Cybersecurity Specialist	
Блок 1. Оборонна кібербезпека	
Модуль	**Зміст**
Модуль 1. --- Вступ до оборонної кібербезпеки	Вступ до оборонної кібербезпеки Ситуаційна обізнаність
Модуль 2. --- Операційний центр безпеки (SOC)	Що таке SOC? Ролі та відповідальності
Модуль 3. --- Адміністрування систем кібербезпеки	Основи Windows Основи Linux
Модуль 4. --- Безпечне адміністрування мережі	Огляд моделі OSI Роль протоколів на кожному рівні моделі OSI Основи IP-адресації (IPv4 та IPv6) Основи маршрутизації та робота маршрутизаторів
Модуль 5. --- Архітектура кібербезпеки	Екосистема систем кібербезпеки Референтні архітектури кібербезпеки
Модуль 6. --- Реагування на інциденти (IR)	Огляд процесу
Модуль 7. --- Криптографія	Криптологія Криптоаналіз

Модуль 8. --- Обмін інформацією про кіберзагрози та збагачення систем кібербезпеки	Індикатори кіберзагроз Збагачення систем кібербезпеки
Модуль 9. --- Кібербезпека в хмарній інфраструктурі	Адміністрування хмарної інфраструктури Інструменти кібербезпеки у відомих хмарних платформах (на прикладі AWS)
Модуль 10. --- Проведення співбесіди для працевлаштування	Навички ефективного спілкування на співбесіді Техніка успішної співбесіди
Блок 2. Наступальна кібербезпека	
Модуль 1. --- Вступ до наступальної кібербезпеки	Вступ до наступальної кібербезпеки Вступ до етичного хакінгу
Модуль 2. --- Соціальна інженерія	Маніпулювання та захист від соціальної інженерії Тестування на проникнення в фізичні приміщення
Модуль 3. --- Розвідка з відкритих джерел	Операційна безпека (OpSec) Інструменти для розвідки та енумерації
Модуль 4. --- Тестування на проникнення, частина 1	Підслуховування трафіку, атаки посередника та перехоплення сесії Злам мобільних пристрої

Модуль 5. --- Тестування на проникнення, частина 2	Злам SQL-серверів Злам веб-серверів
Модуль 6. --- Тестування на проникнення, частина 3	Підготовка звіту з результатами тестування на проникнення Bug bounty
Модуль 7. --- Штучний інтелект	Використання ШІ в наступальній кібербезпеці Виккористання ШІ захисниками
Модуль 8. --- Моделювання поведінки ймовірних зловмисників	Оцінка загроз перед проведенням тестування на проникнення Збір інформації про вибрані загрози та інструменти для моделювання поведінки
Модуль 9. --- Ризики мобільних пристроїв та IoT	Загрози та захист мобільних пристроїв Безпека IoT-пристроїв
Модуль 10. --- Проведення співбесіди для працевлаштування	Навички ефективного спілкування на співбесіді Техніка успішної співбесіди
Блок 3. Управління ризиками кібербезпеки (в запису)	
Модуль 1. --- Вступ до управління ризиками кібербезпеки	Що таке врядування, ризик та відповідність (GRC)

Модуль 2. --- Основні концепції кібербезпеки	Основні концепції кібербезпеки
Модуль 3. --- Роль держави в галузі кібербезпеки	Законодавство та стандарти Правоохоронна діяльність
Модуль 4. --- Основні процеси	Управління доступом в загальному випадку Управління змінами в загальному випадку
Модуль 5. --- Системи управління	Системи управління в загальному випадку ISO 27001
Модуль 6. --- Управління відповідністю	Забезпечення відповідності Відповідність українському та європейському законодавству
Модуль 7. --- Загрози та вразливості	Управління вразливостями Розвідка кіберзагроз в контексті управління вразливостями
Модуль 8. --- Концепції управління ідентифікацією та доступом (IAM)	Аутентифікація та авторизація Моделі доступу
Модуль 9. --- Технології IAM	Мультифакторна аутентифікація Автоматизація доступу на основі різних моделей доступу

Модуль 10. --- Проведення співбесіди для працевлаштування	Навички ефективного спілкування на співбесіді Техніка успішної співбесіди