МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Комп'ютерної інженерії та інноваційних технологій

«ПРИЙНЯТО»
Вченою радою
Міжнародного гуманітарного
університету
Протокол № ____
від «____»_____ 20___

Введено в дію наказом ректора
Міжнародного гуманітарного
університету від 30.08.2024

Ректор _____ К.В. Громовенко

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КРИПТОЛОГІЯ

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

Одеса – 2024

Робоча програма затверджена на засіданні кафедри Комп'ютерної інженерії та інноваційних технологій протокол № 1 від 29.08. 2024 року.

Розробники і викладачі	Контактний тел.	E-mail
доцент кафедри Комп'ютерної інженерії та інноваційних технологій **Онацький Олексій Віталійович**	0503761048	onatsky@meta.ua

Завідувач кафедри комп'ютерної інженерії та інноваційних технологій, доцент _____ Лариса ЙОНА

Гарант освітньої програми _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лариса РАЙЧЕВА

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="2">Кількість кредитів – 4

Загальна кількість годин – 120</td><td>Галузь – 12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="5">Спеціальність – 125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">1-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>1-й</td><td></td></tr>
<tr><td rowspan="11">Мова навчання – українська</td><td rowspan="11">Рівень вищої освіти – другий (магістерський) рівень</td><td colspan="2">Лекції</td></tr>
<tr><td>22 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>22 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>76 год.</td><td>108 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Екзамен</td><td>Екзамен</td></tr>
</table>

Дисципліна **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. Забезпечення знаннями стандартів України та технічних специфікацій для реалізації в засобах криптографічного захисту інформації ДСТУ 7624:2014, ДСТУ 8845:2019, ДСТУ 4145-2002 ДСТУ 7564:2014.

Передумови для вивчення дисципліни. Знання і вміння, отримані студентом при вивченні навчальних дисциплін бакалаврської підготовки. Передбачає підвищення професійної компетентності фахівців з кібербезпеки та сприяє ефективній самореалізації їх.

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

У процесі реалізації програми дисципліни «**Криптологія**» формуються наступні компетентності із передбачених освітньою програмою:

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.

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 захистуінформації 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 дослідженьта 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.

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

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.

Заплановані результати навчання за навчальною дисципліною

Знання

Основні положень законодавчої та нормативно-правової бази України в галузі захисту інформації; структуру криптосистеми з секретним ключем, класифікацію та призначення криптографічних перетворень; принципи побудови асиметричних криптосистем, концепцію криптосистем з відкритим ключем; принципи керування криптографічними ключами та алгоритмів розподілення ключів; методи ідентифікації та автентифікації в комунікаційних системах та основи криптоаналізу.

Уміння

Аналізувати потреби та вимоги користувачів з метою вибору алгоритмів шифрування; вибору режимів роботи блочних алгоритмів шифрування; визначати функції та механізми безпеки до інформації, що підлягає захисту; аналізувати загрози та атаки на безпеку алгоритмів шифрування; використовувати формальні методи аналізу алгоритмів шифрування; виконувати розрахунки необхідних параметрів алгоритмів шифрування; застосовувати схеми електронного підпису; виконувати криптоаналіз несиметричних та симетричних криптосистем.

Навички

Провадити дослідницьку та інноваційну діяльність в сфері криптографічного захисту інформації, а також розвитку технологій створення та використання технічних специфікацій для реалізації в засобах криптографічного захисту інформації; досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного захисту інформації; обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, технологій і процесів в галузі криптографічного захисту інформації на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Криптологія: основні поняття та історичний розвиток

Актуальність проблеми захисту інформації в сучасних системах. Історія криптографії, шлях розвитку криптографічних перетворень від перших відомих криптоалгоритмів до сучасних чинних стандартів. Поняття інформації, види інформації, інформаційні ресурси, класифікація інформаційних ресурсів, властивості інформації конфіденційність, цілісність і доступність, режим доступу до інформації, інформацією з обмеженим доступом, загрози інформації. Способи та засоби захисту інформації. Поняття криптології, криптографія, криптоаналіз, шифрування, зашифровування, розшифровування, інформація, алфавіт, текст, автентифікація, ідентифікації, керування ключами (генерування, зберігання, розподілення), дешифрування, криптографічна система, гамування, крипостійкість, електронний підпис, ключ, геш-функція, атака.

Тема 2. Основи архітектури криптосистем

Типи й класифікація алгоритмів шифрування. Структурна схема симетричних, асиметричних і гібридних криптосистем. Блокові і потокові алгоритми шифрування. Шифри заміни та переставляння. Шифри простої, складної, блокової, поліалфавітної заміни. Поняття розсіювання, перемішування. Синхронні потокові шифри. Умови стійкості шифрів. Поняття стійкості по Шенону. Показники криптостійкості. Принцип шифрування по методу Вермана. Шифри на базі мережі Feistel, modified Feistel, substitution-permutation, unorthodox structure. Методи генерування псевдовипадкових послідовностей чисел. Структура апаратно-програмні засобів. Одноразовий шифрувальний блокнот.

Тема 3. Потокові симетричні шифри. Блокові симетричні шифри

Алгоритм шифрування DES. Схема алгоритму DES. Схема обчислювання функції шифрування алгоритму DES. Схема обчислювання ключів алгоритму DES. Режими роботи DES: Electronic Code Book, Cipher Block Chaining, Cipher Feedback, Output Feedback. Схеми 3DES, DES-EDE2, DES-EEE3, DES-EDE3. Основні характеристики AES. Представлення даних у AES. Стандарт AES: зашифровування, операція SubBytes, операція ShiftRows, операція MixColumns, операція AddRoundKey, схема формування ключів AES, розшифровування AES. Основні характеристики IDEA. Synchronous та asynchronous потокові симетричні шифри. Основні характеристики RC4, Salsa20, ChaCha20. ДСТУ 7624:2014 (Калина) – функція $\pi_l^{(K_t)}$, π'_l, τ_l, ψ_l, $K_l^{(K_v)}$, формування циклових ключів. ДСТУ 8845:2019 (Strumok) – функція ініціалізації INIT, оновлення стану NEXT, ключового потоку STRM, нелінійної підстановки T.

Тема 4. Асиметричні методи шифрування

Модель криптосистеми з відкритим ключем. Поняття односторонньої функції, односторонньої функції з секретом. Алгоритм шифрування RSA, Pascal Paillier, Okamoto-Uchiyama, Шаміра, Ель–Гамаля, Рабіна. Принципи побудови сучасних криптосистем на еліптичних кривих, що базуються на перетвореннях у групі точок еліптичних кривих над полями $GF(p)$, $GF(2^m)$. Математичні основи криптосистем на еліптичних кривих. Еліптична крива над полем $GF(p)$. Вибір параметрів еліптичних кривих. Протокол Мессі–Омури. Алгоритм Ель–Гамаля на еліптичних кривих.

Тема 5. Протоколи керування криптографічними ключами

Генерація ключів, зберігання ключів, розподіл ключів. Життєвий цикл криптографічних ключів. Моделі керування ключами. Методи поширення відкритих ключів. Механізм запиту-відповіді. Механізм оцінки часу. Протокол автентифікації й розподілу ключів для симетричних криптосистем. Інфраструктура відкритих ключів. Протокол Needham-Schroeder. Методи сертифікації відкритих ключів. Протокол для асиметричних криптосистем з використанням сертифікатів відкритих ключів. Прямий обмін ключами між користувачами. Класифікація протоколів розподілу ключів. Властивості протоколів розподілу ключів. Розподіл ключів для класичної криптосистеми Діффі–Хеллмана. Протокол Beller–Yacobi, Шамира, MTI/A0, STS, KEA, MQV, Girault, AKEP2. Апаратні засоби для захисту ключів. Протоколи розподілу ключів на еліптичних кривих. Обмін ключами за схемою Діффі–Хеллмана з використанням еліптичних кривих. Протокол розподілу ключів ECMQV. Протокол обчислення парному зв'язку ключа на еліптичних кривих ECKEP.

