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

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Криптологія

Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека та захист інформації»
Назва освітньої програми Кібербезпека
Рівень вищої освіти другий (магістерський) рівень

Розробники і викладачі	Контактний тел.	E-mail
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій **Йона Лариса Григорівна;**	+380677463777	yonalarysa66@gmail.com
Доцент кафедри Комп'ютерної інженерії та інноваційних технологій **Онацький Олексій Віталійович**	+380503761048	onatsky@meta.ua

1. АНОТАЦІЯ ДО КУРСУ

Криптологія 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 «магістр» 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.

Метою викладання навчальної дисципліни Криптологія є забезпечення здобувачів знаннями з питань принципів побудови криптографічних систем та проблем захисту інформації у системах комунікацій від порушення її конфіденційності, цілісності та доступності з урахуванням сучасного стану та перспективних напрямів розвитку криптографії.

Передумови для вивчення дисципліни – знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки.

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

Інтегральна компетентність

ІК1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні (фахові, предметні) компетентності

КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Програмні результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)			**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
4	120	28 /	28 /	64 /	1	2 /	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**		
		лекц.	**практ.**	**сам. роб.**		**лекц.**	**прак**	**сам. роб.**
Змістовий модуль 1. Криптографічні методи захисту інформації.								
Тема 1. Криптологія: основні поняття та історичний розвиток.	9	2	2	5				
Тема 2. Основи архітектури криптосистем.	9	2	2	5				
Тема 3. Потокові симетричні шифри.	9	2	2	5				
Тема 4. Блокові симетричні шифри.	9	2	2	5				
Тема 5. Асиметричні методи шифрування.	9	2	2	5				
Тема 6. Протоколи керування криптографічними ключами.	9	2	2	5				
Тема 7. Стандарти та схеми електронного підпису	9	2	2	5				
Змістовий модуль 2. Дослідження методів криптоаналізу.								
Тема 8. Теоретична та практична стійкість.	9	2	2	5				
Тема 9. Криптоаналіз шифрів перестановки, одноалфавітної заміни.	8	2	2	4				
Тема 10. Криптоаналіз багатоалфавітної заміни.	8	2	2	4				
Тема 11. Диференціальний та лінійний криптоаналіз.	8	2	2	4				
Тема 12. Методи факторизації.	8	2	2	4				
Тема 13. Методи дискретного логарифмування.	8	2	2	4				
Тема 14. Стійкість та криптоаналіз схем електронного підпису.	8	2	2	4				
Усього годин	**120**	**28**	**28**	**64**				
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 «Криптологія» 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**. Теорія зв'язку в секретних системах.	5	
2	**Тема 2. Основи архітектури криптосистем.** Класифікація та призначення криптографічних перетворень.	5	
3	**Тема 3. Потокові симетричні шифри.** ДСТУ 8845-2019.	5	
4	**Тема 4. Блокові симетричні шифри.** ДСТУ 7624:2014.	5	
5	**Тема 5. Асиметричні методи шифрування.** Криптосистема Меркле–Хеллмана, Idempotent Elements.	5	
6	**Тема 6. Протоколи керування криптографічними ключами.** Протокол MQV, Kerberos, Needham-Schroeder.	5	
7	**Тема 7. Стандарти та схеми електронного підпису.** Електронний підпис Шнорра, Ніберга-Рюпеля	5	
8	**Тема 8. Теоретична та практична стійкість.** Статистичний аналіз криптограм, статистичні моделі Шеннона і Маркова та їх застосування в крипто аналізі.	5	

9	**Тема 9. Криптоаналіз шифрів перестановки, одноалфавітної заміни.** Криптоаналіз омофоніческой (гомофоніческой) заміни.	4	
10	**Тема 10. Криптоаналіз багатоалфавітної заміни.** Частотний криптоаналіз. Метод Казіскі, Фрідмана.	4	
11	**Тема 11. Диференціальний та лінійний криптоаналіз.** Аналіз режимів роботи симетричних алгоритмів шифрування.	4	
12	**Тема 12. Методи факторизації.** Метод решета у числовому полі.	4	
13	**Тема 13. Методи дискретного логарифмування.** Метод Полларда.	4	
14	**Тема 14. Стійкість та криптоаналіз схем електронного підпису.** Класифікація атак на схеми електронного підпису.	4	
	Всього	**64**	

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 ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ СТУДЕНТІВ З ПІДСУМКОВИМ КОНТРОЛЕМ У ФОРМІ ЕКЗАМЕНУ.

Денна та заочна форми навчання			
Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на базі практики			
1.1. Підготовка до практичних занять.	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	**25**

Виконання завдань для самостійного опрацювання			
1.2. Підготовка програмного матеріалу (тем, питань) для самостійного вивчення	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу під час аудиторних занять або індивідуально-консультативна робота (ІКР) викладача зі здобувачами.	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
1.3. Підготовка реферату за заданою тематикою.	Відповідно до розкладу занять і графіку ІКР	Обговорення (захист) матеріалів реферату.	**10**
1.4. Інші види індивідуальних завдань, зокрема, підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до розкладу занять і графіку ІКР	Обговорення результатів проведеної роботи під час аудиторних занять, наукових конференцій та круглих столів.	**5**
Разом балів за поточний контроль			**50**
*Підсумковий контроль – **екзамен***			**50**
Всього балів			**100**

Заочна форма навчання

9. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ
(для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та практичних заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» B - від 82 до 89 балів. Здобувач 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 практичних заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

- «добре» / «зараховано» C - від 74 до 81 балів. Здобувач 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. Здобувач був присутній не на всіх лекціях та практичних 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;

- «задовільно» / «зараховано» E - від 60 до 63 балів. Здобувач був присутній не на всіх лекціях та практичних 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 результатів контролю знань за різними шкалами

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100 (10-12)	A	Відмінно	Зараховано
82-89 (8-9)	B	Добре	
74-81(6-7)	C		
64-73 (5)	D	Задовільно	
60-63 (4)	E		
35-59 (3)	FX	Незадовільно	Не зараховано
1-34 (2)	F		

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Йона Л. Г., Онацький О. В., Швець О. В. Системи банківської безпеки: навч. посіб. Одеса: ДУІТЗ, 2022. 192 с.
2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика: монографія. Харків: Видавництво «Форт», 2012. 880 с.
3. Корченко О. Г., Сіденко В. П., Дрейс Ю. О. Прикладна криптологія: системи шифрування: підручник. Київ: ДУТ, 2014. 448 с.
4. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. Харків: Видавництво «Форт», 2010. 608 с.
5. 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.
6. Онацький О. В., Йона Л. Г., Бєлова Ю. В. Криптографічний захист інформації: навч. посіб. з дисципліни "Криптографічний захист інформації". Одеса: ДУІТЗ, 2023. 250 с. електронний варіант.

Допоміжна

1. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p.
2. Остапо С. Е., Євсеєв 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 № 332 від 18.03.2021 року Про затвердження стандарту вищої освіти за спеціальністю 125 «Кібербезпека» для другого (магістерського) 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=Vcld7CMAnNs
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