ViPNet SIES MC VA

Руководство по развертыванию

infotecs

© ОАО «ИнфоТеКС», 2020

ФРКЕ.00194-02 90 03

Версия продукта 2.2.2

Этот документ входит в комплект поставки продукта ViPNet, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ОАО «ИнфоТеКС».

ViPNet® является зарегистрированным товарным знаком ОАО «ИнфоТеКС».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

ОАО «ИнфоТеКС»

127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1, 2 этаж

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

Содержание

Глава 1. О документе ... **3**
Для кого предназначен документ ... 4
Соглашения документа ... 5
Обратная связь ... 6

Глава 2. Комплект поставки ... **6**

Глава 3. Системные требования ... **7**

Глава 4. Подготовка к развертыванию ViPNet SIES MC VA ... **8**

Глава 5. Развертывание ViPNet SIES MC VA ... **11**

Глава 6. Перезагрузка виртуальной машины ViPNet SIES MC VA ... **17**

Глава 7. Выключение виртуальной машины ViPNet SIES MC VA ... **18**

Глава 8. Загрузка дополнительной инициализирующей последовательности ... **18**

Приложение A. Возможные неполадки и способы их устранения ... **20**
Не запускается виртуальная машина ViPNet SIES MC VA в гипервизоре VMware Workstation ... 21
Администратор не может подключиться к веб-интерфейсу ... 22

Приложение B. Глоссарий ... **23**

О документе

В данном документе вы найдете описание порядка развертывания на разных платформах виртуализации ViPNet SIES MC VA — программного исполнения ViPNet® SIES MC, управляющего компонентами комплекса ViPNet SIES.

Для кого предназначен документ

Данный документ предназначен для администраторов, устанавливающих программное исполнение ViPNet SIES MC VA.

Предполагается, что администратор обладает опытом работы с сертификатами ключа проверки электронной подписи, платформами виртуализации и пользования Linux.

Соглашения документа

Ниже перечислены соглашения, принятые в этом документе для выделения информации.

Таблица 1. Обозначения, используемые в примечаниях

Обозначение	Описание
	Внимание! Указывает на обязательное для исполнения или следования действие или информацию.
	Примечание. Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	Совет. Содержит дополнительную информацию общего характера.

Таблица 2. Обозначения, используемые для выделения информации в тексте

Обозначение	Описание
Название	Название элемента интерфейса. Например, заголовок окна, название поля, кнопки или клавиши.
Клавиша+Клавиша	Сочетание клавиш. Чтобы использовать сочетание клавиш, следует нажать первую клавишу и, не отпуская ее, нажать вторую клавишу.
Меню > Подменю > Команда	Иерархическая последовательность элементов. Например, пункты меню или разделы на панели навигации.
`Код`	Имя файла, путь, фрагмент текстового файла (кода) или команда, выполняемая из командной строки.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ОАО «ИнфоТеКС»:

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ОАО «ИнфоТеКС»:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).
- Служба технической поддержки: hotline@infotecs.ru.

  Форма для обращения в службу технической поддержки через сайт.

  Консультации по телефону для клиентов с расширенной схемой технической поддержки: +7 (495) 737-6196.
- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов ОАО «ИнфоТеКС» регулируется политикой ответственного разглашения.

Комплект поставки

В комплект поставки ViPNet SIES MC VA входят следующие компоненты:

- файл с образом виртуальной машины;
- утилита для получения инициализирующей последовательности RND Maker:
  - `rnd_maker-x86-bin-<версия>.zip` — для 32-разрядных версий Windows;
  - `rnd_maker-x64-bin-<версия>.zip` — для 64-разрядных версий Windows;
- документация в формате PDF:

  1.1 ViPNet SIES MC. Быстрый старт.

1.2 ViPNet SIES MC VA. Руководство по развертыванию (данный документ).

1.3 ViPNet SIES MC. Установка и обслуживание.

1.4 ViPNet SIES MC. Руководство администратора.

1.5 ViPNet SIES MC. Руководство разработчика.

1.6 ViPNet SIES MC. Лицензионные соглашения на компоненты сторонних производителей.

Совет. Рекомендуем вам знакомиться с документами в указанном порядке.

Системные требования

Программное исполнение ViPNet SIES MC VA поставляется в виде файла с образом виртуальной машины SIES MC VA в пакете OVA (см. глоссарий, стр. 23). Пакет OVA предназначен к установке на платформе виртуализации.

