Бауманский учебный центр «Специалист»

Программа курса Введение в сетевую безопасность на базе продуктов UserGate

Код курса: **ЮЗЕРГ1**

Тема	Ак. часов
Модуль 1. Архитектура компьютерных сетей и модель OSI **Принципы передачи данных между узлами сети:** • архитектура сети; • модель OSI; • стек TCP/IP; • инкапсуляция и декапсуляция. **Функции канального уровня модели OSI:** • стандарт Ethernet; • MAC-адрес; • коммутаторы канального уровня (L2-коммутаторы); • принципы работы коммутатора. **Функции сетевого уровня модели OSI:** • протокол IP; • бесклассовая IP-адресация; • ICMP. **Знакомство с интерфейсом межсетевого экрана UserGate:** • подключение к межсетевому экрану UserGate; • графический интерфейс (GUI); • интерфейс командной строки (CLI). **Процесс передачи данных по сети:** • протокол ARP; • шлюз по умолчанию. **Функции транспортного уровня модели OSI:** • протоколы TCP и UDP. **Протоколы прикладного уровня модели OSI:** • DHCP; • DNS; • SSH; • HTTP. **Лабораторная работа 1.1. «Базовая настройка стенда»:** • адресация протокола IPv4; • знакомство со стендом; • знакомство с NGFW UserGate; • знакомство с маршрутизатором VyOS. **Лабораторная работа 1.2. «Механизмы передачи данных в локальной сети»:** • анализ работы ARP; • сетевые сервисы DNS и DHCP; • знакомство со структурой пакета HTTP.	**8**

Модуль 2. Основы IP-маршрутизации и протокол OSPF **Построение таблицы маршрутизации** • таблица маршрутизации; • выбор маршрута в таблице. **Статическая маршрутизация** • статические маршруты на межсетевом экране UserGate; • маршрут по умолчанию. **Протокол OSPF** • динамическая маршрутизация; • OSPF; • настройка OSPF на МЭ UserGate. **Лабораторная работа 2.1. «Основы IP-маршрутизации»** • таблица маршрутизации; • статическая маршрутизация. **Лабораторная работа 2.2. «Внедрение протокола OSPF»** • базовая настройка OSPF с одной областью; • дополнительные настройки OSPF.	**8**
Модуль 3. Угрозы и защита сетевой ИТ-инфраструктуры **Комплексные атаки на ИТ-инфраструктуру** • ключевые термины в области ИБ; • методология целенаправленной атаки (Advanced Persistent Threat, APT); • технические средства защиты. **Атаки на сетевую инфраструктуру** • распространенные техники; • манипуляция сетевыми протоколами. **Предотвращение угроз сетевой безопасности** • контроль доступа; • протоколы AAA; • IEEE 802.1X; • защита сетевых устройств.	**8**

Модуль 4. NGFW UserGate: функции и политики безопасности **Функции межсетевого экрана** • принципы фильтрации трафика: проблемы и решения; • Next-Generation Firewall (NGFW). **Обзор NGFW UserGate** • экосистема продуктов UserGate SUMMA; • межсетевой экран нового поколения; • варианты поставки. **Способы внедрения NGFW UserGate** • способы внедрения одного узла; • внедрение нескольких узлов. **Зоны и библиотеки элементов** • зоны; • библиотеки элементов. **Политики сети** • правила межсетевого экрана; • идентификация приложений; • система обнаружения вторжений. **NAT** • способы трансляции адресов; • настройка правил SNAT. **Обзор политик безопасности** • компоненты политики безопасности. **Обзор идентификации пользователей** • способы идентификации. **Лабораторная работа 3.1. «Инспекция трафика с помощью NGFW UserGate»** • правила межсетевого экрана; • система обнаружения вторжений; • трансляция адресов; • дополнительные настройки безопасности. **Лабораторная работа 3.2. «Политики безопасности на NGFW UserGate»** • инспекция SSL; • фильтрация контента.	**8**

Модуль 5. Технологии VPN и защищённые подключения на NGFW UserGate **Введение в криптографические алгоритмы** • криптографические алгоритмы; • инфраструктура открытых ключей. **Технологии VPN** • типы VPN; • стек протоколов IPsec; • L2TP/1Psec; • GRE/IPsec; • SSL/TLS. **Настройка VPN сайт-сайт на NGFW UserGate** • алгоритм настройки сервера; • алгоритм настройки клиента. **Лабораторная работа 4.1. «Безопасность удаленных подключений»** • настройка L2TP/1Psec VPN-туннеля сайт-сайт; • настройка L2TP/1Psec VPN-туннеля удаленного доступа.	**8**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru