СИЛАБУС

Назва дисципліни: Кібербезпека: рівень advanced

Мета дисципліни: Поглиблення знань з безпеки отриманих на попередніх курсах з мережевої безпеки та криптографії, також вивчення більш важких тем з кібербезпеки.

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.

ЗК13. Здатність діяти на основі етичних міркувань.

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

Мова викладання	**Семестр**	**Кредити ECTS / Тип дисципліни (обов'язкова, вибіркова)**	**Викладач**	**Навчальне навантаження**
Укр.	8	3 / вибіркова	Бабкін В.В., доктор філософії, викладач	90 год. (16 год. лекцій, 16 год. лабораторних занять, 9 год інд робота, 49 год. самостійної роботи)

Результати навчання По закінченню вивчення дисципліни здобувачі будуть здатні	**Методи викладання, навчання**	**Форми оцінювання (поточний та підсумковий контроль)**
РН-3. використовувати знання закономірностей випадкових явищ, їх властивостей та операцій над ними, моделей випадкових процесів та сучасних програмних середовищ для розв'язування задач статистичної обробки даних і побудови прогнозних моделей.	Лекція, семінар-діалог, розбір/ аналіз ситуаційних задач	Участь в семінарі, відповіді на запитання, вирішення ситуаційних задач
РН16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	Лекція, семінар-діалог, розбір практичних case-study, проблемно-пошуковий метод з використанням мережі Інтернет	Усні відповіді на запитання, вирішення/ пояснення практичних case-study
РН-17. Виконувати паралельні та розподілені обчислення, застосовувати чисельні методи та алгоритми для	Проблемна лекція, вирішення практичних case-study, проблемно-пошуковий метод з використанням мережі Інтернет, самостійна робота	Усні відповіді на запитання, вирішення/ пояснення практичних завдань, оцінювання практичних навичок

паралельних структур, мови паралельного програмування при розробці та експлуатації паралельного та розподіленого програмного забезпечення.		

Оцінка

Підсумкова оцінка в результаті 100% постійного оцінювання:

100% - розв'язування задач з використанням програмного забезпечення

Критерії оцінювання:

Бали з дисципліни здобувач отримує, виконуючи 4 поточні роботи по 25 балів кожна:

20-25 балів – здобувач вірно виконав роботу, демонструє глибоке розуміння матеріалу. Вірно обрано алгоритм реалізації, якісне представлення результатів. Обґрунтовані висновки.

15-19 балів – здобувач виконав роботу, однак є незначні неточності, що не здатні вплинути на кінцевий результат. Зроблено висновки і якісне подання результатів.

8-14 балів – здобувач демонструє недостатнє розуміння матеріалу. Однак є помилки у виборі та реалізації алгоритму рішення. Відсутні висновки і здобувач не може якісно пояснити отриманий результат. Завдання виконано частково або в загальному вигляді.

5-7 балів – здобувач демонструє незнання матеріалу, невірно обрано алгоритм реалізації і отриманий результат не є кінцевим, містить істотні помилки.

1-4 бали – здобувач демонструє незнання матеріалу. Виконання завдання не доведено до кінця, а наявне рішення містить грубі помилки.

0 балів – завдання не виконано здобувачем.

Зміст

Змістовий модуль 1. Криптографія публічних ключів. Обмін ключами.

Тема 1. Обмін ключами. Довірені треті сторони. Пазли меркла. Протокол Diffie-Hellman. Криптографія на основі публічних ключів.

Тема 2. Модулярна арифметика — необхідні знання. Прості та важки задачі (через теорію чисел)

Тема 3. RSA та шифри з trapdoor permutations. PKCS 1. Атаки проти RSA.

Тема 4. Система ElGamal.

Змістовий модуль 2. Сучаснеа розробка. Атаки та захист

Тема 5. Мікросервіси — що змінюється, яки є атаки у середовищі мікросервісів. SSRF.

Тема 6. Сучасні методи захисту ПО. Автоматизація пошуку вразливостей.

Змістовий модуль 3. Основи роботи з бінарними файлами

Тема 7. Reverse Engineering: що це і навіщо це необхідно. Практичні приклади.

Тема 8. Як працюють двійкові файли.

Тема 9. Основи Binary Exploitation. Найпростіші атаки, як вони працюють. Практичні приклади.

Література

Основна

1. Rashid A., Chivers H., Danezis G, Lupu E., Martin A., Rigby Y. The Cyber Security Body of Knowledge. The National Cyber Security Centre, 2019. – 834 p. URL: https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

2. https://github.com/rosehgal/BinExp

3. https://www.hoppersroppers.org/roadmap/training/pwning.html

4. Barnum T. The Cybersecurity Manager's Guide: The Art of Building Your Security Program. 1st Ed. Todd Barnum (english). USA: O'Reilly Media, 2021. – 225 p.

Додаткова

1. Jason Edelman. Network Programmability and Automation. Skills for the Next-Generation Network Engineer. 2018

2. https://microservices.io/

3. https://portswigger.net/web-security

4. https://github.com/benwaffle/Senior-Experience/blob/master/doc/w00w00-heap-overflows.txt

5. Електронний курс: https://www.coursera.org/learn/-network-security

6. Adekunle A. Eludire, Olatunji Okesola, Francis B. Osang Advanced cyber security: course guide. National Open University of Nigeria, 2022. URL: https://nou.edu.ng/coursewarecontent/CIT%20855.pdf

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 суперечливі питання, у разі їх виникнення, можуть бути врегульовані шляхом звернення до Комісії з академічної доброчесності та етики, відповідно до п.4.9 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 навчальних 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 пп. 2.4.5. Положення про організацію освітнього процесу. Заява на підвищення оцінки має бути оформлена 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 (ауд. 2504) або надіслати повідомлення на адресу: babkin.v@duan.edu.ua або до гаранта ОПП (bartashevska@duan.edu.ua).