



Міжнародний гуманітарний університет
Факультет Кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра Комп'ютерної інженерії та інноваційних технологій

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Криптографія та криптоаналіз

Галузь знань	<u>12 «Інформаційні технології»</u>
Спеціальність	<u>125 «Кібербезпека та захист інформації»</u>
Назва освітньої програми	<u>Кібербезпека</u>
Рівень вищої освіти	<u>перший (бакалаврський) рівень</u>

Розробники і викладачі	Контактний тел.	E-mail
Йона Лариса Григорівна	067-746-37-77	yonalarisa66@gmail.com

1. АНОТАЦІЯ ДО КУРСУ

Криптографія та криптоаналіз є складовою частиною навчального процесу у підготовці фахівців зі спеціальності 125 «Кібербезпека та захист інформації», а також обов'язковим компонентом освітньої програми для здобуття освітнього рівня «бакалавр» та має на меті формування у здобувачів уявлення про принципи побудови симетричних та асиметричних криптографічних систем, проблеми захисту інформації від порушення її конфіденційності, цілісності та доступності; принципи побудови та режими роботи блокових алгоритмів шифрування; розгляд концепції криптосистем з відкритим ключем; методи побудови схем електронно-цифрових підписів та керування криптографічними ключами, а також методи криптоаналізу для оцінки надійності систем захисту.

Метою викладання навчальної дисципліни Криптографія та криптоаналіз є забезпечення здобувачів знаннями з питань принципів побудови криптографічних систем та проблем захисту інформації у системах комунікацій з урахуванням сучасного стану та перспективних напрямів розвитку криптології; формує критичне мислення щодо вибору та впровадження засобів захисту інформації.

ПЕРЕКВІЗИТИ. Передумовами є знання з вищої математики (ОК 5), теорії ймовірностей та математичної статистики (ОК 6), дискретної математики (ОК 9) та теорії інформації та кодування (ОК 25).

ПОСТРЕКВІЗИТИ. Знання алгоритмів шифрування та методів криптоаналізу є необхідними при вивченні «Захисту інформації в інфокомунікаційних системах та мережах» (ОК 12), «Комплексних систем захисту інформації» (ОК 24), «Систем технічного захисту інформації» (ОК 31), «Безпеки програм та даних» (ОК 16), «Управління інформаційною та кібербезпекою» (ОК 30), «Основ цифрової криміналістики» (ОК 26) та «Етичного хакінгу та тестування на проникнення» (ОК 18).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Криптографія та криптоаналіз» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

Спеціальні (фахові, предметні) компетентності

СК 4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК 8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

СК 11. Здатність здійснювати проектування, адміністрування та керування інформаційно-комунікаційними системами, забезпечуючи їхню надійність, безпеку та ефективність функціонування.

Навчальна дисципліна «Криптографія та криптоаналіз» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності

РН 9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації

РН 18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН 19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН 22. Вміти застосовувати методи та інструменти проектування й адміністрування мереж і систем, виконувати налаштування, моніторинг та підтримку їхньої працездатності з урахуванням вимог інформаційної безпеки.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		Вид заняття (денне відділення / заочне відділення)				Ознаки курсу		
ЄКТС	годин	Лекційні заняття	Лабораторні заняття	Практині заняття	Самостійна робота	Курс, (рік навчання)	Семестр	Обов'язкова / вибіркова
4	120	26/4	6/2	20/4	68/110	3	5	Обов'язкова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лк	лб.	пр.	сам. роб.		лекц.	лр.	пр.	сам. роб.
Змістовий модуль 1. Криптографічні методи захисту інформації										
Тема 1. Криптологія: основні поняття та історичний розвиток.	8	2		2	4	6				6
Тема 2. Основи архітектури криптосистем.	8	2		2	4	8				8
Тема 3. Потоківі симетричні шифри. Блокові симетричні шифри.	10	2		2	6	10	2			8
Тема 4. Асиметричні методи шифрування.	10	2		2	6	8				8
Тема 5. Протоколи керування криптографічними ключами.	10	2		2	6	8				8
Тема 6. Стандарти та схеми електронного підпису	6			2	4	8				8
Змістовий модуль 2. Дослідження методів криптоаналізу										
Тема 7. Теоретична та практична стійкість.	8	2		2	4	8				8
Тема 8. Криптоаналіз шифрів перестановки,	10	2	2		6	10		2		8
Тема 9. Криптоаналіз шифрів одноалфавітної заміни.	10	2	2		6	10	2			8
Тема 10. Криптоаналіз шифрів багатоалфавітної заміни.	8	2	2		4	10			2	8
Тема 11. Диференціальний та лінійний криптоаналіз.	8	2		2	4	8				8
Тема 12. Методи факторизації. Методи дискретного логарифмування.	8	2		2	4	10			2	8
Тема 13. Стійкість та криптоаналіз схем електронного підпису.	10	2		2	6	8				8
Тема 14. Сучасні тенденції та практичні аспекти криптоаналізу	6	2			4	8				8
Усього годин	120	26	6	20	68	120	4	2	4	110
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН										

