ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФІЗИЧНИЙ ФАКУЛЬТЕТ
Кафедра твердотільної електроніки та інформаційної безпеки

«ЗАТВЕРДЖУЮ»
Декан фізичного факультету
_____ /Лазур В.Ю./
«30» червня 2023 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕТОДИ ПОБУДОВИ ТА АНАЛІЗУ КРИПТОСИСТЕМ

Рівень вищої освіти	Другий (магістерський) рівень
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Освітня програма	Безпека інформаційних і комунікаційних систем
Статус дисципліни	Обов'язова
Мова навчання	Українська

Ужгород 2023

Робоча програма навчальної дисципліни «**Методи побудови та аналізу криптосистем**» для здобувачів вищої освіти галузі знань **12 Інформаційні технології** спеціальності **125 Кібербезпека та захист інформації** освітньої програми **Безпека інформаційних і комунікаційних систем**.

Розробник: Мисло Ю.М., к.ф.-м.н., доцент кафедри твердотільної електроніки та інформаційної безпеки

Пагіря М.М., д.ф.-м.н., професор кафедри твердотільної електроніки та інформаційної безпеки

Робочу програму розглянуто та затверджено на засіданні кафедри твердотільної електроніки та інформаційної безпеки

протокол № 9 від «15» червня 2023 р.

Завідувач кафедри _____ проф. Різак В.М.

Схвалено науково-методичною комісією фізичного факультету

протокол № 10 від «28» червня 2023 р.
Голова науково-методичної комісії _____ Карбованець М.І.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Розподіл годин за навчальним планом	
	Денна форма навчання	Заочна форма навчання
Кількість кредитів ЄКТС – 4	Рік підготовки:	
Загальна кількість годин – 120		
Кількість модулів – 2	Семестр:	
	1-й	
Тижневих годин – для денної форми навчання:	Лекції:	
	24	
	Практичні (семінарські):	
аудиторних – 3	24	
самостійної роботи студента – 4		
Вид підсумкового контролю: екзамен	Лабораторні:	
Форма підсумкового контролю: усна	Самостійна робота:	
	72	

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни “Методи побудови та аналізу криптосистем”є формування у студентів знань і навичок щодо базових питань з криптоаналізу і необхідний для його засвоєння математичний апарат.

Відповідно до освітньої програми, вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

Інтегральна компетентність

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.

Загальні компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-6. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

Загальні компетентності (ЗК) згідно професійного стандарту «Фахівець сфери захисту інформації»

ЗК.01. Здатність діяти соціально відповідально та громадсько свідомо.

ЗК.02. Здатність застосовувати знання у практичних ситуаціях, розв’язувати завдання/задачі та практичні проблеми у професійній діяльності.

ЗК.04. Здатність до абстрактного мислення, аналізу та синтезу, вчитися і бути сучасно навченим.

ЗК.05. Здатність до адаптації та дії в новій ситуації.

ЗК.06. Здатність до вибору стратегії спілкування, працювати в команді.

ЗК.07. Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.

Фахові компетентності

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

КФ3. Здатність досліджувати, розробляти і проводжувати 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.

КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

КФ7. Здатність 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.

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

КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Професійні компетентності (за трудовою дією або групою трудових дій) згідно професійного стандарту «Фахівець сфери захисту інформації»

Б4. Здатність проводити оцінку відповідності (державну експертизу) засобів криптографічного захисту інформації.

Д1. Здатність аналізувати, інтегрувати і використовувати кращі світові практики, стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації.

Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо систем технічного та криптографічного захисту інформації.

Е1. Здатність здійснювати технічне керівництво фахівцями структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки.

Е2. Здатність взаємодіяти із керівництвом і фахівцями технологічних та інших підрозділів підприємства/організації з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту.

Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень.

Е4. Здатність надавати консультативні послуги та технічну допомогу з питань технічного та криптографічного захисту інформації та кіберзахисту.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумов вивчення навчальної дисципліни "Методи побудови та аналізу криптосистем" немає.

