ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ
Луцького національного технічного університету

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ ШИФРУВАННЯ ТА КРИПТОГРАФІЇ

Галузь знань: 12 Інформаційні технології
Освітньо-професійна програма: Комп'ютерна інженерія
Обслуговування комп'ютерних систем та мереж
Інформаційні системи та технології
Спеціальність: 123 Комп'ютерна інженерія
126 Інформаційні системи та технології

Рівень освіти	Фахова передвища освіта
Освітньо-професійний /освітній ступінь	Фаховий молодший бакалавр
Статус навчальної дисципліни	Вільного вибору студента (професійної підготовки)
Обсяг дисципліни (кредити ЄКТС/ загальна кількість годин)	5 кредитів ЄКТС/ 150 годин
Циклова комісія	Циклова комісія комп'ютерних систем та інформаційних технологій
Мова викладання	Українська
Мета навчальної дисципліни	**Метою вивчення** навчальної дисципліни «Основи криптографії» є ознайомлення з теоретичними основами криптології, придбання навичок в практичному використанні, постановці і вирішенні задач шифрування інформації, розуміння суті інформаційних процесів в криптографічних системах, застосування комп'ютерів для вирішення завдань шифрування і дешифрування, розробка і використання математичних і обчислювальних моделей процесів шифрування інформації, їх оптимізація та вироблення напрямків вдосконалення.
Предмет і завдання дисципліни	**Предметом** вивчення дисципліни «Основи криптографії» є основні методи захисту інформації від несанкціонованого доступу, застосування симетричних та асиметричних алгоритмів криптографії, алгоритмів генерування ключів, цифрового підпису, розподілу таємниці. **Основними завданнями** вивчення дисципліни «Основи криптографії» є: формування у студентів певних професійних компетенцій, знань та вмінь з теорії та практики криптографічного захисту інформації та криптографічного аналізу.
Форма підсумкового контролю	Диференційований залік
Зміст дисципліни	**Змістовий модуль 1.** Види криптографічних перетворень інформації. Сучасні симетричні криптографічні системи **Тема 1.** Основні поняття і визначення криптографії. Принципи криптографічного захисту інформації. Історія розвитку криптографії.

	Тема 2. Шифрувальні криптографічні перетворення. Односторонні функції. Хешфункції. Електронний цифровий підпис. Генератори псевдовипадкових послідовностей. **Тема 3.** Шифри перестановки. Шифри заміни (підстановки). Шифри гамування. **Тема 4.** Композиційні блокові шифри і принципи їх побудови. **Тема 5.** Криптоаналіз і види криптоаналітичних атак. **Тема 6.** Стандарт шифрування даних DES. Алгоритм криптографічного перетворення даних ГОСТ 28147-89. Стандарт шифрування США нового покоління (AES). **Змістовий модуль 2**. Криптографічні системи з відкритим ключем **Тема 7**. Алгоритми шифрування з відкритим ключем. **Тема 8**. Криптосистема шифрування RSA. Алгоритм цифрового підпису RSA. **Тема 9.** Криптосистема Діффі-Хеллмана. Криптосистема Ель Гамаля. Алгоритм цифрового підпису Ель Гамаля (EGSA). **Тема 10.** Криптосистема на основі еліптичних кривих. **Тема 11.** Алгоритм безпечного хешування (SHA). Односторонні хеш-функції на основі симетричних блокових алгоритмів. Алгоритми шифрування з відкритим ключем. **Тема 12.** Алгоритм цифрового підпису DSA.
Рекомендована література	**Основна** 1. Гребенніков В.В. Історія криптології & секретного зв'язку Ужгород: Ліра, 2012. – 664 с. 2. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – Житомир : ДУТ, 2014. - 448 с. 3. Прикладна криптологія. Теорія. Практика. Застосування : монографія / Горбенко І. Д., Горбенко Ю. І. ; Харк. нац. ун-т радіоелектрон., Приват. АТ "Ін-т інформ. технологій". - Вид. 2-ге, переробл. й допов. - Х. : Форт, 2012. - 878 с. **Додаткова** 4. Ван Тилборг Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. – М.: Мир, 2006. – 471 с. 5. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтак. Ужгород: Видавництво УжНУ «Говерла», 2020. 28 с. **Інтернет-ресурси** 6. Лекції_КК [Електронний ресурс]. – Режим доступу: http://dspace.wunu.edu.ua/jspui/bitstream/316497/24961/1/%D0%9B%D0%B5%D0%BA%D1%86%D1%96%D1%97_%D0%9A%D0%9A.pdf 7. Курс «Основи криптології» [Електронний ресурс]. – Режим доступу: https://moodle.znu.edu.ua/course/view.php?id=4199
Види занять, методи і форми навчання	Форми організації освітнього процесу: лекції, лаборторні заняття, самостійна робота, консультації зі викладачами, дистанційне навчання. Освітні технології: традиційні, інтерактивні, інформаційно-комунікативні, проектного навчання.
Пререквізити	Дисципліни «Вища математика», «Теорія ймовірностей і математична статистика», «Програмування»
Постреквізити	«Комп'ютерні системи». Здійснення професійної діяльності.

Критерії оцінювання	**Критерії оцінювання:** Оцінка «**відмінно**» виставляється, якщо здобувач освіти у повному обсязі володіє навчальним матеріалом, вільно, самостійно й аргументовано його викладає, глибоко та всебічно розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу, вільно послуговується науковою термінологією, розв'язує задачі стандартним або оригінальним способом, наводить аргументи на підтвердження власних думок, здійснює аналіз та робить висновки. Оцінка «**добре**» виставляється, якщо здобувач освіти достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає, в основному розкриває зміст теоретичних запитань та практичних завдань, використовуючи при цьому обов'язкову літературу, розв'язує задачі стандартним способом, послуговується науковою термінологією, але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі неістотні неточності та незначні помилки. Оцінка «**задовільно**» виставляється, якщо здобувач освіти відтворює значну частину навчального матеріалу, висвітлює його основний зміст, виявляє елементарні знання окремих положень, записує основні формули, рівняння, закони, однак нездатний до глибокого, всебічного аналізу, обґрунтування та аргументації, не користується необхідною літературою, допускає істотні неточності та помилки. Оцінка «**незадовільно**» виставляється, якщо здобувач освіти достатньо не володіє навчальним матеріалом, однак фрагментарно, поверхово (без аргументації й обґрунтування) викладає окремі питання навчальної дисципліни, не розкриває зміст теоретичних питань і практичних завдань.
Політика курсу	Курс передбачає індивідуальну та групову роботу. Усі завдання, передбачені програмою, мають бути виконані у встановлений термін. Якщо здобувач освіти відсутній з поважної причини, він/вона презентує виконані завдання під час консультації викладача. Під час роботи над індивідуальними завданнями та проектами не допустимо порушення академічної доброчесності.