Тема 6. Стандарти та схеми електронного підпису

Вимоги до системи електронного підпису. Структура системи електронного підпису України. Узагальнена схема структури відкритих ключів України. Методів побудови схем ЕП. Основні поняття та застосування геш-функції. Геш-функція MD4, MD5, SHA-1, SHA-2: SHA-256, SHA-512. Алгоритм електронного підпису RSA, Ель–Гамаля, DSA, Guillou-Qisquater, Шнорра, Ніберга-Рюпеля, ECDSA, EC-GDSA, ECSS. ДСТУ 4145–2002, ДСТУ ISO/IEC 14888-3:2019. Схеми композиційної, колективної та сліпої підпису на основі ДСТУ 4145–2002. Дослідження анонімності в схемі сліпого підпису.

Тема 7. Теоретична та практична стійкість

Класифікація криптосистем за стійкістю: безумовно стійкі або теоретично не дешифровані, обчислювально стійкі, ймовірно стійкі, обчислювально нестійкі. Поняття атаки на протокол. Класифікація атак на безпеку криптографічних протоколів: спосіб впливу, мети, область застосування, клас протоколу, необхідні ресурси, наявність і характер додаткової інформації. Атаки на криптографічні протоколи підміна, повторне нав'язування повідомлення, затримка передачі повідомлення, атака відбиттям, комбінована атака, атака з використанням підібраних текстів, атака з паралельним сеансом, супротивник у середині, атака з відомим сеансовим ключем, атака з невідомим загальним ключем. Види атак MITM, TF, Replay, STS, PS, KN, UKS на криптографічні протоколи. Формальні методи аналізу протоколів забезпечення безпеки. Формальні системи аналізу на основі логік: логіки довіри, автоматичний доказ теорем. Формальні системи аналізу на основі верифікативної техніки: верифікація на основі автоматів, верифікація на основі перевірки на моделі.

Тема 8. Криптоаналіз шифрів перестановки, одноалфавітної заміни

Поняття ентропії та надлишковості повідомлення, розрахунок відстані єдиного вирішення криптограми. Статистичний аналіз криптограм, статистичні моделі Шеннона і Маркова та їх застосування в криптоаналізі. Основні поняття криптоаналізу. Принципи Керкхоффа, Керкхоффа-Шеннона, Жеверже. Атака на основі шифротексту. Атака на основі відкритого тексту. Атака на основі підібраного відкритого тексту. Криптоаналітична атака з адаптивним вибором відкритого тексту. Криптоаналіз шифрів за методом перестановок, заміни. Криптоаналіз шифру Цезаря. Криптоаналіз шифру стовпцевої перестановки, подвійної перестановки.

Тема 9. Криптоаналіз багатоалфавітної заміни

Універсальні методи криптоаналізу. Метод повного перебору ключа. Атака на ключі. Частотний аналіз. Лінійний аналіз. Різницевий аналіз. Методи безключового читання. Метод

Полларда. Метод колізій для геш-функцій. Метод «зустрічі посередині». Криптоаналіз шифрів за методом багатоалфавітної заміни. Метод Казискі. Перший метод Фрідмана. Другий метод Фрідмана. Криптоаналіз шифру Віжінера. Методи криптоаналізу потокових шифрів.

Тема 10. Диференціальний та лінійний криптоаналіз

Розкриття шифрів блокових алгоритмів. Лінійний криптоаналіз. Приклад лінійного крипто аналізу криптосистеми DES. Знаходження ефективного лінійного статистичного аналогу і обчислення його ймовірності. Визначення ключа (або декількох біт ключа) з використанням ефективного лінійного статистичного аналогу. Диференціальний криптоаналіз. Приклад диференціального крипто аналізу для блоки заміни. Напрямки розвитку лінійного та диференціального крипто аналізу.

Тема 11. Методи факторизації. Методи дискретного логарифмування

Криптоаналіз систем шифрування, заснованих на складності задачі факторизації. Метод Полларда, решета у числовому поля. Криптоаналіз систем шифрування на основі складної задачі дискретного логарифмування. Методи Поліга-Хелмана, «кроків немовляти – кроків велетня», Полларда. Застосування в криптоаналізі сучасних двоключових криптографічних систем. Атаки на криптосистему RSA. Стійкість та криптоаналіз RSA: атака при використовуванні спільного модуля, метод безключового читання RSA, злам RSA на основі дібраного шифртексту, атака Вінера. Методи ECDLP: Exhaustive Search, Pohlig–Hellman, Baby-step Giant-step, λ-метод Полларда, ρ-метод Полларда, індексного обчислення.