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Здобувачі отримують теми та питання дисципліни, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання, зокрема

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Криптографія та криптоаналіз» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання теоретичного матеріалу, здобутого під час семестру.
3. Виконання практичних та індивідуальних завдань, сформованих викладачем.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання індивідуальних завдань.
7. Підготовка до підсумкового контролю знань.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	Тема 1. Криптологія: основні поняття та історичний розвиток. Криптографія в класичних шифрах.	6	6
2	Тема 2. Основи архітектури криптосистем. Класифікація та призначення криптографічних перетворень. Принципи побудови криптосистем.	8	8
3	Тема 3. Сучасні симетричні криптосистеми. Особливості побудови ДСТУ 7624:2014.	10	8
4	Тема 4. Асиметричні методи шифрування. Криптосистеми RSA та Ель Гамала.	8	8
5	Тема 5. Протоколи керування криптографічними ключами. Протокол Діффі-Геллмана, MQV, Kerberos, Needham-Schroeder.	8	8
6	Тема 6. Стандарти та схеми електронного підпису. Електронний підпис Шнорра, Ніберга-Рюпеля	8	8
7	Тема 7. Теоретична та практична стійкість. Статистичний аналіз криптограм, статистичні моделі Шеннона і Маркова та їх застосування в криптоаналізі.	4	8
8	Тема 8. Криптоаналіз шифрів перестановки	6	8
9	Тема 9. Криптоаналіз шифрів одноalfавітної заміни. Криптоаналіз омофоніческой (гомофоніческой) заміни.	6	8

10	Тема 10. Криптоаналіз багатоалфавітної заміни. Частотний криптоаналіз. Метод Казіскі, Фрідмана.	4	8
11	Тема 11. Диференціальний та лінійний криптоаналіз. Аналіз режимів роботи симетричних алгоритмів шифрування.	4	8
12	Тема 12. Методи факторизації. Методи дискретного логарифмування. Метод решета у числовому полі. Метод Полларда	4	8
13	Тема 13. Стійкість та криптоаналіз схем електронного підпису. Класифікація атак на схеми електронного підпису.	6	8
14	Тема 14. Сучасні тенденції та практичні аспекти криптоаналізу	4	8
	Всього	68	110

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю		Складові оцінювання
Поточний контроль , який здійснюється під час проведення практичних занять, виконання індивідуального завдання, проведення консультацій та відпрацювання пропущених здобувачем занять.		50%
Підсумковий контроль , який здійснюється під час проведення екзамену.		50%
Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, тези доповіді, наукова стаття, індивідуальне опитування, тестування, екзамен.	

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ (поточний контроль, підсумковий контроль, загальний результат оцінювання)

ЕКЗАМЕН

Поточний контроль			
Види роботи	Планові терміни виконання	Форми контролю та звітності	Максимальний відсоток оцінювання
Систематичність і активність роботи на практичних (лабораторних) заняттях			

1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних (лабораторних) занять	30
Виконання завдань для самостійного опрацювання			
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або ІКР ¹ , перевірка конспектів навчальних текстів тощо	10
Виконання індивідуальних завдань, дослідна робота здобувача			
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	10
Разом балів за поточний контроль			50
Підсумковий контроль екзамен			50
<i>Загальний результат оцінювання</i>			100

Поточний контроль знань здобувачів освіти при формі контролю **екзамен** (максимум 50 балів) оцінюється за шкалою («2», «3», «4», «5»), з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 30 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переведу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 6;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 10 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переведу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 2;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 10- балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переведу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 2.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;

¹ Індивідуально-консультаційна робота викладача зі здобувачами

- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.
- «5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати теоретичні знання в практичній площині.

