КОНКУРСНОЕ ЗАДАНИЕ
категория «Студенты»

Компетенция: informatsionnaya-bezopasnost-o

Выдержка из официального конкурсного задания, опубликованного на abilympics-russia.ru (раздел «Компетенции 2026»).
Страницы источника, относящиеся к категории, приведены далее в исходном виде.

Собрано автоматически: Региональный центр Абилимпикс республики Башкортостан.

2. Конкурсное задание

Конкурсное задание может быть изменено на 30% в пределах существующих модулей.

2.1. Краткое описание задания

2.1.1. Категория участников «ШКОЛЬНИКИ»:

В ходе выполнения конкурсного задания участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- настройка VPN-сети на существующей и вычислительной инфраструктуре, администрирование узлов и пользователей;
- развертывание ViPNet Client для Windows, Linux, ViPNet Coordinator, ViPNet xFirewall;
- выполнение компрометации узлов, ключей, пользователей. Восстановление связи;
- проверка работоспособности VPN-сети.

2.1.2. Категория участников «СТУДЕНТЫ»:

В ходе выполнения конкурсного задания участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- настройка VPN-сети на существующей и вычислительной инфраструктуре, администрирование узлов и пользователей;
- развертывание ViPNet Client для Windows, Linux, ViPNet Coordinator, ViPNet xFirewall;
- выполнение компрометации узлов, ключей, пользователей. Восстановление связи;
- организацию межсетевого взаимодействия и туннелирования;
- проверка работоспособности VPN-сети.

2.1.3. Категория участников «СПЕЦИАЛИСТЫ»:

В ходе выполнения конкурсного задания участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- настройка VPN-сети на существующей и вычислительной инфраструктуре, администрирование узлов и пользователей;
- развертывание ViPNet Client для Windows, Linux, ViPNet Coordinator, ViPNet xFirewall;
- выполнение компрометации узлов, ключей, пользователей. Восстановление связи;
- организацию межсетевого взаимодействия и туннелирования;
- проверка работоспособности VPN-сети.
- внедрение централизованных политик безопасности. Обеспечение защиты рабочих мест.

2.2. Структура и подробное описание конкурсного задания

Категория участников	Наименование и описание модуля	Время	Результат
Школьники	**Модуль А.** Настройка защищенной VPN сети.	45 минут	Создана защищенная сеть ViPNet.
	Модуль Б. Развертывание узлов сети.	45 минут	Узлы сети развернуты и настроены.
	Модуль В. Компрометация узла.	45 минут	Произведена компрометация ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.
	Модуль Г. Работоспособность сети.	45 минут	Сделаны скриншоты работоспособной сети ViPNet.
Время выполнение всех модулей: **3 часа**			
Студенты	**Модуль А.** Настройка защищенной VPN сети.	40 минут	Создана защищенная сеть ViPNet.
	Модуль Б. Развертывание узлов сети.	1,5 часа	Узлы сети развернуты и настроены.
	Модуль В. Компрометация узла.	20 минут	Произведена компрометация ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.
	Модуль Г. Работоспособность сети.	1,5 часа	Сделаны скриншоты работоспособной сети ViPNet

			Проверено взаимодействие узлов. Настроено туннелирование. Установлены клиенты для Linux.
Время выполнение всех модулей: **4 часа**			
Специалисты	**Модуль А.** Настройка защищенной VPN сети.	40 минут	Создана защищенная сеть ViPNet.
	Модуль Б. Развертывание узлов сети.	1,5 часа	Узлы сети развернуты и настроены.
	Модуль В. Компрометация узла.	20 минут	Произведена компрометация ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.
	Модуль Г. Работоспособность сети.	1,5 часа	Сделаны скриншоты работоспособной сети ViPNet Проверено взаимодействие узлов, Настроено туннелирование. Установлены клиенты для Linux. Настроены централизованные политики безопасности.
Время выполнение всех модулей: **4 часа**			

2.3 Последовательность выполнения задания.

2.3.1. Категория участников «ШКОЛЬНИКИ»:

Модуль А. Настройка защищенной VPN сети.

С помощью системы виртуализации необходимо установить компоненты для администрирования защищенной сети VPN, настроить узлы сети ViPNet.

Модуль Б. Развертывание узлов сети.

Развернуть в системе виртуализации узлы защищенной сети, настроить сетевые интерфейсы, настроить необходимые фильтры.

Модуль В. Компрометация узла.

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя. Сделать скриншоты экрана «защищенная сеть» на двух координаторах. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.

Модуль Г. Работоспособность сети.

Проверить работоспособность сети VPN, сделать соответствующие скриншоты.

2.3.2. Категория участников «СТУДЕНТЫ»:

Модуль А. Модуль А. Настройка защищенной VPN сети.

С помощью системы виртуализации необходимо установить компоненты для администрирования защищенной сети VPN, настроить узлы сети ViPNet.

Модуль Б. Развертывание узлов сети.

Развернуть в системе виртуализации узлы защищенной сети, настроить сетевые интерфейсы, настроить необходимые фильтры.

Модуль В. Компрометация узла.

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя. Сделать скриншоты экрана «защищенная сеть» на двух координаторах. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.

Модуль Г. Работоспособность сети.

Проверить работоспособность сети VPN, сделать соответствующие скриншоты. Настроить туннелирование между открытыми узлами. Установит Linux клиенты.

2.3.3. Категория участников «СПЕЦИАЛИСТЫ»:

Модуль А. Модуль А. Настройка защищенной VPN сети.

С помощью системы виртуализации необходимо установить компоненты для администрирования защищенной сети VPN, настроить узлы сети ViPNet.

Модуль Б. Развертывание узлов сети.

Развернуть в системе виртуализации узлы защищенной сети, настроить сетевые интерфейсы, настроить необходимые фильтры.

Модуль В. Компрометация узла.

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя. Сделать скриншоты экрана «защищенная сеть» на двух координаторах. Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС.

Модуль Г. Работоспособность сети.

Проверить работоспособность сети VPN, сделать соответствующие скриншоты. Настроить туннелирование между открытыми узлами. Установит Linux клиенты. Настроить политики безопасности для защищенных узлов с помощью ViPNet Policy Manager. Настроено межсетевое взаимодействие.

Особые указания по компетенции:

Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от участия в конкурсе.

Перед началом соревнований участникам будет предоставлена возможность проверить работоспособность системы виртуализации, наличие необходимого программного обеспечения, проверить работоспособность виртуальных машин.

При выполнении задания доступ в сеть Интернет для участников разрешен. Разрешается использовать только открытые источники сети Интернет, включая официальные сайты производителей программного обеспечения и организаций. Запрещено обращаться к форумам, личным страницам, ресурсам, требующим аутентификации и/или авторизации, нейросетям.

2.4. Региональный (вариативный):

Примеры изменений для регионального (вариативного) модуля:

Модуль Г. Работоспособность сети.

Задание

- настройка политик безопасности ViPNet Policy Manager;
- настройка туннелирования на координаторах или с помощью ЦУС;
- настройка политик безопасности с помощью командного интерпретатора;
- настройка межсетевого взаимодействия;
- сменить мастер ключи своей сети, восстановить работоспособность;
- установить ViPNet Client 4U или 5 под Linux;
- установить ViPNet EPP сервер и клиент на машину администратора;
- установить ViPNet EPP агент на машину клиента филиала, проверить работоспособность.