Тема 12. Стійкість та криптоаналіз схем електронного підпису

Класифікація атак на схеми електронного підпису: атака на основі відомого відкритого ключа, на основі відомих підписаних повідомлень, проста атака з вибором підписаних повідомлень– спрямована, вибором повідомлень, адаптивна атака з вибором повідомлень, екзистенційна підробка, селективна підробка, універсальна підробка, повне розкриття. Стійкість та криптоаналіз ЕП RSA. Мультиплікативна атака. Атака на спільний модуль. Атака дешифрування ітераціями. Атака повторного використання числа для ЕП DSA, Ель-Гамаля. Стійкість геш-функції. Стійкість до пошуку першого прообразу. Стійкість до пошуку другого прообразу (колізій першого роду). Стійкість до колізій (колізій другого роду). Атаки на хеш паролі – rainbow table (програма RainbowCrack).

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин							
	денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		лекц.	прак.	сам. роб.		лекц.	прак.	сам. роб.
Тема 1. Криптологія: основні поняття та історичний розвиток	10	2		8	10			10
Тема 2. Основи архітектури криптосистем	10		2	8	10			10
Тема 3. Потокові симетричні шифри. Блокові симетричні шифри	10	2	2	6	10	2		8
Тема 4. Асиметричні методи шифрування	10	2	2	6	10			10
Тема 5. Протоколи керування криптографічними ключами	10	2	2	6	10			10
Тема 6. Стандарти та схеми електронного підпису	10	2	2	6	10			10
Тема 7. Теоретична та практична стійкість	10	2	2	6	10	2		8
Тема 8. Криптоаналіз шифрів перестановки, одноалфавітної заміни	10	2	2	6	10		2	8
Тема 9. Криптоаналіз багатоалфавітної заміни	10	2	2	6	10			10
Тема 10. Диференціальний та лінійний криптоаналіз	10	2	2	6	10		2	8
Тема 11. Методи факторизації. Методи дискретного логарифмування	10	2	2	6	10	2		8
Тема 12. Стійкість та криптоаналіз схем електронного підпису	10	2	2	6	10		2	8
Усього годин	**120**	**22**	**22**	**76**	**120**	**6**	**6**	**108**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЕКЗАМЕН								

5. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Основи архітектури криптосистем** ***Питання до підготовки:*** 1. Загальні поняття в галузі криптології 2. Способи та засоби захисту інформації 3. Типи й класифікація алгоритмів шифрування	2	
2	**Тема 2. Блокові симетричні шифри** ***Питання до підготовки:*** 1. Алгоритм шифрування DES 2. Алгоритм шифрування AES 3. ДСТУ 7624:2014	2	
3	**Тема 3. Асиметричні методи шифрування**	2	

	Питання до підготовки: 1. Алгоритм шифрування RSA, Pascal Paillier, Ель–Гамаля, Шаміра 2. Криптосистеми та стандарти на еліптичних кривих 3. Протокол Мессі–Омури, Ель–Гамаля на еліптичних кривих		
4	**Тема 4. Протоколи керування криптографічними ключами** ***Питання до підготовки:*** 1. Протокол Шамира, MTI, KEA, MQV 2. Протокол ECDH з використанням еліптичних кривих 3. Протокол ECKEP	2	
5	**Тема 5. Стандарти та схеми електронного підпису** ***Питання до підготовки:*** 1. Методів побудови схем ЕП 2. Алгоритм електронного підпису Шнорра, Ніберга-Рюпеля 3. ДСТУ ISO/IEC 14888-3:2019	2	
6	**Тема 6. Теоретична та практична стійкість** ***Питання до підготовки:*** 1. Атаки на криптографічні протоколи 2. Класифікація криптосистем за стійкістю 3. Формальні методи аналізу забезпечення безпеки	2	
7	**Тема 7. Криптоаналіз шифрів перестановки, одноалфавітної заміни** ***Питання до підготовки:*** 1. Основні поняття криптоаналізу 2. Криптоаналіз шифру Цезаря 3. Криптоаналіз шифру стовпцевої перестановки	2	
8	**Тема 8. Криптоаналіз багатоалфавітної заміни** ***Питання до підготовки:*** 1. Математичні моделі систем та процесів захисту 2. Методи попарних порівнянь 3. Методи крапкових оцінок	2	2
9	**Тема 9. Криптоаналіз багатоалфавітної заміни** ***Питання до підготовки:*** 1. Метод повного перебору ключа 2. Метод Казискі 3. Криптоаналіз шифру Віжінера	2	
10	**Тема 10. Диференціальний та лінійний криптоаналіз** ***Питання до підготовки:*** 1. Лінійний криптоаналіз криптосистеми DES 2. Диференціальний криптоаналіз блоки заміни	2	2
11	**Тема 11. Методи факторизації. Методи дискретного логарифмування** ***Питання до підготовки:*** 1. Метод Поліга-Хелмана 2. **Метод** Baby-step Giant-step 3. Методи λ-метод Полларда, ρ-метод Полларда	2	
12	**Тема 12. Стійкість та криптоаналіз схем електронного підпису** ***Питання до підготовки:*** 1. Атаки ЕП RSA 2. Атаки на хеш паролі 3. Атаки для ЕП DSA, Ель-Гамаля	2	2
	Всього	**22**	**4**

