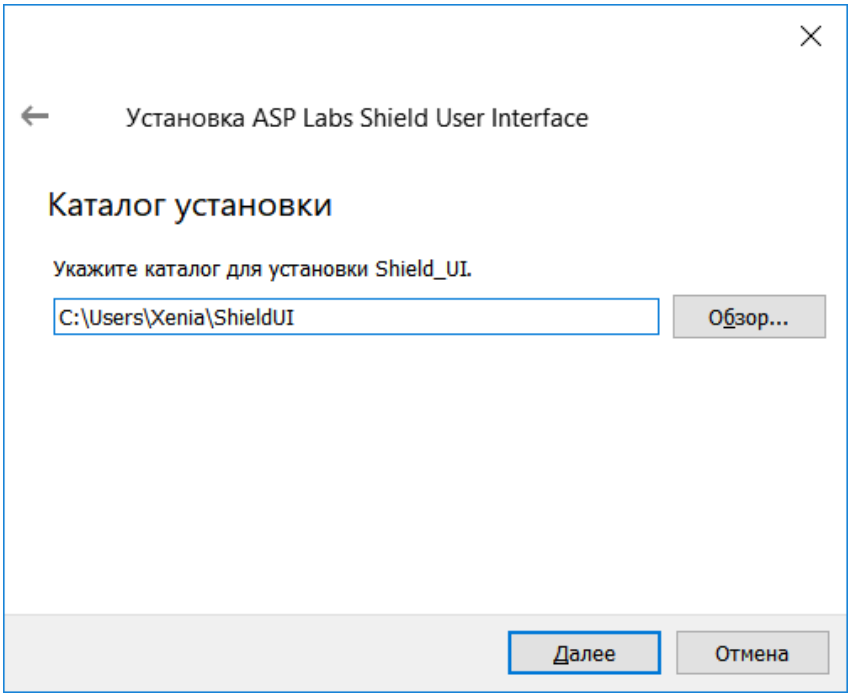

Рисунок 2 – Выбор директории для установки

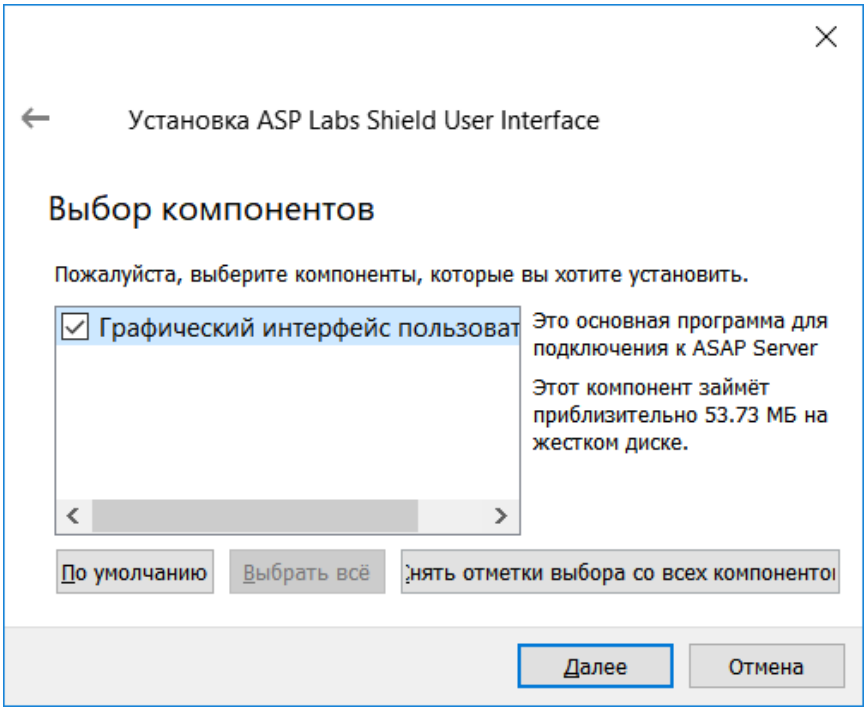

Рисунок 3 – Выбор компонентов

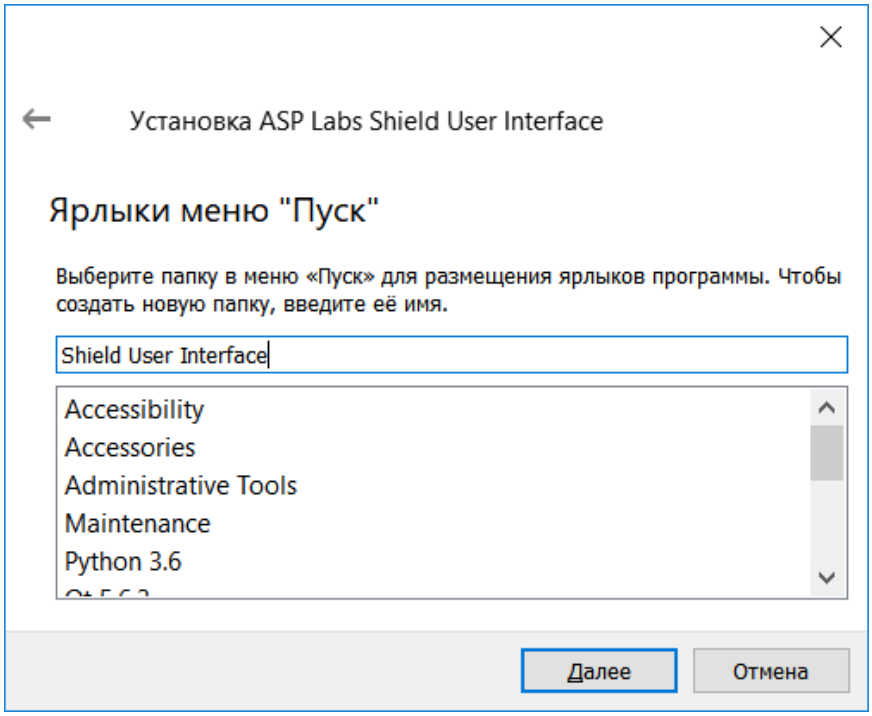

Рисунок 4 – Выбор ярлыка

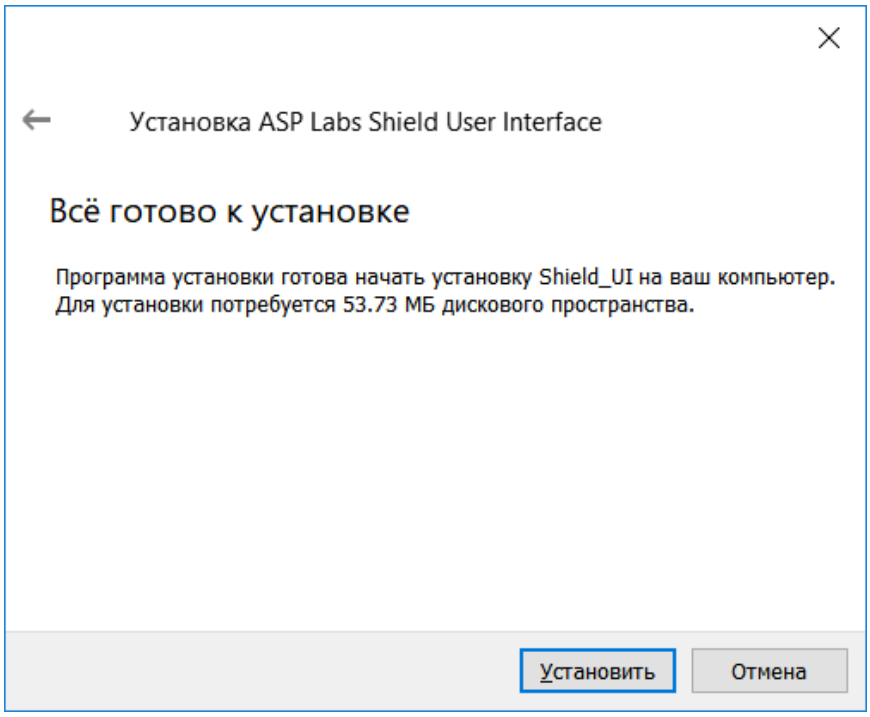

Рисунок 5 – Окно подтверждения установки

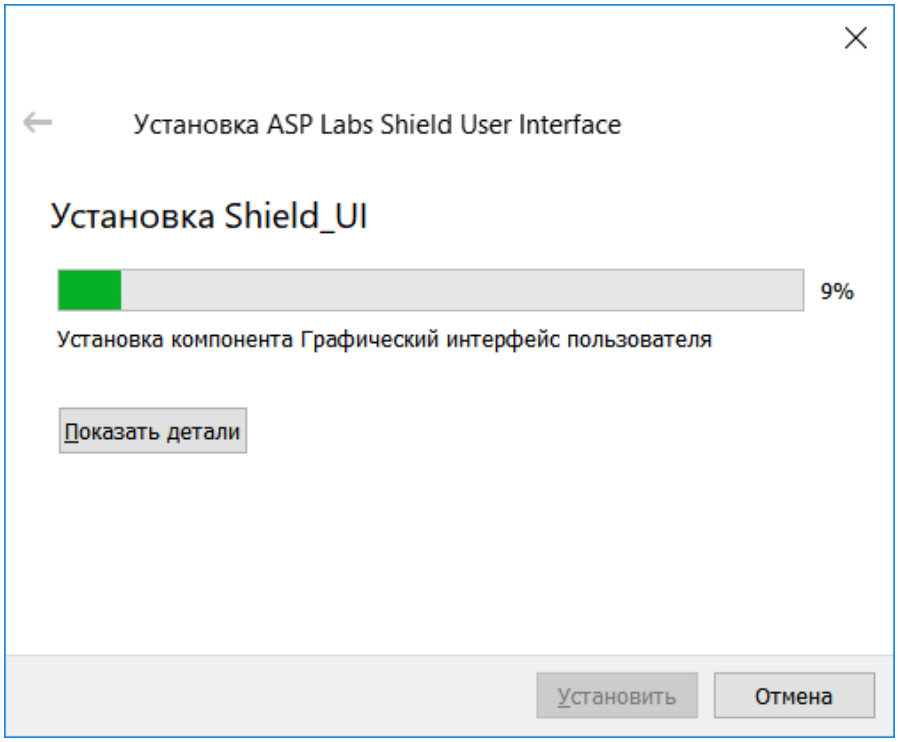

