Міністерство освіти і науки України
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ

Гарант ОНП «Кібербезпека»
_____ М.О. Колісник
(підпис) (ініціали та прізвище)
«31» 08 2020 р.

СИЛАБУС ВИБІРКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи кіберзахисту розподілених систем
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код і найменування спеціальності)

Освітня програма: "Кібербезпека"
(найменування освітньої програми)

Форма навчання: денна

Рівень вищої освіти: третій (освітньо-науковий)

Харків 2020 рік

Силабус Методи кіберзахисту розподілених систем
(назва дисципліни)

для аспірантів за спеціальністю 125 "Кібербезпека"
(код та найменування спеціальності)

Освітньо-наукова програма "Кібербезпека"
(найменування програми)

«26» 08 2020 р., – 8 с.

Розробник: Тецький А. Г., асистент
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Розробник: Узун Д. Д., доцент, к.т.н., доцент
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус розглянуто на засіданні кафедри
Комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол №1 від «27» 08 2020 р.

Завідувач кафедри д.т.н., професор В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

1. Опис навчальної дисципліни

Галузь знань – 12 "Інформаційні технології".
Спеціальність – 125 "Кібербезпека".
Освітня програма – "Кібербезпека".
Рівень вищої освіти – третій (освітньо-науковий).
Форма навчання – денна.
Семестр, в якому викладається дисципліна – 4-й.
Дисципліна вибіркова.
Загальна кількість годин за навчальним планом - _165_ **годин/** _5,5_ **кредитів ЄКТС.**
Види занять – лекції, практичні заняття.
Вид контролю – іспит.

2. Мета та завдання навчальної дисципліни

Мета: дати знання про сучасні методи наукового дослідження кіберзахисту розподілених інформаційних систем для забезпечення і дослідження гарантоздатної обробки, передачі та зберігання інформації.

Завдання: вивчення і дослідження основних методів і моделей кіберзахисту інформації в гарантоздатних розподілених інформаційних системах.

Компетентності, які набуваються:
Здатність до пошуку, оброблення та аналізу інформації з різних джерел
Здатність працювати в міжнародному контексті.
Здатність застосовувати сучасні інформаційні технології, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності.
Здатність здійснювати науково-педагогічну діяльність у вищій освіті.
Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру в сфері кібербезпеки.
Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проекти в кібербезпеці та дотичні до неї міждисциплінарні проекти, лідерство під час їх реалізації.

Очікувані результати навчання:
Планувати і виконувати експериментальні та/або теоретичні дослідження з кібербезпеки та дотичних міждисциплінарних напрямів з використанням сучасних інструментів, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу сучасних знань щодо досліджуваної проблеми.

Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.

Здійснювати пошук та критичний аналіз інформації, концептуалізацію та реалізацію наукових проектів з кібербезпеки.

Знати, розуміти та вміти застосовувати методи та засоби створення інформаційних технологій та програмного забезпечення розподілених систем, Інтернету речей, хмарних обчислень, систем штучного інтелекту, віртуальної реальності у різних предметних областях, в тому числі в аерокосмічній галузі.

Пререквізити: матеріал дисципліни базується на знаннях, отриманих під час вивчення дисциплін "Обробка та аналіз результатів наукових досліджень з використанням ІТ".

Постреквізити: матеріал дисципліни є підґрунтям щодо написання дисертаційної роботи.

3. Програма навчальної дисципліни

Модуль 1.

Змістовний модуль 1. Огляд сучасних проблем кібербезпеки веб-застосунків.

Тема 1. Підготовка тестового оточення. Встановлення Damn Vulnerable Web Application.

Встановлення на локальній машині платформи з вразливостями для наукового дослідження. Закріплення навичок роботи в Linux-подібних системах. Отримання навичок встановлення і налаштування веб-сервера для подальшого встановлення на нього вразливого застосунка.

Кількість годин на тему – 16, з них лекції – 2, практичні заняття – 2, самостійна робота – 12.

Тема 2. Аналіз трафіку комп'ютерних мереж і наукове дослідження сценарію атаки типу Man-in-the-Middle.

Отримання навичок роботи з аналізатором трафіку Wireshark і платформою Burpsuite, знайомство з атакою Man-in-the-Middle. Знайомство зі структурою мережевих пакетів. Отримання навичок роботи в сніффером на прикладі Wireshark і Burpsuite. Аналіз сценаріїв MitM-атак веб-застосунку. Розробка методів захисту веб-застосунку від даного виду атак.

Кількість годин на тему – 16, з них лекції – 2, практичні заняття – 2, самостійна робота – 12.

Тема 3. SQL-ін'єкції. Принципи, пошук і експлуатація SQL-ін'єкцій. Методи ін'єкцій та їх наслідки.

Атаки з порушенням логіки запитів до бази даних. Робота з інструментальним засобом для пошуку і експлуатації ін'єкцій. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти sqlmap для експлуатації SQL-ін'єкцій. Порівняльний аналіз та наукове дослідження методів ін'єкцій при різній складності експлуатації вразливостей в DVWA.

