

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Российский Государственный Социальный Университет»**

Специальность – Информационные системы (по отраслям)

Дисциплина «**Вычислительные системы сети и телекоммуникации**»

«**Практика 5**»

**Выполнил:**

студент 2 курса

группы ИН-К-0-Д-2020-2-11,

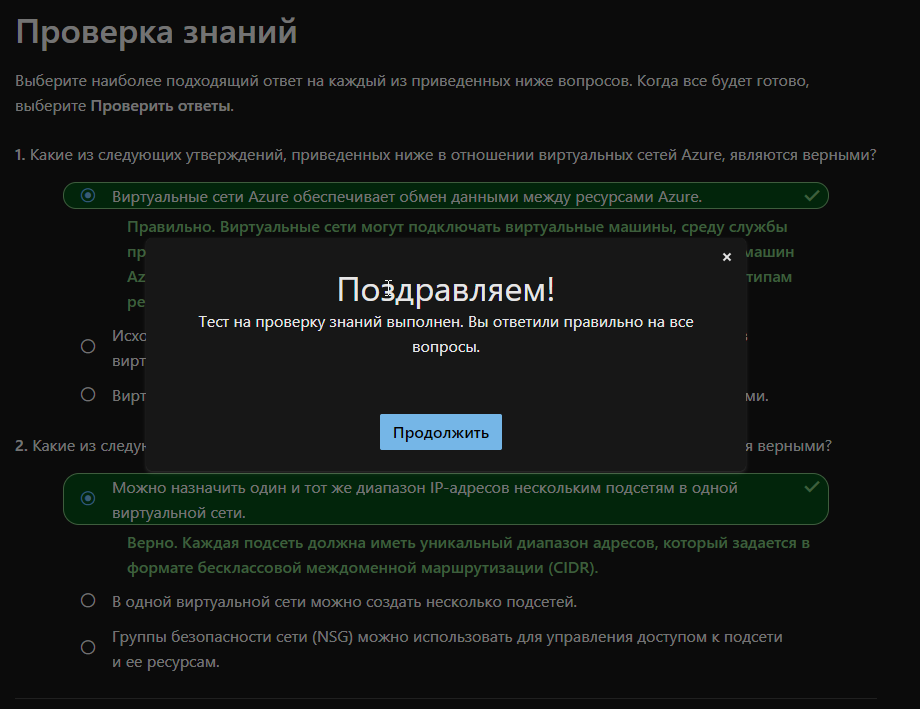
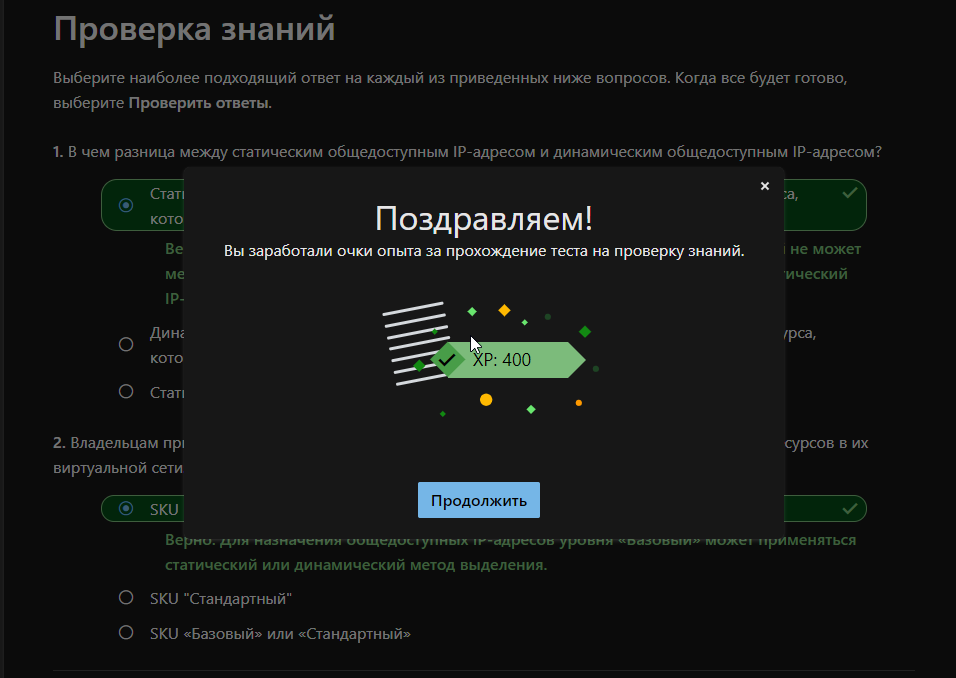
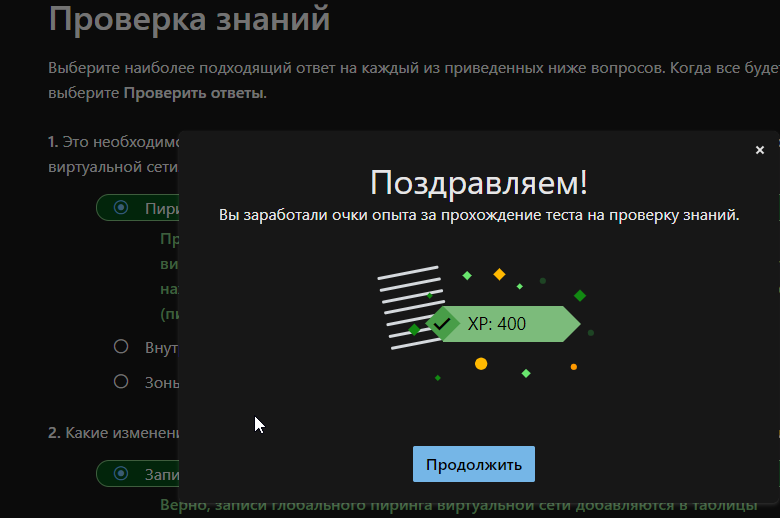
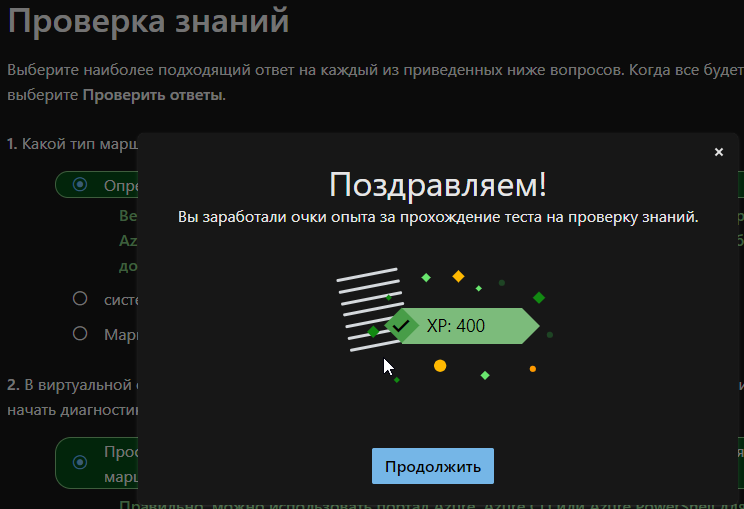
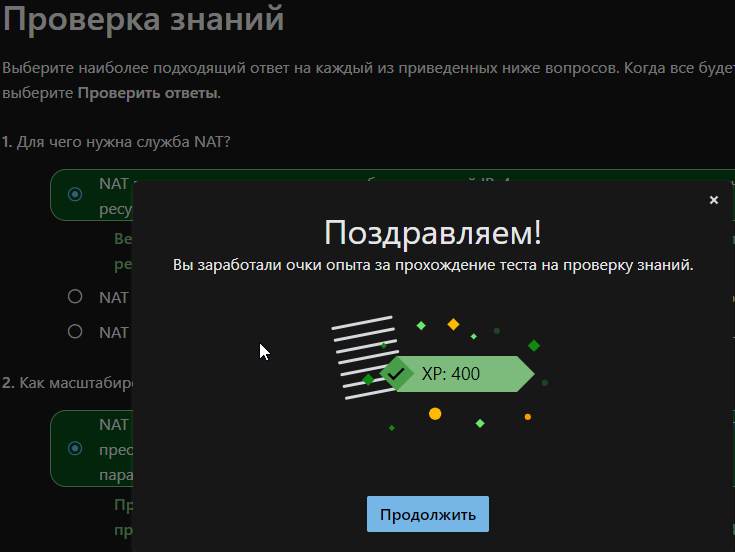
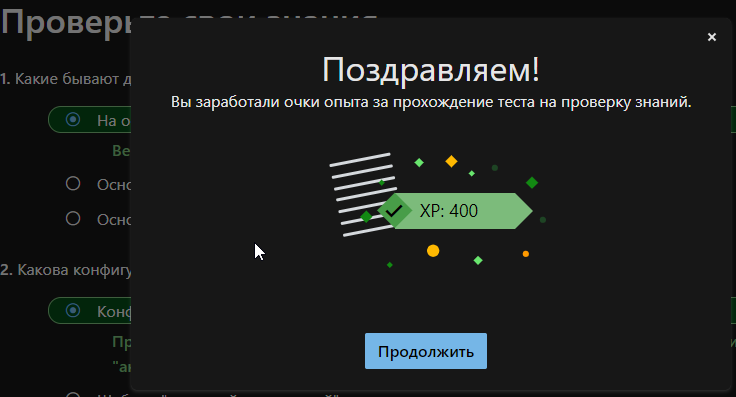
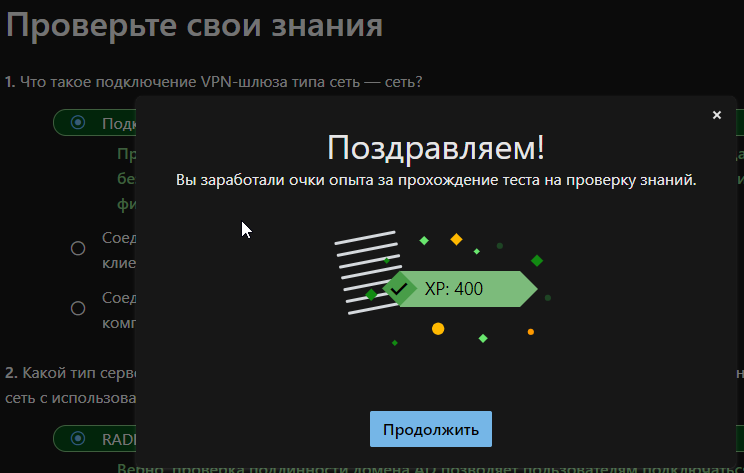