КРИТЕРІЇ ОЦІНЮВАННЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ ЗДОБУВАЧІВ ЗА ІСПИТ (максимум 50 балів)

Рівень знань оцінюється:

- від 40 до 50 балів - студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки;
- 30 до 40 балів - студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді;
- 20 - 30 балів - студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки.
- 10 - 20 балів - володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих;
- 0 10 балів - володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки.

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ (для екзамену / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» А - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» В - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» С - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним

матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);

- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D		
60-63	E	Задовільно	
35-59	Fx		
1-34	F	Незадовільно	Не зараховано

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України “Про освіту” (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України “Про освіту” академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилення на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Онацький О.В., Йона Л.Г., Белова Ю.В. Криптографічний захист інформації: Навч.посібник. - Одеса: Одеса : «Астропринт» 2023. 252с. <https://surl.li/onvhbl>
2. Онацький О. В., Йона Л. Г. Криптографічні системи : навчальний посібник з дисциплін "Криптографія та криптоаналіз" для освітньо-професійної підготовки бакалаврів в галузі знань 12 "Інформаційні технології" за спеціальністю 125 "Кібербезпека" / О. В. Онацький, Л. Г. Йона. – Одеса : Міжнародний гуманітарний університет, 2023. – 156 с. <https://surl.li/oqiqhk>
3. Йона Л.Г., Онацький О.В., Швець О.В. Системи банківської безпеки: Навч.посібник.- Одеса: ДУІТЗ. 2022. 192с. <https://surl.li/hpdpub>
4. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія. Харків: Видавництво «Форт», 2012. 880 с.
5. Корченко О. Г., Сіденко В. П., Дрейс Ю. О. Прикладна криптологія: системи шифрування: підручник. Київ: ДУТ, 2014. 448 с.
6. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. Харків: Видавництво «Форт», 2010. 608 с.
7. Захарченко М. В., Онацький О. В., Йона Л. Г., Шинкарчук Т. М. Асиметричні методи шифрування в телекомунікаціях: навч. посіб. Одеса: ОНАЗ ім. Попова, 2011. 184 с.

Допоміжна

1. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p.
2. Остапо С. Е., Євсєєв С. П., Король О. Г. Технології захисту інформації: навч. посіб. Харків: ХНЕУ, 2013. 476 с.
3. Бабенко Т. В., Гулак Г. М., Сушко С. О., Фомичова Л. Я. Криптологія у прикладах, тестах і задачах: навч. посіб. Дніпро: Національний гірничий університет, 2013. 318 с.
4. Кузнецов Г. В., Фомічов В. В., Сушко С. О. Математичні основи криптографії. Дніпропетровськ: НГУ, 2004. 389 с.

Інформаційні ресурси

1. Наказ МОН № 1074 від 04.10.2018 року (у редакції наказу МОН №1547 від 29.10.2024) Про внесення змін до стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти. URL: https://osvita.ua/legislation/Vishya_osvita.
2. Національна бібліотека України ім. В.І. Вернадського. URL: <http://www.nbuv.gov.ua>.
3. ДСТУ 4145-2002. URI: <https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798>
4. AES Rijndael Cipher explained as a Flash animation. URI: <https://www.youtube.com/watch?v=gP4PqVGudtg>
5. DES Animation. URI: <https://www.youtube.com/watch?v=Vcld7CMAAnNs>
6. Presentation over Cryptographic Primitives (RC4). URI: <https://www.youtube.com/watch?v=KM-xZYZXElk>
7. IDEA algorithm. URI: https://www.youtube.com/watch?v=vt1Zfs_qz3Q