Бауманский учебный центр «Специалист»

Программа курса Управление кибербезопасностью (CyberOps Associate)

Код курса: **СА-КИБ3**

Тема	Ак. часов
Модуль 1. Опасность (The Danger) • Лабораторная работа: Installing the Virtual Machines	**0.5**
Модуль 2. Борцы в борьбе с киберпреступлениями (Fighters in the War Against Cybercrime)	**0.5**
Модуль 3. Операционная система Windows (The Windows Operating System) • Лабораторная работа: Exploring Processes, Threads, Handles, and Windows Registry • Лабораторная работа: Create User Accounts • Лабораторная работа: Using Windows PowerShell • Лабораторная работа: Windows Task Manager • Лабораторная работа: Monitor and Manage System Resources in Windows	**3**
Модуль 4. Операционная система Linux (Linux Overview) • Лабораторная работа: Working with Text Files in the CLI • Лабораторная работа: Getting Familiar with the Linux Shell • Лабораторная работа: Linux Servers • Лабораторная работа: Locating Log Files • Лабораторная работа: Navigating the Linux Filesystem and Permission Settings	**4**
Модуль 5. Сетевые протоколы (Network Protocols) • Лабораторная работа: Tracing a Route • Лабораторная работа: Introduction to Wireshark	**1**
Модуль 6. Протоколы Ethernet и IP (Ethernet and Internet Protocol)	**1**
Модуль 7. Проверка связи (Connectivity Verification)	**1**
Модуль 8. Протокол ARP (Address Resolution Protocol) • Лабораторная работа: Using Wireshark to Examine Ethernet Frames	**1**
Модуль 9. Транспортный уровень (The Transport Layer) • Лабораторная работа: Using Wireshark to Observe the TCP 3-Way Handshake • Лабораторная работа: Exploring Nmap	**1**
Модуль 10. Сетевые сервисы (Network Services) • Лабораторная работа: Using Wireshark to Examine a UDP DNS Capture • Лабораторная работа: Using Wireshark to Examine TCP and UDP Captures • Лабораторная работа: Using Wireshark to Examine HTTP and HTTPS Traffic	**1**
Модуль 11. Устройства для обеспечения связи (Network Communication Devices)	**1**
Модуль 12. Устройства для обеспечения сетевой безопасности (Network Security Infrastructure)	**1**
Модуль 13. Атакующие и их инструменты (Attackers and Their Tools)	**1**
Модуль 14. Распространённые угрозы и атаки (Common Threats and Attacks)	**1**

Модуль 15. Мониторинг и утилиты для работы с сетью (Network Monitoring and Tools)	**1**
Модуль 16. Атаки на основные протоколы (Attacking the Foundation)	**1**
Модуль 17. Атаки на основные сервисы (Attacking What We Do) • Лабораторная работа: Exploring DNS Traffic • Лабораторная работа: Attacking a MySQL Database • Лабораторная работа: Reading Server Logs	**1**
Модуль 18. Подходы к обеспечению защиты (Understanding Defense)	**1**
Модуль 19. Контроль доступа (Access Control)	**1**
Модуль 20. Интеллектуальные средства борьбы с угрозами (Threat Intelligence)	**1**
Модуль 21. Криптография (Cryptography) • Лабораторная работа: Hashing Things Out • Лабораторная работа: Encrypting and Decrypting Data Using OpenSSL • Лабораторная работа: Encrypting and Decrypting Data Using a Hacker Tool • Лабораторная работа: Examining Telnet and SSH in Wireshark • Лабораторная работа: Certificate Authority Stores	**2**
Модуль 22. Защита конечных устройств (Endpoint Protection)	**1**
Модуль 23. Оценка уязвимостей конечных устройств (Endpoint Vulnerability Assessment)	**1**
Модуль 24. Технологии и протоколы (Technologies and Protocols)	**1**
Модуль 25. Данные, собранные системами обеспечения безопасности (Network Security Data)	**1**
Модуль 26. Оценка предупреждений (Evaluating Alerts) • Лабораторная работа: Snort and Firewall Rules	**1**
Модуль 27. Работа с данными, собранными системами обеспечения безопасности (Working with Network Security Data) • Лабораторная работа: Convert Data into a Universal Format • Лабораторная работа: Regular Expressions Tutorial • Лабораторная работа: Extract an Executable from a PCAP • Лабораторная работа: Interpret HTTP and DNS Data to Isolate Threat Actor • Лабораторная работа: Isolate Compromised Host Using 5-Tuple • Лабораторная работа: Investigate a Malware Exploit • Лабораторная работа: Investigating an Attack on a Windows Host	**4**
Модуль 28. Цифровая криминалистика, анализ и реагирование на инциденты (Digital Forensics and Incident Analysis and Response)	**1**
Аудиторная нагрузка в классе с преподавателем	**36 ак.ч. + 36 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