СИЛАБУС

Назва дисципліни: Мережеві технології та безпека: кібербезпека

Мета дисципліни: забезпечити теоретичну та практичну підготовку щодо мережевої безпеки, а саме – ознайомлення з теоретичними та практичними основами мережевої та веб-безпеки.

Основні **компетентності**, що формуються:

ІК-1. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування певних теорій та методів і має комплексний характер.

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК11. Здатність приймати обґрунтовані рішення.

ЗК13. Здатність діяти на основі етичних міркувань.

СК7. Здатність застосовувати теоретичні та практичні основи методології та технології моделювання для дослідження характеристик і поведінки складних об'єктів і систем, проводити обчислювальні експерименти з обробкою й аналізом результатів.

Мова викладання	**Семестр**	**Кредити ECTS / Тип дисципліни (обов'язкова, вибіркова)**	**Викладач**	**Навчальне навантаження**
Укр.	4	3 / обов'язкова	Бабкін В.В., доктор філософії, викладач	90 год. (14 год. лекцій, 28 год. лабораторних занять, 9 год. інд. роботи, 39 год. самостійної роботи)

Результати навчання По закінченню вивчення дисципліни здобувачі будуть здатні	**Методи викладання, навчання**	**Форми оцінювання (поточний та підсумковий контроль)**
РН-1. застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук	Лекція, семінар-діалог, розбір/ аналіз ситуаційних задач	Участь в семінарі, відповіді на запитання, вирішення ситуаційних задач
РН-13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.	Лекція, семінар-діалог, розбір практичних case-study, проблемно-пошуковий метод з використанням мережі Інтернет	Усні відповіді на запитання, вирішення/ пояснення практичних case-study
РН16. Розуміти концепцію інформаційної безпеки, принципи безпечного	Проблемна лекція, вирішення практичних case-study, проблемно-пошуковий метод з використанням мережі Інтернет, самостійна робота	Усні відповіді на запитання, вирішення/ пояснення практичних завдань,

проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.		оцінювання практичних навичок

Оцінка

Підсумкова оцінка в результаті 100% постійного оцінювання:

30% виконання індивідуальних практичних завдань
20% екзамен (есе)

Критерії оцінювання:

Оцінювання проводиться на підставі 6 груп практичних завдань (в кожній по 5 невеликих завдань спільної тематики) у вигляди CTF-завдань. За їх виконання здобувач отримує 30 балів максимально. Кожне завдання оцінюється максимально в 1 бал.

Критерії оцінювання:

1 бал – здобувач вірно виконав роботу, демонструє глибоке розуміння матеріалу. Вірно обрано алгоритм реалізації, якісне представлення результатів. Обґрунтовані висновки.

0 балів – завдання не виконано здобувачем.

Оцінка за групу завдань — сума оцінок за усі роботи в ній.

Екзамен з дисципліни – максимально 40 балів, з них 20 балів за відповіді у частині комп'ютерні мережі (20 балів; есе, практичне завдання) та 20 балів у частині кібербезпеки (есе).

Зміст

Змістовий модуль 1. Веб-безпека

Тема 1. Введення до веб-безпеки.
Тема 2. Injection-атаки та вразливості.
Тема 3. Аутентифікація.
Тема 4. Авторизація.
Тема 5. XML та десеріалізація.

Змістовий модуль 2. Безпека ком'ютерних мереж.

Тема 6. Введення до безпеки комп'ютерних мереж.
Тема 7. TLS та HTTPS.
Тема 8. MITM-атаки.
Тема 9. WiFi.

Змістовий модуль 3. Тема на вибір.

Поглиблення певної тематики за вибором студентів.

Література

Основна

1. Jon Erickson. Hacking: The Art of Exploitation, 2nd Edition, 2008.
2. Dafydd Stuttard, Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2011.
3. Ryan C. Barnett, Jeremiah Grossman. Web Application Defender's Cookbook: Battling Hackers and Protecting Users, 2012

Додаткова

1. Jason Edelman. Network Programmability and Automation. Skills for the Next-Generation Network Engineer. 2018
2. https://portswigger.net/web-security
3. Електронний курс: https://www.coursera.org/learn/-network-security

Політика курсу

Політика щодо відвідування занять: Здобувачі мають відвідувати заняття регулярно. У випадку ситуацій, коли здобувач пропускає заняття, він несе особисту відповідальність за опрацювання матеріалів лекції, розміщених у Google Classroom. Частина матеріалу, який виноситься на іспит у вигляді есе та тесту, базується на лекціях. Пропущені заняття здобувач має відпрацювати, захистивши виконані практичні завдання під час чергової консультації викладача.

Здобувачі з особливими освітніми потребами: Мають право на індивідуальне визначення способів проходження поточного модульного та підсумкового контролю за письмовою заявою, яка

подається до загального деканату на початку викладання курсу. Можливе навчання за індивідуальним графіком, який оформлюється відповідно до п. 3.4 Положення про організацію освітнього процесу.

Академічна доброчесність: Здобувач має усвідомити, що академічна недоброчесність є неприпустимою. Викриття будь-якого порушення академічної доброчесності під час виконання будь-якого завдання призведе до його нульової оцінки. Порушення академічної доброчесності на екзамені призведе до негативної оцінки за весь курс та можливого виключення з програми. Під час екзамену здобувачам забороняється користуватися жодним електронним пристроєм (окрім ПК для виконання завдання), навчальними та додатковими матеріалами. Всі спірні питання, у разі їх виникнення, можуть бути урегульовані шляхом звернення до Комісії з академічної доброчесності та етики, відповідно до Положення про організацію освітнього процесу.

Політика щодо використання телефонів та інших електронних пристроїв: Під час проведення навчальних занять електронні пристрої та телефони мають перебувати в безшумному режимі роботи і можуть використовуватися для доступу до начальних матеріалів у Google Classroom. У разі невиконання даної вимоги, викладач може запропонувати здобувачу залишити аудиторію.

Політика щодо скарг здобувачів. Здобувач може обговорити проблемне питання з викладачем після заняття. Якщо питання залишається невирішеним, здобувач має право звернутися до завідувача кафедри інформаційних технологій.

Політика щодо підвищення оцінки з дисципліни: Здобувач має право підвищити оцінку з дисципліни відповідно до Положення про організацію освітнього процесу. Документи на підвищення оцінки мають бути оформлені у загальному деканаті.

Пропозиції від здобувачів вищої освіти: Протягом вивчення курсу здобувачі можуть звернутися до викладача з пропозиціями щодо вдосконалення курсу (доповнення тем, зміни методів викладання, форм оцінювання та ін.). Дані пропозиції можуть бути висловлені усно або письмово (електронною поштою, коментарі у Google Classroom). Для вирішення будь-якого питання, яке пов’язане із вивченням даної дисципліни, здобувач може звернутися до викладача (усно – в ауд. 2311 або письмово (babkin.v@duan.edu.ua) або до гаранта ОПП (bartashevska@duan.edu.ua).