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. Основи архітектури криптосистем** ***Питання до підготовки:*** 1. Чим відрізняються монограмні шифри від біграмних? 2. Які способи та засоби захисту інформації є? 3. Описати типи й класифікація алгоритмів шифрування.	8	10
2	**Тема 2. Блокові симетричні шифри** ***Питання до підготовки:*** 1. Описати алгоритм шифрування DES. 2. Описати алгоритм шифрування AES. 3. Описати стандарт ДСТУ 7624:2014.	8	10
3	**Тема 3. Асиметричні методи шифрування** ***Питання до підготовки:*** 1. Описати протокол шифрування RSA, Ель–Гамаля, Шаміра. 2. На чому заснована криптографічна стійкість протоколу ECMQV? 3. Які переваги та недоліки алгоритмів на еліптичних кривих?	6	8
4	**Тема 4. Протоколи керування криптографічними ключами** ***Питання до підготовки:*** 1. Описати протокол Діффі–Хеллмана. 2. Які переваги та недоліки протоколу Діффі–Хеллмана? 3. На чому заснована криптографічна стійкість протоколу Діффі–Хеллмана?	6	10
5	**Тема 5. Стандарти та схеми електронного підпису** ***Питання до підготовки:*** 1. Описати методів побудови схем ЕП. 2. Описати виконання електронного підпису алгоритмом RSA. 3. Описати виконання електронного підпису стандартом ДСТУ 4145-2002.	6	10
6	**Тема 6. Теоретична та практична стійкість** ***Питання до підготовки:*** 1. Які атаки на криптографічні протоколи відомі? 2. Визначить класифікацію криптосистем за стійкістю. 3. Формальні методи аналізу забезпечення безпеки	6	10
7	**Тема 7. Криптоаналіз шифрів перестановки, одноалфавітної заміни** ***Питання до підготовки:*** 1. Які методи криптоаналізу шифрів одноалфавітної заміни? 2. Описати метод криптоаналізу шифру Цезаря. 3. У чому полягає криптоаналіз шифрів стовпцевої перестановки?	6	8
8	**Тема 8. Криптоаналіз багатоалфавітної заміни**	6	8

	Питання до підготовки: 1. Які методи криптоаналізу шифрів багатоалфавітної заміни? 2. У чому полягає метод попарних порівнянь? 3. У чому полягає метод крапкових оцінок?		
9	**Тема 9. Криптоаналіз багатоалфавітної заміни** ***Питання до підготовки:*** 1. Описати метод Фрідмана. 2. Описати метод Казискі. 3. У чому полягає криптоаналіз шифру Віжінера?	6	10
10	**Тема 10. Диференціальний та лінійний криптоаналіз** ***Питання до підготовки:*** 1. У чому полягає лінійний криптоаналіз? 2. У чому полягає диференціальний?	6	8
11	**Тема 11. Методи факторизації. Методи дискретного логарифмування** ***Питання до підготовки:*** 1. Описати метод Поліга-Хелмана. 2. Описати метод кроків немовляти – кроків велетня. 3. Описати методи λ-метод Полларда, ρ-метод Полларда	6	8
12	**Тема 12. Стійкість та криптоаналіз схем електронного підпису** ***Питання до підготовки:*** 1. Які недоліки ЕП за системою RSA? 2. У чому полягає стійкість функції гешування? 3. Які переваги ЕП Ель-Гамаля порівняно з ЕП RSA?	6	8
	Всього	**76**	**108**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю		**Складові оцінювання**
Поточний контроль, який здійснюється у ході: проведення практичних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань		**50%**
Підсумковий контроль, який здійснюється у ході проведення іспиту		**50%**
Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, усне повідомлення, індивідуальне опитування; робота у групах; розв`язання ситуаційних завдань, кейсів, практичних завдань, іспит	

