

При выполнении заданий необходимо, при помощи текстового редактора, сформировать отчет, в котором представить скриншоты ключевых настроек. Отчет необходимо сохранить на рабочем столе ПК.

Название машины	IP-адрес	Маска	Шлюз
Net1-AdminCA	192.168.1.1	255.255.255.0	192.168.1.4
Net1-Open	192.168.1.2	255.255.255.0	192.168.1.4
Net1-OpenCA	192.1.3	255.255.255.0	192.168.1.4
Net2-Client	10.10.10.129	255.255.255.192	10.10.10.130
Net1-Coord	Eth0: 192.168.1.4	Eth0: 255.255.255.0	203.73.66.2
	Eth1: 203.73.66.1	Eth1: 255.255.255.0	
Net2-Coord	Eth0: 10.10.20.130	Eth0: 255.255.255.192	203.73.66.1
	Eth1: 203.73.66.2	Eth1: 255.255.255.0	

Имя	Путь
Visual C	Vipnet_A.7_R\SOFT___000\SERVER_I\PACKAGES\VISUAL_C
ЦУС Сервер	Vipnet_A.7_R\SOFT___000\SERVER_I\PACKAGES\RU_RU
ЦУС Клиент	Vipnet_A.7_R\SOFT___000\CLIENT_I\PACKAGES\RU_RU
УКЦ	Vipnet_A.7_R\SOFT_____\ (power shell)
Vipnet Client	VIPNET_C.5\SOFTWARE
БД	Vipnet_A.7_R\SOFT___000\SERVER_I\PACKAGES\SQLXPRES
CA Inform	vipnet c/ ca inform
Publication Service	vipnet p6/____/soft/setup
Reg Point	VIPnet r629/____/soft/ setup

Название машины	Программы
Net1-AdminCA	Visual C, ЦУС Сервер, УКЦ, Vipnet Client, CA Informing
Net1-OperCA	Visual C, Vipnet Client, Publication Service, Registration point
Net1-Open	Visual C, SQL, ЦУС Клиент
Net2-Client	Visual_C, Client_R(C.5)

Пользователь	Base_Coordinator	Administrator_VPN	Operator_CR	Sub_Coordinator	Branch_Client
Base_Coordinator	X	*	*	*	
Administrator_VPN	*	X	*		*
Operator_CR	*	*	X	*	
Sub_Coordinator	*		*	X	*
Branch_Client		*		*	X

Название машины	Роли узла
Base_Coordinator, Sub_Coordinator	Coordinator HW-VA
Administrator_VPN	Registration Point, Policy Manager
Operator_CR	Registration Point

Адреса выбираются самостоятельно из указанного диапазона. Необходимо записать все IP адреса, логины и пароли в текстовый файл VPN.txt на рабочем столе компьютера.

Net1-Open

Сделать снимок

Сделать скрин

Убрать галочку

Visual C – Vipnet_A.7_R\SOFT___000\SERVER_I\PACKAGES\VISUAL_C

SQL – Vipnet_A.7_R\SOFT___000\SERVER_I\PACKAGES\SQLEXPRESS

После установки в пуске нахожу SQL Server (manager), тут нужно поставить в Enabled, после этого (где WINN) делаю – Restart

Net1-Admin

Сделать снимок

Сделать скрин

Убрать галочку

Visual C – Vipnet_A.7_R\SOFT___000\SERVER_I\PACKAGES\VISUAL_C

ЦУС сервер - Vipnet_A.7_R\SOFT___000\SERVER_I\PACKAGES\RU_RU

VipNet client - VIPNET_C.5\SOFTWARE\

Заходим в ЦУС вводим IP-адрес (172.16.224.226, проверка подлинности SQL, имя sa, пароль xxXX1234 и проверить подключение, если всё успешно, то продолжаем установку)

Net1-Open

Сделать снимок

Сделать скрин

Убрать галочку

ЦУС

клиент - Vipnet_A.7_R\SOFT___000\CLIEYNT_IPACKAGES\RU_RU (установка через power shell!) **Сделать скрин и закинуть в отчёт**

Net2-Client

Сделать снелшот

Сделать скрин

Убрать галочку

Панель управления → часы и регионы → региональные стандарты → дополнительно → изменить язык системы

Visual C – Vipnet_A.7_R\SOFT___000\SERVER_IPACKAGES\VISUAL_C

VipNet client - VIPNET_C.5\SOFTWARE\

В отчете необходимо зафиксировать процесс установки скриншотами форм, сделать скриншот директории, в которую установлено ПО, и скриншот первого запуска приложения.