Рисунок 6 – Процесс установки

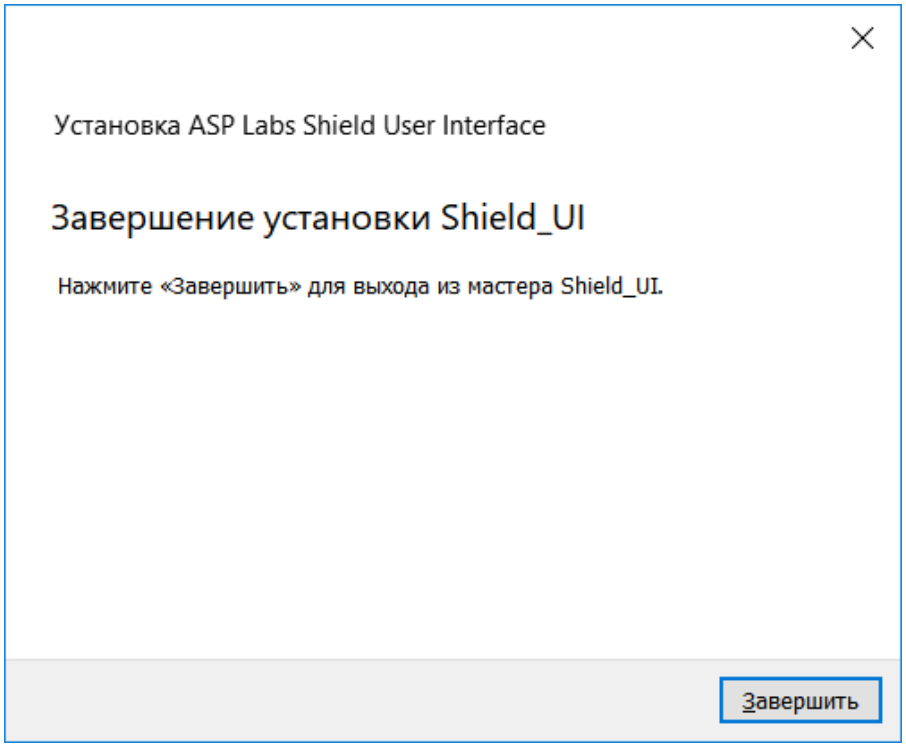

Рисунок 7 – Завершение установки

4. Запустить созданный ярлык с рабочего стола двойным нажатием левой кнопки мыши. Откроется следующее окно (Рисунок 8):

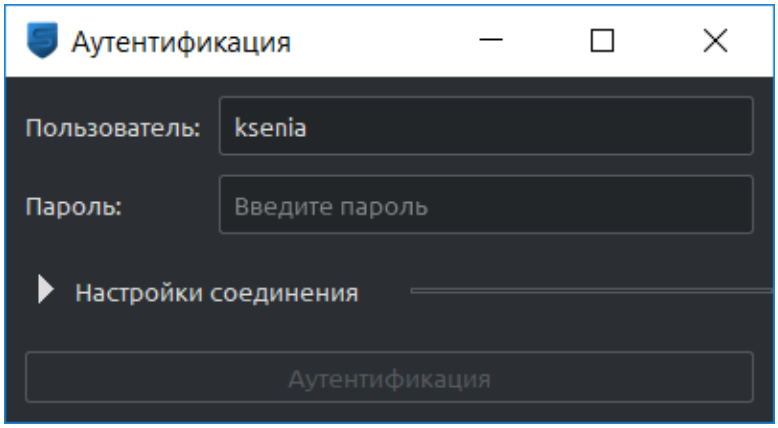

Рисунок 8 – Окно аутентификации

5. Необходимо ввести имя пользователя и пароль в поле «Пользователь» и «Пароль» соответственно. Имя пользователя по умолчанию имеет значение admin, пароль по умолчанию имеет значение password (после подключения необходимо изменить пароли уже созданных учетных записей со стандартных на уникальные).

6. Нажать на треугольник слева от надписи: «Настройки соединения». Окно изменит свой вид на следующее окно (Рисунок 9).

