ПК «СОВ «Плутон-М1.0»

Краткая инструкция по установке

Листов 18

Инв.№ подл.	Подп. и дата	Взам.инв.№	Инв.№ дубл.	Подп. и дата

2018

СОДЕРЖАНИЕ

1. СРЕДА УСТАНОВКИ

Установка программного обеспечения программного комплекса «Система обнаружения вторжений «Плутон-М1.0» (далее – ПК «СОВ «Плутон-М1.0») должна выполняться на технических средствах с установленной операционной системой Astra linux Special Edition «Смоленск» 1.5.

2. ЗАГРУЗКА АРХИВА С УСТАНОВОЧНЫМИ ПАКЕТАМИ

Архив с дистрибутивом программного обеспечения компонентов ПК «СОВ «Плутон-М1.0» размещён по ссылке: http://files.jet.su/d/plt. Пароль к архиву предоставляется по запросу на адрес электронной почты pluton@jet.su.

3. ОБЩИЕ СВЕДЕНИЯ

ПК «СОВ «Плутон-М1.0» состоит из двух программных средств (далее – ПС):

- Программное средство «СУС-Плутон-М1.0» (далее - ПС СУС) ДБАР.62.01.12.000.182-01;
- Программное средство «Сенсор-Плутон-М1.0» (далее - ПС Сенсор) ДБАР.62.01.12.000.183-01.

В комплект поставки дистрибутива ПК «СОВ «Плутон-М1.0» входят два ISO образа – один с установочными пакетами ПК «СОВ «Плутон-М1.0», другой со средой функционирования. Установка обоих ПС происходит из одного дистрибутива. При установке в качестве параметра задается тип устанавливаемого ПС.

4. УСТАНОВКА ПС СУС

Перед установкой необходимо выполнить следующие подготовительные операции с техническим средством, на которое устанавливается ПС СУС:

1) Проверить правильность подключения клавиатуры и дисплея (KVM-консоли) к ТС.

2) В случае использования KVM-консоли – переключить KVM-консоль на взаимодействие с ТС.

3) Включить ТС.

4) Если внешний носитель с установочными пакетами ПС СУС – оптический диск, то при отсутствии в составе ТС оптического привода CD-ROM необходимо подключить переносной CD-ROM-привод к свободному USB-разъёму ТС.

5) Убедиться, что основной порт сетевого интерфейса ПС СУС не переключён на bypass-порт.

После выполнения всех указанных выше действий необходимо выполнить следующие подготовительные операции с программными средствами, под функционированием которых работает ПС СУС:

1) Настроить в конфигурационном файле /etc/network/interfaces сетевой интерфейс, с помощью которого будет выполняться взаимодействие компонента с установленным ПС СУС с другими компонентами. Пример настройки выглядит следующим образом:

```
auto eth3
iface eth3 inet static
address 192.168.1.1
netmask 255.255.255.0
```

2) Для генерации корректного SSL-сертификата и для настройки протокола HTTPS, который будет поддерживать взаимодействие компонентов, необходимо

настроить сетевое взаимодействие ПС СУС и подчинёнными ему компонентами в таблице /etc/hosts. Для этого необходимо:

а) указать команду `hostname -f`, которая вернёт полное доменное имя (FQDN) сервера.

б) использовать полученное полное доменное имя для установки доменного имени сервера в файле /etc/hosts. Для этого указать следующую команду:

`# ipaddress fqdn hostname`, где

– `ipaddress` – IP-адрес хоста, например, 192.168.1.1;

– `fqdn` – полное доменное имя хоста, полученное командой `hostname -f`, например, pluton-sensor-1.domain.tld;

– `hostname` – доменное имя хоста, например, pluton-sensor-1

Пример команды:

```
192.168.1.1 pluton-sensor-1.domain.tld pluton-sensor-1
```

3) Для генерации корректного SSL-сертификата и для настройки протокола HTTPS, необходимо настроить системное время. Чтобы узнать точное время с поправкой на часовой пояс, необходимо указать команду:

```
# date
```

После выполнения команды в командной строке пользователя появится сообщение с указанием временной метки и часового пояса:

```
Tue Mar 6 13:20:51 MSK 2018
```

4) Убедиться, что на сервере доступен установочный диск с Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

После проведения всех подготовительных действий для установки ПС СУС на ТС необходимо выполнить следующие инструкции:

1) Подключить внешний носитель с установочными пакетами и средой функционирования ПК «СОВ «Плутон-М1.0» ДБАР.62.01.12.000.181-01 к ТС одним из следующих способов:

– если внешний носитель – оптический диск, то поместить внешний носитель в оптический привод CD-ROM;

– если внешний носитель – USB-накопитель, то использовать для подключения USB-порт.