Вы можете развернуть виртуальную машину SIES MC VA на одной из следующих платформ виртуализации:

- VMware vSphere ESXi версий 6.0, 6.5 и 6.7;
- VMware Workstation версии 15.0;
- Oracle VM VirtualBox версий 5.2.18 и 6.0.4.

Внимание! ViPNet SIES MC VA поставляется в формате открытого стандарта OVF (Open Virtualization Format). Формат OVF поддерживается всеми современными платформами виртуализации. Вы можете установить ViPNet SIES MC VA на любой платформе виртуализации, поддерживающей OVF, но работоспособность ViPNet SIES MC в этом случае не гарантируется.

Не используйте один и тот же компьютер для установки ViPNet SIES MC VA в гипервизоре VirtualBox и организации рабочего места администратора ViPNet SIES MC с использованием ViPNet PKI Client или ViPNet CSP.

Для развертывания виртуальной машины SIES MC VA нужен компьютер со следующими параметрами:

- процессор — Intel Core i5 или другой схожий по производительности;
- объем оперативной памяти — не менее 16 Гбайт;
- количество сетевых адаптеров — не менее 2;
- свободное место на жестком диске — не менее 500 Гбайт.

Для подготовки к развертыванию виртуальной машины SIES MC VA нужны:

- криптопровайдер ViPNet CSP версии 4.2 и выше — можно загрузить на сайте компании ИнфоТеКС;
- USB-носитель с файловой системой FAT32.

Совет. При использовании гипервизора VMware vSphere ESXi подбирайте конфигурацию компьютера в соответствии с таблицей совместимости.

Подготовка к развертыванию ViPNet SIES MC VA

Перед использованием убедитесь в целостности архива с утилитой для получения инициализирующей последовательности:

1. С помощью утилиты ViPNet HashCalc вычислите контрольную сумму архива с утилитой по алгоритму ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.
2. Сравните вычисленное значение контрольной суммы со значением из раздела «Контрольные суммы» документа «ViPNet SIES MC. Формуляр. ФРКЕ.466219.009ФО».
3. Если значения контрольных сумм не совпали, не выполняя дальнейших действий, обратитесь к представителю компании ИнфоТеКС.

Примечание. Описание подготовки к развертыванию и установки ViPNet SIES MC VA приведено на примере платформы виртуализации VMware Workstation.

Перед развертыванием виртуальной машины SIES MC VA:

1. Выполните действия раздела «Порядок действий» главы «Подготовка к эксплуатации» документа «ViPNet SIES MC. Установка и обслуживание» до действия «Установите ViPNet SIES MC».
2. Установите на компьютере дату и время согласно всемирному координированному времени (UTC) и локальному часовому поясу с погрешностью не более 1 минуты.
3. У администратора локальной сети получите:
   - IP-адрес для подключения ViPNet SIES MC;
   - маску подсети, к которой принадлежит IP-адрес;
   - IP-адрес сетевого шлюза по умолчанию;
   - IP-адрес DNS-сервера.
4. У представителя компании ИнфоТеКС получите:
   - архив с файлом лицензии;

- пароль к архиву.

5 Установите гипервизор VMware Workstation на компьютер.

6 Установите ViPNet CSP на компьютер. См. документ «ViPNet CSP. Руководство пользователя».

Примечание. Не устанавливайте ViPNet CSP в виртуальную машину. Необязательно устанавливать ViPNet CSP на одном компьютере с гипервизором. Например, вы можете использовать компьютер с установленным ПО ViPNet CSP, например, ViPNet SIES Workstation.

---

7 Для развертывания виртуальной машины SIES MC VA нужна инициализирующая последовательность датчика случайных чисел. На компьютере с установленным ViPNet CSP:

7.1 Распакуйте в любое место утилиту для получения инициализирующей последовательности RND Maker.

7.2 Отключите файл подкачки Windows.

7.3 Подключите USB-носитель.

7.4 Запустите командную строку Windows от имени администратора.

7.5 Чтобы создать инициализирующую последовательность, запустите утилиту с помощью команды:

```
rnd_maker.exe -o <путь>
```

Здесь `<путь>` — полный путь к каталогу на USB-носителе для сохранения файла с инициализирующей последовательностью, например: `e:\`. Все промежуточные каталоги в указываемом пути создайте до запуска утилиты.

