

Лабораторный модуль №7 "Мониторинг и диагностика системы защиты"

Лабораторная работа №1 "Мониторинг состояния компонентов системы и передаваемого трафика, настройка реакции на события"

Сценарий. Для проверки корректности отражения в подсистеме мониторинга сведений о событиях, связанных с работой компонентов защиты АПКШ "Континент", администратор централизованно (с помощью ПУ ЦУС) выполняет над различными сетевыми устройствами (ЦУС и КШ) ряд мероприятий и оценивает отражение информации по ним в соответствующих журналах. В рамках данной лабораторной работы будут выполнены следующие процедуры:

- смена ключей парной связи для КШ с ЦУС и КШ, в ходе которой по определенным причинам ключ на КШ не обновился;
- попытка передачи пакетов, которые не соответствуют установленным правилам фильтрации межсетевого экрана, и последующий просмотр соответствующих сведений в журнале сетевого трафика;
- передача пакетов, которые не соответствуют установленным правилам фильтрации, но пропускаются из-за включенного мягкого режима межсетевого экрана, с последующим просмотром журналов НСД и регистрации сетевого трафика;
- установка соединения ПУ ЦУС с ЦУС с указанием неправильного пароля расшифрования ключа администратора;
- загрузка записей журналов СД.

Перед началом


- в ПУ ЦУС в папке "Центр управления сетью / Сетевые объекты" присутствуют объекты ARM_vpn и WS1_vpn, имеющие тип "Защищаемый".
- В папке "Центр управления сетью / Правила фильтрации" включите созданные для этих объектов правила "from ARM to WS1 vpn" и "from WS1 to ARM vpn".

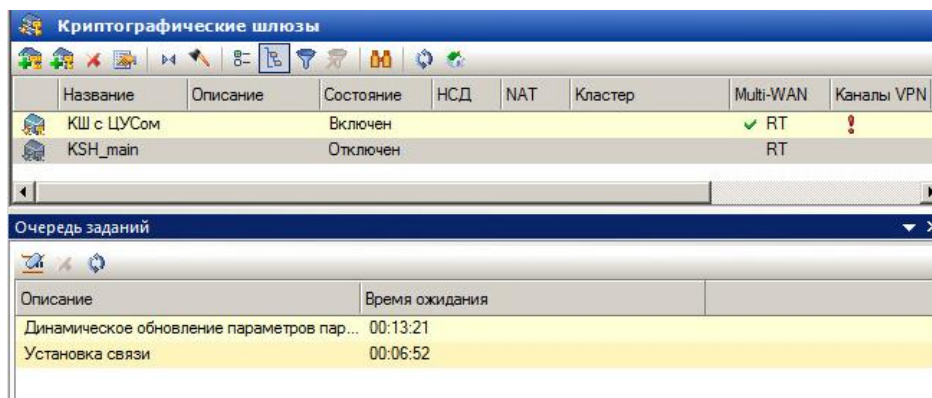
1. Установите связь (шифрованное соединение) между КШ с ЦУС и КШ. Для этого выполните следующие действия:

- в папке "Сетевые устройства Континент / Криптошлюзы" вызовите контекстное меню КШ с ЦУСом. Переключитесь на вкладку "Связи", переместите объект KSH_main в список "Связанные криптографические шлюзы" и нажмите кнопку "ОК";
- дождитесь применения изменений состояния на КШ с ЦУС и КШ. Запустите от имени администратора утилиту командной строки и с помощью команды ping 10.0.2.200 убедитесь в доступности VM WS1.

2. Теперь проведите смену ключей парной связи так, чтобы на KSH_main обновление ключа не произошло. Для этого выполните следующие действия:

- выключите (локально или из ПУ ЦУС) VM KSH_main;
- вызовите окно свойств КШ с ЦУС и на вкладке "Связи" перенесите KSH_main в список свободных криптографических шлюзов, а затем – обратно в список связанных. Нажмите кнопку "ОК";