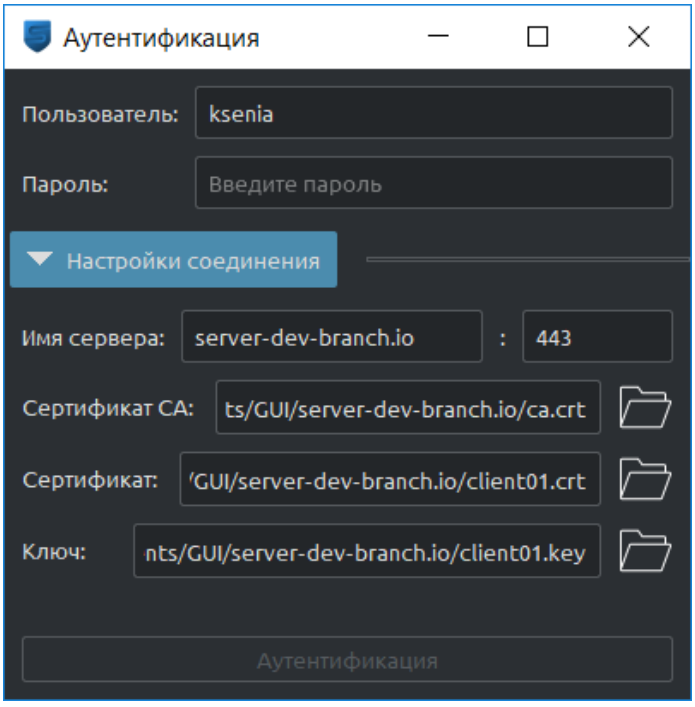

Рисунок 9 – Параметры окна аутентификации

7. В поле «Имя сервера» указать адрес из пункта 1 (asp-server-cert.io) и в поле после двоеточия «:» указать порт «443».

8. Нажать на кнопку открытия файла сертификата в строке «Сертификат CA» (Рисунок 10):

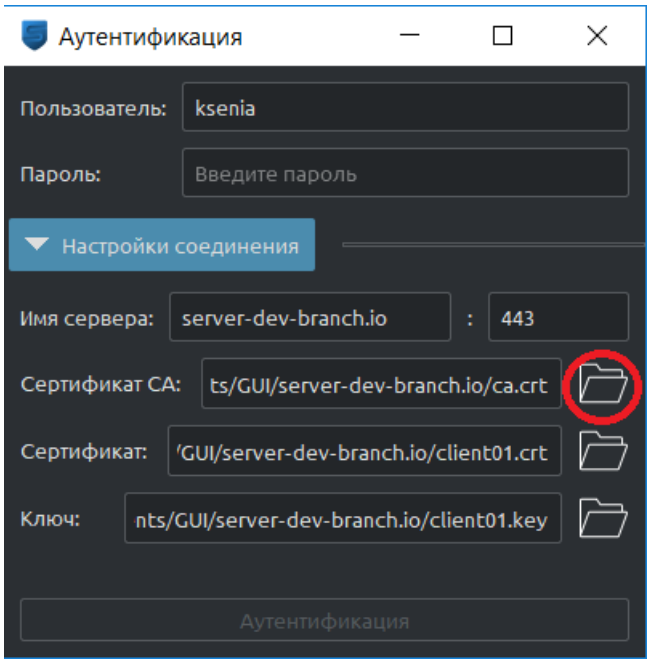

Рисунок 10 – Окно входа. Раздел выбора файлов сертификатов и ключей

9. Выбрать файл «ca.crt» из каталога с сертификатами, полученном при установке ПО сервера ПК «Аркан».

10. Нажать на кнопку открытия файла сертификата в строке «Сертификат» (Рисунок 11):

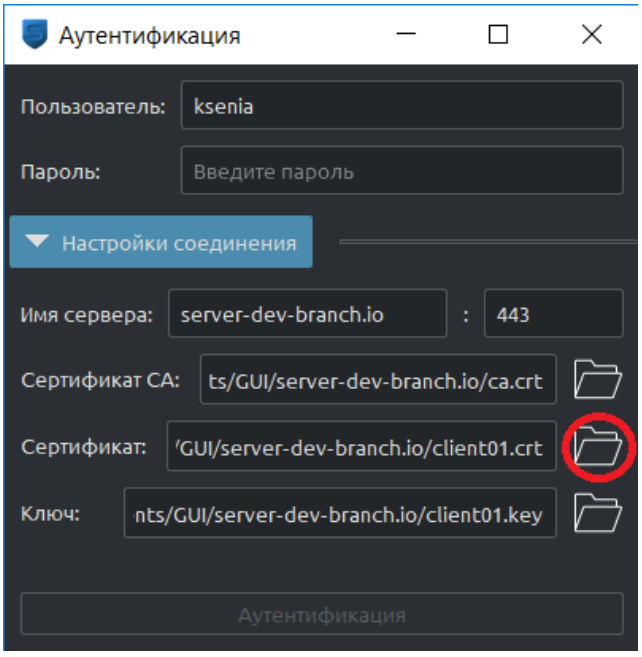

Рисунок 11 – Окно входа. Раздел выбора файлов сертификатов и ключей

11. Выбрать файл «client01.crt» из каталога с сертификатами, полученном при установке ПО сервера ПК «Аркан».