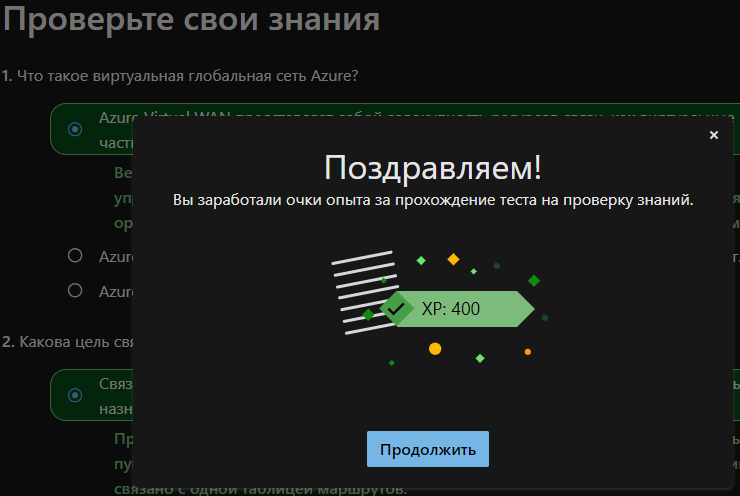
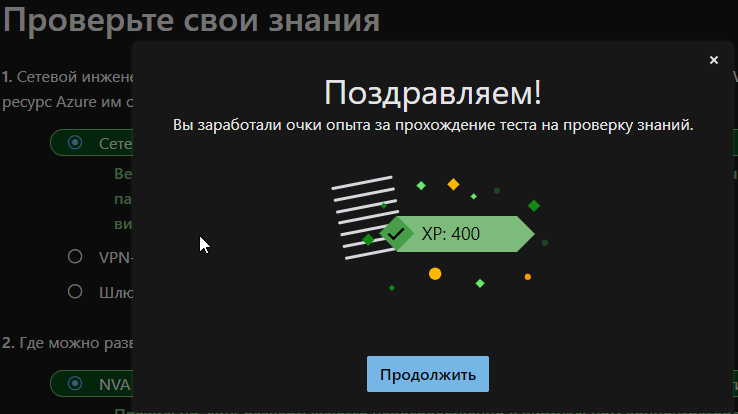
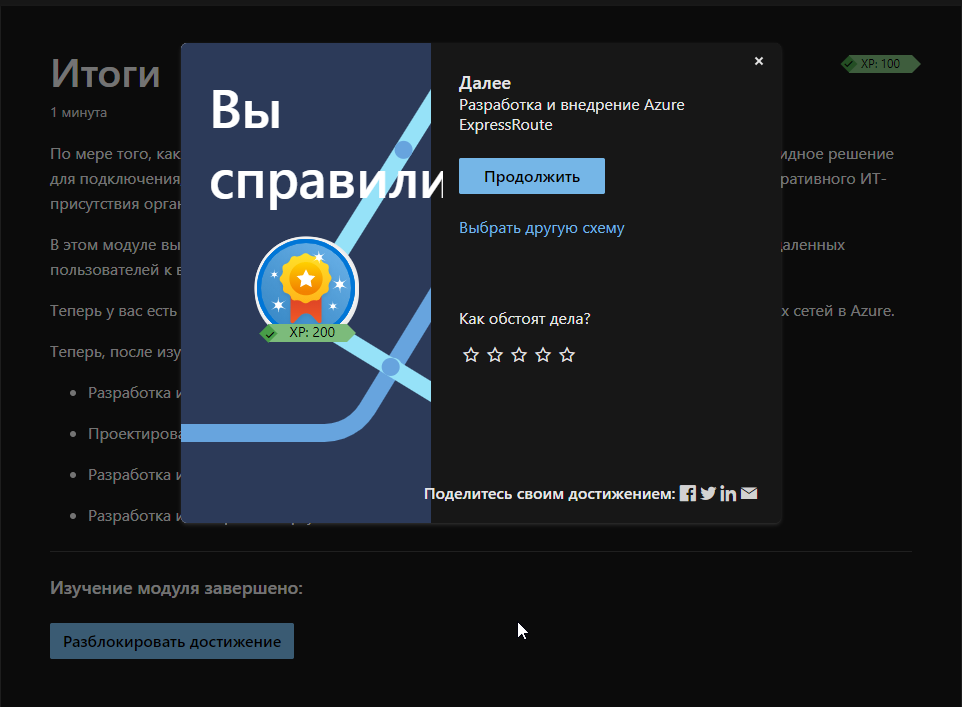
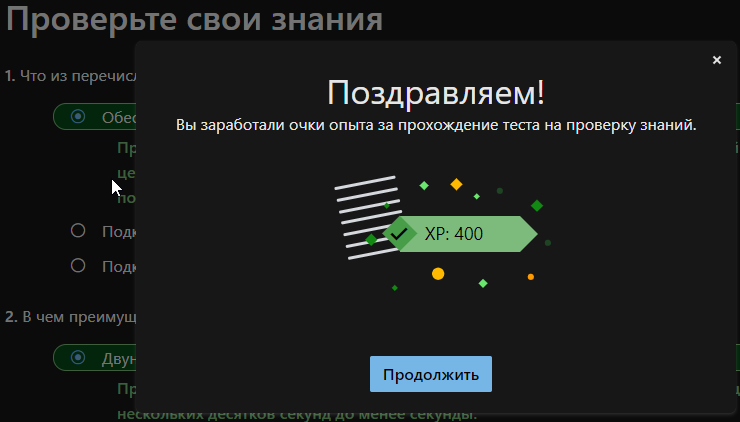
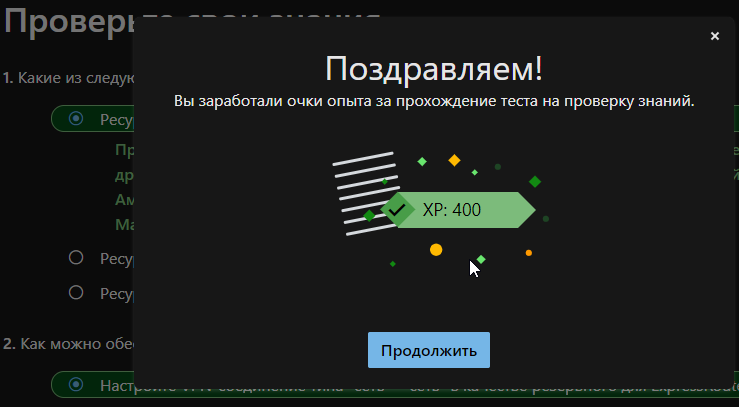
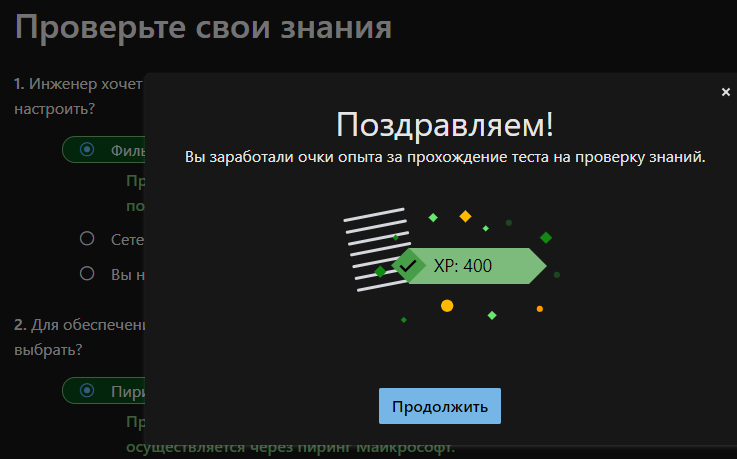
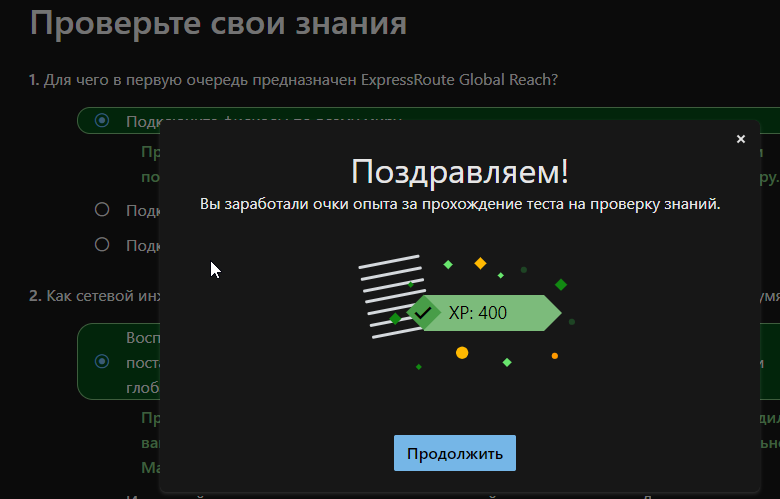