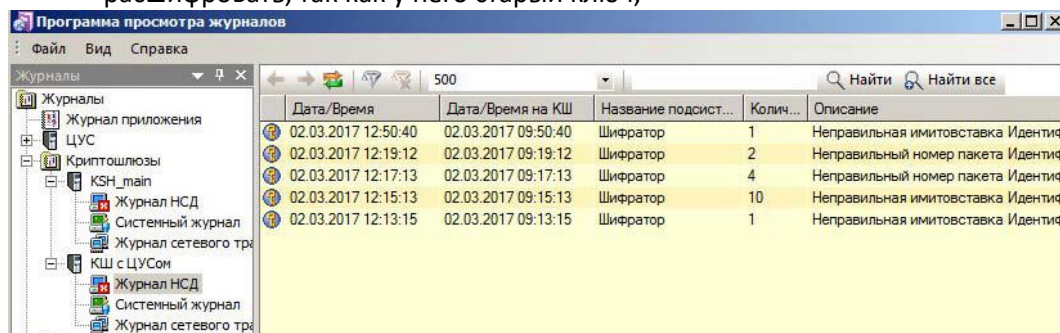
- в папке "Сетевые устройства Континент / Криптошлюзы" выберите объект KSH_main. В нижней части окна "Криптографические шлюзы" выберите вкладку "Очередь заданий" и с помощью кнопки "Очистить очередь заданий" () удалите все сформированные для данного КШ задания на изменение ключей парной связи;



- локально включите VM KSH_main;
- на VM ARM повторите проверку доступности VM WS1 с использованием команды ping 10.0.2.200 и убедитесь, что узел недоступен;
- обратите внимание, что в ПУ ЦУС в таблице "Криптографические шлюзы" для КШ с ЦУС и КШ в поле "НСД" появился индикатор несанкционированного доступа, а в поле "Каналы VPN" – индикатор отсутствия канала.

3. Проведите сбор журналов и в ППЖ просмотрите соответствующие записи.
Для этого:

- в главном меню ПУ ЦУС выберите опцию "Объекты / Сбор журналов". В окне информационного сообщения нажмите кнопку "OK";
- откройте ППЖ. В диалоговом окне запроса пароля введите 11111. В дереве журналов выберите: "Криптошлюзы / КШ с ЦУСом / Журнал НСД". Обратите внимание на записи с описанием "Неправильная имитовставка" – они означают, что КШ с ЦУС отправляет пакет, зашифрованный на новом ключе, а KSH_main, получив такой пакет, не может его расшифровать, так как у него старый ключ;

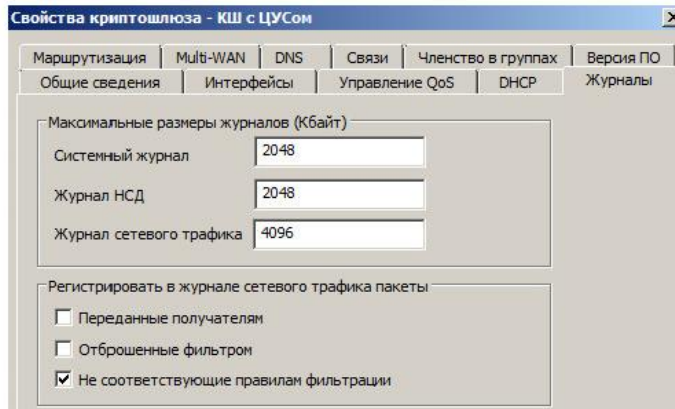


- в дереве журналов выберите: "Криптошлюзы / KSH_main / Журнал НСД" и просмотрите аналогичные записи;
- в дереве журналов выберите: "Криптошлюзы / KSH_main / Системный журнал". Просмотрите полученные записи и обратите внимание, что после "ручного" удаления заданий на изменение ключей парной связи ЦУСом автоматически была проведена замена этих ключей. Поэтому зашифрованное соединение между КШ с ЦУС и KSH_main восстановилось.

Таким образом, была проведена смена ключей парной связи так, чтобы на одном из узлов обновления ключей не произошло, с последующим просмотром сведений в соответствующих журналах.

