

Kypc Security+

Ориентирован на:

всех ІТ-специалистов, заинтересованных в получении минимального набора знаний и навыков по основам кибербезопасности

Предварительный уровень подготовки:

Сертификации CompTIA A+, Network+ и Server+ ИЛИ 2-летний опыт администрирования гетерогенной сети (Windows\Linux\Unix) ИЛИ эквивалентный набор знаний и навыков

Продолжительность и формат:

5-дневный семинар (80% времени лекции/20% практические занятия)

Методические материалы:

Учебное пособие с теоретической и практической частью на английском языке

Документ об окончании курса:

Свидетельство учебного центра

Сертификационные статусы и экзамены:

Сертификация CompTIA Security+, экзамен SY0-601



Для всех IT-специалистов мы предлагаем интенсивный курс, соответствующий требованиям American National Standards Institute к набору знаний и навыков по основам кибербезопасности. Курс готовит к сдаче экзамена на получение международного сертификационного статуса Security+ от лидирующего провайдера вендорнезависимых ITсертификаций Computing Technology Industry Association (CompTIA).

Программа курса:

Модуль I: Угрозы, атаки и уязвимости

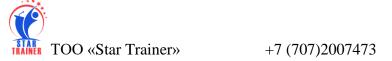
- Урок 1. Методы социальной инженерии
- Урок 2. Основы атак
- Урок 3. Атаки приложений
- Урок 4. Сетевые атаки
- Урок 5. Субъекты угроз, векторы и интеллект
- Урок 6. Слабые места
- Урок 7. Методы оценки безопасности
- Урок 8. Методы испытания на проникновение

Модуль II: Архитектура и проектирование

- Урок 9. Концепции корпоративной безопасности
- Урок 10. Виртуализация и облачные вычисления
- Урок 11. Безопасность разработки, развертывания и автоматизации приложений
- Урок 12. Проектирование аутентификации и авторизации
- Урок 13. Устойчивость к кибербезопасности
- Урок 14. Встраиваемые и специализированные системы Встраиваемые системы SCADA и **ICS**
- Урок 15. Контроль физической безопасности
- Урок 16. Криптографические концепции

Модуль III: Внедрение

- Урок 17. Защищенные протоколы
- Урок 18. Решения для обеспечения безопасности серверов и приложений
- Урок 19. Проектирование безопасной сети
- Урок 20. Параметры безопасности беспроводной сети
- Урок 21. Методы связи с защищенными мобильными решениями
- Урок 22. Решения для облачной кибербезопасности
- Урок 23. Управление идентификационными данными и учетными записями
- Урок 24. Аутентификация и авторизация



2

Урок 25. Инфраструктура открытых ключей

Модуль IV: Операции и реагирование на инциденты

- Урок 26. Организационная безопасность
- Урок 27. Реагирование на инциденты
- Урок 28. Расследование инцидента
- Урок 29. Смягчение последствий инцидентов
- Урок 30. Цифровая криминалистика

Модуль V: Управление, риски и соответствие нормативным требованиям

- Урок 31. Типы управления
- Урок 32. Правила, стандарты и основы
- Урок 33. Политики безопасности организации
- Урок 34. Управление рисками
- Урок 35. Конфиденциальные данные и конфиденциальности

Соответствие уроков курса и доменов сертификации Security+:

Урок 1, 2, 3, 4, 5, 6, 7 и 8: Treats, Attacks and Vulnerabilities

Урок 9, 10, 11, 12, 13, 14, 15 и 16: Architecture and Design

Урок 17, 18, 19, 20, 21, 22, 23, 24 и 25: Implementation

Урок 26, 27, 28, 29 и 30: Operations and Incident Response

Урок 31, 32, 33, 34 и 35: Governance, Risk, and Compliance

В качестве практики в семинар включены оценочный, промежуточные и итоговый тесты общим количеством в 270 вопросов формата и уровня сложности как на экзамене.

Требования к оборудованию учебного класса:

На каждого студента выделенный ПЭВМ с доступом в сеть Интернет, установленной ОС Windows и пакетом программ Office

