ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ /
CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «07» серпня 2024 р.)
завідувач кафедри
_____ Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ /** CRYPTOGRAPHIC METHODS OF INFORMATION PROTECTION
Спеціальність	125 «Кібербезпека»
Освітній ступінь	Перший (бакалавр)
Освітньо-професійна програма	**БЕЗПЕКА ІНФОРМАЦІЙНИХ І КОМУНІКАЦІЙНИХ СИСТЕМ В ЕКОНОМІЦІ**
	Лектор: **Криворучко Олена** -завідувач кафедри інженерії програмного забезпечення та кібербезпеки, гарант освітньої програми «Комп'ютерні науки» (PhD) -доктор технічних наук -пофесор Резюме викладача: https://knute.edu.ua/blog/read/?pid=39648&uk Науковий профіль: https://knute.edu.ua/blog/read/?pid=46714 е-пошта: kryvoruchko_ev@knute.edu.ua
	Асистент лектора: **Сергій Бульба** -ст.викладач, гарант освітньої програми «Інженерія програмного забезпечення» -к.е.н. Резюме викладача: https://knute.edu.ua/blog/read/?pid=48084&uk Практична діяльність: Senior System Analyst, Solution Architect е-пошта: s.bulba@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48215
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Історичний огляд криптографічних методів захисту інформації	1. Історія криптографії. 2. Базові поняття криптографії. 3. Роль криптографії у захисті даних. 4. Поняття та види шифрів. 5. Вимоги до шифрів - принцип Керхгоффса. 6. Шифрувальні машини та підходи до їх аналізу.

	7. Ідеальний шифр і класи стійкості шифрів.
Тема 2. Сучасні криптографічні методи захисту інформації	1. Основні види криптографічних методів 2. Реалізація криптографічних методів 3. Симетричні і асиметричні методи шифрування 4. Шифри на основі мережі Фейстеля. Мережа Фейстеля. 5. Американський шифр DES. 6. Шифри на основі SP-мережі.
Тема 3. Основні принципи роботи блокових шифрів	1. Сучасні блокові шифри 2. Компоненти сучасного блокового шифру 3. Розгляд відомих блокових шифрів (ГОСТ 28147, DES, AES, ДСТУ 7624 і т.д.). Переваги недоліки. 4. Складені шифри 5. Режими роботи блокових шифрів
Тема 4. Криптографія та криптоаналіз. Інфраструктура відкритих ключів	1. Криптографічне перетворення. 2. Електронний цифровий підпис. 3. Параметри і ключі цифрового підпису. 4. Процедури створення та перевіряння підпису. 5. Параметри та формат цифрового підпису. 6. Особливості надання послуг безпеки в електронному документообігу. 7. Алгоритм механізму цифрового підпису ДСТУ. 8. Техніка управління ключами.
Тема 5. Основні концепції інфраструктури відкритих ключів	1. Прості моделі установлення ключів. 2. Ролі третіх сторін. 3. Проблеми життєвого циклу ключів. 4. Вимоги до захисту протягом терміну експлуатації. 5. Життєвий цикл управління ключами. 6. Техніка управління використанням ключів, обмеження на їх використання. 7. Порівняльний аналіз схем цифрового підпису. 8. Практичні криптопротоколи. 9. Спеціальні види цифрового підпису. 10. Сліпий підпис на основі RSA. Сліпий підпис під прийнятним повідомленням. 11. Неспростовний підпис. Протокол виявлення фальсифікації неспростовного підпису. 12. Рандомізовані схеми цифрового підпису, рекомендовані ISO, та MQV протокол.
Тема 6. Типові технології використання інфраструктури відкритих ключів	1. Сервіси, що базуються на ІВК. Послуги з підтримкою ІВК: безпечне спілкування, захищене проставлення міток часу, нотаризація. 2. Механізми, що необхідні для створення служб із підтримкою ІВК. 3. Типові технології використання інфраструктури відкритих ключів в інформаційно-комунікаційних системах.

	Протоколи, що базуються на ІВК. 4. Протоколи безпеки SSL і TLS. Засоби безпеки транспортного рівня. 5. Підтримка безпеки транспортного рівня на основі ІВК. Політика застосування сертифікатів.
Тема 7. Криптографічні протоколи	1. Поняття криптографічних протоколів. Їх опис. 2. Класифікація криптографічних протоколів. Властивості, що визначають безпеку криптографічних протоколів. 3. Атаки на протоколи. 4. Аналіз та моделювання криптографічних протоколів. 5. Протоколи електронного цифрового підпису.
Тема 8. Протоколи аутентифікації (ідентифікації)	1. Основні етапи аутентифікації та авторизації. 2. Чинники аутентифікації. 3. Класифікація видів аутентифікації 4. Розмежування доступу. 5. Моделі розмежування доступу.
Тема 9. Управління криптографічним и ключами	1. Сутність управління ключами. Принцип Керкгоффса. 2. Стандарти генерації ключів. Накопичення, розподілення, оновлення, зберігання, резервування ключів. 3. Генерація та модифікація ключа. 4. Зберігання та розподіл ключів. 5. Протоколи обміну ключами.
Тема 10. Стеганографічний захист інформації	1. Історичний огляд стеганографії. 2. Стеганографічна система. Стеганографічний контейнер. Стегано-графічний канал. 3. Виявлення стеганографічного каналу. 4. Типи та класи порушників безпеки стеганографічних систем.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

1. Бабак В. П. Теоретичні основи захисту інформації : підручник // Бабак В. П. – Книжкове видавництво НАУ, 2008. – 752 с.
2. Основи криптографічного захисту інформації : підручник / авт.: Г.М. Гулак, В.А. Мухачов, В.О. Хорошко, Ю.Є. Яремчук. – Вінниця : ВНТУ, 2011. – 94 с.
3. Основи захисту інформації : навч. посібн. / О. А. Смірнов, Л. Г. Віхрова, С. І. Осадчий та ін. – Кіровоград, 2010. – 322 с.
4. Основи інформаційної безпеки / С. В. Кавун, О. А. Смірнов, В. Ф. Столбов – Кіровоград : Вид. КНТУ, 2012. – 414 с.
5. Фаль О. М. Криптографія : основні ідеї та застосування / О. М. Фаль. – К. : ІВЦ Видавництво «Політехніка», 2003. – 28 с.

