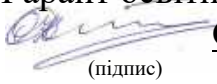
Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№ 503)

ЗАТВЕРДЖУЮ
Гарант освітньої програми

О. Ілляшенко
(підпис) (ініціали та прізвище)
« 29 » серпня 2025 р.

СИЛАБУС *ОБОВ'ЯЗКОВОЇ* НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Прикладна криптологія
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

F
Спеціальність: 125 "Кібербезпека та захист інформації"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Рівень вищої освіти: перший (бакалаврський)

Силабус введено в дію з 01.09.2025 року

Харків 2025 рік

Розробник: Лисицький К.Є., ст.викладач, p.h.d
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри «Комп'ютерних систем, мереж і кібербезпеки»
(назва кафедри)
Протокол № 1 від « 29 » 08 2025 р.

Завідувач кафедри д.т.н., професор В. С. Харченко
(науковий ступінь та вчене звання) (підпис) (ініціали та прізвище)

Погоджено з представником здобувачів освіти:

Ілля МІЦИК
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Лисицький Костянтин Євгенійович

Посада: ст. викладач кафедри комп'ютерних систем, мереж і кібербезпеки

Науковий ступінь: PhD

Вчене звання: старший викладач

Перелік дисциплін, які викладає: Прикладна криптологія, Захист інформації в ІКС, Управління кібербезпекою

Напрями наукових досліджень: криптографічні алгоритми, симетрична криптографія, методи диференційного, лінійний, алгебраїчного криптоаналізу

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	*6*
Мова викладання	*Українська*
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС / кількість годин	*Денна: 4,5 кредити / 135 годин (64 аудиторних, з яких: лекції – 32, лабороторні – 32, СРЗ - 71)*
Види навчальної діяльності	*Лекції, лабораторні заняття, самостійна робота здобувача*
Види контролю	*Поточний контроль, модульний контроль, семестровий контроль – іспит*
Пререквізити	*"Вища математика", "Дискретна математика", "Теоретичні основи криптології".*
Кореквізити	*"Організація та безпека баз даних", "Побудова та кібербезпека інтернету речей", "Захист інформації в інформаційно-комунікаційних системах", "Комплексні системи захисту інформації: проектування, впровадження, супровід", " Кваліфікаційна робота бакалавра"*

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета: володіння науковими методами обґрунтування, вибору та аналізу криптографічних алгоритмів і протоколів, їх використання для вирішення задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах.

Завдання: придбання здобувачами необхідних знань та вмінь в сфері використання моделей та структур даних; формування знань і навичок аналізу та синтезу алгоритмів вирішення задач, що виникають у практиці інженерної та дослідницької діяльності.

Компетентності, які набуваються:

***Інтегральна компетентність*:** Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

***Загальні компетентності (ЗК)*:**

- КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
- КЗ 2. Знання та розуміння предметної області та розуміння професії.
- КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
- КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
- КЗ 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності спеціальності (ФК):

- КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
- КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
- КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).
- КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
- КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання (ПРН):

- ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
- ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
- ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
- ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
- ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
- ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
- ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
- ПРН 13. Аналізувати поректи інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
- ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
- ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
- ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
- ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.

4. Зміст навчальної дисципліни

Змістовий модуль 1.

Тема 1. Класичні криптосистеми з відкритим ключем.

Класичні двоключові криптосистеми RSA, Ель – Гамала. Система відкритого розповсюдження ключів Діфі - Хелмана. Використання великих простих чисел в криптографії. Криптоаналіз двоключових криптосистем.

Алгоритми факторизації.
Тема лекції 1: Вступ в теорію асиметричних криптоперетворень. Концепція криптосистем з відкритим ключем.
Тема лекції 2: Проблема аутентифікації даних і електронний цифровий підпис.
Тема лекції 3: Тестування чисел на простоту, імовірнісні алгоритми з однобічною помилкою.
Тема лекції 4: Побудова великих простих чисел.
Тема лекції 5: Загальні відомості відносно методів криптоаналізу двоключових криптосистем, алгоритми факторизації. Метод Поларда та ρ – Поларда.
Тема лекції 6: Загальні відомості відносно методів криптоаналізу двоключових криптосистем, алгоритми факторизації Ферма та Діксона.
Тема лабораторного заняття 1. Дослідження двоключових алгоритмів RSA та Ель – Гамала.
Тема лабораторного заняття 2. Дослідження алгоритмів факторизації Поларда та ρ – Поларда.
Тема лабораторного заняття 3. Дослідження алгоритмів факторизації Ферма та Діксона.
Самостійна робота здобувачів: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з лабораторної роботи , проходження тестування, формування питань до викладача.
Модульний контроль 1.