Совет. По умолчанию утилита вырабатывает инициализирующую последовательность размером 5 Мбайт. Вы можете задать больший размер в байтах, кратный 32, с помощью команды `rnd_maker.exe -o <путь> -s <длина>`. Использование инициализирующей последовательности большего размера позволит реже обновлять ее (на стр. 18) в ViPNet SIES MC.

7.6 Дождитесь появления окна **ViPNet CSP - инициализация контейнера ключей** и нажмите кнопку **OK**.

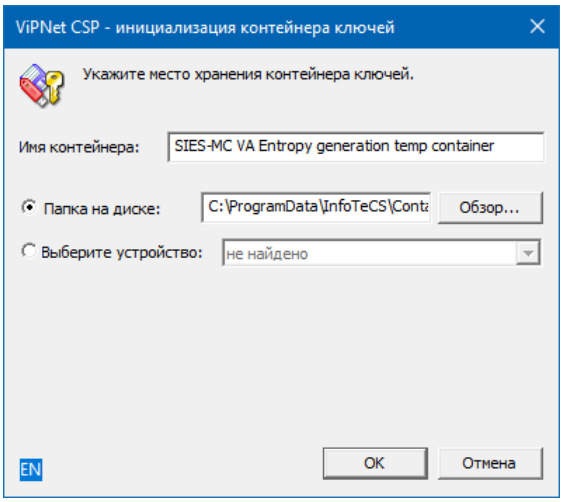

Рисунок 1. Создание контейнера ключей

7.7 Поводите курсором в пределах появившегося окна **Электронная рулетка** (см. глоссарий, стр. 25).

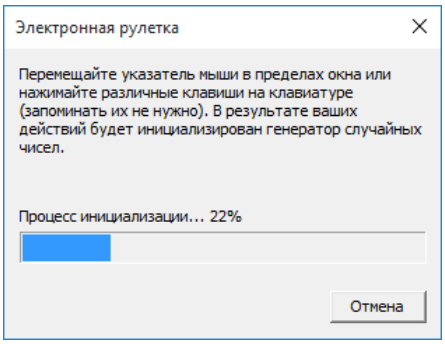

Рисунок 2. Биологический датчик случайных чисел (электронная рулетка)

Утилита выдаст сообщение **Entropy has been generated successfully** и создаст на USB-носителе файл `sies_mc_va_initialization_ГГГГММДДЧЧММССZ`. Здесь:

- `ГГГГММДДЧЧММСС` — метка с временем создания инициализирующей последовательности в UTC-кодировке;
- `Z` — флаг UTC-кодировки метки времени.

7.8 Закройте командную строку Windows.

7.9 Включите файл подкачки Windows.

8 Извлеките файл `*.itcslic` с лицензией из архива.

Развертывание ViPNet SIES MC VA

Перед использованием убедитесь в целостности файла с образом виртуальной машины ViPNet SIES MC VA:

1. С помощью утилиты ViPNet HashCalc вычислите контрольную сумму файла с образом по алгоритму ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит.
2. Сравните вычисленное значение контрольной суммы со значением из раздела «Контрольные суммы» документа «ViPNet SIES MC. Формуляр. ФРКЕ.466219.009ФО».
3. Если значения контрольных сумм не совпали, не выполняя дальнейших действий обратитесь к представителю компании ИнфоТеКС.

Чтобы развернуть виртуальную машину SIES MC VA:

1. В VMware Workstation выберите **Файл** > **Открыть** и укажите путь к файлу `*.ova` с образом SIES MC VA.
2. В окне **Импорт виртуальной машины** измените имя виртуальной машины, путь хранения и нажмите кнопку **Импорт**.
3. Дождитесь завершения процесса импорта и создания виртуальной машины.
4. Щелкните ссылку **Изменить настройки**.
5. На вкладке **Оборудование**:
   - **5.1** Щелкните **Память** и задайте объем `8192` Мбайт или больше.
   - **5.2** Щелкните **Процессор** и задайте количество ядер `2` или больше.
   - **5.3** Щелкните **Жесткий диск**. Нажмите кнопку **Расширить** и задайте максимальный размер `500` Гбайт.

     Внимание! Нельзя менять объем жесткого диска SIES MC VA в ходе эксплуатации виртуальной машины.