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Безпека інформаційних і комунікаційних систем»,** вивчення навчальної дисципліни **"Методи побудови та аналізу криптосистем"** повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (РН)**:**

Програмні результати навчання	Шифр ПРН
Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	РН2
Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	РН3
Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки	РН4

та/або кібербезпеки.	
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.	РН5
Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	РН6
Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	РН7
Досліджувати, розробляти і супроводжу системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	РН8
Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	РН9
Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	РН10
Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	РН11
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.	РН12
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.	РН13
Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	РН14
Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персонолу, партнерів та інших осіб.	РН15
Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи	РН19

кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	
Ставити та вирішувати складні інженерноприкладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	РН20
Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	РН21
Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	РН22
Обґрунтовувати вибір програмно забечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної та/або кібербезпеки на основі сучасних знань у суміжних галузях, науково, технічної та довідкової літератури та іншої доступної інформації.	РН23

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни “Методи побудови та аналізу криптосистем”

Очікувані результати навчання з дисципліни	**Шифр ПРН**
Вміти інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.	РН2
Вміти впроваджувати дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	РН3
Знати застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	РН4
Вміти правильно 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.	РН5
Вміти правильно аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	РН6
Бути здатним обґрунтовувати використання, а також вміти впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або	РН7

кібербезпеки.	
Вміти досліджувати, розробляти і супроводжу системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.	РН8
Вміти аналізувати, розробляти, а також супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.	РН9
Знати забезпечувати безперервність бізнес/операційних процесів, виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.	РН10
Вміти аналізувати, а також контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	РН11
Знати та вміти 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.	РН12
Вміти 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.	РН13
Бути здатним аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.	РН14
Вміти правильно, зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персонолу, партнерів та інших осіб.	РН15
Вміти обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.	РН19
Вміти ставити та вирішувати складні інженерноприкладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.	РН20
Знати використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.	РН21
Вміти планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези,	РН22

обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.	
Вміти правильно обґрунтовувати вибір програмно забечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної та/або кібербезпеки на основі сучасних знань у суміжних галузях, науково, технічної та довідкової літератури та іншої доступної інформації.	РН23

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- поточний контроль;
- модульний контроль;
- підсумковий контроль.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю:

- вибіркове усне опитування;
- фронтальне усне та/або письмове опитування за основними питаннями теми заняття;
- перевірка якості виконання завдань для самостійної роботи, зокрема за конспектами матеріалів;
- оцінювання якості та повноти виконання завдань модульної контрольної роботи.

Форма модульного контролю: виконання модульної контрольної роботи. Кожен модуль оцінюється в 100 балів.

Форма підсумкового семестрового контролю: екзамен. До екзамену допускаються студенти, які виконали модульні контрольні роботи й опрацювали пропущені заняття.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота				Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	50	100
10	10	10	20		

Т1, Т2, Т3, Т4 – Основні поняття криптоаналізу.Джерела відкритого тексту. Надійність шифрів.Криптоаналіз класичних шифроалгоритмів.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота						Модульна контрольна робота	Сума
Т5	Т6	Т7	Т8	Т9	Т10	50	100
10	10	10	10	10	10		

Т5, Т6, Т7, Т8, Т9, Т10 – Криптоаналіз блокових шифрів. Криптоаналіз потокових шифрів. Криптоаналіз систем шифрування з відкритим ключем. Довідна стійкість. Криптоаналіз за побічними каналами. Новітні технології криптоаналізу.