Кількість годин на тему – 22, з них лекції – 4, практичні заняття – 2, самостійна робота – 16.

Тема 4. Робота з XSS-атаками. Особливості атак та їх наслідки.

Сценарії здійснення атак та інструменти атак. Освоєння природи походження і принципів експлуатації вразливості в браузері. Отримання навичок використання утиліти xsser для пошуку вразливостей. Можливості XSS-атак. Розроблення заходів щодо захисту веб-застосунка від XSS-атак.

Кількість годин на тему – 24, з них лекції – 4, практичні заняття – 4, самостійна робота – 16.

Модульний контроль – 1 година.

Змістовний модуль 2. Аналіз проблем кібербезпеки мереж та системного програмного забезпечення.

Тема 5. Робота з шеллом в Metasploit. Наукове дослідження можливостей виконання довільних команд в атакованій системі.

Отримання навичок роботи в фреймворку на прикладі модуля управління шеллом. Отримання навичок використання модулів фреймворка Metasploit. Отримання навичок управління атакованим сервером. Можливі наслідки експлуатації шелл. Розроблення заходів щодо захисту веб-застосунка від завантаження шелл.

Кількість годин на тему – 26, з них лекції – 4, практичні заняття – 4, самостійна робота – 18.

Тема 6. Основи сканування IP-мереж.

Знайомство з призначенням і функціоналом утиліти nmap в ОС Kali Linux, знайомство з основними відкритими базами даних вразливостей. Отримання навичок використання утиліти nmap. Отримання навичок пошуку інформації у відкритих базах вразливостей. Наукове дослідження методів і засобів виявлення сканування. Розроблення заходів щодо захисту мережі від сканування.

Кількість годин на тему – 26, з них лекції – 4, практичні заняття – 4, самостійна робота – 18.

Тема 7. Забезпечення безпеки багатокомпонентного веб-застосунка.

Аналіз можливих проблем безпеки веб-застосунка на етапі проєктування. Список вимог, які повинні бути перевірені перед здачею проєкту замовнику. Методи і засоби захисту від поширених атак. Наукове дослідження методів Web Application Firewall для виявлення потенційно небезпечного трафіку.

Кількість годин на тему – 33, з них лекції – 4, практичні заняття – 4, самостійна робота – 25

Модульний контроль – 1 година.

4. Індивідуальні завдання

Не передбачено.

5. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота аспірантів за матеріалами, опублікованими кафедрою.

6. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

7. Критерії оцінювання та розподіл балів, які отримують аспіранти

7.1. Розподіл балів, які отримують аспіранти (кількісні критерії оцінювання)

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист практичних робіт	0...6	4	0...24
Модульний контроль	0…25	1	0…25
Змістовний модуль 2			
Робота на лекціях	0…0,5	8	0…4
Виконання і захист практичних робіт	0...6	3	0...18
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови аспіранта від балів поточного тестування. Під час складання семестрового іспиту аспірант має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість балів за кожне із запитань складає 33 бали.

7.2. Якісні критерії оцінювання

Необхідний обсяг знань для одержання позитивної оцінки

1. Знати особливості функціонування ОС Linux
2. Знати основні команди для роботи в ОС Linux
3. Знати принципи роботи серверного програмного забезпечення під керуванням ОС Linux

Необхідний обсяг умінь для одержання позитивної оцінки

1. Уміти працювати з файловою системою в ОС Linux
2. Уміти встановлювати програмне забезпечення в ОС Linux
3. Уміти розробляти скрипти на мові shell
4. Уміти працювати з інструментальними засобами пошуку проблем безпеки в ОС Linux

7.3 Критерії оцінювання роботи аспіранта протягом семестру

Задовільно (60-74). Показати мінімум знань та умінь. Захистити не менше 75% від усіх завдань практичних занять.

Добре (75-89). Твердо знати мінімум, захистити не менше 90% завдань практичних занять.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати.

Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

8. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки.

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://moodle.csn.khai.edu

9. Рекомендована література

Базова

1. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. – 115 p.
2. Ron Lepofsky. The Manager's Guide to Web Application Security: A Concise Guide to the Weaker Side of the Web / Apress, 2014. – 232 p.
3. David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni. Metasploit. – 2011. – 328 p.

4. А. Г. Тецький, О. О. Ілляшенко, Д. Д. Узун. Методи та засоби тестування на проникнення веб-додатків і мереж. Практикум / під ред. В.С. Харченка – Міністерство освіти і науки України, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ». 2017. – 77 с.

Допоміжна

1. William Shotts. The Linux Command Line, 2nd Edition: A Complete Introduction. – No Starch Press, 2019. – 504 p.

OccupyTheWeb. Linux Basics for Hackers: Getting Started with Networking, Scripting, and Security in Kali. – No Starch Press, 2018. – 504 p.

10. Інформаційні ресурси

1. https://www.kali.org/
2. https://nvd.nist.gov/
3. https://owasp.org/
4. http://csn.khai.edu