Net1-OperCA

Сделать снелшот

Сделать скрин

Убрать галочку

Visual C – Vipnet_A.7_R\SOFT___000\SERVER_IPACKAGES\VISUAL_C

VIPNet Client – VIPNET_C.5\SOFTWARE\

Net1 – Admin

УКЦ - Vipnet_A.7_R\SOFT_____ \

Net1 – Open

Заходим в ЦУС, входим под IP Admina (172.16.224.225)

Далее подключаю диск с лицензией (_____.ITC)

Net1 – Admin

Захожу в УКЦ, (Вход по IP Open1, SQL-сервер: 172.16.224.226)

Net1 – Open

Заходим в ЦУС

Создаю координаторов и пользователей по заданию

Координаторы(добавить в межсерв канал, удалить другие роли и добавить роль - Coordinator HW-VA)

Добавление роли для AdminS - Registration Point, Policy Manager, для Node_CR - Registration Point

Создаем связи с пользователями

Сохранение структуры файла в формат html

Далее отправить

Net1 – Admin

Заходим в УКЦ, меняем пароль на собственный

Далее сетевые узлы, выделяем всё ПКМ и выдать новый дистрибутив ключей.

Теперь на каждой машине захожу в VipNet – Admin – AdminS, OperCA – Node_CR, Net2-Client – Rem_Client

+создать фильтры защищённой и открытой сети

Net1 – Coord

Убрать галочку

Root_Coordinator

UP, Static(тут IP-адрес), Up, Static(тут IP-адрес), Down(IP-адрес), Off,Off, No,No, Yes, Finish.

Net2 – Coord

Убрать галочку

Sub_Coordinator

UP, Static(тут IP-адрес), Up, Static(тут IP-адрес), Down(IP-адрес), Off,Off, No,No, Yes, Finish.

Захожу в VipNet на каждую машину

Net1 – AdminCA = Administrator_VPN(192.168.1.1)

Net1 – OperCA = Operator_CR(192.168.1.2)

Net2 – Client = Branch_Client(10.10.20.129)

Net1 – Coord = Base_Coordinator(192.168.1.4, 203.73.66.2)

Net2 – Coord = Sub_Coordinator(10.10.20.130, 203.73.66.1)

Отправить письмо по Деловой почте пользователю Branch_Client(Net2_Client) с узла Администратор ViPNet, отправить текстовое сообщение пользователю Administrator_VPN от пользователя Branch_Client(Net2_Client).

В отчете необходимо зафиксировать процесс настройки скриншотами ключевых моментов и заполненных форм:

- скриншоты деловой почты на отправителе и получателе (при отправке письма);
- скриншоты текстового сообщения на отправителе и получателе.

Создание и отправка письма

Открыть «Делова почта», выбрать на панели «Письмо»

В открывшемся окне введите тему и текст письма, при необходимости измените формат текста письма.

Нажмите кнопку «Получатели» и в окне «Выбрать контакты» выберите получателей

Чтобы удалить получателя, выберите его на вкладке Получатели и нажмите на клавиатуре клавишу «Delete».

Нажмите кнопку «Отправить»:

Просмотр входящих писем

При получении новых писем на экране рабочего стола появится уведомление.

Поставьте галочку «Запустить программу Деловая почта», чтобы открыть программу, и нажмите «ОК».

Непрочитанные письма выделяются в списке полужирным шрифтом.

Папки программы ViPNet Деловая почта, в которых есть непрочитанные письма, также выделяются полужирным шрифтом, при этом в скобках после имени папки указано количество непрочитанных писем.

Чтобы прочитать письмо:

В окне программы VipNet Деловая почта на левой панели выберите папку, в которой находится письмо

Выберите письмо в списке. Если письмо не зашифровано, его текст отобразится в поле под списком писем.

Компрометация

25)Заходим в УКЦ, переходим в раздел пользователи и выбираем Usera-ПКМ-Ключи пользователя -Создать и сохранить РНПК в файл

26)Заходим в УКЦ, переходим в раздел пользователи и выбираем Usera-ПКМ-Безопасность и плановые работы- Считать ключи скомпрометированными

27)Заходим в УКЦ, переходим в раздел пользователи и выбираем Usera-ПКМ-Ключи пользователя - Создать и передать ключи в ЦУС(оповещаем ЦУС о компрометации)

28)Заходим в УКЦ, переходим в раздел Сетевые узлы и выбираем Все узлы-ПКМ->Ключи пользователя - Создать и передать ключи в ЦУС (говорим всем клиентам что пользователь скомпрометирован)