   - **5.4** Щелкните **Сетевой адаптер** и задайте **Подключение к сети**, из которой будете подключаться к веб-интерфейсу ViPNet SIES MC.
6. Перейдите на вкладку **Параметры** и в списке слева в графе **Параметры** щелкните **VMWare Tools**.
7. Установите флажок **Синхронизация времени гостевой ОС с узлом** группы **Функции VMWare Tools**.
8. Для сохранения настроек нажмите кнопку **OK**.

9 Запустите виртуальную машину, щелкнув ссылку **Включить виртуальную машину**. Дождитесь окончания загрузки Linux.

10 Авторизуйтесь в консоли Linux:

- на приглашение **login** введите `root` и нажмите клавишу **Enter**;
- на приглашение **Password** введите технологический пароль `vipnet` и нажмите клавишу **Enter**.

Примечание. Ввод любой последовательности символов следует завершать клавишей **Enter**. В дальнейшем описании последовательности инициализации упоминание этого шага опущено.

---

11 После загрузки Linux начнется контроль целостности ПО ViPNet SIES MC.

Таблица 3. Пример сообщений, выдаваемых при успешном завершении контроля целостности

Сообщение мастера инициализации	Описание
`ViPNet SIES MC system version: 2.2.2-61731`	Версия ПО ViPNet SIES MC
`System integrity check succeed`	Сообщение об успешном завершении контроля целостности
`ViPNet SIES MC OS checksum: AE6FA992`	Контрольная комбинация ОС
`ViPNet SIES MC software checksum: A36DE33A`	Контрольная комбинация ПО ViPNet SIES MC

Если проверка не выявила нарушения целостности, на экране появится соответствующее сообщение, а также номер версии ViPNet SIES MC и значения контрольных комбинаций ОС и ПО ViPNet SIES MC, которые следует сверить со значениями из раздела «Контрольные суммы» документа «ViPNet SIES MC. Формуляр. ФРКЕ.466219.009ФО».

12 Подключите USB-носитель с инициализирующей последовательностью к виртуальной машине ViPNet SIES MC VA.

13 Задайте новый пароль учетной записи администратора с правом локального доступа:

Внимание! Пароль должен соответствовать следующим требованиям:

- иметь длину от 8 до 32 символов;
- содержать хотя бы одну цифру от 0 до 9;
- содержать хотя бы одну букву латинского алфавита от «A» до «Z» или от «a» до «z».

Пароль может содержать символы «@», «#», «$», «%», «^», «&», «*», «(», «)», «-», «_», «+», «=», «;», «:», «'», «"», «,», «.», «<», «>», «/», «?», «\», «|», «`», «~», «[», «]», «{», «}».

Дополнительно не рекомендуется использовать:

- три и более символа, расположенные подряд на клавиатуре;
- три и более символа, идущие подряд в алфавитном порядке;
- один и тот же символ более двух раз.

13.1 На запрос **Enter new password** введите пароль.

13.2 На запрос **Confirm password** повторно введите тот же пароль.

14 Из предложенного списка действий выберите первичную инициализацию **First initialization**, введя символ `1`.

Примечание. В случае перезагрузки ViPNet SIES MC в ходе инициализации, мастер инициализации предложит вам пропустить ранее пройденные шаги. Если вы уверены в заданных настройках, на запрос **Skip** о каждом ранее пройденном шаге инициализации введите символ `y` для пропуска шага.

---

15 Задайте часовой пояс, дату и время:

15.1 На запрос выбора континента **Please select a continent or ocean** введите номер вашего континента из предложенного списка. Например, Российская Федерация отнесена к континенту **Europe** (Европа), поэтому введите значение `8`.

15.2 На запрос выбора страны **Please select a country** введите номер вашей страны из предложенного списка. Например, чтобы выбрать **Russia** (Россия), введите значение `39`.

15.3 На запрос выбора часового пояса **Please select one of the following time zone regions** введите номер вашего часового пояса из предложенного списка. Например, чтобы выбрать часовой пояс **Moscow area** (Московский регион) введите значение `2`.

15.4 На запрос **Is the above information OK** введите `y`, если заданные вами значения верны или введите символ `n` для повторного ввода значений часового пояса.