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кількість	Максимальна кількістьбалів (сумарна)	Кількість	Максимальна кількістьбалів (сумарна)
Практичні (семінарські) заняття	4	40	5	50
Модульна контрольна робота	1	60	1	50
Разом	5	100	6	100

Критерії оцінювання модульної контрольної роботи

Форма модульного контролю: Поточно-модульний контроль здійснюється та оцінюється за двома складовими: практичний модульний контроль і лекційний (теоретичний) модульний контроль. Оцінка за практичну складову модульного контролю виставляється за результатами оцінювання знань студента під час практичних занять, виконання індивідуального завдання та проміжного тестового контролю згідно з графіком навчального процесу. Лекційний модульний контроль здійснюється в письмовій формі за відповідними білетами або тестами. Структура білетів (тестів) з модульного контролю аналогічна структурі білетів (тестів) з іспиту. Для підведення підсумків роботи студентів зі змістовного модуля виставляється підсумкова оцінка з поточно-модульного контролю, яка враховує оцінки за практичний модульний контроль і лекційний модульний контроль. Критерії оцінювання модульної контрольної роботи ті ж що і при оцінці знань на екзамені (див. нижче).

Критерії оцінювання підсумкового семестрового контролю

Відповідно до «**Положення про порядок та методику проведення семестрових (курсових) екзаменів і заліків в Ужгородському національному університеті**» (затверджено Наказом Ректора ДВНЗ «УжНУ» No 698/01-17 від 08.05.2015 р.) знання здобувачів оцінюється як з теоретичної, так і з практичної підготовки за такими критеріями:

оцінку «відмінно» (90-100 балів, А) заслуговує здобувач, який: всебічно і глибоко володіє навчально-програмовим матеріалом; вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння в нестандартних ситуаціях; засвоїв основну і ознайомлений з додатковою літературою, яка рекомендована програмою; засвоїв взаємозв'язок основних понять дисципліни та усвідомлює їх значення для професії, яку він набуває; вільно висловлює власні думки, самостійно оцінює різноманітні життєві явища і факти, виявляючи особистісну позицію; самостійно визначає окремі цілі власної навчальної діяльності, виявляє творчі здібності і використовує їх під час вивченнія навчально-програмового матеріалу, проявляє нахил до наукової роботи;

оцінку «добре» (82-89 балів, B) заслуговує здобувач, який: повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, у тому числі застосовує його на практиці, має системні знання в достатньому обсязі відповідно до навчально-програмового матеріалу, аргументовано використовує їх у різних ситуаціях; має здатність до самостійного пошуку інформації, а також до аналізу, постановки і розв'язування проблем професійного спрямування; під час відповіді допустив деякі неточності, які самостійно виправив, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, C) заслуговує здобувач, який: в цілому навчальну програму засвоїв, але відповідає на екзамені з певною кількістю помилок; вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, загалом самостійно застосовувати на практиці, контролювати власну діяльність; опанував навчально-програмовий матеріал, успішно виконав завдання, передбачені програмою, засвоїв основну літературу, яка рекомендована програмою;

оцінку «задовільно» (64-73 бали, D) заслуговує здобувач, який: знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його в майбутній професії; виконує завдання непогано, але зі значною кількістю помилок; ознайомлений з основною літературою, яка рекомендована програмою; допускає на заняттях чи екзамені помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення;

оцінку «задовільно» (60-63 бали, E) заслуговує здобувач, який: володіє основним навчально-програмовим матеріалом в обсязі, необхідному для подальшого навчання і використання його у майбутній професії, а виконання завдань задовольняє мінімальні критерії. Знання мають репродуктивний характер.

оцінка «незадовільно» (35-59 балів, FX) виставляється здобувачу, який: виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань;

оцінка «незадовільно» (35 балів, F) виставляється здобувачу, який: володіє навчальним матеріалом тільки на рівні елементарного розпізнавання і відтворення окремих фактів або не володіє зовсім; допускає грубі помилки при виконанні завдань, передбачених програмою; не може продовжувати навчання і не готовий до професійної діяльності після закінчення університету без повторного вивчення даної дисципліни.