2) Нажать на клавиатуре (KVM-консоли) ТС клавиши Ctrl+Alt+F2 и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root». После ввода учётных данных привилегированного технологического пользователя этот пользователь получит доступ к командной строке операционной системы

3) Смонтировать внешний носитель. Для этого указать команду:

– для установки через оптический привод CD-ROM

```
# sudo mount -r -t iso9660 /dev/cdrom /media/cdrom
```

– для установки через USB-порт

```
# sudo mount -r -t iso9660 /dev/sdb
```

4) Перейти в каталог /media/cdrom, выполнив команду:

```
# cd /media/cdrom
```

5) Выполнить команду установки ПС СУС. Для этого ввести следующие параметры:

– тип устанавливаемого компонента -- scs;

– географические координаты ПС СУС с ключами --ln (долгота) и --lt (широта);

– IP-адрес сервера синхронизации времени с ключом --ntp;

– путь до оптического диска со средой функционирования ПС СУС -- prt.

Примеры команды:

```
# sudo bash ./pluton_install.sh scs --ln <долгота ПС СУС> --lt <широта ПС СУС> --ntp <IP-адрес сервера синхронизации времени> --prt <путь к точке
```

```
монтирования оптического диска со средой функционирования ПС СУС>
```

При установке ПС СУС автоматически создаётся технологический пользователь «admin».

По завершении установки необходимо указать команду перезагрузки системы:

```
# sudo init 6
```

Внимание! Выполнение перезагрузки после установки обязательно, в противном случае корректная настройка и запуск ПС СУС будут невозможны.

После перезагрузки следует:

1) Нажать на клавиатуре (KVM-консоли) ТС клавиши Ctrl+Alt+F2.

2) Ввести рабочее имя и пароль технологического пользователя (заводская установка – «admin»/ «54C?1W9o#I»).

После этого будет выполнен вход в командную среду технологического пользователя, предоставляющую доступ к технологическим возможностям ПС СУС.

3) Изменить пароль технологического пользователя. Для этого в командной среде технологического пользователя указать команду:

```
# passwd admin
```

4) В ответ на запрос системы дважды ввести новый пароль согласно требованиям парольной политики ПК СОВ.

5) Создать при необходимости дополнительных технологических пользователей – указать команду:

```
# sudo useradd <имя_пользователя>
```

6) Настроить программные средства. Инструкции по настройке и эксплуатации ПС СУС см. в документе ДБАР.62.01.12.000.182-01 32 Руководство системного программиста ПС СУС.

7) Завершить сеанс работы – на клавиатуре KVM-консоли нажать клавиши Ctrl+D.

5. УСТАНОВКА ПС СЕНСОР

Предварительно необходимо выполнить подготовительные операции с техническим средством, на которое будет устанавливаться ПС Сенсор:

1) Проверить правильность подключения клавиатуры и дисплея (KVM-консоли) к ТС.

2) В случае использования KVM-консоли – переключить KVM-консоль на взаимодействие с ТС.

3) Включить ТС.

4) Если внешний носитель с установочными пакетами ПС Сенсор – оптический диск, то при отсутствии в составе ТС оптического привода CD-ROM необходимо подключить переносной CD-ROM-привод к свободному USB-разъёму ТС.

5) Убедиться, что основной порт сетевого интерфейса ПС Сенсор не переключён на bypass-порт.

После выполнения всех указанных выше действий необходимо выполнить подготовительные операции с программными средствами, под функционированием которых работает ПС Сенсор:

6) Настроить в конфигурационном файле /etc/network/interfaces сетевой интерфейс, с помощью которого будет выполняться взаимодействие ПС Сенсор с ПС СУС. Пример настройки выглядит следующим образом:

```
auto eth3
iface eth3 inet static
address 192.168.1.1
netmask 255.255.255.0
gateway 192.168.1.2
```

7) Для генерации корректного SSL-сертификата и настройки протокола HTTPS, который будет поддерживать взаимодействие компонентов, необходимо настроить сетевое взаимодействие ПС Сенсор и вышестоящего ПС СУС в таблице

/etc/hosts.