12. Нажать на кнопку открытия файла сертификата в строке «Ключ» (Рисунок 12):

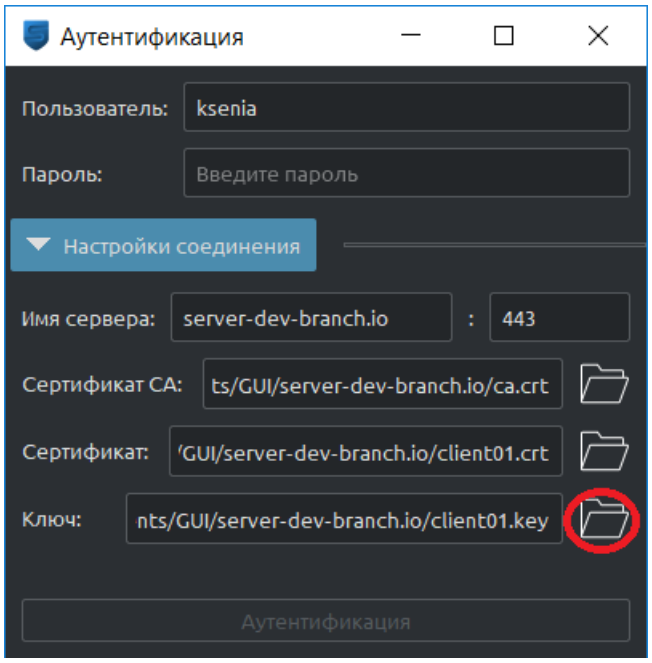

Рисунок 12 – Окно входа. Раздел выбора файлов сертификатов и ключей

13. Выбрать файл «client01.key» из папки «certificates» из каталога с сертификатами, полученном при установке ПО сервера ПК «Аркан».

14. Для работы с приложением нажмите кнопку «Аутентификация».

Примечание: Инструкция по работе с приложением описана в «Руководстве оператора».

5 Подключение по SSH

Для подключения по SSH к устройству защиты необходимо иметь возможность подключения по SSH с локальной машины. Для ОС Linux это ПО, входящее в стандартный набор, в большинстве случаев, а для ОС Windows необходимо использовать различное стороннее ПО для подключения (PuTTY, SecureCRT и другие). В данном руководстве подключение рассмотрено на примере использования командной строки Linux (для стороннего ПО необходимо использовать руководство к соответствующему ПО).

В первую очередь необходимо иметь следующие данные:

- имя учетной записи на удаленной машине;
- пароль к соответствующей учетной записи;
- IP-адрес удаленной машины.

Для подключения к удаленной системе с помощью SSH в Linux существует одноименный инструмент – ssh. Установить OpenSSH (если системе не удается найти команду «ssh») можно из терминала командой: `sudo apt-get install ssh` либо с помощью другого пакетного менеджера установить ssh. Базовый вид команды: `ssh <удаленный_хост>`. В данном примере фраза «удаленный_хост» заменяет IP-адрес или доменное имя хоста, к которому нужно подключиться. Эта команда предполагает, что имя пользователя на удаленной и локальной системах совпадают. Если же на удаленной системе установлено другое имя пользователя, его нужно указать с помощью следующего синтаксиса:

`ssh <имя_пользователя>@<удаленный_хост>`

После подключения к серверу необходимо указать пароль, чтобы пройти авторизацию. Чтобы вернуться в локальную сессию, необходимо ввести: `exit`.

Изменение пароля

Для смены пароля пользователя в Linux, необходимо выполнить в терминале (или консоли) следующую команду, предварительно войдя от имени пользователя, для которого необходимо сменить пароль: `passwd`. После ввода этой команды, система потребует корректно и дважды ввести новый пароль. Если необходимо сменить пароль другого пользователя, то необходимы права суперпользователя – root. Если у пользователя отсутствуют root права, то необходимо ввести в терминале команду: `sudo passwd <имя_пользователя>`,

где <имя_пользователя> – логин пользователя, для которого меняется пароль.

После чего введите пароль суперпользователя root. После ввода пароля суперпользователя необходимо корректно и дважды ввести новый пароль для пользователя.

Создание и удаление пользователя

Добавление пользователя

Добавление пользователя осуществляется при помощи команды `useradd`. Пример использования: `sudo useradd <username>`. Эта команда создаст в системе нового пользователя <username>. Чтобы изменить настройки создаваемого пользователя, используются ключи, представленные в таблице 3.