Питання до екзамену

У чому полягає сутність шифрів перестановки?
Охарактеризувати різновиди шифрів перестановки.
В чому полягає зміст шифру маршрутної перестановки?
Який метод шифрування називається подвійною перестановкою?
У чому полягає сутність шифрів простої заміни?
Охарактеризувати різновиди шифрів простої заміни.
Чим відрізняються монограмні шифри від біграмних?
Як виконується зашифрування за допомогою шифру Плейфейра?
Як влаштований шифр Цезаря?
Чим відрізняються шифри складної заміни від шифрів простої заміни?
У чому полягає відмінність поміж шифром Гронсфельда й шифром Віженера?
Чому шифри складної заміни мають більшу крипостійкість, аніж шифри простої заміни?
У чому полягає сутність процесу гамування?

Як здійснюється процес зашифрування методом гамування?
Як здійснюється процес розшифрування методом гамування?
Чим потоковий шифр відрізняється від блокового?
Описати алгоритм шифрування криптосистемою Хілла.
Які математичні операції використовуються в алгоритмі DES?
Як здійснюється процес шифрування в алгоритмі DES?
Описати схему обчислення функції шифрування f в алгоритмі DES.
Чим відрізняється процедура розшифрування на боці приймача від процедури зашифрування в алгоритмі DES?
Які існують режими роботи алгоритму DES?
Які слабкі місця алгоритму DES?
Якщо усі перші старші 48 бітів 64-бітового ключа алгоритму DES дорівнюють нулю, то яка ефективна довжина такого ключа?
За допомогою якої операції в алгоритмі DES довжина раундового ключа зменшується до 48 бітів?
Назвати основні параметри (розмір блока, ключа та кількість раундів) для трьох версій стандарту AES.
Які вимоги до архітектури AES?
Які функціональні перетворення використовуються в алгоритмі AES?
Пояснити перетворення SubBytes (State) та InvShiftRows (State).
Пояснити перетворення ShiftRows (State) та InvSubBytes (State).
Пояснити перетворення MixColumns (State) та InvMixColumns (State).
Пояснити перетворення AddRoundKey (State, RoundKey).
Описати раундові перетворення в стандарті AES.
Яке розширене поле використається у стандарті AES?
Опишіть ітераційні перетворення у стандарті AES.
Які існують режими роботи AES?
Яка довжина раундових ключів встановлена у стандарті AES?
Пояснити вибір раундового ключа у стандарті AES.
Пояснити принцип розширення ключа у стандарті AES.
Чим відрізняється зашифрування в останньому раунді алгоритму AES від зашифрування у попередніх раундах?
Яка алгебра використовується в операції MixColumns (State)?
Пояснити процедури оберненого (інверсного) та прямого (еквівалентного) розшифрування у стандарті AES.
Від чого залежить довжина ключа у стандарті AES?
Що забезпечує стійкість криптоалгоритму AES?
Які переваги алгоритму AES над DES?
Які основні параметри (розмір блока, розмір ключа шифру, розмір ключа раунду та кількість раундів) алгоритму IDEA?
Чому операція множення в алгоритмі IDEA виконується за mod$(2^{16} + 1)$, а не за mod 2^{16}?
Які функціональні перетворення використовуються в алгоритмі IDEA?
Пояснити алгоритм формування раундових ключів при зашифруванні та розшифруванні в алгоритмі IDEA.
Які переваги алгоритму IDEA над DES?
Які параметри алгоритму IDEA впливають на його криптостійкість?
На чому ґрунтується криптостійкість алгоритму RSA?
Описати алгоритм зашифрування та розшифрування в RSA.
Яка швидкодія асиметричних криптосистем порівняно з симетричними?
Яке є призначення асиметричних криптосистем?
За якими принципами обирається пара ключів в асиметричній криптосистемі RSA?
Який ключ використовується для зашифрування відкритого повідомлення в криптосистемі RSA?
Який ключ використовується для розшифрування криптограми в криптосистемі RSA?