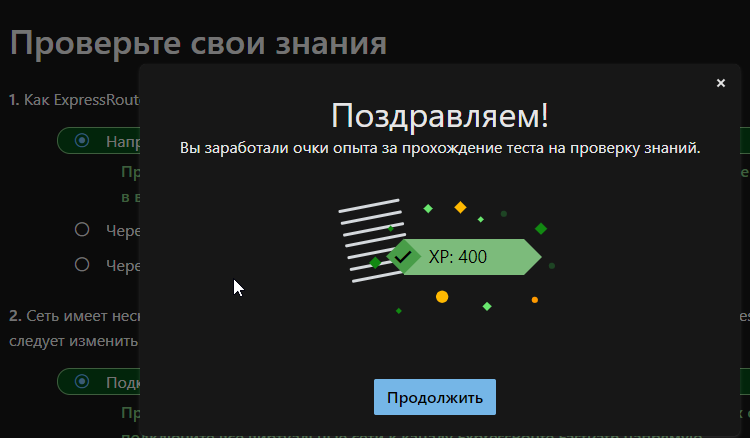
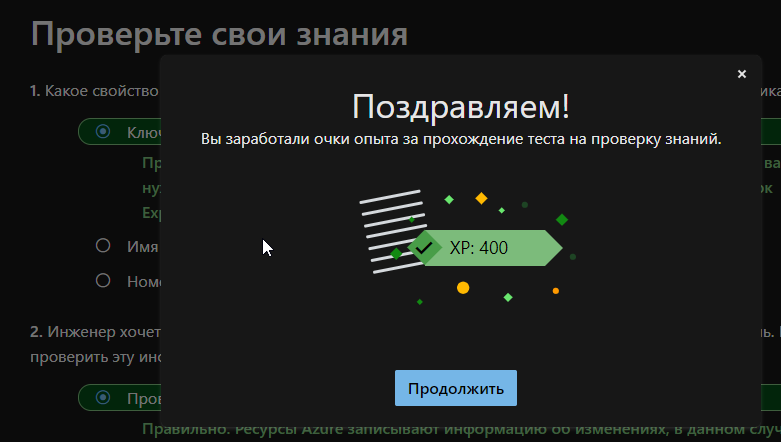
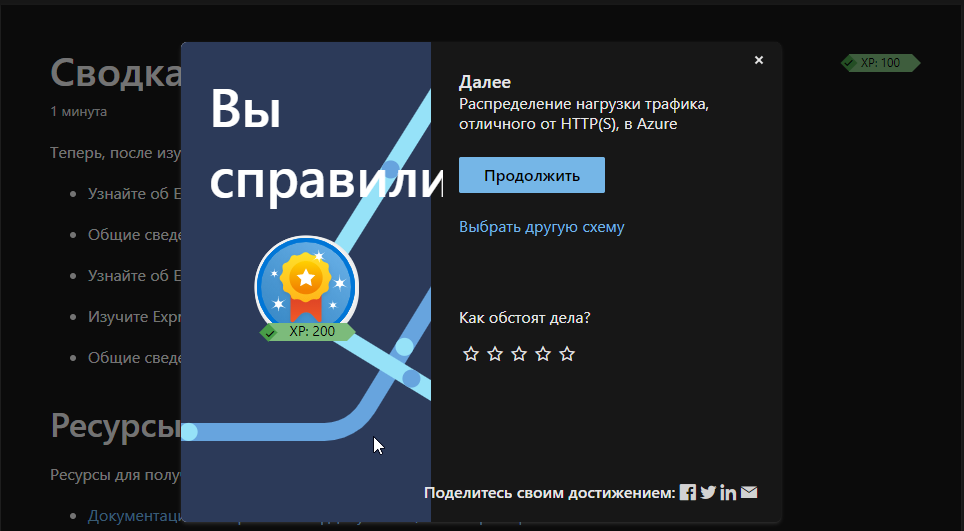
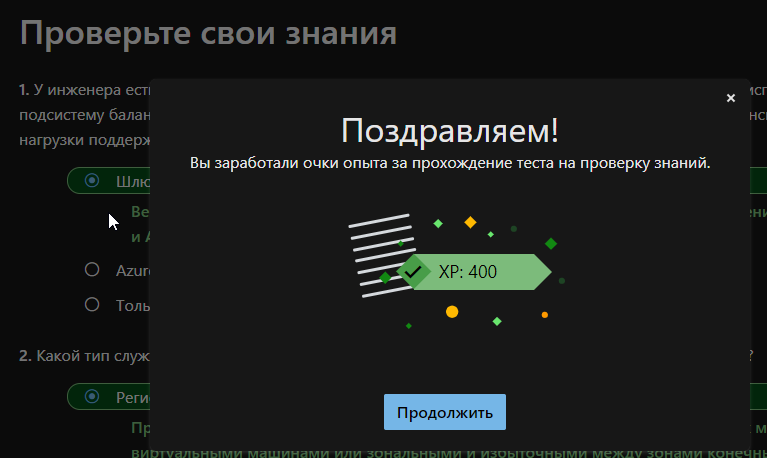
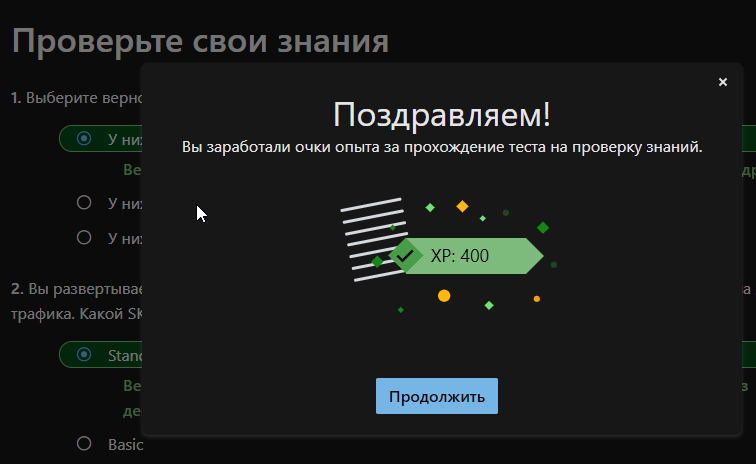
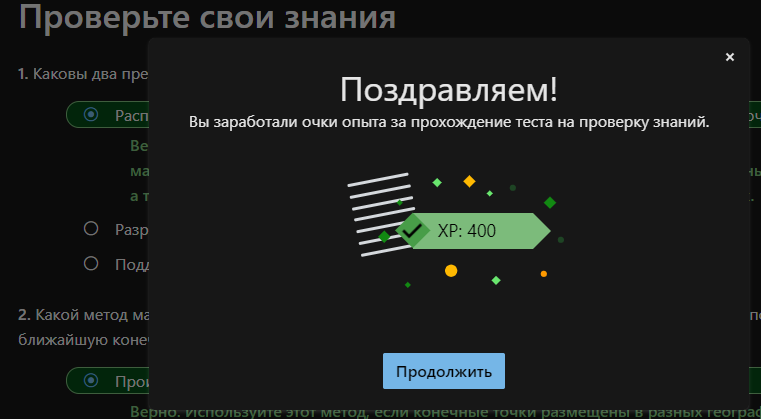
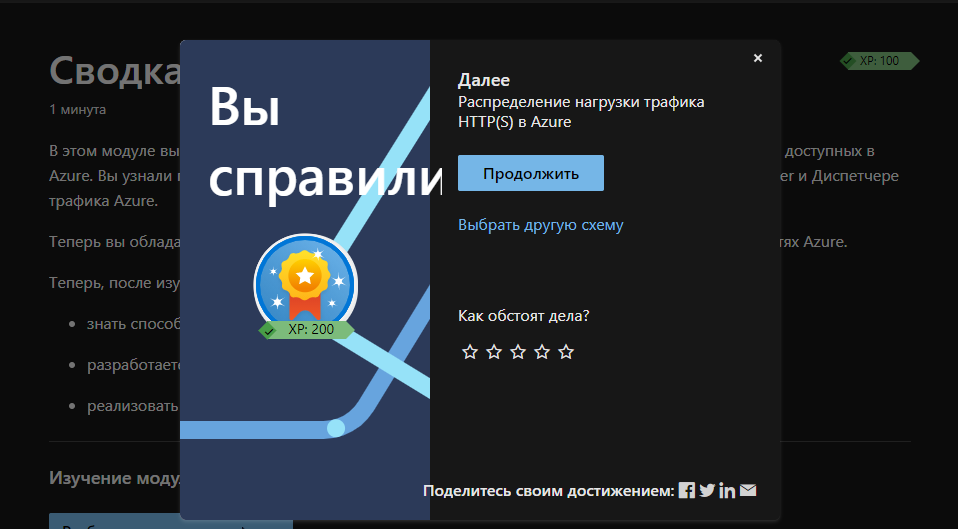
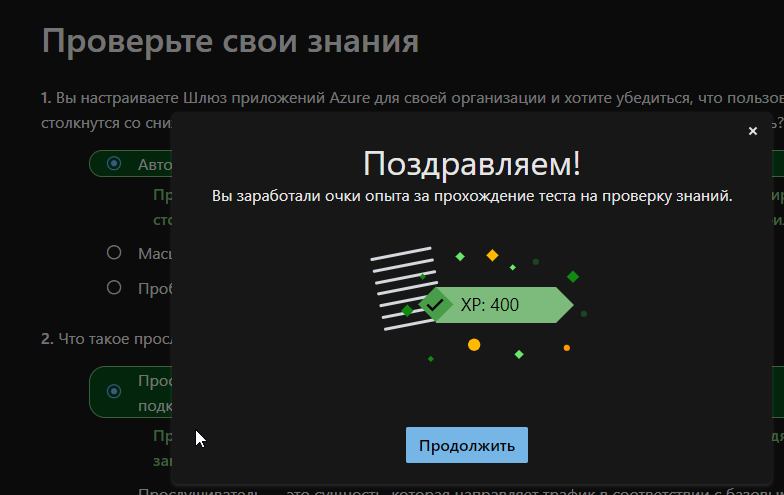