29)Переходим в ЦУС-Клиенты- Выбираем нашего пользователя(User`a)-ПКМ- отправить справочники и ключи (доводим информацию до узлов, что User скомпрометирован)

30)Дожидаемся пока на машине Net2 Client не вылетит VipNet Client, далее переносим РНПК на машину клиента

31)Запускаем VipNet Client и выходим из под пользователя, далее пробуем зайти обратно(Должна появиться ошибка)

32)Далее необходимо вернуть пользователя обратно в работу, на диалоговом окне с ошибкой нажимаем ОК и указываем путь до РНПК

33)Далее необходимо сменить пароль-выбираем открыть настройки параметров- «Тип пароля» - собственный -Сменить пароль- Задаем пароль

34)Переходим в ЦУС - Справочник и ключи- отправить справочники и ключи

В отчете необходимо зафиксировать процесс настройки скриншотами:

- **компрометация пользователя,**
- **смена ключей пользователя и сетевых узлов,**
- **процедура смены ключа на клиенте с использованием резервного набора ключей,**
- **результат проверки доступности узлов.**

Компроментация 2 Вариант

Пользователи:

Рнпк в файл на рабочий стол

Считать скомпрометировать

Создать и передать в цус

Сетевые узлы:

Выделяем все и передаём в цус

Цус:

Выбираем клиента

Отправить справочник и ключи только для клиента

Должен вылететь либо самим закрыть

На рабочем столе админа файл рнпк копируем на диск f

Далее открываем диск на клиенте файл рнпк и копируем на рабочий стол

Заходим в випнет под резервным пользователем рнпк

- открыть настройки паролей

- собственный

- ввод пароля

Пользователь должен восстановиться

Отправка справочников на все узлы

Ждать восстановления всего

СЕРТИФИКАТЫ

НЕ ЗАБЫТЬ Снэпшот и скрины

Вопросик: все это настраиваем при установке укц, но при входе на видео там уже и координаторы и клиенты есть, значит как действовать???

Решение (возможно): после установки укц создать и настроить пользователей

Задание 1.3 Настройка работы удостоверяющего центра в аккредитованном режиме

Цус:

Клиенты - оператор (у нас это клиент какой под ?) - роли узла - добавить registration point

Укц:

Запускаем установщик и после заходим в приложение, доходим до создания административной сети випнет и вводим имя админа (имя пользователя), после тыкаем далее до момента инициализации и заполняем владельца:

Имя: <Имя пользователя или узла>

Электронная почта: <Имя пользователя>@demo.lab

Город: Адлер

Область: Краснодарский край

Организация: ООО Легион

Подразделение: ИТ-отдел

Почтовый индекс:354340.

PS: почтовый индекс заполняется "дополнительные сведения о владельце сертификата", т.е. 2 раза на индекс, заполняем значение и ОК

ДАЛЕЕ ТАКЖЕ В УКЦ: нажимаем далее и в окне "программные средства" ставим галочку на "функционировать в режиме аккредитованного центра" и после "настроить" введя (ищем данные параметры в окне):

-средство электронной подписи издателя: CSP,

-средства удостоверяющего центра: ПК УЦ 4

-сертификат на средство электронной подписи издателя: Сертификат DemoC.lab.crt

-сертификат на средство удостоверяющего центра: Сертификат DemoC.lab.p7b

Нажимаем далее и в окне автоматический режим (при бездействии администратора) ставим передачу на публикацию и обновление CRL с периодичностью 1 день.

Далее создаём собственный пароль

Нажимаем далее и установить

Цус:

Отправить справочники

Укц:

Выдать новый дистрибутив и после ввода пароля заполняем на всех пользователей кроме координаторов: имя, эл.почта, организация и тд

PS: создаём квалифицированные ключи для пользователей сети

И после выводим ключи на рабочий стол

Ставим ключи на пользователей, фильтры

Устанавливаем на operCA registration point, publication service.