При виставленні оцінки враховуються результати навчальної роботи здобувача протягом семестру.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	ОцінкаECTS	Оцінка за національною шкалою	
		Екзамен та диференційований залік	Залік
90 – 100	**A**	відмінно	Зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з	Не зараховано

		можливістю повторного складання	
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	

За бажанням студента результуюча підсумкова екзаменаційна оцінка може бути визначена як інтегрована оцінка засвоєння всіх тем дисципліни і кількісно дорівнює середньому арифметичному балів, отриманих за кожний модуль.

Результати підсумкового контролю знань заносяться до екзаменаційної відомості.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Програма побудована за модульним принципом. Кожний з модулів є логічно завершеною часткою системи знань та умінь, що визначені як необхідні для формування фахівця.

Змістовий модуль І.

Тема 1. Основні поняття криптоаналізу.

Терміни, визначення та основні ідеї. Принцип Керкгоффса. Симетричні алгоритми. Криптосистеми з відкритим ключем. Модель загрози Долева-Яо. Основні параметри шифрів. Стійкість шифру. Статистичні характеристики шифру. Складність зламу шифру. Складність виконання операцій шифрування та дешифрування. Типи криптоаналітичних атак. Шкода, завдана зламом шифру. Універсальні методи та інструменти криптоаналізу. Частотний аналіз. Метод повного перебору. Атаки, базовані на властивостях ключів. Диференціальний криптоаналіз. Лінійний криптоаналіз. Атаки на криптосистеми з відкритим ключем. Криптоаналіз за допомогою побічних каналів. Метод Полларда. Метод "зустрічі посередині".

Тема 2. Джерела відкритого тексту.

Характеристики відкритих текстів. Абетки відкритих текстів. Повторюваність букв, біграм, n--грам (частотні характеристики тексту). Стійкість та частотні характеристики біграм, триграм та чотириграм осмислених текстів. Тематика відкритих текстів. Внутрішня структура текстів. Імовірнісні моделі відкритих текстів. Посимвольна ймовірнісна модель відкритого тексту. Імовірнісна модель відкритого тексту з незалежними біграмами. Імовірнісна модель відкритого тексту з Марковськими залежними буквами. Нестаціонарні джерела повідомлень. Критерії розпізнавання осмислених відкритих текстів.

Тема 3. Надійність шифрів.

Імовірнісна модель шифру. Теоретико-інформаційна стійкість шифрів. Досконало стійкі шифри. Шифр Вернама за модулем. Деякі відомості з математичної теорії інформації. Невизначеність шифру за ключем. Ентропія та надлишковість мови. Відстань єдиності. Практична стійкість шифрів. Імітостійкість шифрів.

Тема 4. Криптоаналіз класичних шифроалгоритмів.

Шифри простої заміни (буквенні підстановки). Криптоаналіз шифрів простої заміни. Лінійна алгебра над Z_m. Шифр Хілла. Криптоаналіз шифру Хілла за вибраним відкритим текстом. Криптоаналіз шифру Віженера. Елементи криптоаналізу шифрів перестановки. Міра неоднозначності відновлення відкритого тексту за криптограмою.

Змістовий модуль ІІ.

Тема 5. Криптоаналіз блокових шифрів

Принципи побудови блокових шифрів. Мережа Фейстеля. Алгоритм DES. Режими роботи блокових шифрів. Слабкість ключів блокових шифрів. Атака "зустріч посередині". Атаки на зв'язаних ключах. Зсувні атаки. Основна ідея диференціального криптоаналізу.

Диференціальний криптоаналізоднораундового блокового шифру. Загальна схема диференціального криптоаналізу блокових r-раундових шифрів. Спрощений алгоритм S-DES. Ефективність диференціального криптоаналізу. Перспективні подальші напрямки розвинення диференціального криптоаналізу. Бумеранг-атаки. Основні ідеї лінійного криптоаналізу. Ефетивні статистичні лінійні аналоги для одного раунду алгоритму DES. Алгоритм AES. Про криптоаналіз алгоритму AES.

Тема 6. Криптоаналіз потокових шифрів.