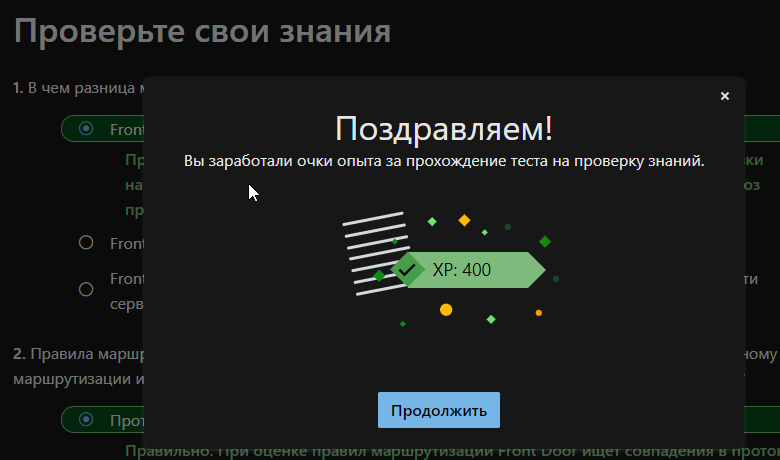
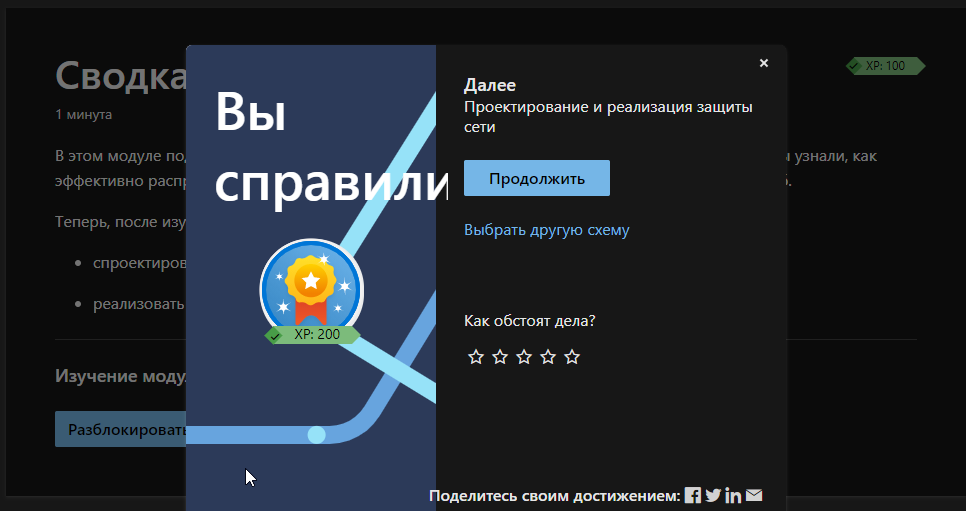
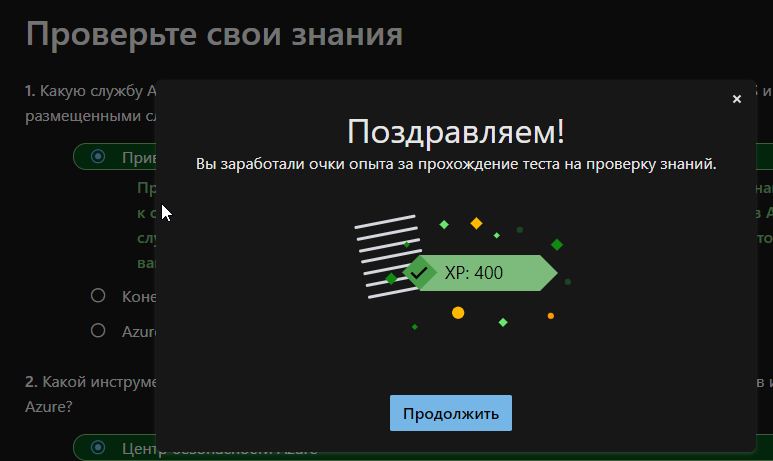
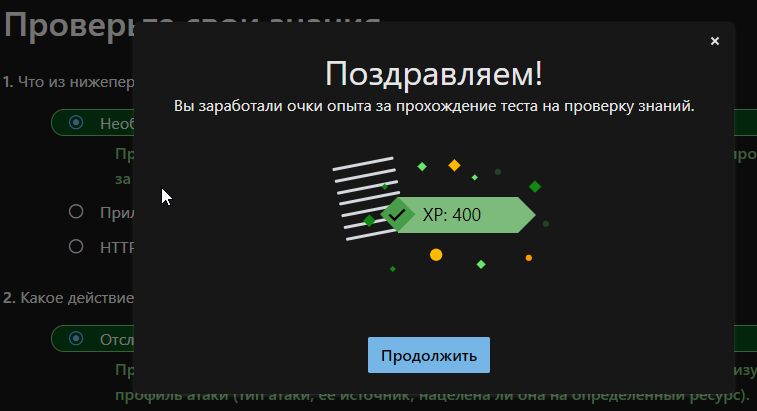
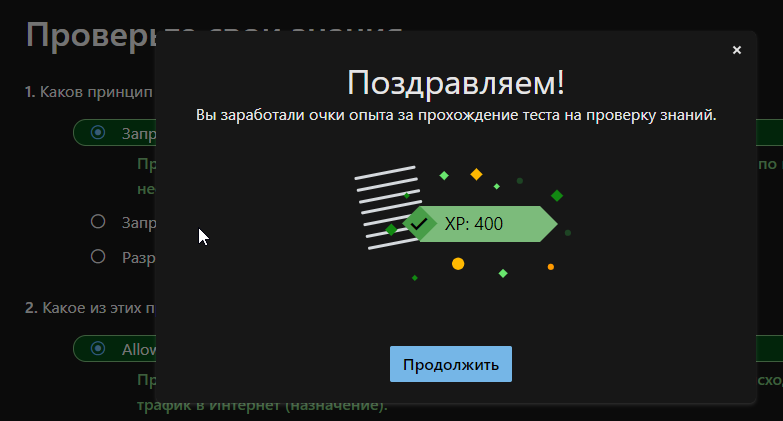
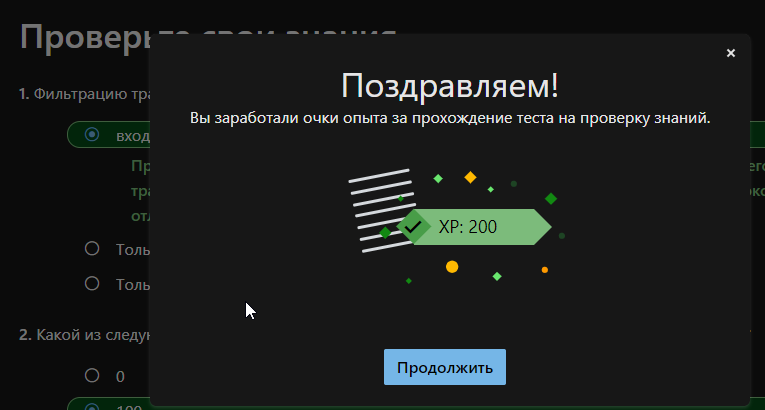
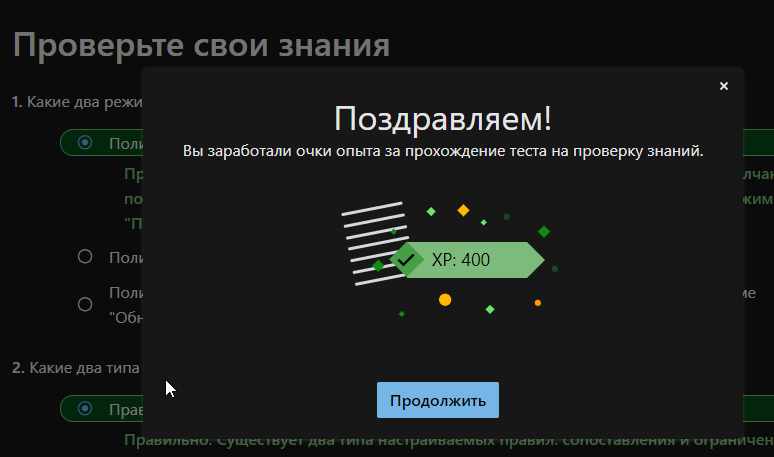