15.5 На запрос **Enter new system date** введите дату и время согласно всемирному координированному времени (UTC) и локальному часовому поясу с погрешностью не более 1 минуты. Новые значения вводите в формате в формате `Год-месяц-день часы:минуты:секунды`. Если изменять дату и время не требуется, нажмите клавишу **Enter**.

16 Задайте сетевые настройки ViPNet SIES MC и параметры подключения администраторов к веб-интерфейсу ViPNet SIES MC по TLS-каналу:

16.1 На запрос **Enter ViPNet SIES MC web interface port** введите номер порта подключения администраторов к веб-интерфейсу ViPNet SIES MC, если вы хотите изменить установленное по умолчанию значение порта, указанное в скобках (`443`). Если изменять номер порта не требуется, нажмите клавишу **Enter**.

16.2 На запрос **Choose network interface for ViPNet SIES MC web interface** введите номер виртуального сетевого интерфейса локальной сети `3`.

16.3 На запрос **Enter new IP address** для заданного сетевого интерфейса введите IP-адрес, полученный у администратора локальной сети.

16.4 На запрос **Enter new netmask** введите маску подсети, полученную у администратора локальной сети.

16.5 На запрос **Enter default gateway** введите IP-адрес сетевого шлюза по умолчанию, полученный у администратора локальной сети.

16.6 На запрос **Enter new DNS servers** введите IP-адрес DNS-сервера, полученный у администратора локальной сети. При вводе нескольких значений IP-адресов разделяйте их точкой с запятой без пробелов.

16.7 На запрос **Select new DNS servers** введите символ `n`, если заданные вами значения верны или введите символ `y` для повторного ввода значений IP-адреса DNS-сервера.

17 На запрос **Enter full path to random key material file** введите полный путь к файлу с инициализирующей последовательностью. Например, если инициализирующая последовательность находится в файле `sies_mc_va_initialization_20191209115231Z` корневого каталога USB-носителя, укажите каталог автоматического монтирования USB-носителя и имя файла: `/media/usb0/sies_mc_va_initialization_20191209115231Z`.

18 Задайте параметры сертификата ViPNet SIES MC для подключения администраторов к веб-интерфейсу ViPNet SIES MC по TLS-каналу.

На запрос **Enter Subject.CN field value for ViPNet SIES MC administrator connection certificate** введите заданный вами ранее IP-адрес или соответствующее заданному IP-адресу доменное имя узла ViPNet SIES MC.

Введите одно или несколько DNS-имен ViPNet SIES MC или сохраните значение IP-адреса сетевого интерфейса, указанное в скобках, нажав клавишу **Enter**. При вводе нескольких значений DNS-имен или IP-адресов разделяйте их точкой с запятой без пробелов.

Затем запустится процесс создания ключей электронной подписи. На экране этот процесс отображается сообщением **Keys generation may take several minutes**.

Внимание! Процесс может занять продолжительное время. Дождитесь окончания процесса, не прерывая его.

Признаком окончания процесса служит появление на экране следующего запроса мастера инициализации ViPNet SIES MC.

19 На запрос **Do you want to create backup set of keys** введите символ `y`, чтобы создать резервную копию ключевой информации ViPNet SIES MC.

Внимание! Настоятельно рекомендуем создать и сохранить в надежном месте резервную копию ключевой информации. Вы сможете создать резервную копию повторно по завершении инициализации ViPNet SIES MC. Создание файла с резервной копией ключевой информации может занять до 15 минут.

19.1 На запрос **Enter full path to backup set of keys file** введите полный путь к файлу на подключенном USB-носителе для экспорта резервной копии ключевой информации.

Например, чтобы сохранить резервную копию в файл `keys.backup` в корневом каталоге USB-носителя, введите `/media/usb0/keys.backup`.

Примечание. Следует заранее создать все промежуточные каталоги, используемые в указанном пути.

19.2 На запрос **Enter password to protect backup file** введите пароль к файлу с резервной копией.

19.3 На запрос **Confirm password** вновь введите тот же пароль.

После подтверждения пароля на USB-носитель будет экспортирована резервная копия ключевой информации ViPNet SIES, которую вы сможете использовать для восстановления работоспособности ViPNet SIES MC после аппаратного или программного сбоя.

20 На запрос **Enter full path to save ViPNet SIES MC administrator connection certificate request file** введите полный путь к каталогу на подключенном USB-носителе для экспорта запроса на сертификат ViPNet SIES MC для подключения администраторов.