Для этого необходимо:

в) запустить команду `hostname -f`, которая вернёт полное доменное имя (FQDN) сервера;

г) использовать полученное полное доменное имя для установки доменного имени сервера в файле /etc/hosts. Для этого запустить команду:

`# ipaddress fqdn hostname`, где

– `ipaddress` – IP-адрес хоста, например, 192.168.1.1;

– `fqdn` – полное доменное имя хоста, полученное командой `hostname -f`, например, pluton-sensor-1.domain.tld;

– `hostname` – доменное имя хоста, например, pluton-sensor-1

Пример команды:

```
192.168.1.1 pluton-sensor-1.domain.tld pluton-sensor-1
```

8) Для генерации корректного SSL-сертификата и настройки протокола HTTPS необходимо настроить системное время. Чтобы узнать точное время с поправкой на часовой пояс, необходимо запустить команду:

```
# date
```

После выполнения команды в командной строке появится сообщение с указанием временной метки и часового пояса:

```
Tue Mar 6 13:20:51 MSK 2018
```

9) Установить пакеты `ifenslave` и `bridge-utils`. Для этого запустить команду:

```
# apt-get install bridge-utils ifenslave
```

10) Настроить сетевые интерфейсы, с помощью которых ПС Сенсор получает сетевой трафик, предназначенный для анализа. ПС Сенсор анализирует сетевой трафик, который направляют на агрегированный виртуальный сетевой интерфейс `bond0`. В `bond0` могут быть объединены несколько физических

сетевых интерфейсов. Пример объединения физических интерфейсов в `bond0` представлен на рисунке 1 .

