

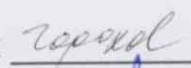



## СЕРТИФІКАТНА ПРОГРАМА

### « ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ »

	Дисципліна	Семестр	год./тиж.	Форма контролю	Кредити ЄКТС
1	Методи та засоби збору чутливої інформації	4д	4	залік	2
2	Інформаційна безпека веб-застосунків	5	3	залік	4
3	Низькорівневі вразливості програмного забезпечення	6	3	залік	4
4	Інформаційна безпека мереж	6д	3	залік	2
5	Інформаційна безпека цільових систем	7	2	залік	3


Залікових балів на 15 кредитів ЄКТС

Завідувач кафедри інформатики  С.С. Гороховський

Декан  А.М. Глибовець

Ухвалено радою ФІ протокол № 13 від «25» листопада 2020 р.

Голова ради ФІ  А.М. Глибовець

Погоджено: навчальний відділ  О.О. Корольова

## **Бакалаврська сертифікатна програма**

### **«Основи інформаційної безпеки»**

#### **Рівень кваліфікації**

Бакалавр (перший цикл вищої освіти).

#### **Спеціальні положення про визнання попереднього навчання (формального, неформального, неофіційного)**

Немає.

#### **Профіль програми**

Дана сертифікатна програма спрямована на вивчення засобів та підходів, що використовуються при перевірці програмних рішень та цільових систем на предмет виявлення вразливостей. Представлено широкий спектр підходів до виявлення й подальшої експлуатації вразливостей. Незважаючи на різноманітність цільових систем, в даній галузі існують різні підходи до тестування та виявлення вразливостей програмного забезпечення, а також для перевірки вразливостей цільових систем. Слухачі даної сертифікатної програми познайомляться з збором інформації, пошуком та виявленням вразливостей як веб-застосунків, так і прикладних застосунків, виявлення сторонніх рішень у цільовій системі, перевірки мережі на вразливості.

Сертифікатна програма поєднує теоретичні знання з великою кількістю практичних робіт які дозволять студентам отримати навички пошуку так виявлення векторів експлуатації вразливостей як в програмних рішеннях, так і в цільових системах.

#### **Методи та засоби збору чутливої інформації**

- OSINT
- Робота з закритими джерелами інформації
- Робота з людським фактором

#### **Інформаційна безпека веб-застосунків**

- Збір інформації про веб-застосунок та цільову систему(у контексті веб-застосунків)
- Проблеми неправильного налаштування середовища
- Проблеми недостатньою фільтрацією даних
- Вразливості бізнес логіки
- Обхід систем запобігання атак на веб-застосунки
- Закріплення доступу до цільових систем
- Використання програмного забезпечення
- Статичний аналіз вихідних кодів

### **Низькорівневі вразливості програмного забезпечення**

- Робота з пам'яттю
- Виявлення вразливостей за допомогою фазінгу
- Зворотна розробка програмних рішень
- Переповнення буферу та стеку
- Робота з корисним навантаженням та розробка автоматизованих утиліт для експлуатації вразливостей
- Шкідливі програмні засоби

### **Інформаційна безпека мереж**

- Збір та аналіз мережної інформації
- Робота з бездротовими мережами
- Робота з відкритими мережевими ресурсами
- Перехоплення мережових даних
- Атаки типу «людина посередині»
- Розшифрування даних та хеш-сум паролів
- Атаки типу «відмова у обслуговуванні», та її розподілена варіація

### **Інформаційна безпека цільових систем**

- Корпоративні правила та протоколи безпеки для роботи у компаніях
- Розмежування прав та доступів у мережі, системи єдиного входу
- Безпечне налаштування середовища
- Налаштування систем резервного копіювання
- Системи запобігання вторжень
- Системи виявлення вторгнень
- Системи спостереження та журналювання дій
- Комп'ютерна криміналістика вторгнень