Например, чтобы сохранить запрос на сертификат в корневой каталог USB-носителя, укажите каталог автоматического монтирования USB-носителя: `/media/usb0/`.

Примечание. При вводе пути соблюдайте регистр букв в названиях каталогов. Вы можете автоматически дополнять вводимые последовательности символов нажатием клавиши **Tab**. Все введенные вами значения запоминаются в текущем сеансе работы с мастером. Для выбора значения из истории ввода можно использовать клавиши со стрелками вверх и вниз.

После ввода пути на USB-носитель в указанную папку будет экспортирован файл `admin_nginx.p10` с запросом на сертификат ViPNet SIES MC для подключения администраторов.

21 Отключите USB-носитель.

22 Передайте файл `admin_nginx.p10` с запросом на сертификат администратору внешнего удостоверяющего центра для издания сертификата ViPNet SIES MC.

Если в удостоверяющем центре издание сертификата ViPNet SIES MC для подключения администраторов займет длительное время, вы можете прервать инициализацию ViPNet SIES MC и выключить аппаратную платформу с инициализируемым ПО ViPNet SIES MC.

Чтобы прервать инициализацию ViPNet SIES MC:

1 Нажмите клавиши **Ctrl+C**.

2 На запрос **Do you want to quit from initialization process** введите символ `y`.

3 Отключите питание аппаратной платформы с инициализируемым ПО ViPNet SIES MC.

Получив изданный сертификат ViPNet SIES MC для подключения администраторов из удостоверяющего центра:

1 Запишите на USB-носитель следующие файлы:

- изданный внешним удостоверяющим центром сертификат ViPNet SIES MC для подключения администраторов (должен удовлетворять требованиям, приведенным в документе «ViPNet SIES MC. Общее описание»);
- корневой сертификат внешнего удостоверяющего центра;
- список аннулированных сертификатов внешнего удостоверяющего центра;
- сертификат администратора ViPNet SIES MC, которому будет назначена роль супер-администратора.

2 Подключите USB-носитель к аппаратной платформе с инициализируемым ПО ViPNet SIES MC.

3 Если вы выключали аппаратную платформу с инициализируемым ПО ViPNet SIES MC:

3.1 Включите аппаратную платформу с инициализируемым ПО ViPNet SIES MC.

3.2 Дождитесь загрузки Linux.

3.3 Авторизуйтесь в консоли Linux как суперпользователь `root`.

3.4 Из предложенного списка действий выберите первичную инициализацию **First initialization**, введя символ `1`.

3.5 Пропустите все ранее пройденные шаги инициализации. Если вы уверены в заданных настройках, на запрос **Skip** о каждом ранее пройденном шаге инициализации введите символ `y` для пропуска шага.

4 На запрос **Enter full path to CA certificate of ViPNet SIES user key management subsystem file to import** введите полный путь к файлу:

- с корневым сертификатом пользовательской ключевой подсистемы ViPNet SIES;
- с корневым сертификатом головного удостоверяющего центра, если цепочка сертификатов удостоверяющего центра, выдавшего корневой сертификат пользовательской ключевой подсистемы ViPNet SIES, состоит более чем из одного сертификата.

5 На запрос **Enter full path for CRL file to import** введите полный путь к файлу со списком аннулированных сертификатов удостоверяющего центра для сертификата, загруженного на предыдущем шаге.

6 Если цепочка сертификатов удостоверяющего центра, выдавшего корневой сертификат пользовательской ключевой подсистемы ViPNet SIES, состоит более чем из одного сертификата издателей, загрузите промежуточные сертификаты и соответствующие списки аннулированных сертификатов:

6.1 На запрос **Do you want to install other CA certificate and CRL** введите символ `y`.

6.2 На запрос **Enter full path to CA certificate of ViPNet SIES user key management subsystem file to import** введите полный путь к файлу с промежуточным сертификатом цепочки.

6.3 На запрос **Enter full path for CRL file to import** введите полный путь к файлу со списком аннулированных сертификатов, соответствующим загруженному промежуточному сертификату.

6.4 Если нужно загрузить другой промежуточный сертификат и соответствующий список аннулированных сертификатов, на запрос **Do you want to install other CA certificate and CRL** введите символ `y` и повторите шаги 6.2–6.3.

Если все сертификаты цепочки загружены, введите символ `n`.

