Бауманский учебный центр «Специалист»

Программа курса SCOR: Внедрение и эксплуатация ключевых технологий Cisco Security Core Technologies

Код курса: **СКОР**

Тема	Ак. часов
Модуль 1. Концепции сетевой безопасности* • Обзор принципов информационной безопасности • Управление рисками • Оценка уязвимостей • Анализ CVSS	
Модуль 2. Распространенные атаки TCP/IP * • Уязвимости TCP/IP • Уязвимости сервисов IP • Уязвимости ICMP • Уязвимости TCP • Уязвимости UDP • Векторы атак • Разведывательные атаки • Атаки на протоколы доступа • Атаки типа "человек по середине" • Denial of Service и Distributed Denial of Service • Атаки отражения и усиления • Атаки типа Spoofing • Атаки на DHCP	
Модуль 3. Распространенные атаки на сетевые приложения * • Атаки на пароли • Атаки на DNS • DNS-туннелирование • Атаки на веб-сервисы • HTTP 302 Cushioning • Command Injections • SQL Injections • Cross-Site Scripting и Request Forgery • Атаки на почтовый трафик	
Модуль 4. Распространенные атаки на конечные устройства * • Переполнение буфера • Вредоносное ПО • Разведка • Получение доступа и контроля • Получение доступа с использованием социальной инженерии • Получение доступа с использованием атак на веб-трафик • Exploit Kits и Rootkits • Повышение привилегий • Фаза после внедрения • Angler Exploit Kit	

Модуль 5. Технологии сетевой безопасности • Стратегия Defense-in-Depth • Сегментация сети и обзор механизмов виртуализации • Обзор Stateful Firewall • Обзор Security Intelligence • Стандартизация информации об угрозах • Обзор сетевой защиты от вредоносного ПО • Обзор систем предотвращения вторжений • Обзор МСЭ нового поколения • Обзор Email Content Security • Обзор Web Content Security • Обзор Threat Analytic Systems • Обзор механизмов безопасности DNS • Аутентификация, авторизация, учет • Управление пользовательскими учетными данными и доступом • Обзор технологий Virtual Private Network • Обзор устройств сетевой безопасности	**5**
Модуль 6. Внедрение МСЭ Cisco ASA • Режимы работы Cisco ASA • Уровни безопасности интерфейсов Cisco ASA • Объекты и группы объектов в Cisco ASA • Network Address Translation • ACL на интерфейсах Cisco ASA • Глобальные ACL на Cisco ASA • Политики инспектирования Cisco ASA • Отказоустойчивые топологии Cisco ASA	**5**
Модуль 7. Внедрение МСЭ нового поколения Cisco Firepower • Режимы работы Cisco Firepower NGFW • Процесс обработки пакетов и политики • Объекты • NAT • Политики пред-фильтрации • Политики контроля доступа • Cisco Firepower NGFW Security Intelligence • Политики Discovery • Политики IPS • Детектирование вредоносного ПО и файловые политики	**5**
Модуль 8. Внедрение Email Content Security • Обзор Cisco Email Content Security • Обзор SMTP • Обзор Email Pipeline • Public и Private Listeners • Host Access Table • Recipient Access Table • Обзор политик фильтрации почтового трафика • Защита от Spam и Graymail • Защита от вирусов и вредоносного ПО • Фильтры Outbreak • Фильтрация контента • Защита от утечки данных • Шифрование почтового трафика	**5**