Класифікація потокових шифрів. Шифри гамування. Атака з перехрестям шифру. Атака на синхронні потокові шифри за допомогою вставки. Дешифрування шифрів модульного гамування при неякісній гамі. Істинно випадкові числові послідовності. Лінійний конгруентний генератор і його криптоаналіз. Регістр зсуву із зворотнім лінійним зв'язком.

Тема 7. Криптоаналіз систем шифрування з відкритим ключем.

Оцінка обчислювальної складності алгоритмів. Поняття про імовірнісні алгоритми. Класи складності задач. Криптографічна система RSA. Безпека криптосистеми RSA і задача розкладання на множники. Криптоаналіз системи RSA за допомогою факторизації її модуля. Атака "зустріч посередині".Метод безключового читання RSA. Атака на основі використання спільного модуля. Атака на основі використання спільної невеликої відкритої експоненти. Атака Франкліна-Рейтера. Атака Вінера. Елементи теорії граток. Атаки на RSA, базовані на гратках. Часткове розкриття ключа криптосистеми RSA. Криптоаналіз систем шифрування, які ґрунтуються на дискретному логарифмуванні.

Тема 8. Довідна стійкість

Поняття про довідну стійкість криптосистем. Семантична та поліноміальна стійкість криптосистеми. Жорсткість і текстозалежність криптосистем. Стійкість криптосистеми RSA і Ель-Гамаля. Стійкість криптосистеми Голдвассер-Мікалі та деяких сучасних систем шифрування.

Тема 9. Криптоаналіз за побічними каналами.

Класифікація криптоатак за побічними каналами. Атаки за часом. Атаки за потужністю. Атаки за помилками обчислень. Диференціальний аналіз на основі перебоїв. Атаки за електромагнітним випромінюванням. Інші види атак за побічними каналами.

Тема 10. Новітні технології криптоаналізу.

Квантові комп'ютери. Генераторні алгоритми. Нейронні мережі.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Форма навчання: денна					
	Усього	у тому числі				
		лекції	практичні (семінарські)	лабораторні	індивідуальна робота	самостійна робота
1-й семестр						
Змістовий модуль 1						
Тема 1.Основні поняття криптоаналізу.	12	2	2			8
Тема 2. Джерела відкритого тексту.	12	2	2			8
Тема 3. Надійність шифрів.	12	2	2			8
Тема 4. Криптоаналіз класичних шифроалгоритмів.	16	4	4			8
Модульна контрольна робота						
Разом за модуль	52	10	10			32

Змістовий модуль 2						
Тема 5. Криптоаналіз блокових шифрів.	12	2	2			8
Тема 6. Криптоаналіз потокових шифрів.	10	2	2			6
Тема 7. Криптоаналіз систем шифрування з відкритим ключем.	16	4	4			8
Тема 8. Довідна стійкість.	10	2	2			6
Тема 9. Криптоаналіз за побічними каналами.	12	2	2			8
Тема10. Новітні технології криптоаналізу.	8	2	2			4
Модульна контрольна робота						
Разом за модуль	68	14	14			40
Разом за семестр	**120**	**24**	**24**			**72**

6.3. Теми практичних (семінарських, лабораторних) занять

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Характеристики відкритих текстів. Абетки відкритих текстів.	2	
2	Посимвольна ймовірнісна модель відкритого тексту.	2	
3	Імовірнісна модель відкритого тексту з незалежними біграмами.	2	
4	Імовірнісна модель відкритого тексту з Марковськими залежними буквами.	2	
5	Криптоаналіз шифрів простої заміни	2	
6	Шифр Хілла. Криптоаналіз шифру Хілла за вибраним відкритим текстом.	2	
7	Криптоаналіз шифру Віженера.	2	
8	Диференціальний криптоаналіз одноразундового блокового шифру.	2	
9	Шифри гамування. Атака з перехрестям шифру.	4	
10	Криптографічна система RSA.	4	
Разом		**24**	