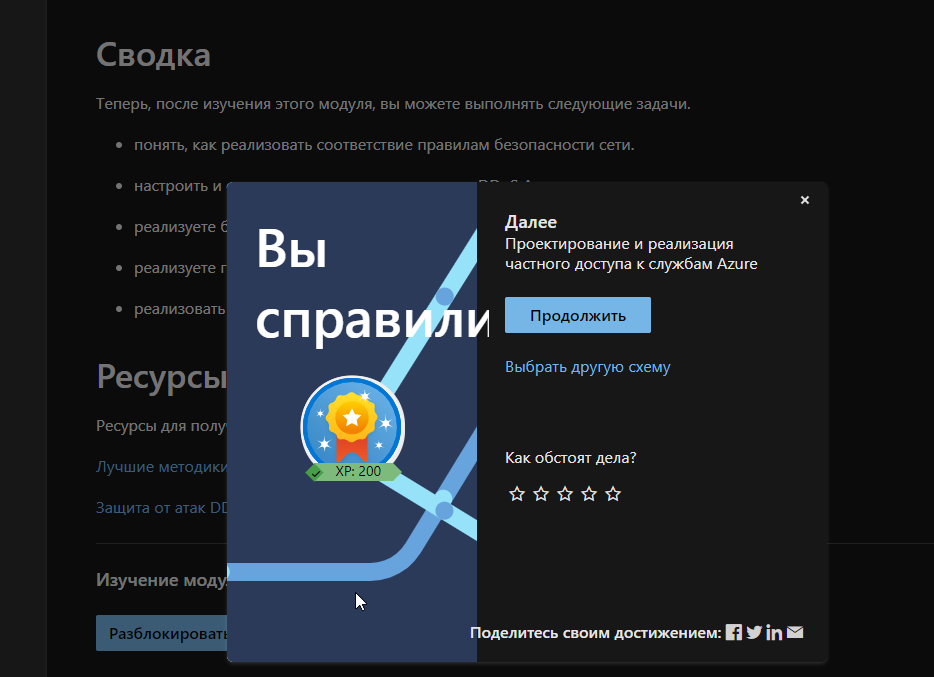
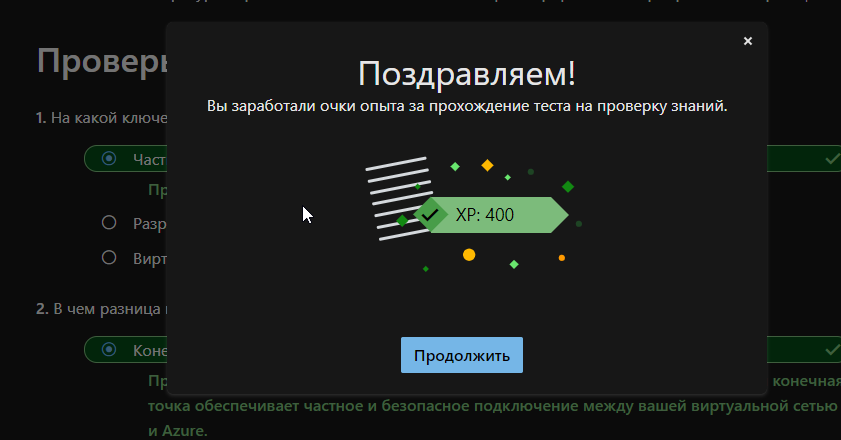
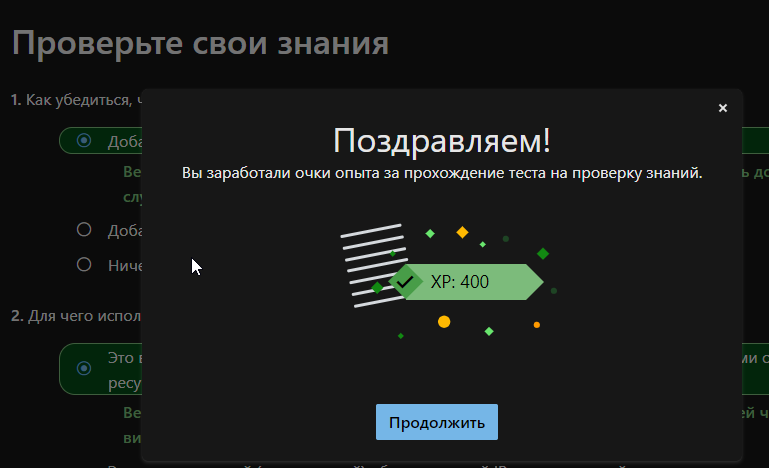
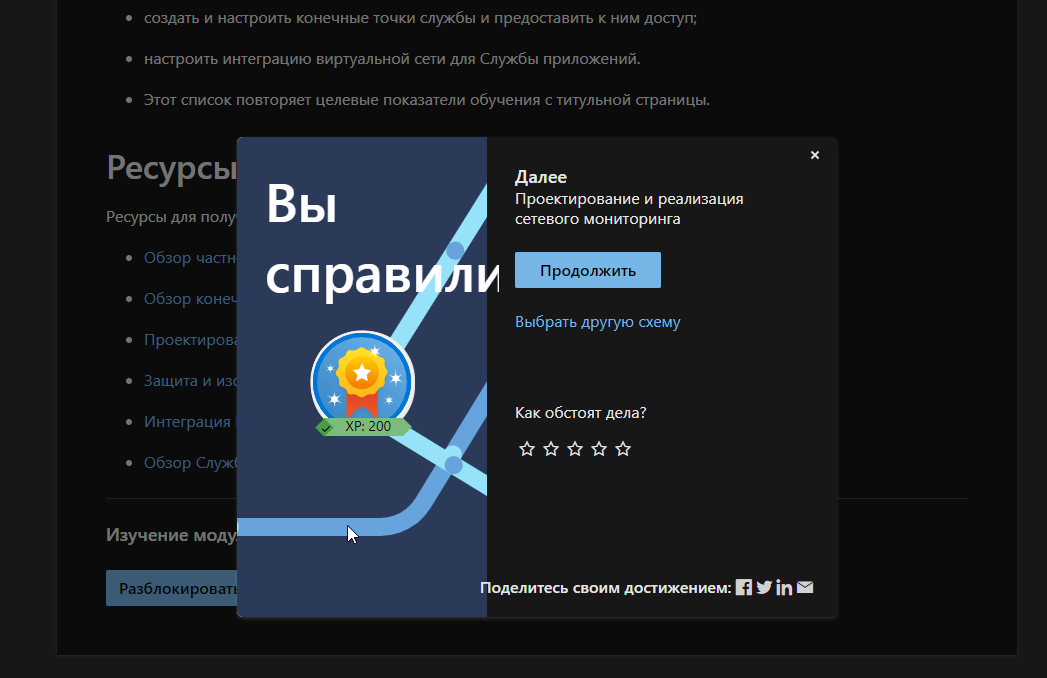
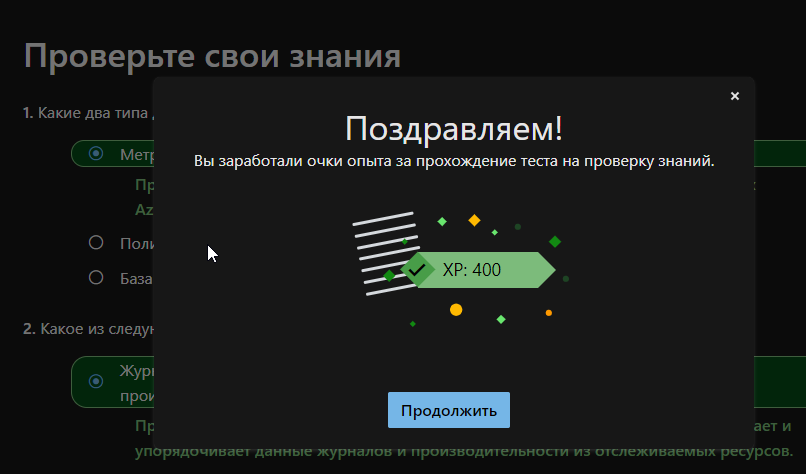
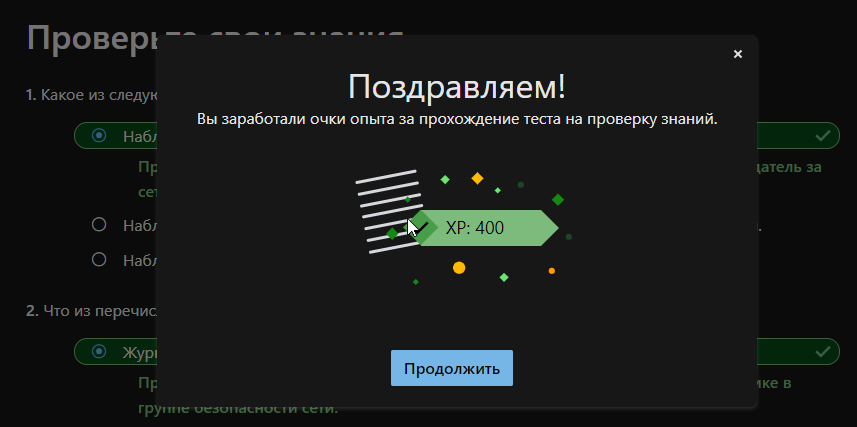
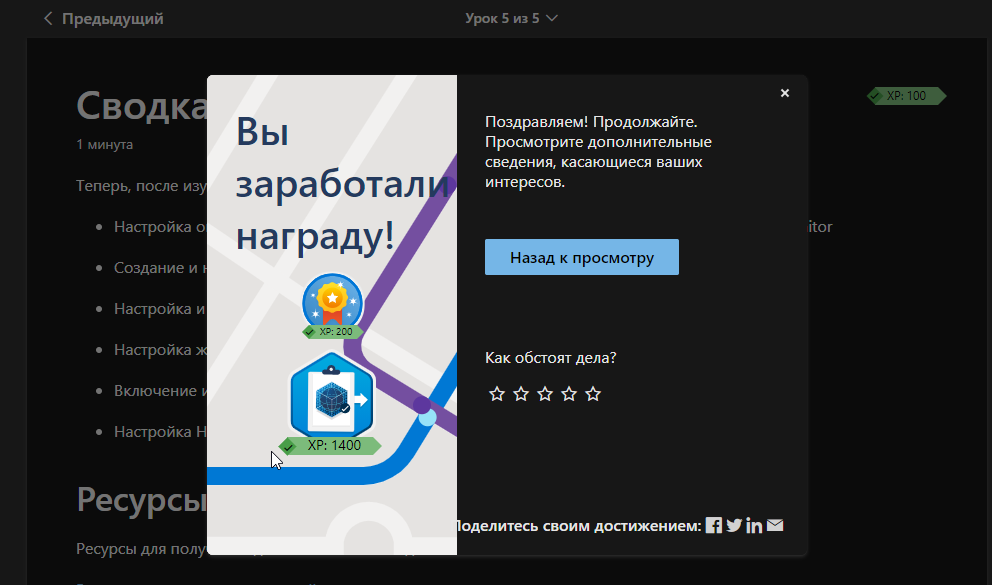
Чайковский Н. О.