5. Проведите попытку передачи пакетов, которые не соответствуют заданным в настройках межсетевого экрана правилам фильтрации (т.е. такие пакеты запрещены и должны быть отброшены). Для этого:

- в ПУ ЦУС в папке "Центр управления сетью / Правила фильтрации" **отключите все действующие правила фильтрации** (по умолчанию, если не создано ни одного правила фильтрации – прохождение трафика запрещено). На панели инструментов нажмите кнопку "Сохранить изменения" ();
- в папке "**Сетевые устройства Континент / Кристошлюзы**" вызовите окно свойств КШ с ЦУС, переключитесь на вкладку "**Журналы**" и в разделе "**Регистрировать в журнале сетевого трафика пакеты**" установите отметку в поле "Не соответствующие правилам фильтрации";



- нажмите кнопку "OK" и проведите такую же настройку для KSH_main;
 - на BM ARM проведите проверку доступности BM WS1 с использованием команды ping 10.0.2.200 и убедитесь, что узел недоступен
 - в ПУ ЦУС обратите внимание, что в таблице "Криптографические шлюзы" в поле "НСД" появился индикатор несанкционированного доступа.
6. Проведите сбор журналов и в ППЖ просмотрите соответствующие записи.

Таким образом, проведена попытка передачи запрещенных правилами фильтрации пакетов с последующим просмотром сведений об этом в журналах

8. Проверьте регистрацию запрещенных правилами фильтрации пакетов, которые пропускаются из-за включенного мягкого режима. Для этого:

- в окне ПУ ЦУС в таблице "Криптографические шлюзы" включите мягкий режим для КШ с ЦУСом и KSH_main: последовательно для каждого из них вызовите окно свойств, на вкладке "Общие сведения" установите флажок в поле "Мягкий режим" и нажмите кнопку "OK".

- на **BM ARM** проведите проверку доступности **BM WS1** с использованием команды ping 10.0.2.200 и убедитесь, что узел доступен;

9. Проведите сбор журналов и просмотрите в ППЖ соответствующие записи.

Для этого:

- в главном меню ПУ ЦУС выберите опцию "Объекты / Сбор журналов". В окне информационного сообщения нажмите кнопку "OK";
- переключитесь в окно ППЖ. В дереве журналов выберите: "Кристошлюзы / КШ с ЦУСом / Журнал НСД". Обратите внимание на записи, для которых в поле "Название подсистемы" указано "Пакетный фильтр", а в поле описания – параметры источника пакетов;
- в дереве журналов выберите: "Кристошлюзы / КШ с ЦУСом / Журнал сетевого трафика" и убедитесь, что значок записей журнала сетевого трафика изменился – появился символ "S", который обозначает мягкий режим работы пакетного фильтра (т.е. пакеты пропускаются, даже если они не соответствуют правилам фильтрации).

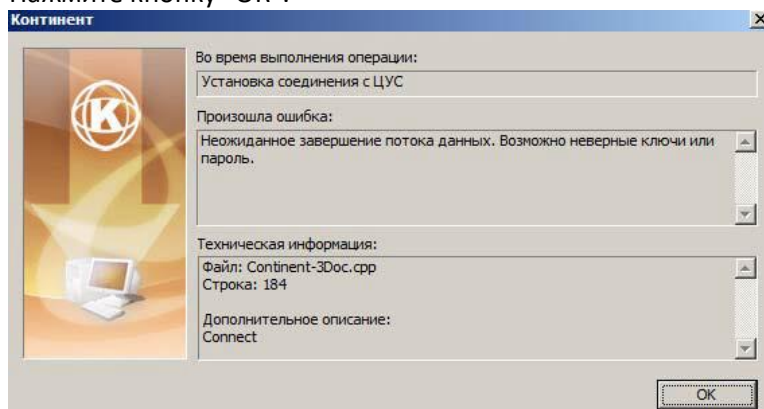
10. Самостоятельно. Переключитесь в окно ПУ ЦУС. В списке криптошлюзов с помощью опции "Сбросить признак НСД" из контекстного меню узла снимите признак несанкционированного доступа.

Отмените связь (шифрованное соединение) между КШ с ЦУС и КШ (см. п. 1). В папке "Центр управления сетью / Правила фильтрации" включите правила "from ARM to WS1 vpn" и "from WS1 to ARM vpn".

