**ЗАДАНИЕ**

**ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА**

(2024 год)

|  |  |
| --- | --- |
| **Код и наименование профессии (специальности) среднего профессионального образования** | 10.02.05 Обеспечение информационной безопасности автоматизированных систем |
| **Наименование квалификации (направленности)** | Техник по защите информации |
| **Вид аттестации** | Государственная итоговая аттестация |
| **Уровень демонстрационного экзамена** | Базовый |
| **Шифр варианта задания** | В1\_КОД 10.02.05-1-2024-БУ |

**Вариант № 1**

|  |
| --- |
| Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении |
| Задание модуля 1:  С помощью технологии виртуальных машин для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах (Главный офис — виртуальные машины, Офис филиал — виртуальные машины).  При выполнении заданий необходимо ключевые настройки подтверждать скриншотами. Скриншоты необходимо сохранить на рабочем столе в папке «Отчет».  В ходе выполнения данного задания нужно установить основное ПО на рабочие станции будущей защищенной сети.  Доступ на все машины указан в дополнительной карточке задания   * Все пароли пользователей в сети сделать xxXX4455 * Все пароли администраторов в сети сделать 5544XXxx.   В случае изменения каких-либо логинов или паролей необходимо отобразить это в отчете.  Настройки сетевого окружения  Для правильной работы сети надо создать или убедиться в наличии 3 сетей:   * Host only или внутренняя сеть адаптер для сети центрального офиса * Host only или внутренняя сеть адаптер для сети филиала * Host only адаптер, NAT или Bridge для виртуального «Интернета» (в соответствии с инфраструктурой площадки, для связи всех координаторов между собой)   IP адреса защищенных сетей   * Центральный офис «Сеть 1 ЦО»: 192.168.1.0/24 * Офис филиал «Сеть 1 Филиал»: 10.10.10.128/26 * Офис сеть 2 «Сеть 2 Офис»: 172.110.110.192/26 * «Интернет» для всех координаторов: 203.73.66.0/24   Адреса выбираются самостоятельно из указанного диапазона.  Необходимо записать все IP адреса, логины и пароли в текстовый файл VPN.txt на рабочем столе компьютера.  В связи с особенностями работы системы на серверных версиях Пользовательская или серверная ОС необходимо устанавливать компоненты системы вручную (например, БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов. Необходимо произвести установку и настройку основных компонентов VPN-сети.  Задача 1.1 Установить базу данных MSSQL на ВМ Net1-DB (незащищенный узел) |
| Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| Задание модуля 2:  Задача 2.1 Развертывание ПК Administrator в качестве центра сертификации  Установить и настроить рабочее место администратора Certification Authority (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД.  Установить клиент ЦУС на ВМ Net1-DB (незащищенный узел)  Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.  Задача 2.2 Установка ПО VPN Coordinator и ПО VPN Client для Certification Authority   1. На компьютере Net1-AdminCA (ЦО) установить ПО Client (Пользовательская или серверная ОС), рабочее место администратора; 2. На компьютере на Net1-OperCA (ЦО) установить ПО Client (Пользовательская или серверная ОС). 3. На компьютере Net1-CoordCA (ЦО) установить и инициализировать Coordinator HW-VA;   Задача 2.3 Установка ПО Coordinator и ПО Client для организации сети филиала   1. На компьютере на Net2-Coord (Филиал) установить и инициализировать Coordinator HW-VA; 2. На ВМ на Net2-Client (филиал) установить ПО Client, рабочее место пользователя.   Необходимо зафиксировать процесс установки скриншотами форм + сделать скриншот директории, в которую установлено ПО, и скриншот первого запуска приложения. |
| Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении |
| Задание модуля 1:  Задача 1.2 Установка центра регистрации, сервиса публикации и сервиса информирования Certification Authority на соответствующие виртуальные машины   1. На компьютере на Net1-OperCA (ЦО) установить ПО Client, Publication Service. 2. На компьютере на Net1-OperCA (ЦО) установить ПО Registration Point. 3. На компьютере на Net1-AdminCA (ЦО) установить ПО CA Informing |
| Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| Задание модуля 2:  Задача 2.4 Развертывание удостоверяющего центра в составе защищенной сети  Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.  Схема сети, которую требуется создать, приведена далее.  IP адреса сетей перечислены в начале задания (по названию сетей).    Рисунок 1 Схема защищенной сети  В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).  Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Вирт. машина | Название сетевого узла | ПО | ОС сетевого узла | Имя пользователя сетевого узла, уровень полномочий | | Net1-AdminCA (ЦО) | Администратор ViPNet (VM) | Administrator (ЦУС клиент и сервер + УКЦ), Client, CA Informing | Пользовательская или серверная ОС | Administrator\_  VPN | | Net1-CoordCA (ЦО) | Основной координатор (VM) | Coordinator | HW-VA | Base\_ Coordinator | | Net1-OperatorCA (ЦО) | Оператор УЦ (VM) | Client, Publication Service, Registration Point | Пользовательская или серверная ОС | Operator\_CR | | Net2-Coord (Филиал) | Дочерний координатор (VM) | Coordinator | HW-VA | Sub\_Coordinator | | Net2-Client (филиал) | Клиент филиала (VM) | Client | Пользовательская или серверная ОС | Branch\_Client |   Связи между узлами необходимо настроить самостоятельно.  