Додатковий

6. Блінцов В. С. Захист програмних продуктів : навчальний посібник / В. С. Блінцов, С. С. Козирев. – Миколаїв : НУК, 2010. – 146 с.
7. Голубєв В. О. Інформаційна безпека : проблеми боротьби з кіберзлочинами : монографія / В. О. Голубєв. – Запоріжжя : ГУ «ЗІДМУ», 2003. – 250 с.

8. Гулак Г. Н. Основы криптографической защиты информации / Г. Н. Гулак. – К. : Вид. ГУІКТ, 2009. – 228 с.
9. Довгий С. О. Сучасні телекомунікації : Мережі, технології, безпека, економіка, регулювання: монографія / С. О. Довгий, П. П. Воробієнко, К. Д. Гуляєв; За загальною ред. С. О. Довгого. – [2-ге видання (доповнене)]. – К. : Аимут-Україна, 2013. – 608 с.
10. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. – К. : ДМК Пресс, 2008. – 544 с.
11. Інформаційний та кіберпростори : проблеми безпеки, методи та засоби боротьби : посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. – К. : ДУТ – КНУ, 2016. – 178 с.
12. Кавун С. В. Інформаційна безпека : підручник / С. В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.
13. Конахович Г. Ф. Захист інформації в мережах передачі даних : підручник / Г. Ф. Конахович. – К. : Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714 с.
14. Криптографія [Електронний ресурс]. – Режим доступу : http://uk.wikipedia.org/wiki/Криптографія.
15. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 512 с.
16. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. Правовий захист інформації : навчальний посібник / Н. І. Логінова, Р. Р. Дробожур. – Одеса : Фенікс, 2015. – 264 с.
17. Державна служба спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua/dsszzi/control/uk/index
18. Офіційний вебпортал парламенту України http://www.rada.gov.ua

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ

Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:

КЗ 1	Здатність застосовувати знання у практичних ситуаціях.
КЗ2	Знання та розуміння предметної області та розуміння професії.
КЗ4	Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
КФ10	Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
РН17	Збирати, аналізувати, оцінювати необхідну для розв'язання наукових і прикладних задач інформацію, використовуючи науково-технічну літературу, бази даних та інші джерела.

ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ

Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних/практичних заняттях, свідчить про ступінь оволодіння ним програмою освітньої компоненти на конкретному етапі її вивчення. Протягом семестру здобувачі освіти можуть набрати від 0 до 100 балів, що переводяться у національну шкалу оцінювання і

відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни			
Довідник з розподілу оцінок ДТЕУ (Шкала ЄКТС):			
Бали ДТЕУ	Відсоток балів відносно загальної кількості одержаних прохідних балів	Кумулятивний відсоток отриманих прохідних балів	
90-100	20	20	
82-89	10	30	
75-81	20	50	
69-74	10	60	
60-68	40	100	
Роподіл балів за видами робіт:			
Вид роботи	**Бали**	**Вид роботи**	**Бали**
Лабораторна робота 1	10	Самостійна робота 1	5
Лабораторна робота 2	10	Самостійна робота 2	5
Лабораторна робота 3	10	Самостійна робота 3	5
Лабораторна робота 4	10	Самостійна робота 4	5
Лабораторна робота 5	10		
Додаткові бали	20	Наукова робота	10
Вимоги до критеріїв оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)			
40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.		
40%	Обґрунтованість аргументів, підтвердження особистого ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.		
20%	Оформлення звіту у відповідності вимог		
Критерії оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)			
100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов’язкову та додаткову літературу. Правильно вирішив усі тестові завдання.		
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов’язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації,		

	допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.
ОСНОВНІ ПОЛОЖЕННЯ, ЩО РЕГЛАМЕНТУЮТЬ ОСВІТНІЙ ПРОЦЕС	
діючі положення	https://knute.edu.ua/blog/read/?pid=44402
нормативно-правова база організації освітнього процесу	https://knute.edu.ua/blog/read/?pid=7330&uk
студенту	https://knute.edu.ua/#forstudent
НЕФОРМАЛЬНА ОСВІТА Рекомендовані сертифікаційні програми, курси, посібники користувача	
UDEMY: Cryptography - Past, Present and Future	https://shorturl.at/HFuW0
Cryptography: Learn All Encryption Algorithm in details.	https://www.udemy.com/course/learn-cryptography-s/
Cisco Academy: Introduction to cybersecurity	https://shorturl.at/jg4Nj
Udacity: System Security	https://shorturl.at/COs1n
ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:	
Відвідування лекційних та лабораторних занять:	Відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому

відвідування	конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).
Відпрацювання пропущених занять:	відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).
Правила поведінки під час занять	обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)
Політика академічної доброчесності ДТЕУ	https://knute.edu.ua/blog/read/?pid=38987&uk