Таким образом, была проведена проверка регистрации запрещенных правилами фильтрации пакетов, которые пропускаются из-за включенного мягкого режима межсетевого экрана, и последующий просмотр соответствующих сведений в журналах.

11. Проверьте регистрацию в журналах событий установки из ПУ ЦУС соединения с ЦУС с указанием неправильного пароля к ключу администратора. Для этого:

- в окне ПУ ЦУС разорвите соединение с ЦУС – в главном меню выберите опцию "ЦУС / Разорвать соединение";
- выполните попытку установить соединение заново, указав при этом неправильный пароль – в главном меню выберите опцию "ЦУС / Установить соединение" и в диалоговом окне ввода пароля для расшифрования ключей введите 22222. На экране появится окно с сообщением об ошибке. Нажмите кнопку "ОК".



12. Самостоятельно. В ПУ ЦУС установите соединение с ЦУС, указав правильный пароль 11111, проведите сбор журналов и просмотрите в ППЖ записи журнала "ЦУС / Журнал НСД".

13. Самостоятельно. В ППЖ просмотрите содержимое журнала СД: "Серверы доступа / КШ с ЦУСом".

Результат. Для проверки корректности отражения в подсистеме мониторинга сведений о событиях, связанных с работой компонентов защиты АПКШ "Континент", централизованно (с помощью ПУ ЦУС) над различными сетевыми устройствами (ЦУС и КШ) выполнен ряд мероприятий и проверено отражение информации по ним в соответствующих журналах. Выполнение лабораторной работы завершено.

Лабораторный модуль №8 "Обновление ПО"

Лабораторная работа №1 "Обновление ПО ЦУС"

Сценарий. Администратор проводит обновление ПО ЦУС. В лабораторной работе обновление будет проводиться на ту же версию ПО "Континент" 3.7.6, которая установлена на учебном стенде.

Процедура обновления ПО ЦУС выполняется в следующей последовательности:

- в ПУ ЦУС сохранить конфигурацию ЦУС;
- провести локальную установку новой версии ПО на ЦУС (в лабораторной работе вместо установки новой версии проводится переинициализация ЦУС);
- в ПУ ЦУС восстановить сохраненную конфигурацию ЦУС и убедиться, что управляемые сетевые устройства подключены к ЦУС.

Перед началом выполнения лабораторной работы убедитесь, что на VM ARM подключен съемный USB-флеш-накопитель для записи конфигурации.

1. Для того чтобы сохранить конфигурацию ЦУС, сделайте следующее:

- в главном меню ПУ ЦУС выберите опцию "ЦУС / Сохранить файл конфигурации ЦУС". В открывшемся диалоговом окне ввода пароля для шифрования ключей в поля пароля и подтверждения введите **11111** и нажмите кнопку **"ОК"**;
- откроется стандартное окно сохранения файла. Сохраните конфигурации КШ с ЦУС в файле "ncc.cfg" на внешнем USB-флеш-накопителе. В диалоговом окне с сообщением об успешной записи нажмите кнопку **"ОК"**.



2. В окне VM ARM откройте содержимое USB-флеш-накопителя и создайте на нем папку "cus_old", в которую скопируйте файл действующего ключа администратора "contkey.str".

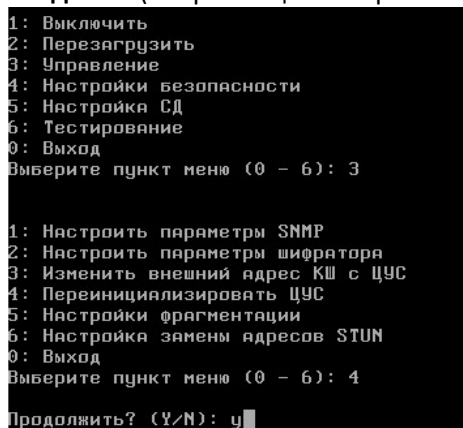
Внимание! При установке ПО ЦУС будет создан новый идентификатор администратора, который нужен только для первого запуска программы управления ЦУС. Поэтому обязательно следует сохранять старый **идентификатор администратора**, соответствующий обновляемой версии ПО и использовавшийся при создании резервных копий. После восстановления из резервной копии конфигурации запуск ПУ ЦУС будет осуществляться с использованием старого идентификатора.