При установке зайти в компоненты windows (optionalfeatures) поставить Службы IIS и везде поставить галочки для работы с ftp

Далее на локальном диске создаём папку и в папке создать папки "un", "out", "unpublished" для директорий УКЦ; далее на диске создаём папку "сертификаты" и в этой папке ещё папка

Заходим в диспетчер служб IIS - сайты - добавить IP сайт - заполняем имя (FTP), физич.путь папка "сертификаты" - далее - запретить сайт без SSI -

далее - проверка подлинности (галочка анонимный, обычный), разрешить доступ (всем пользователям), разрешения (галочка чтение, запись) - готово

Заходим в registration point - ключи выбираем сетевого узла (3 точки - сетевые узлы) - vipnet client

Заходим в public service и расшариваем его: мой компьютер - ПКМ на public service - свойства - доступ - общий доступ - все - добавить - чтение запись - поделится - готово

Заходим на админа - мой компьютер - путь вводим IP operCA - ПКМ на public service - подключить в виде сетевого диска - готово

Делаем связку с укц и точкой регистрации:

Укц - справка - настройка - публикация данных

(2 строки папка "out", далее одна строка "un" и последняя "unpublished") ;

Точка распространения - добавить - заполняем данные, путь указывается через проводник (путь к FTP (ftp\\ip адрес)) - ок - ок

Укц - настройка - автоматический режим - раз в 24 часа

Public service - запустить - далее - обзор (первая строка out, вторая строка un)

Публикации - добавить - сертификаты издателей - FTP сервер - IP сервера (operCA) - пользователь Admin, пароль xxXX1234 - папка в папке сертификаты - далее, проверить, готово

Для проверки заходим в укц - администрирование - корневые сертификаты - ПКМ по администратору - опубликовать - ок

Registration point - сервис - настройка - запросы на дистрибутив - связь оператора со 2 координатором

сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов (на рабочем столе).

CA informing + сертификаты (Стасян)

Настройки

ОбщиеУведомленияOID

Выдача уведомлений

Способ выдачи уведомлений:

☒ Отправлять по электронной почте

Параметры отправки

☐ Сохранять в папку:

C:\Users\tester\Documents\CaInformingEme

Обзор...

Свойства сообщений с уведомлениями:

Адрес электронной почты отправителя:

admin@infotecs.ru

Имя отправителя:

Администратор УКЦ

Адреса электронной почты администраторов УКЦ для отправки уведомлений:

test@infotecs.ru

База данных удостоверяющего центра

Тип базы данных:

SQL Server (УКЦ 4.x)

Строка подключения к базе данных:

Data Source=.;winccsq\Initial Catalog=VIPNetAdministrator;Use

Кросс-сертификаты

☒ Использовать кросс-сертификаты

Путь к файлу с кросс-сертификатами:

C:\ProgramData\InfoTeCS\VIPNet Administrator\KC\K

Обзор...

Отчеты

Путь сохранения отчетов:

C:\Users\tester\Documents\CaInformingReports

Обзор...

Проверить настройки

?

ОКОтмена

Свойства отчета

ОбщиеВидФильтрация сертификатов

Фильтрация по сроку действия сертификата

☒ Начало: 01.01.2013 15

☒ Окончание: 01.02.2013 15

Фильтрация по OID полей сертификата в базе данных УКЦ

☒ OID поля "Расширенное использование ключа"

1.3.6.1.5.5.7.3.2;1.3.6.1.5.5.7.3.4

☒ Допустимые OID
 ☐ Недопустимые OID

☐ OID поля "Политики сертификата"

☐ Допустимые OID
 ☐ Недопустимые OID

Внимание! Для перечисления нескольких значений используйте точку с запятой.