Модуль 9. Внедрение Web Content Security • Обзор решения Cisco WSA • Особенности внедрения • Сетевая аутентификация пользователей • Расшифровка трафика HTTPS • Политики доступа и идентификационные политики • Настройки Acceptable Use Controls • Защита от вредоносного ПО	**5**
Модуль 10. Внедрение Cisco Umbrella * • Архитектура Cisco Umbrella • Внедрение Cisco Umbrella • Cisco Umbrella Roaming Client • Управление Cisco Umbrella • Исследование функций Cisco Umbrella	
Модуль 11. Технологии VPN и криптографические алгоритмы • Знакомство с VPN • Типы VPN • Secure Communication and Cryptographic Services • Типы ключей в криптографии • Инфраструктура публичных ключей	**5**
Модуль 12. Cisco Secure Site-to-Site VPN • Технологии Site-to-Site VPN • Обзор IPsec VPN • IPsec Static Crypto Maps • IPsec Static Virtual Tunnel Interface • Dynamic Multipoint VPN • Cisco IOS FlexVPN	**5**
Модуль 13. Cisco IOS VTI-Based Point-to-Point • Cisco IOS VTIs • Настройка VTI Point-to-Point IPsec IKEv2 VPN	**5**
Модуль 14. Point-to-Point IPsec VPNs на Cisco ASA и Cisco Firepower NGFW • Point-to-Point VPN на Cisco ASA и Cisco Firepower NGFW • Настройка Cisco ASA Point-to-Point VPN • Настройка Cisco Firepower NGFW Point-to-Point VPN	**4**
Модуль 15. Cisco Secure Remote Access VPN • Remote Access VPN • Компоненты и технологии • Обзор SSL	**4**
Модуль 16. Remote Access SSL VPN на Cisco ASA и Cisco Firepower NGFW • Профили подключения • Групповые политики • Настройки Cisco ASA Remote Access VPN • Настройки Cisco Firepower NGFW Remote Access VPN	**4**

Модуль 17. Контроль доступа в сетях Cisco • Безопасный доступ к сети • Сервисы AAA • Обзор возможностей платформы Cisco Identity Services Engine • Архитектура Cisco TrustSec	**4**
Модуль 18. Аутентификация по стандарту 802.1X • 802.1X и EAP • Методы EAP • Роль протокола RADIUS в системе 802.1X • RADIUS Change of Authorization	**4**
Модуль 19. Конфигурация аутентификации 802.1X • Настройки 802.1X на Cisco Catalyst Switch • Настройки 802.1X на Cisco WLC 802.1X • Настройки 802.1X на Cisco ISE 802.1X • Supplicant 802.1x • Cisco Central Web Authentication	**4**
Модуль 20. Технологии обеспечения безопасности конечный устройств * • Хостовые МСЭ • Хостовые антивирусы • Хостовые системы предотвращения вторжений • Белые и черные списки ресурсов на хостах • Защита от вредносного ПО • Обзор песочниц • Проверка файлов	
Модуль 21. Внедрение Cisco AMP for Endpoints * • Архитектура решения Cisco AMP for Endpoints • Cisco AMP for Endpoints Engines • Ретроспективная защита с использованием Cisco AMP • Построение траектории файлов с помощью Cisco AMP • Управление Cisco AMP for Endpoints	
Модуль 22. Защита сетевой инфраструктуры * • Плоскости работы сетевого устройства • Механизмы безопасности плоскости контроля • Механизмы безопасности плоскости управления • Телеметрия трафика • Защита плоскости передачи данных на канальном уровне • Защита плоскости передачи данных на сетевом уровне	
Модуль 23. Внедрение механизмов защиты плоскости контроля * • Infrastructure ACLs • Control Plane Policing • Control Plane Protection • Механизмы защиты протоколов маршрутизации	

Модуль 24. Внедрение механизмов защиты плоскости передачи данных на канальном уровне * • Обзор механизмов защиты плоскости передачи данных • Защита от атак на систему VLAN • Защита от атак на протокол STP • Port Security • Private VLANs • DHCP Snooping • ARP Inspection • Storm Control • Шифрование MACsec	
Модуль 25. Внедрение механизмов защиты плоскости передачи данных на сетевом уровне * • Infrastructure Antispoofing ACL • Unicast Reverse Path Forwarding • IP Source Guard	
Аудиторная нагрузка в классе с преподавателем	**64 ак.ч. + 64 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