**Проверил:**

преподаватель

Ерпелев А. В.

Ход работы

* Общие сведения о виртуальных сетях Azure
  + Общие сведения о виртуальных сетях Azure
  + Разрешение имени проекта для виртуальной сети
  + Создание возможности подключения между виртуальными сетями с использованием пиринга
  + Реализация маршрутизации трафика в виртуальной сети
  + Настройка доступа к Интернету с помощью NAT виртуальной сети Azure
* Проектирование и реализация гибридных сетей
  + Проектирование и реализация VPN-шлюза Azure
  + Подключайте устройства к сетям с помощью VPN-подключений типа точка — сеть
  + Подключение удаленных ресурсов с помощью виртуальных глобальных сетей Azure
  + Создание сетевого виртуального устройства (NVA) в виртуальном концентраторе
  + Итоги
* Разработка и внедрение Azure ExpressRoute
  + Знакомство с Azure ExpressRoute
  + Проектирование развертывания ExpressRoute
  + Настройка пиринга для цепи ExpressRoute
  + Соединяйте географически разнесенные сети с глобальным охватом ExpressRoute
  + Повышение производительности пути передачи данных между сетями с помощью ExpressRoute FastPath
  + Устранение проблем с подключением ExpressRoute
  + Итоги
* Распределение нагрузки трафика, отличного от HTTP(S), в Azure
  + Варианты балансировки нагрузки
  + Проектирование и реализация подсистемы балансировки нагрузки Azure с помощью портала Azure
  + Сведения о Диспетчере трафика Azure
  + Итоги
* Распределение нагрузки трафика HTTP(S) в Azure
  + Настройка Шлюза приложений Azure
  + Проектирование и настройка Azure Front Door
  + Итоги
* Проектирование и реализация защиты сети
  + Защита виртуальных сетей на портале Azure
  + Развертывание Защиты от атак DDoS с помощью портала Azure
  + Развертывание групп безопасности сети с помощью портала Azure
  + Проектирование и реализация Брандмауэра Azure
  + Реализация брандмауэра веб-приложения в Azure Front Door
  + Итоги
* Проектирование и реализация частного доступа к службам Azure
  + Определение службы "Приватный канал" и частной конечной точки
  + Интеграция Приватного канала с DNS
  + Итоги
* Проектирование и реализация сетевого мониторинга
  + Мониторинг сетей с помощью Azure Monitor
  + Мониторинг сетей с помощью наблюдателя за сетями Azure
  + Итоги

Реферат-анализ

Пройдя обучение на платформе Microsoft Learn по курсу AZ-700: Designing and Implementing Microsoft Azure Networking Solutions (Проектирование и реализация сетевых решений Microsoft Azure) я должен был узнать, как спроектировать и реализовать безопасную сетевую инфраструктуру в Azure и как установить гибридное подключение, настроить маршрутизацию и частный доступ к службам Azure, а также как вести мониторинг в Azure. И я действительно сделал это.

Я прошёл следующие очень интересные, а главное так полезные в моей текущей жизненной стадии, прекрасные, написанные чудесным человеком, и очень понятным, качественным языком, примеры в которых понятны буквально с первого взгляда - модули:

* Общие сведения о виртуальных сетях Azure
* Проектирование и реализация гибридных сетей
* Разработка и внедрение Azure ExpressRoute
* Распределение нагрузки трафика, отличного от HTTP(S), в Azure
* Распределение нагрузки трафика HTTP(S) в Azure
* Проектирование и реализация защиты сети
* Проектирование и реализация частного доступа к службам Azure
* Проектирование и реализация сетевого мониторинга

Детали модуля Общие сведения о виртуальных сетях Azure

Я узнал, как проектировать и внедрять фундаментальные сетевые ресурсы Azure, такие как виртуальные сети, общедоступные и частные IP-адреса, DNS, пиринг между виртуальными сетями, маршрутизация и преобразование сетевых адресов в виртуальных сетях Azure.

Так же узнал про настройку служб для динамических и статических общедоступных IP-адресов.

Такой ресурс можно связать с одним из таких ресурсов:

* сетевые интерфейсы виртуальных машин;
* Балансировщики нагрузки, доступные в Интернете
* VPN-шлюзы
* шлюзы приложений
* Брандмауэр Azure

Детали модуля Проектирование и реализация гибридных сетей

Я узнал, как разрабатывать и внедрять гибридные сетевые решения, такие как VPN-подключения типа "сеть — сеть", VPN-подключения типа "точка — сеть", виртуальные глобальные сети Azure и концентраторы виртуальных глобальных сетей.

Так же узнал о возможности подключения VPN-шлюза Azure. Он нужен когда необходимо создать зашифрованное подключение. Вы можете подключиться через Интернет или выделенный канал. Шлюз предоставляющий конечную точку для входящих подключений из локальных сред.

Узнал про возможность создания сетевого виртуального устройства (NVA) в виртуальном концентраторе. После подключения виртуальных сетей к виртуальному концентратору NVA обеспечивает транзитивное подключение во всей виртуальной глобальной сети организации. NVA можно развернуть непосредственно в виртуальном концентраторе глобальной сети.

Детали модуля Разработка и внедрение Azure ExpressRoute

Я узнал, как разработать и внедрить Azure ExpressRoute, ExpressRoute Global Reach, ExpressRoute FastPath и когда использовать каждую службу в соответствии с требованиями среды.