3. На VM CUS проведите инициализацию ЦУС (здесь будет использоваться та же версия ПО, которая установлена на учебном стенде). Еще раз отметим, что в реальных условиях вместо переинициализации проводится процедура установки новой версии ПО на ЦУС.

Подробное описание процедуры инициализации ЦУС см. в лабораторной работе №1 лабораторного модуля №1. Для инициализации ЦУС сделайте следующее:

- на **VM CUS** подключите съемный USB-флеш-накопитель;
- на VM CUS с помощью комбинации клавиш **[Alt+F2]** вызовите локальное меню ЦУС и введите команду **перезагрузки устройства – 10**;

- для инициализации **ЦУС** введите **команду 3 ("Управление")**. В открывшемся меню введите **4 ("Переинициализировать ЦУС")**. На запрос о продолжении введите **y**;



- в перечне начальной конфигурации ЦУС появится список интерфейсов и предложение указать параметры внешнего интерфейса. Введите:

- номер внешнего **интерфейса – 1**;
- внешний IP-адрес шлюза – **196.115.92.1/24**;
- на запрос продолжения **введите y**.

Вновь появится перечень интерфейсов с предложением указать внутренний (принадлежащий защищаемой сети КШ либо использующийся в качестве промежуточной сети к защищаемым сетям);

- последовательно введите следующие значения:
- номер внешнего **интерфейса** – **3**;
- внешний IP-адрес **шлюза** – **10.0.1.1/24**;
- на запрос продолжения **введите у**;
- адрес маршрутизатора по умолчанию – **196.115.92.254** (маршрутизатор и регистрируемый КШ должны находиться в одной подсети, заданной указанными ранее IP-адресом и маской внешнего интерфейса КШ);
- на запрос продолжения **введите у**;

```
Обнаруженные интерфейсы:
Номер  Имя
2.     em1
3.     em2
4.     em3

Укажите номер внутреннего интерфейса. Если их несколько -- того, к которому
подключается АРМ администратора: 3
Введите внутренний IP адрес шлюза: 10.0.1.1/24
Продолжить? (Y/N): y
Введите адрес маршрутизатора по умолчанию: 196.115.92.254
Адрес маршрутизатора 196.115.92.254
Продолжить? (Y/N): y
Использовать внешний носитель для инициализации? (Y/N):
```

- как и в лабораторной работе №1 лабораторного модуля №1, на учебном стенде источником инициализации является имитация ПАК "Соболь" в виде файлов "sblm1" и "sblm2", и на данном шаге следует указать, что внешний носитель для инициализации использоваться **не будет** – **введите n**;

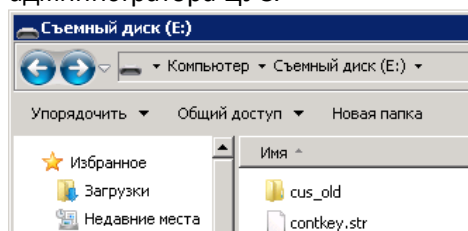
```
Использовать внешний носитель для инициализации? (Y/N): n
Идет формирование инициализирующей последовательности. Пожалуйста, подождите.
Загружена ключевая информация
Введите пароль ключа администратора ЦУС:
```

- исходный ключевой материал будет загружен в ЦУС, где будет сформирован ключ администратора ЦУС, и система предложит ввести пароль и подтверждение ключа администратора. **Введите 11111** (при вводе символы не отображаются);

```
Использовать внешний носитель для инициализации? (Y/N): n
Идет формирование инициализирующей последовательности. Пожалуйста, подождите.
Загружена ключевая информация
Введите пароль ключа администратора ЦУС:
Повторите пароль:
Вставьте носитель для записи ключа администратора ЦУС и нажмите Enter
```

4. Инициализация ЦУС завершена. **Отключите** внешний USB-флеш-накопитель от **BM CUS** и подключите его в окне **BM ARM**.

Убедитесь, что на USB-флеш-накопителе записан файл **"contkey.str"** с новым ключом администратора ЦУС.