Таблица 3 – Ключи

Ключ	**Описание**
-b	Базовый каталог. Это каталог, в котором будет создана домашняя папка пользователя. По умолчанию /home.
-c	Комментарий. В нем вы можете напечатать любой текст.
-d	Название домашнего каталога. По умолчанию название совпадает с именем создаваемого пользователя.
-e	Дата, после которой пользователь будет отключен. Задается в формате ГГГГ-ММ-ДД. По умолчанию отключено.
-f	Количество дней, которые должны пройти после устаревания пароля до блокировки пользователя, если пароль не будет изменен (период неактивности). Если значение равно 0, то запись блокируется сразу после устаревания пароля, при -1 - не блокируется. По умолчанию -1.
-g	Первичная группа пользователя. Можно указывать как GID, так и имя группы. Если параметр не задан будет создана новая группа название которой совпадает с именем пользователя.
-G	Список вторичных групп, в которых будет находится создаваемый пользователь
-k	Каталог шаблонов. Файлы и папки из этого каталога будут помещены в домашнюю папку пользователя. По умолчанию /etc/skel.
-m	Ключ, указывающий, что необходимо создать домашнюю папку. По умолчанию домашняя папка не создается.
-p	Зашифрованный пароль пользователя. По умолчанию пароль не задается, но учетная пользователь будет заблокирован до установки пароля.
-s	Оболочка, используемая пользователем. По умолчанию /bin/sh.
-u	Вручную задать UID пользователю.

Параметры создания пользователя по умолчанию

Если при создании пользователя не указываются дополнительные ключи, то берутся настройки по умолчанию. Эти настройки доступны по команде: `useradd -D`.

Результат будет следующий:

```
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/sh
SKEL=/etc/skel
```

Если необходимо изменить настройки, нужно выполнить следующую команду: `sudo useradd -D -s /bin/bash`, где s – это ключ из таблицы 3.

Таким образом, могут быть заданы параметры, определяемые только ключами `-b, -e, -f, -g, -s`.

Изменение пользователя

Изменение параметров пользователя происходит с помощью утилиты usermod. Пример использования: `sudo usermod -c "Эта команда поменяет комментарий пользователю" vasyapupkin`, usermod использует те же опции, что и useradd.

Удаление пользователя

Для удаления пользователя используется команда – deluser. Команда имеет следующий вид: `$ deluser «параметры пользователя»`.

Настройки команды deluser находятся в файле /etc/deluser.conf. В этом файле предоставляется возможность просматривать и при необходимости изменять настройки, выполнив следующую команду:

```
$ vi /etc/deluser.conf
```

Подробнее настройки рассмотрены ниже:

- REMOVE_HOME – удалить домашний каталог пользователя;
- REMOVE_ALL_FILES – удалить все файлы пользователя;

- BACKUP – выполнять резервное копирование файлов пользователя;
- BACKUP_TO – папка для резервного копирования;
- ONLY_IF_EMPTY – удалить группу пользователя если она пуста.

Эти настройки определяют поведение утилиты по умолчанию, когда выполняется удаление пользователя.

Также существуют параметры для команды deluser:

- - system – удалить только если это системный пользователь;
- - backup – делать резервную копию файлов пользователя;
- - backup-to – папка для резервных копий;
- - remove-home – удалять домашнюю папку;
- - remove-all-files – удалять все файлы пользователя в файловой системе.

6 Настройка резервного копирования

Для выполнения резервного копирования базы данных ПК «Аркан» по УЗ ПК «Аркан» требуется выполнить следующую команду:

```
PGPASSWORD=passwd pg_dump -U postgres -Fc shield > path,
```

где, passwd – пароль от базы данных, а path – путь к файлу, в который будет сохранена резервная копия.

Для восстановления базы данных ПК «Аркан» из резервной копии необходимо выполнить следующие команды на УЗ ПК «Аркан»:

```
echo "drop schema public cascade;" | PGPASSWORD=passwd psql -U postgres shield
echo "create schema public;" | PGPASSWORD=passwd psql -U postgres shield
PGPASSWORD=passwd pg_restore -U postgres -d shield < path
```

где, passwd – пароль от базы данных, а path – путь к файлу резервной копии.

Для настройки автоматического создания резервных копий необходимо выполнить следующие шаги:

1. Создать bash скрипт на УЗ ПК «Аркан». Для этого необходимо создать файл с расширением «*.sh» со следующим содержимым:

```
#!/bin/sh
PGPASSWORD= passwd
export PGPASSWORD
pathB=path
dbUser=postgres
database=shield
find $pathB -mtime +days -delete
pg_dump -U $dbUser -Fc $database  > $pathB/pgsql_$(date "+%Y-%m-%d-%H-%M")
unset PGPASSWORD,
```

где, path – путь к папке, в которой будут храниться резервные копии, passwd – пароль от базы данных, days – количество дней в течении которых храниться резервная копия

2. Создать задание в планировщике cron, для запуска, описанного выше скрипта:

```
0 * */days * * path,
```

где, days – периодичность снятия резервной копии в днях, path – путь к файлу со скриптом.

7 Административная утилита

Административная утилита – это вспомогательная компьютерная программа для диагностирования и исправления неполадок в ПО АРМ ИБ ПК «Аркан». Для того чтобы её использовать необходимо выполнить следующие действия:

1. Запустите приложение с правами администратора (Рисунок 13).

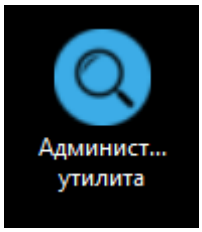

Рисунок 13 – Ярлык запуска административной утилиты

2. В поле адреса хоста следует указывать IP адрес устройства защиты (УЗ) (DNS не поддерживается).