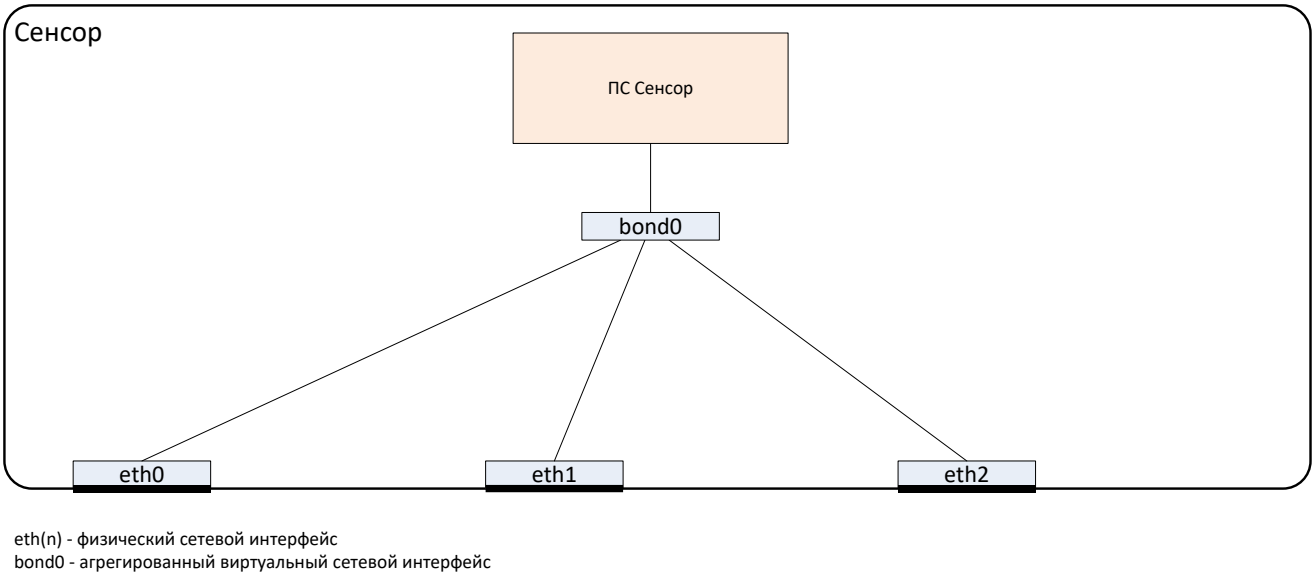

Рисунок 1 – Объединения физических интерфейсов в bond0

Пример настройки `bond0` в конфигурационном файле /etc/network/interfaces выглядит следующим образом:

```
auto eth0
iface eth0 inet static
address 0.0.0.0

auto eth1
iface eth1 inet static
address 0.0.0.0

auto eth2
iface eth2 inet static
address 0.0.0.0

auto bond0
```

```
iface bond0 inet static
address 0.0.0.0
slaves eth0 eth1 eth2
bond-mode balance-rr
bond-miimon 100
bond-downdelay 200
bond-updelay 200
```

В зависимости от используемых физических сетевых интерфейсов может возникать следующая ситуация: после отсоединении от физического сетевого интерфейса сетевого кабеля `bond0` автоматически не восстанавливает получение сетевого трафика даже после восстановления подключения кабеля.

Для решения этой проблемы можно использовать программный сетевой мост. В этом случае пример объединение физических интерфейсов в `bond0` выглядит следующим образом (см. рисунок 2).

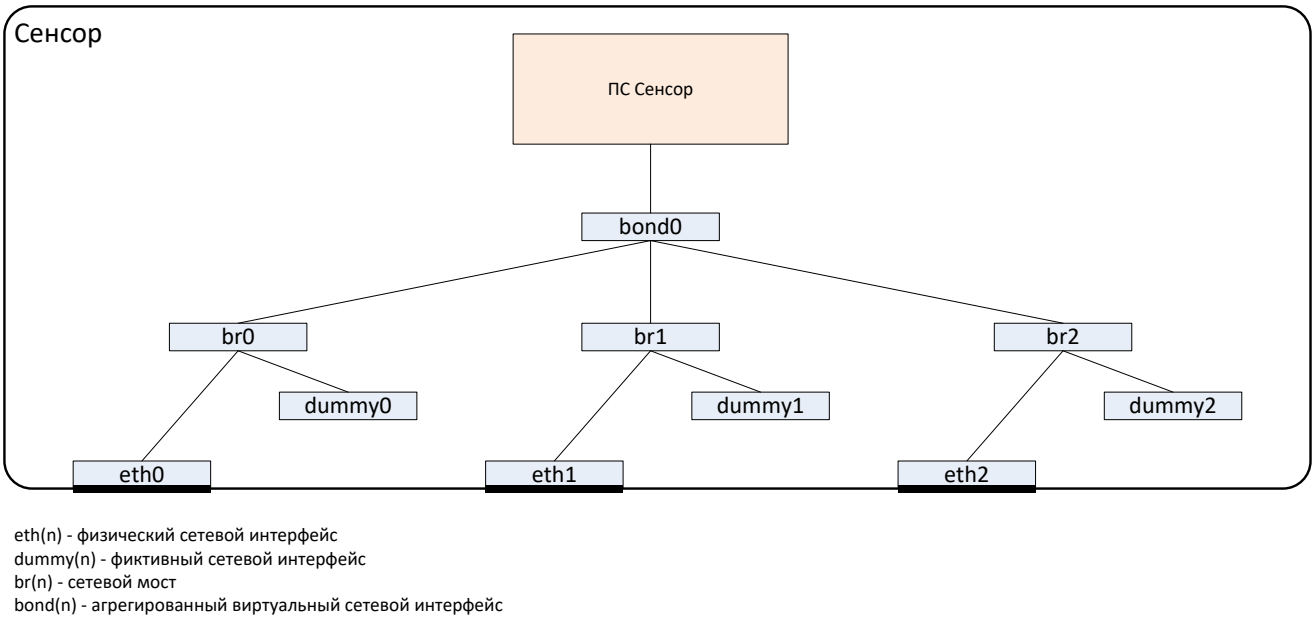

Рисунок 2 - Объединения физических интерфейсов в bond0 с применением сетевых мостов