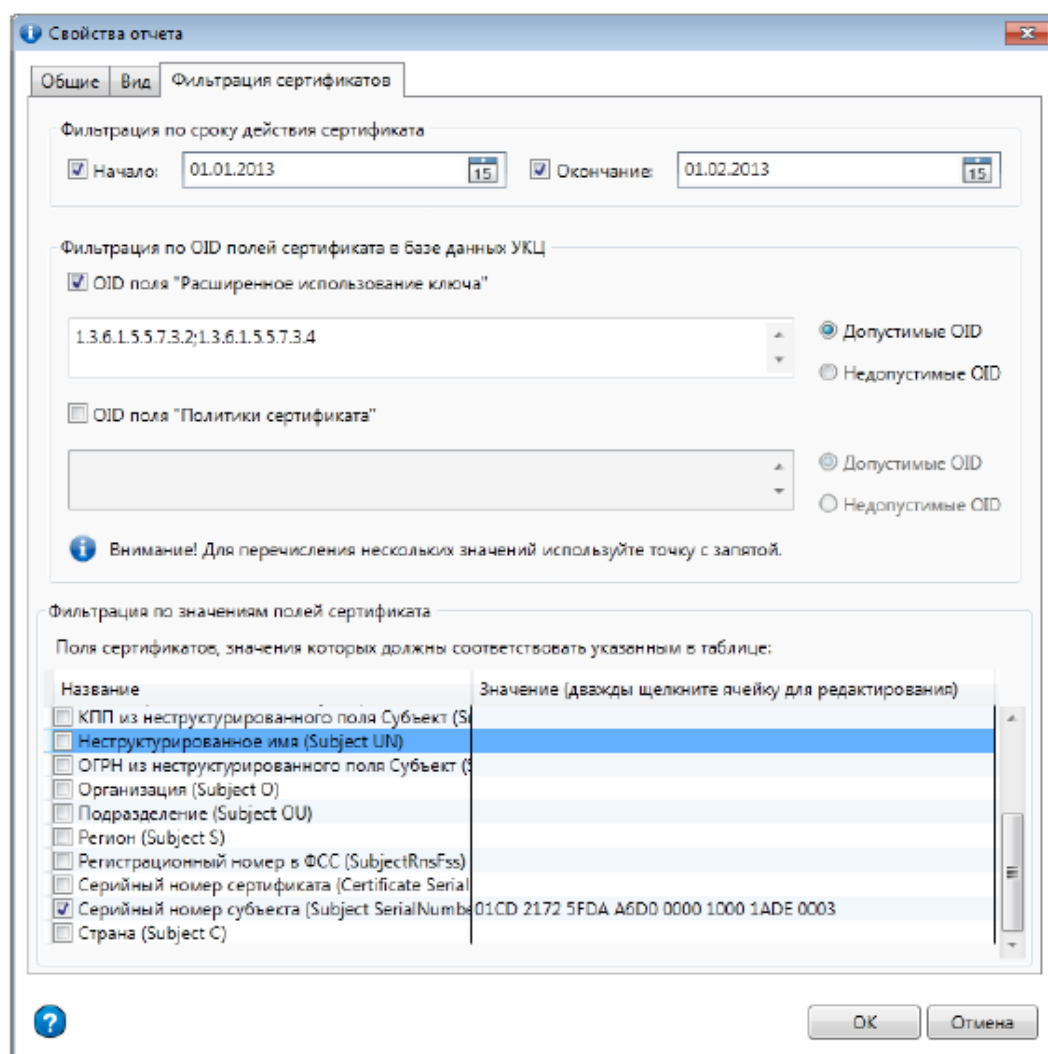
Фильтрация по значениям полей сертификата

Поля сертификатов, значения которых должны соответствовать указанным в таблице:

Название	Значение (дважды щелкните ячейку для редактирования)
<input type="checkbox"/> КПП из неструктурированного поля Субъект (S)	
<input type="checkbox"/> Неструктурированное имя (Subject UN)	
<input type="checkbox"/> ОГРН из неструктурированного поля Субъект (S)	
<input type="checkbox"/> Организация (Subject O)	
<input type="checkbox"/> Подразделение (Subject OU)	
<input type="checkbox"/> Регион (Subject S)	
<input type="checkbox"/> Регистрационный номер в ФСС (SubjectRnsFss)	
<input type="checkbox"/> Серийный номер сертификата (Certificate Serial)	
<input checked="" type="checkbox"/> Серийный номер субъекта (Subject SerialNumbe	01CD 2172 5FDA A6D0 0000 1000 1ADE 0003
<input type="checkbox"/> Страна (Subject C)	

OK

Отмена



Как подписать скрины

Для AdminCA

Отключение Брандмауэра (так же можно увидеть, что изменена дата)

Настройка IP-адресов

Успешная установка C++

Успешная установка VipNet Client

Успешная проверка подключения к серверу SQL

Успешная установка ЦУС

Успешная установка УКЦ

Успешная инициализация УКЦ

Успешно созданные ключи

Создание фильтров защищённой сети и открытой сети

Успешная связь между машинами(скрин из VipNet Client)

Успешная установка CA Informing

Для Open

Отключение Брандмауэра

Настройка IP - адресов

Успешная установка C++

Установленный SQL

Успешная настройка SQL

Этап настройки SQL (После установки в пуске нахожу SQL Server (manager), тут нужно поставить в Enabled, после этого (где WINN) делаю – Restart)

Успешная установка ЦУС

Использование лицензии (Далее подключаю диск с лицензией (_____.ITC)

Установка ролей у координатора

Установка связей между координаторами

Созданные клиенты

Для OperCA

Отключение Брандмауэра

Настройка IP - адресов

Успешная установка VipNet Client

Создание фильтров

Установка Registration Point

Успешная установка VipNet Publication Service