5. подключитесь заново к ЦУС – в главном меню ПУ ЦУС выберите опцию **"ЦУС / Установить соединение"**. Программа считывает информацию с вновь созданного в корневом каталоге USB-флеш-накопителя ключевого файла **"contkey.str"**. **Введите пароль 11111** и нажмите кнопку "ОК".

6. Откроется диалоговое окно управления лицензиями. Обратите внимание, что для обновления ПО КШ необходимо ввести лицензию. При этом количество обновляемых КШ комплекса не может превышать указанное в лицензии значение. В лабораторной работе лицензию вводить не нужно, поскольку была загружена не новая, а уже используемая версия ПО.

В окне **"Управление лицензиями ЦУС"** нажмите кнопку **"Закрыть"**.

7. В дереве объектов ПУ ЦУС выберите "Сетевые устройства Континент / Кристошлюзы". Обратите внимание, что на данном этапе на ЦУС установлена новая конфигурация, которая не содержит информацию о подключенных к нему КШ.

8. Чтобы восстановить управление подключенными к ЦУС сетевыми устройствами, в ПУ ЦУС необходимо загрузить сохраненный ранее (в п. 1) файл конфигурации ЦУС. Для этого:

- в главном меню ПУ ЦУС выберите опцию **"ЦУС / Загрузить файл конфигурации ЦУС"**;
- в стандартном окне открытия файла укажите файл **"ncc.cfg"**, сохраненный в корневом каталоге USB-флеш-накопителя, и нажмите кнопку **"Открыть"** (см. п. 1 данной лабораторной работы);
- в открывшемся окне ввода пароля для расшифрования конфигурации ЦУС **введите 11111** и нажмите кнопку **"ОК"**.

После загрузки файла конфигурации ЦУС автоматически перезагрузится, и соединение ЦУС с программой управления будет разорвано. Ознакомьтесь с сообщением в диалоговом окне и нажмите кнопку **"ОК"**.

9. Установите заново соединение, используя старый ключ администратора ЦУС, сохраненный на USB-флеш-накопителе в папке "cus_old" (см. п. 2). Для этого:

- из папки **"cus_old"** скопируйте файл **"contkey.str"** со старым ключом администратора в корневую папку USB-флеш-накопителя;
- в главном меню ПУ ЦУС выберите опцию **"ЦУС / Установить соединение"**.

Программа считывает информацию из старого ключевого файла **"contkey.str"**. **Введите пароль 11111 и нажмите кнопку "ОК"**.

10. В дереве объектов ПУ ЦУС выберите **"Сетевые устройства Континент / Кристошлюзы"** и убедитесь, что в ПУ ЦУС появилась информация о подключенных к ЦУС сетевых устройствах.

Результат. Проиллюстрирована процедура обновления ПО ЦУС на примере уже установленной версии.

Выполнение лабораторной работы завершено.

Лабораторная работа №2 "Обновление ПО КШ"

Сценарий. Администратор проводит дистанционное обновление ПО КШ на KSH_main. В лабораторной работе обновление будет проводиться на ту же версию ПО "Континент" 3.7.6, которая установлена на учебном стенде.

Описание процедуры дистанционного обновления ПО КШ см. в разделе "Обновление текущей версии ПО" главы 8.

Поскольку в данной лабораторной работе для обновления используется текущая версия ПО, предварительная загрузка файла "preupdate.tar" проводиться не будет.

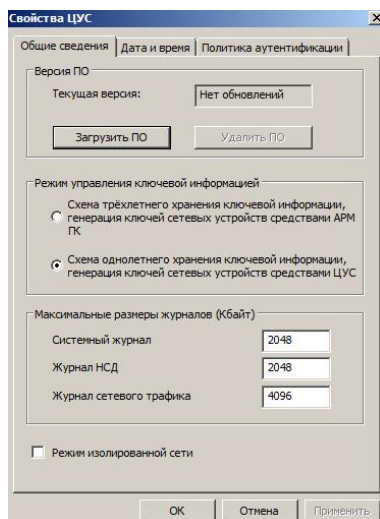
Примите к сведению, что процедура локального обновления ПО сетевых устройств подробно описана в руководстве администратора к продукту.