Пример настройки bond0 в конфигурационном файле /etc/network/interfaces выглядит следующим образом:

```
auto eth0
iface eth0 inet static
address 0.0.0.0
auto dummy0
iface dummy0 inet static
address 0.0.0.0
pre-up modprobe dummy;:

auto eth1
iface eth1 inet static
address 0.0.0.0
auto dummy1
iface dummy1 inet static
address 0.0.0.0
pre-up modprobe dummy;:

auto eth2
iface eth2 inet static
address 0.0.0.0
auto dummy2
iface dummy2 inet static
address 0.0.0.0
pre-up modprobe dummy;:

auto br0
```

```
iface br0 inet static
bridge_ports eth0 dummy0
address 0.0.0.0

auto br1
iface br1 inet static
bridge_ports eth1 dummy1
address 0.0.0.0

auto br2
iface br2 inet static
bridge_ports eth2 dummy2
address 0.0.0.0

auto bond0
iface bond0 inet static
address 0.0.0.0
slaves br0 br1 br2
bond-mode balance-rr
bond-miimon 100
bond-downdelay 200
bond-updelay 200
```

11) Убедиться, что на сервере доступен установочный диск с Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

После проведения всех подготовительных действий для установки ПС Сенсор на ТС необходимо выполнить следующие инструкции:

12) Подключить внешний носитель с установочными пакетами и средой функционирования ПК «СОВ «Плутон-М1.0» ДБАР.62.01.12.000.181-01 к ТС одним из следующих способов:

– если внешний носитель – оптический диск, то поместить внешний носитель в оптический привод CD-ROM;

– если внешний носитель – USB-накопитель, то использовать для подключения USB-порт.

13) Нажать на клавиатуре (KVM-консоли) ТС клавиши Ctrl+Alt+F2 и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root».

После ввода учётных данных привилегированного технологического пользователя этот пользователь получит доступ к командной строке операционной системы.

14) Смонтировать внешний носитель. Для этого указать команду:

– для установки через оптический привод CD-ROM:

```
# sudo mount -r -t iso9660 /dev/cdrom /media/cdrom
```

– для установки через USB-порт:

```
# sudo mount -r -t iso9660 /dev/sdb
```

15) Перейти в каталог /media/cdrom. Для этого указать команду:

```
# cd /media/cdrom
```

16) Выполнить команду установки ПС Сенсор. Для этого ввести следующие параметры:

– тип устанавливаемого компонента -- sensor;

– географические координаты ПС Сенсор с ключами --ln (долгота) и --lt (широта);

– IP-адрес сервера синхронизации времени с ключом --ntp;

– путь до оптического диска со средой функционирования ПС СУС -- prt.

Примеры команды:

```
# sudo bash ./pluton_install.sh sensor --ln <долгота ПС Сенсор> --lt <широта ПС Сенсор> --ntp <IP-адрес сервера синхронизации времени> --prt <путь к точке монтирования оптического диска со средой функционирования ПС СУС>
```

При установке ПС Сенсор автоматически создаётся технологический пользователь «admin».

17) По завершении установки указать команду перезагрузки системы:

```
# sudo init 6
```

ВНИМАНИЕ! Выполнение перезагрузки после установки обязательно, в противном случае корректная настройка и запуск ПС Сенсор будут невозможны.

После перезагрузки следует:

18) Переключить основной порт сетевого интерфейса ПС Сенсор на bypass-порт.

19) Нажать на клавиатуре (KVM-консоли) ТС клавиши Ctrl+Alt+F2.

20) Ввести рабочее имя и пароль технологического пользователя (заводская установка – «admin»/ «7O0zKX4${8»).

После этого будет выполнен вход в командную среду технологического пользователя, предоставляющую доступ к технологическим возможностям ПС Сенсор.

21) Изменить пароль технологического пользователя. Для этого в командной среде технологического пользователя указать команду:

```
# passwd admin
```

22) В ответ на запрос системы дважды ввести новый пароль согласно требованиям парольной политики ПК СОВ.

23) Создать при необходимости дополнительных технологических пользователей. Для этого указать команду:

```
# sudo useradd <имя_пользователя>
```

24) Настроить программные средства. Инструкции по настройке и эксплуатации ПС Сенсор см. в документе ДБАР.62.01.12.000.183-01 32 Руководство системного программиста ПС Сенсор.

25) Завершить сеанс работы – на клавиатуре KVM-консоли нажать клавиши Ctrl+D.