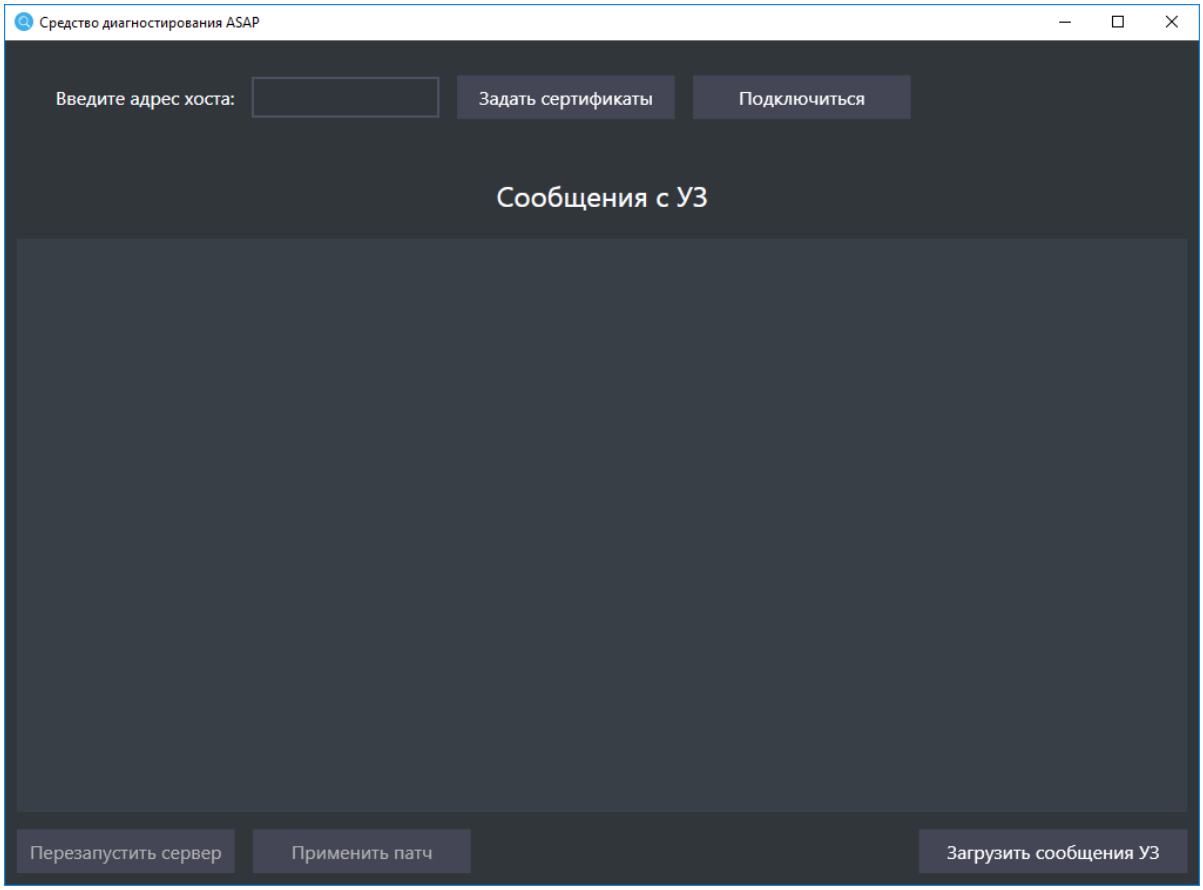

Рисунок 14 – Главное окно приложения

3. Перед подключением задать сертификаты, которые Вы используете при работе с ПК «Аркан».

4. Произвести подключение к устройству защиты, нажав на кнопку «Подключиться». Вам станут доступны следующие возможности:

- *Перезапустить сервер* – позволяет перезапустить сервер.
- *Применить патч* – при нажатии на кнопку нужно выбрать файл C:\Program Files (x86)\AsapDiagnosticTools\patch.asap. Этот файл содержит необходимые исправления в специальном формате. После применения патча в той же директории (C:\Program Files (x86)\AsapDiagnosticTools\), будет сгенерирован файл diagnostics.asap. Этот файл необходимо отправить разработчику ПК «Аркан» для дальнейшей диагностики.

Загрузить сообщения УЗ – позволяет сохранить содержимое вывода в текстовом файле.

8 Диагностика и устранение неполадок

В ПО АРМ ИБ ПК «Аркан» в разделе «Устройства» при переходе на конкретное устройство защиты во вкладке «Сервисы» (Рисунок 15) содержится список всех сервисов из состава ПО АРМ ИБ ПК «Аркан», использующихся на УЗ. В таблице представлены имя сервисов, их тип, статус и время с последнего перезапуска.