Яка атака на криптоалгоритм RSA базується на властивості мультиплікативності цього алгоритму?
Описати процедуру генерації ключів в RSA.
Описати атаки на алгоритм RSA.
На чому ґрунтується криптостійкість алгоритму Ель-Гамаля?
Описати послідовність дій при виконані алгоритму Ель-Гамаля.
Пояснити принцип атаки знання вхідного тексту для алгоритму Ель-Гамаля.
Для яких цілей може застосовуватися алгоритм Ель-Гамаля?
Пояснити поняття первісний корінь.
У чому полягає завдання дискретного логарифмування?
Описати послідовність дій при використанні алгоритму Шаміра.
На чому ґрунтується криптостійкість алгоритму Шаміра?
Для яких цілей може застосовуватися алгоритм Шаміра?
Чим відрізняються алгоритм Шаміра від алгоритму Ель-Гамаля?
Які недоліки асиметричних криптосистем?
Що таке комбінований метод зашифрування?
Які переваги використання комбінованого методу зашифрування?
Які відмінності симетричних від асиметричних криптосистем?
Що таке електронний підпис, які його переваги?
Які процедури включає електронний підпис?
Що таке геш-функція?
Яку інформацію містить ЕП?
Які математичні схеми використовуються для генерації пари ключів в алгоритмах ЕП?
Описати алгоритм ЕП на основі алгоритму RSA.
Які недоліки ЕП за системою RSA?
Описати ЕП на основі алгоритму Ель-Гамаля.
Які переваги ЕП Ель-Гамаля порівняно з ЕП RSA?
Описати алгоритм ЕП DSA.
Описати алгоритм ДСТУ 4145-2002.
Описати алгоритм ECDSA.
Описати алгоритм EC-GDSA.
У чому полягає стійкість функції гешування до колізій першого роду?
Дати визначення поля.
Що таке поле Галуа?
Дати приклади простого і розширеного полів.
Що таке мультиплікативна група поля?
Що таке примітивний елемент поля?
Як задається еліптична крива над простим полем?
Як визначити точку еліптичної кривої, протилежну даній?
Які параметри є загальносистемними у стандарті підпису ДСТУ 4145-2002?
Описати процедуру генерації ключів у ДСТУ 4145-2002.
Описати процедуру формування підпису в ДСТУ 4145-2002.
Описати процедуру перевірки підпису в ДСТУ 4145-2002.
Які параметри впливають на криптостійкість підпису ДСТУ 4145-2002?
Які параметри еліптичної кривої необхідно знати для її застосування?
Дати визначення порядку групи точок еліптичної кривої.
Описати алгоритм пошуку точки еліптичної кривої над простим полем.
Як визначити базову точку?
Сформулювати задачу дискретного логарифмування в групі точок еліптичної кривої.
Які атаки можливі на схеми електронного підпису?
Які загрози для схем електронного підпису можливі?
Яку властивість геш-функції характеризує її стійкість до колізій другого роду?
Що таке ключова інформація?

Що таке процес керування ключами?
Описати процес генерування ключів згідно зі стандартом ANSI X9.17.
Описати процес накопичування ключів.
Що таке майстер-ключ?
Які вимоги є до процесу розподілення ключів?
Назвіть методи розподілення ключів.
Що таке ієрархія ключів?
Якими засобами гарантується правомочність сеансу зв'язку?
Що повинен забезпечувати протокол розподілення ключів?
Дати поняття система керування ключами.
Назвати методи розв'язання задачі дискретного логарифмування.
Описати протокол Діффі–Хеллмана.
На чому заснована криптографічна стійкість протоколу Діффі–Хеллмана?
Як впливає розмір простого числа p на криптостійкість протоколу Діффі–Хеллмана?
Як визначити бітовий розмір спільного ключа за вхідними відкритими параметрами?
Які переваги та недоліки протоколу Діффі–Хеллмана?
Яка часова складність протоколу Діффі–Хеллмана?
Навіщо в протоколі Діффі–Хеллмана доцільно передбачати автентифікацію абонентів?
Описати протокол MTI/A(0).
Описати протокол ECMQV.
На чому заснована криптографічна стійкість протоколу ECMQV?
Які переваги протоколу ECMQV?

8. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ ЗДОБУВАЧІВ
(для екзамену)

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 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» 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 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» 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 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.*** Здобувач 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***. Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

- ***«незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 1 до 34 балів.*** Здобувач 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		

9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика: монографія. Харків: Форт, 2012. 880 с.
2. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування: підручник. Київ: ДУТ, 2014. 448 с.
3. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C: 20th Anniversary Edition. Wiley, 2015. 784 p.
4. 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.
5. Йона Л. Г., Онацький О. В., Швець О. В. Системи банківської безпеки: навч. посіб. Одеса: ДУІТЗ, 2022. 192 с.
6. 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.
7. Остапо С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: навч. посіб. Харків: ХНЕУ, 2013. 476 с.
8. Кузнецов Г. В., Фомічов В. В., Сушко С. О. Математичні основи криптографії. Дніпропетровськ: НГУ, 2004. 389 с.
9. Горбенко Ю. І., Горбенко І. Д. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. Харків: Форт, 2010. 608 с.
10. Онацький О. В. Криптографічний захист інформації: навчальний посібник з дисципліни «Криптографічний захист інформації» /О. В. Онацький, Л. Г. Йона, Ю. В. Белова ; Держ. ун-т інтелект. технологій і зв'язку. – Одеса : Астропринт, 2023. – 252 с.
11. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посіб. Запоріжжя: НУ «Запорізька політехніка», 2020. 192 с.

Допоміжна

1. ДСТУ 4145-2002. URI: https://dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798
2. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Мінекономрозвитку України, 2016. 228 с.
3. ДСТУ 8845-2019. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. ДП «УкрНДНЦ», 2019. 228 с.

4. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2010. 863 p.
5. Daemen J., Rijmen V. Design of Rijndael. AES – The Advanced Encryption Standard. Berlin: Springer-Verlag, 2002. 238 p.
6. Бобало Ю.Я. Інформаційна безпека: навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін. Львів: Видавництво Львівської політехніки, 2019. 580 с.
7. Manz O. Encrypt, Sign, Attack. A compact introduction to cryptography. Berlin: Springer Nature, 2022. 134 p.
8. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція гешування. Мінекономрозвитку України, 2015. 39 с.
9. Stavroulakis P., Stamp M. Handbook of Information and Communication Security. Berlin: Springer-Verlag, 2010. 863 p.
10. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. New York: Springer-Verlag, 2004. 358 p.
11. Фільштінський В.А., Бережний А. В. Математичні основи криптографії: конспект лекцій. Суми: Сумський державний університет, 2011. 138 с.

Інформаційні ресурси

1. Сайт Законодавство України. URL: https://zakon.rada.gov.ua/laws.
2. Про електронні довірчі послуги: Закон України. URI: https://zakon.rada.gov.ua/ laws/show/2155-19#Text
3. AES Rijndael Cipher explained as a Flash animation. URI: https://www.youtube.com/watch?v=gP4PqVGudtg
4. DES Animation. URI: https://www.youtube.com/watch?v=Vcld7CMAnNs
5. DES Visualization. URI: https://www.youtube.com/watch?v=XjZmirLc4k4
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
8. Practical TLS. Diffie-Hellman Key Exchange. URI: https://www.youtube.com
9. Practical TLS. RSA Algorithm. URI: https://www.youtube.com
10. How asymmetric (public key) encryption works. URI: https://www.youtube.com/watch?v=E5FEqGYLL0o
11. Robert G. Underwood. Cryptography for Secure Encryption. Springer Nature Switzerland AG, 2022. 324 p.
12. Al Sweigart. Cracking Codes with Python: An Introduction to Building and Breaking Ciphers, 2018. 416 p.