Познакомился с Azure ExpressRoute. Это такой инструмент который позволяет переносить локальные сети в Microsoft Cloud по частному подключению, обеспечиваемому поставщиком услуг подключения. С помощью ExpressRoute вы можете устанавливать подключения к различным облачным службам Майкрософт, таким как Microsoft Azure и Microsoft 365. Это может быть подключение типа "любой к любому" (IP VPN), подключение Ethernet типа "точка-точка" или виртуальное кросс-подключение через поставщика услуг подключения на совместно используемом сервере. Поскольку соединения ExpressRoute не проходят через общедоступный Интернет, этот подход позволяет соединениям ExpressRoute обеспечивать большую надежность, более высокую скорость, постоянные задержки и более высокую безопасность.

Ключевые преимущества ExpressRoute:

* Связь уровня 3 между вашей локальной сетью и Microsoft Cloud через поставщика подключения
* Связь может осуществляться по сети "любой к любому" (IPVPN), по Ethernet-соединению "точка — точка" или через виртуальное кросс-соединение через обмен Ethernet
* Возможность подключения к облачным сервисам Майкрософт во всех регионах геополитического региона
* Глобальное подключение к службам Майкрософт во всех регионах с помощью надстройки ExpressRoute премиум
* Встроенная избыточность в каждом расположении пиринга для более высокой надежности

Детали модуля Распределение нагрузки трафика, отличного от HTTP(S), в Azure

Я узнал о различных вариантах подсистемы балансировки нагрузки в Azure, а также о том, как выбрать и реализовать подходящее решение Azure для трафика, отличного от HTTP(S).

Существуют разные балансировки нагрузки для Microsoft Azure:

* Azure Load Balancer — высокопроизводительная служба балансировки нагрузки уровня 4 с крайне низкой задержкой (как для входящего, так и для исходящего трафика) для всех протоколов UDP и TCP. Она разработана для обработки миллионов запросов в секунду, обеспечивая высокую доступность решения. Служба Azure Load Balancer является избыточной между зонами, обеспечивая высокий уровень доступности для разных зон доступности.
* Диспетчер трафика — подсистема балансировки нагрузки трафика на основе DNS, которая позволяет оптимально распределять трафик между службами в глобальных регионах Azure, обеспечивая высокий уровень доступности и скорость отклика. Так как Диспетчер трафика является службой балансировки нагрузки на основе DNS, балансировка нагрузки выполняется только на уровне домена. По этой причине эта служба не может выполнять отработку отказа так же быстро, как Front Door. Это связано с распространенными проблемами с кэшированием DNS и системами, не поддерживающими значения срока жизни DNS.
* Шлюз приложений Azure предоставляет контроллер доставки приложений (ADC) в качестве службы, предлагая различные возможности балансировки нагрузки уровня 7. Используйте его, чтобы оптимизировать производительность веб-фермы за счет разгрузки операций завершения SSL-запросов, требующих значительных ресурсов ЦП, на шлюз.
* Azure Front Door — это сеть доставки приложений, которая предоставляет службу глобальной балансировки нагрузки и ускорения сайтов для веб-приложений. Она предоставляет для приложения возможности балансировки нагрузки уровня 7, например разгрузку SSL, маршрутизацию на основе путей, быструю отработку отказа и кэширование, чтобы повысить производительность и обеспечить высокий уровень доступности приложений.

Службы балансировки подразделяются на глобальные и локальные.

Детали модуля Распределение нагрузки трафика HTTP(S) в Azure

Я узнал, как разрабатывать решения подсистемы балансировки нагрузки для трафика HTTP(S) и как реализовать Шлюз приложений Azure и Azure Front Door.

Шлюз приложений Azure — это подсистема балансировки нагрузки веб-трафика, предназначенная для управления трафиком веб-приложений. Традиционные подсистемы балансировки нагрузки работают на транспортном уровне (уровень 4 OSI — протоколы TCP и UDP) и маршрутизируют трафик к IP-адресу и порту назначения в зависимости от исходного IP-адреса и порта.

Этот тип маршрутизации называется балансировкой нагрузки на уровне приложения (уровень 7 OSI). Шлюз приложений Azure может выполнять маршрутизацию на основе URL-адреса и многие другие действия.

Шлюз приложений содержит ряд компонентов, которые объединяются для маршрутизации запросов к пулу веб-серверов и проверки работоспособности этих веб-серверов.

Маршрутизация обычно происходит на основе пути.

Детали модуля Проектирование и реализация защиты сети

Я узнал, как проектировать и реализовывать такие решения безопасности сети, как Защита от атак DDoS Azure, группы безопасности сети, Брандмауэр Azure и Брандмауэр веб-приложений.

Для Microsoft Azure обеспечение безопасности и предоставление возможности защищать различные ресурсы, например микрослужбы, виртуальные машины, данные, имеет первостепенное значение. Для этого в Microsoft Azure используется распределенный виртуальный брандмауэр.

Виртуальная сеть в Microsoft Azure изолирована от других сетей и обменивается данными с помощью частных IP-адресов.

Реализация Тестирования безопасности Azure:

* Спланируйте реализацию Тестирования безопасности Azure, изучив документацию по корпоративным элементам управления и базовым показателям для служб, чтобы составить план платформы управления и ее соответствие рекомендациям, относящимся к CIS (элементам управления версии 7.1) и NIST (SP 800-53).
* Следите за соблюдением состояния Тестирования безопасности Azure (и других наборов элементов управления) с помощью панели мониторинга соответствия нормативным требованиям в Центре безопасности Azure.
* Установите проверки для автоматизации безопасных конфигураций и обеспечения соответствия требованиям Тестирования безопасности Azure (и другим требованиям в вашей организации) с помощью Azure Blueprints и Политики Azure.

Детали модуля Проектирование и реализация частного доступа к службам Azure

Я узнал, как спроектировать и реализовать частный доступ к службам Azure с помощью Приватного канала Azure и конечных точек службы для виртуальной сети.

Приватный канал Azure обеспечивает доступ к службам Azure PaaS (например, к службе хранилища Azure и Базе данных SQL), а также размещенным в Azure службам, которые принадлежат клиенту или партнеру, через частную конечную точку виртуальной сети.

Наличие общедоступной конечной точки означает, что ресурсу назначается общедоступный IP-адрес. Таким образом, несмотря на то что виртуальная сеть и база данных SQL Azure находятся в облаке Azure, подключение между ними выполняется через Интернет.

Проблема заключается в том, что база данных SQL Azure доступна через Интернет посредством общедоступного IP-адреса. Эта доступность создает несколько угроз безопасности. Те же угрозы безопасности существуют при доступе к ресурсу Azure через общедоступный IP-адрес из следующих расположений:

* одноранговая виртуальная сеть Azure;
* локальная сеть, которая подключается к Azure с помощью ExpressRoute и пиринга Майкрософт;
* виртуальная сеть Azure клиента, которая подключается к службе Azure вашей организации.

Детали модуля Проектирование и реализация сетевого мониторинга

Я узнал, как проектировать и реализовывать решения для мониторинга сети, такие как Azure Monitor и наблюдатель за сетями.

Azure Monitor помогает максимизировать доступность и производительность приложений и служб. Эта служба обеспечивает комплексное решение для сбора, анализа и использования телеметрии из облака и локальных сред. Эта информация поможет вам понять, насколько производительны приложения, а также заранее определить имеющиеся в них проблемы и ресурсы, от которых они зависят.

Несколько примеров того, что можно сделать с помощью Azure Monitor:

* Выявлять и диагностировать проблемы и зависимости между приложениями с помощью Application Insights.
* Сопоставлять проблемы инфраструктуры с аналитикой виртуальных машин и аналитикой контейнеров.
* Анализировать данные мониторинга с помощью Log Analytics для устранения неполадок и выполнения глубокой диагностики.
* Поддерживать работу при масштабировании с помощью интеллектуальных оповещений и автоматизированных действий.
* Создавать визуализации с помощью информационных панелей и книг Azure.
* Собирать данные от отслеживаемых ресурсов с помощью метрик Azure Monitor.