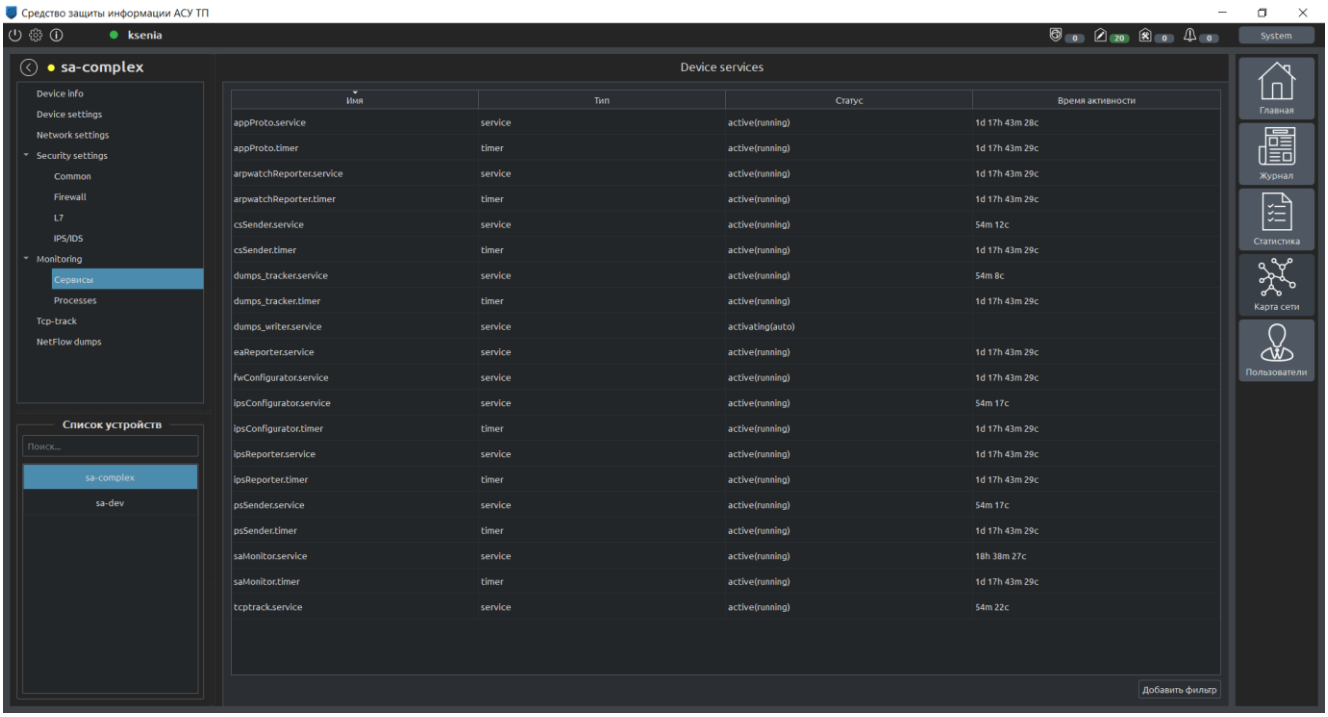

Рисунок 15 – Сервисы

В штатном режиме работы системы все сервисы должны быть активны и работать без ошибок (статус active(running)), а состояние устройства защиты должно быть «Активно» и иметь индикатор активности зеленого цвета.

В случае, если один из сервисов имеет статус, отличный от нормального (active(running)), необходимо, подключившись по SSH к устройству зашиты выполнить команду:

`sudo systemctl status -l <имя_сервиса>`,

где <имя_сервиса> - имя сервиса, состояние которого необходимо исправить.

Данная команда позволит вывести последние записи системного журнала сервиса. Если же последних записей недостаточно, то необходимо выполнить команду:

`sudo journalctl -u <имя_сервиса> -b`,

где <имя_сервиса> - имя сервиса, для которого необходимо открыть полный журнал (журнал будет иметь записи с момента последнего запуска до настоящего времени).

С помощью информации, доступной в журналах становится возможным выполнить восстановление работоспособности сервиса. Если восстановление невозможно, необходимо обратиться к разработчику с журналами неисправных сервисов.

9 Возможные ошибки и их решение

7.1 Команды выполнены не от имени суперпользователя root:

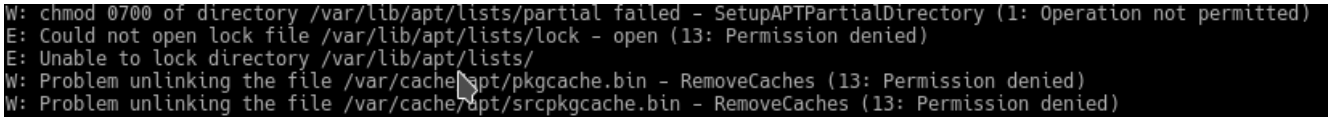

Рисунок 16 – Команды выполнены не от имени суперпользователя root

Необходимо выполнить команду от имени суперпользователя root.

7.2 Отсутствует соединение с интернетом:

Рисунок 17 – Отсутствует соединение с интернетом

Необходимо обеспечить соединение с интернетом.