СИЛАБУС

Назва дисципліни: Основи криптографії

Мета дисципліни: забезпечити теоретичну та практичну підготовку щодо методів сучасної криптографії, а саме – ознайомлення з теоретичними основами сучасної криптографії починаючі від стародавньої криптографії, и завершуючи сучасними криптографічними системами.

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.

СК6. Здатність до системного мислення, застосування методології системного аналізу для дослідження складних проблем різної природи, методів формалізації та розв’язування системних задач, що мають суперечливі цілі, невизначеності та ризики.

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.	7	5 / вибіркова	Бабкін В.В., доктор філософії, викладач	150 год. (28 год. лекцій, 28 год. лабораторних занять, 15 год інд робота, 79 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-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	Лекція, семінар-діалог, розбір практичних case-study, проблемно-пошуковий метод з використанням мережі Інтернет	Усні відповіді на запитання, вирішення/ пояснення практичних case-study

прогнозних моделей. РН16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	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

Оцінка

Підсумкова оцінка в результаті 100% постійного оцінювання:

100% виконання індивідуальних практичних завдань

Критерії оцінювання:

Оцінювання проводиться на підставі двох практичних завдань. За повне виконання 1-ї роботи здобувач отримує 75 балів максимально. За повне виконання 2-ї – 25 балів максимально.

Кожна робота у відсотках, відповідно:

90-100% – здобувач вірно виконав роботу, демонструє глибоке розуміння матеріалу. Вірно обрано алгоритм реалізації, якісне представлення результатів. Обґрунтовані висновки.

70-80% – здобувач виконав роботу, однак є незначні неточності, що не здатні вплинути на кінцевий результат. Зроблено висновки і якісне подання результатів.

50-60% – здобувач демонструє недостатнє розуміння матеріалу. 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.

30-40% – здобувач демонструє переважне незнання матеріалу, невірно обрано алгоритм реалізації і отриманий результат не є кінцевим, містить істотні помилки.

10-20% – здобувач демонструє незнання матеріалу. Виконання завдання не доведено до кінця, а наявне рішення містить грубі помилки.

0% – завдання не виконано здобувачем.

Зміст

Змістовий модуль 1. Поточні шифри

Тема 1. Що таке криптографія. Короткий курс з дискретної ймовірності.

Тема 2. One-time-pad та поточні шифри.

Тема 3. Атаки на поточні шифри.

Тема 4. Практичні прикладки. Поняття безпечного шифру.

Змістовий модуль 2. Блочні шифри

Тема 5. Що таке блочні шифри. DES.

Тема 6. AES та інши конструкції.

Тема 7. Блочні шифри з одноразовими та багаторазовими ключами.

Змістовий модуль 3. Цілістність повідомлень

Тема 8. Що таке цілістність повідомлень. MAC. MAC з PRF.

Тема 9. CBC-MAC. NMAC. PMAC. Carter-Wegman MAC. MAC Padding

Тема 10. Стійкість від колізій. Атака днів народження.

Тема 11. Парадігма Merkle-Damgard. Функції стиснення.

Тема 12. HMAC, атаки с заміром часу.

Змістовий модуль 4. Авторізоване шифрування

Тема 13. Що таке авторізоване шифрування. Активні атаки проти CPA-безпечних схем. Атаки з обраним шифротекстом.

Тема 14. Стандартні конструкції з шифрів та MAC. Атаки проти CBC Padding. Атаки проти Non-Atomic Decryption. Приклад: TLS v1.2.

Тема 15. Виведення ключів.

Тема 16. Детерміністичне шифрування. SIV, Wide PRP.

Тема 17. Дискове шифрування. Шифрування зі збереженням формату.

Література

Основна

1. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C. – Wiley, 2015. – 784 p.
2. Технології захисту інформації [Електронний ресурс]: підручник для студ. спеціальності 122 «Комп'ютерні науки» / Ю. А. Тарнавський. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
3. Криптографія від історії до сучасних стандартів: навч. посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
4. Jean-Philippe Aumasson. Serious Cryptography. A Practical Introduction to Modern Encryption. 2017.

Додаткова

1. https://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Discrete_Probability
2. https://toc.cryptobook.us/
3. https://www.rfc-editor.org/rfc/rfc5246
4. Електронний курс: https://www.coursera.org/learn/crypto
5. Christof Paar. Understanding Cryptography. A Textbook for Students and Practitioners, 2009.

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 – в ауд. 2311 або письмово (babkin.v@duan.edu.ua) або до гаранта ОПП (bartashevska@duan.edu.ua).