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Вивчення основних понять криптографічного захисту інформації.	8	
2	Вивчення загальних принципів побудування криптографічних примітивів та типів атак на них.	10	
3	Вивчення принципів побудування симетричних примітивів та диференційного криптоаналізу.	12	
4	Вивчення особливостей блокового шифру AES.	14	
5	Вивчення принципів побудування потокових	14	

	шифрів.		
6	Вивчення принципів побудування алгоритмів з відкритим ключем та атак на них.	14	
	Разом	**72**	

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Технічні засоби: Мультимедійний проектор, інтерактивна дошка.
Обладнання: персональні комп'ютери, ноутбуки, планшети, веб-камери.
Програмне забезпечення: MicrosoftOffice.
Інформаційні ресурси в мережі Інтернет.
Тексти лекцій з дисципліни "Методи побудови та аналізу криптосистем".

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Основна література

1. Сушко С.О.,Кузнецов Г.В.,Фомичова Л.Я., Корабльов А.В. Математичні основи криптоаналізу: Навчальний посібник. -- Дніпропетровськ: Нац. гірн. ун--т, 2010. -- 465 с.
2. Мисло Ю.М., Пагіря М.М., Різак В.М. Математичні основи криптографії. Методичний посібник до практичних занять. Ужгород, УжНУ, 2022. 77 с.
3. Мисло Ю.М., Пагіря М.М., Різак В.М. Елементи математичних методів у криптології. Навчальний посібник для студентів спеціальність "Кібербезпека та захист інформації" Ужгород, Вид-во УжНУ "Говерла", 2023. 136 с.
4. Гапак О. М. Криптоаналіз. Криптографічні протоколи. Ужгород, 2021, 93с.

2. Допоміжна література

1. Мисло Ю., Пагіря М. Оскуляторний інтерполяційний ланцюговий дріб Тіле // Proceedings of the International Geometry Center. 2022. Vol. 15. No. 2. P. 138–160.
2. Мисло Ю., Пагіря М. Криптоаналіз асиметричних ключів алгоритмами ланцюгових дробів // ITSec: Безпека інформаційних технологій: матеріали XII Міжнар. наук.-техн. конф., м. Ужгород, 2-4 трав. 2023 р. К.: НАУ, 2023. С. 36.
3. Кузнецов, О., Кіян, А., Кузнецова, Т. (2020). Удосконалена схема електронного цифрового підпису на основі кодів. *Комп'ютерні науки та кібербезпека*, *1*(1), 49-57. https://doi.org/10.26565/2519-2310-2020-1-05
4. Богуш В. М. Криптографічні застосування елементарної теорії чисел : Навч. посібник / В. М. Богуш, В. А. Мухачов. – К. : Державний ун-т інформаційно-комунікаційних технологій, 2006. – 126 с.
5. Методи та алгоритми симетричної криптографії: Навч. посіб. / Кузнецов О. О., Євсеев С. П., Смірнов О. А., Мелешко Є. В., Король О. Г. – Кіровоград :Вид. КНТУ, 2012. – 316 с.

3. Дистанційні курси та інформаційні ресурси

1. Елетронний ресурс курсу за посиланням https://e-learn.uzhnu.edu.ua/course/view.php?id=3167
2. https://cryptography.org/
3. https://zakon.rada.gov.ua/laws/show/852-15#Text

Додаток 2

Результати перегляду
робочої програми навчальної дисципліни

Робоча програма перезатверджена на 20___ / 20___ н.р. без змін; зі змінами (Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р. Завідувач кафедри _________ ____________
(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р. без змін; зі змінами (Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р. Завідувач кафедри _________ ____________
(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р. без змін; зі змінами (Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р. Завідувач кафедри _________ ____________
(підпис) (Прізвище ініціали)

Робоча програма перезатверджена на 20___ / 20___ н.р. без змін; зі змінами(Додаток ___).
(потрібне підкреслити)

протокол № ___ від «____»__________ 20 ___ р. Завідувач кафедри _________ ____________
(підпис) (Прізвище ініціали)