7 На запрос **Enter full folder path, from which ViPNet SIES MC administrator connection certificate file will be imported** введите полный путь к каталогу с файлом сертификата ViPNet SIES MC для подключения администраторов.

8 На запрос **Enter full path for ViPNet SIES MC Super-administrator certificate file to import** введите полный путь к файлу с сертификатом администратора ViPNet SIES MC, которому будет назначена роль супер-администратора.

9 На запрос **Do you want to complete ViPNet SIES MC initialization** подтвердите завершение настроек, введя символ `y`.

Появится сообщение мастера инициализации о завершении настройки.

10 Отсоедините USB-носитель.

11 Для продолжения нажмите клавишу **Enter**.

Последует перезагрузка Linux и ПО ViPNet SIES MC.

12 По окончании загрузки виртуальной машины выполните оставшиеся действия раздела «Порядок действий» главы «Подготовка к эксплуатации» документа «ViPNet SIES MC. Установка и обслуживание».

13 Установите лицензию. См. раздел «Обновление и активация лицензии» главы «Управление и настройка» документа «ViPNet SIES MC. Установка и обслуживание».

Перезагрузка виртуальной машины ViPNet SIES MC VA

Внимание! Перезагружайте виртуальную машину ViPNet SIES MC VA только описанным ниже способом.

Чтобы перезагрузить виртуальную машину ViPNet SIES MC VA:

1 Авторизуйтесь в консоли Linux как суперпользователь `root`.

Дождитесь появления меню мастера инициализации ViPNet SIES MC.

2 Из предложенного списка действий выберите перезагрузку **Reboot**, введя символ `6`.

3 Нажмите клавишу **Enter**.

Выключение виртуальной машины ViPNet SIES MC VA

Внимание! Выключайте виртуальную машину ViPNet SIES MC VA только описанным ниже способом.

Чтобы выключить виртуальную машину ViPNet SIES MC VA:

1. Авторизуйтесь в консоли Linux как суперпользователь `root`.

   Дождитесь появления меню мастера инициализации ViPNet SIES MC.

2. Из предложенного списка действий выберите выключение **Power off**, введя символ `7`.
3. Нажмите клавишу **Enter**.

Загрузка дополнительной инициализирующей последовательности

Если в ходе эксплуатации ViPNet SIES MC вы получили сообщение мониторинга **Заканчивается запас инициализирующей последовательности** или **Запас инициализирующей последовательности исчерпан**, загрузите дополнительную инициализирующую последовательность датчика случайных чисел через консоль Linux:

1. Создайте инициализирующую последовательность (на стр. 8).
2. Подключите USB-носитель с инициализирующей последовательностью к виртуальной машине ViPNet SIES MC VA.
3. В виртуальной машине ViPNet SIES MC VA авторизуйтесь в консоли Linux как суперпользователь `root`.

   Дождитесь появления меню мастера инициализации ViPNet SIES MC.

4. Из предложенного списка действий выберите загрузку инициализирующей последовательности **Import random key material**, введя символ `9`.

5 На запрос **Enter full path to random key material file** введите полный путь к файлу с инициализирующей последовательностью, например, `/media/usb0/sies_mc_va_initialization_20191209115231Z`.

6 После получения сообщения **Random key material is imported successfully** об успешной загрузке инициализирующей последовательности, закройте мастер инициализации, введя символ `8`.

A

Возможные неполадки и способы их устранения

Не запускается виртуальная машина ViPNet SIES MC VA в гипервизоре VMware Workstation

Выдается сообщение **You have started VMware Workstation with an out-of-date copy of the application. VMware Workstation cannot power on virtual machines using this copy (version X.X.X). To power on this virtual machine, run VMware Workstation from the default location.**

Способ устранения

1. В любом текстовом редакторе откройте файл `*.vmx` виртуальной машины ViPNet SIES MC VA.
2. В конец файла добавьте строку:

   ```
   vmx.noUIBuildNumberCheck = "TRUE"
   ```

3. Сохраните файл `*.vmx`.
4. Повторите запуск виртуальной машины ViPNet SIES MC VA.

Администратор не может подключиться к веб-интерфейсу

Администратор с рабочего места не может подключиться к веб-интерфейсу ViPNet SIES MC VA.

Возможная причина

Исчерпана инициализирующая последовательность датчика случайных чисел ViPNet SIES MC VA.