Таблица 2. Схема связей пользователей   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Схема связей пользователей | Base\_ Coordinator | Administrator\_  VPN | Operator\_CR | Sub\_Coordinator | Branch\_Client | | Base\_ Coordinator | × | **\*** | **\*** | **\*** |  | | Administrator\_  VPN | **\*** | × | **\*** |  | **\*** | | Operator\_CR | **\*** | **\*** | × | **\*** |  | | Sub\_Coordinator | **\*** |  | **\*** | × | **\*** | | Branch\_Client |  | **\*** |  | **\*** | × |   Задача 2.5 Создание структуры защищенной сети  ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой (выгрузить отчет в HTML). Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой.  УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папке (создать подпапку Задача 2.5), поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса (удостоверяющего центра) и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп (проверить, что пароль работает).  На всех узлах сети корректно настроить или проверить корректность настройки сетевых интерфейсов в соответствии со схемой, проверить доступность соседних узлов.  Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов. |
| Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении |
| Задание модуля 1:  Задача 1.3 Настройка работы удостоверяющего центра в аккредитованном режиме  Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов, указав:   * сведения о средствах УЦ, * средство электронной подписи издателя: CSP, * средства удостоверяющего центра: ПК УЦ 4 * сертификат на средство электронной подписи издателя: Сертификат DemoС.lab.crt * сертификат на средство удостоверяющего центра: Сертификат DemoС.lab.p7b * класс защищенности, которому соответствуют программные средства УЦ, * место хранения контейнеров ключа ЭП и ключа защиты УКЦ (файл на диске).   После перевода УКЦ в аккредитованный режим необходимо выпустить:   * Корневой квалифицированный сертификат. Назначить текущим. * Квалифицированную электронную подпись для пользователя Administrator\_VPN. Выдать с новым дистрибутивом ключей. * Квалифицированную электронную подпись для пользователя Branch\_Client. Сохранить электронные ключи в файл.   При формировании сертификатов необходимо заполнить следующие поля:   * Имя: <Имя пользователя или узла> * Электронная почта: <Имя пользователя>@demo.lab * Город: Пермь * Область: Пермский край * Организация: ООО Надежда * Подразделение: ИТ-отдел * Почтовый индекс:614000   Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети.  Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (Publication Service).  Настроить переход в автоматический режим (при бездействии администратора): передачу на публикацию и обновление CRL с периодичностью 1 день.  Реализовать автоматическую публикацию сертификатов издателей на FTP-сервере.  Посредством Центра Регистрации (Registration Point):   1. зарегистрировать пользователя: Branch\_Client; 2. отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос. Результат выпуска сертификата зафиксировать скриншотом; 3. отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос. Результат зафиксировать скриншотом. 4. Посредством Сервиса Информирования ( CA Informing): 5. настроить способ выдачи уведомлений (файлы \*.eml локально для последующей отправки должны сохраняться в папке на рабочем столе); 6. сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов (на рабочем столе). |
| Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| Задание модуля 2:  Задача 2.6 Отправить письмо по Деловой почте пользователю Branch\_Client с узла Administrator\_VPN, отправить текстовое сообщение пользователю Administrator\_VPN от пользователя Branch\_Client. 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. |
| Модуль 1: Эксплуатация автоматизированных (информационных) систем в защищенном исполнении |
| Задача 1.4. Модификация структуры защищенной сети  Перед началом выполнения сделать HTML выгрузку структуры сети и сделать скриншот ЦУС окна с пользователями.  Модификация структуры сети:   1. добавить новый сетевой узел User и пользователя User за координатором «Основной координатор» (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем Branch\_Client. На указанных узлах проверить появление нового узла; 2. Добавить пользователя Branch\_Client\_2 на узле Клиент филиала (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи. |
| Модуль 2: Защита информации в автоматизированных системах программными и программно-аппаратными средствами |
| Задание модуля 2:  Задача 2.7 Отправить письмо по Деловой почте пользователю Branch\_Client\_2 с узла Administrator\_VPN, отправить текстовое сообщение пользователю Administrator\_VPN от пользователя Branch\_Client\_2. 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; * скриншоты журнала IP-пакетов на координаторах, подтверждающие прохождение письма через координаторы.   Кроме того, необходимо сохранить файл HTML с обновленной структурой защищенной сети, выгруженный из ЦУС. |