1. В реальной ситуации перед обновлением ПО КШ необходимо загрузить соответствующие лицензии. В главном меню ПУ ЦУС выберите опцию "ЦУС / Лицензии...". Откроется окно управления лицензиями.

*Поскольку в лабораторной работе для обновления будет использоваться уже установленная версия ПО – номер лицензии вводить не нужно. Нажмите кнопку **"Заккрыть"** и вернитесь в окно ПУ ЦУС*

2. Для того чтобы скопировать файл обновления на жесткий диск ВМ ЦУС, выполните следующие действия:

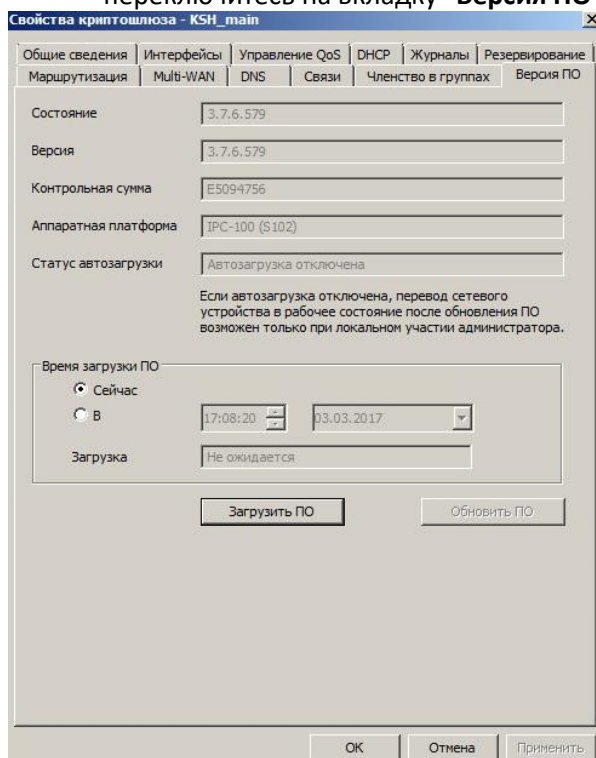
- в ПУ ЦУС в дереве объектов вызовите контекстное меню папки **"Центр управления сетью"** и выберите опцию **"Свойства..."**. Откроется диалоговое окно **"Свойства ЦУС"**;



- нажмите кнопку **"Загрузить ПО"**. В стандартном окне открытия файла выберите из папки **"C:\Дистрибутивы"** общий для всех сетевых устройств файл обновления **"update_all_release.tar"** и нажмите кнопку **"Открыть"**;
- в окне **"Свойства ЦУС"** нажмите кнопку **"Применить"**, а затем – кнопку **"ОК"**. Файл обновления загружен на жесткий диск ЦУС.

3. Для того чтобы загрузить файл обновления на КШ, сделайте следующее:

- в окне ПУ ЦУС выберите объект **"Сетевые устройства Континент / Критошлюзы"**, из контекстного меню KSH_main выберите опцию **"Свойства..."** и в открывшемся окне переключитесь на вкладку **"Версия ПО"**;



- нажмите кнопку **"Загрузить ПО"**. В окне информационного сообщения нажмите кнопку **"ОК"**.
- нажмите кнопку **"Загрузить ПО"**. В окне информационного сообщения нажмите кнопку **"ОК"**. После окончания загрузки файла обновлений на КШ станет доступной кнопка **"Обновить ПО"**.

4. Для установки обновления на КШ в окне свойств криптошлюза нажмите кнопку **"Обновить ПО"**. В окне информационного сообщения нажмите кнопку **"ОК"** и закройте окно свойств криптошлюза. В процессе обновления дважды автоматически выполняется перезагрузка сетевого устройства. Примите к сведению, что в реальной ситуации по окончании обновления в

ПУ в свойствах КШ изменится номер версии ПО, и в ПАК "Соболь" автоматически пересчитаются контрольные суммы файлов ПО "Континент".

Результат. Проведена процедура дистанционного обновления ПО КШ на примере текущей версии. Выполнение лабораторной работы завершено.