Способ устранения

1. Создайте инициализирующую последовательность (на стр. 8).
2. Подключите USB-носитель с инициализирующей последовательностью к виртуальной машине ViPNet SIES MC VA.
3. В виртуальной машине ViPNet SIES MC VA авторизуйтесь в консоли Linux как суперпользователь `root`.
4. На запрос **Enter full path to random key material file** введите полный путь к файлу с инициализирующей последовательностью, например, `/media/usb0/sies_mc_va_initialization_20191209115231Z`.
5. После получения сообщения **Random key material is imported successfully** об успешной загрузке инициализирующей последовательности, закройте мастер инициализации, введя символ `8`.

Работоспособность ViPNet SIES MC VA восстановится автоматически.

B

Глоссарий

OVF (Open Virtualization Format)

Открытый стандарт переносимого и расширяемого формата хранения и распространения образов виртуальных машин. Образы виртуальных машин распространяются в пакете OVA (Open Virtual Appliance), представляющие собой архив `tar` с пакетом OVF.

TLS (Transport Layer Security)

Криптографический протокол защищенной передачи данных между узлами в Интернете с применением асимметричной криптографии для аутентификации, симметричного шифрования для конфиденциальности и кодов аутентичности для сохранения целостности сообщений. Используется для подключения рабочего места администратора к веб-интерфейсу ViPNet SIES MC и для подключения рабочего места оператора ViPNet SIES Workstation к ViPNet SIES MC.

VA (Virtual Appliance)

Виртуальное устройство — образ предварительно настроенной и готовой к использованию виртуальной машины с установленным специфичным программным обеспечением. Предназначен для установки на платформу виртуализации (гипервизор).

ViPNet CSP

Криптопровайдер, обеспечивающий вызов криптографических функций из различных приложений. Может использоваться как средство электронной подписи — для формирования ключей электронной подписи.

ViPNet SIES (Security for Industrial and Embedded Solutions)

Комплекс продуктов компании ИнфоТеКС для защиты информации в индустриальных системах.

ViPNet SIES MC

Система управления SIES-узлами. Отправляет SIES-узлам защищенные команды управления и мониторинга по каналам связи индустриальной системы. Выполняет роль центра управления ключевой системой ViPNet SIES.

VLAN

Виртуальная локальная компьютерная сеть, представляет собой группу узлов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет узлам группироваться вместе, даже если они не находятся в одной физической сети.

Индустриальная система

Комплекс средств, обеспечивающий полный цикл функционирования производства или отдельного технологического процесса в различных областях экономики.

Ключ проверки электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом проверки электронной подписи называется открытый ключ, который является не секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, однозначно связанную с закрытым ключом и предназначенную для проверки подлинности электронной подписи.

Ключ электронной подписи

В соответствии с федеральным законом N 63-ФЗ «Об электронной подписи» от 6 апреля 2011 г. ключом электронной подписи называется закрытый ключ, который является секретной частью пары асимметричных ключей и представляет собой уникальную последовательность символов, предназначенную для создания электронной подписи.

Контролируемая зона

Территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового доступа.

Криптопровайдер

Независимый программный модуль, позволяющий выполнять криптографические функции в операционной системе.

Сертификат ключа проверки электронной подписи

Электронный документ или документ на бумажном носителе, выданный удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Сетевой интерфейс

Физическое или виртуальное устройство для подключения компьютера к сети. С помощью сетевого интерфейса компьютер осуществляет прием и передачу IP-пакетов. В качестве физического интерфейса может служить сетевая плата, модем и другие подобные устройства, в качестве виртуального — агрегированный интерфейс, интерфейс для VLAN (см. глоссарий, стр. 24).

Хэширование

Преобразование массива данных произвольной длины в битовую строку фиксированной длины, выполняемое определенным алгоритмом. Результат применения хэш-функции (хэш-код или хэш-сумма) однозначно определяется первоначальным массивом данных. Повторное применение хэш-функции к массиву данных и сравнение повторного хэш-кода с первоначальным хэш-кодом позволяет проверить целостность массива данных.

Электронная подпись

Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронная рулетка

Встроенный компонент программного обеспечения ViPNet, позволяющий инициализировать датчик случайных чисел по действиям пользователя. Полученная последовательность используется при формировании криптографических ключей.