Змістовий модуль 2.

Тема 2. Вибрані питання теорії груп, кілець та полів.

Алгебраїчні структури. Кінцеві поля, засновані на кільцях многочленів. Властивості та побудова мінімальних та незвідних многочленів.
Тема лекції 7: Алгебраїчні структури.
Тема лекції 8: Кінцеві поля, засновані на кільцях многочленів.
Тема лекції 9: Кінцеві поля, засновані на кільцях многочленів. Многочлени над скінченими полями.
Тема лекції 10: Кінцеві поля, засновані на кільцях многочленів. Мінімальні многочлени та їх властивості.
Тема лекції 11: Кінцеві поля, засновані на кільцях многочленів. Незвідні многочлени.
Тема лабораторного заняття 4. Дослідження мінімальних многочленів.
Тема лабораторного заняття 5. Дослідження незвідних многочленів.
Самостійна робота здобувачів: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з лабораторної роботи , проходження тестування, формування питань до викладача.
Модульний контроль 2.

Змістовий модуль 3.

Тема 3. Криптосистеми на еліптичних кривих.

Криптосистеми на еліптичних кривих. Математика у групі точок еліптичних кривих. Проблема дискретного логарифмування у групі точок еліптичної кривої.

Тема лекції 12. Вступ в теорію еліптичних кривих.

Тема лекції 13: Еліптичні криві та операції у групах точок еліптичних кривих.

Тема лекції 14: Сліди та базиси розширеного поля. Поліноміальний та нормальний базиси

Тема лекції 15: Оптимальний нормальний базис поля F_2^m.

Тема лекції 16: Проблема дискретного логарифмування у групі точок еліптичної кривої.

Тема лабораторного заняття 6. Дослідження властивостей поліноміального та нормального базисів.

Тема лабораторного заняття 7. Дослідження властивостей оптимального нормального базису поля F_2^m. Пошук добутку двох елементів в оптимальному нормальному базисі.

Тема лабораторного заняття 8. Дослідження операцій у групах точок еліптичних кривих.

Самостійна робота здобувачів: опрацювання матеріалу лекцій, підготовка до лабораторного заняття, формування звіту з лабораторної роботи , проходження тестування, формування питань до викладача

Модульний контроль 3.

5. Методи навчання

Словесні, наочні, практичні; пояснювально-ілюстративні, репродуктивні, частково-пошукові; перевірки та оцінювання знань, умінь і навичок, усного викладу знань, закріплення навчального матеріалу, самостійної роботи з осмислення й засвоєння нового матеріалу.

6. Методи контролю

Проведення поточного контролю, електронного тестування, модульного контролю, підсумковий контроль у вигляді іспиту.

7. Критерії оцінювання та розподіл балів, які отримують здобувачі

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1			
Виконання і захист лабораторних робіт	0...5	3	0...15
Модульний контроль	0…20	1	0…20
Змістовий модуль 2			

Виконання і захист лабораторних робіт	0...5	2	0...10
Модульний контроль	0…20	1	0…20
Змістовий модуль 3			
Виконання і захист лабораторних робіт	0...5	3	0...15
Модульний контроль	0…20	1	0…20
Усього за семестр			**0…100**

Лабораторна робота має бути здана протягом двох тижнів. Для отримання максимальної оцінки повіни здати протягом трьох днів з моменту виконання за розкладом занять; 4 – 6; 3 – 9; 2 – 12; 1-14 днів.
Участь у конференції – 10 балів.
Стаття у фаховому журналі – 20 балів.
Сумарна кількість балів не може бути більш 100.

Семестровий контроль у вигляді іспиту проводиться у разі відмови здобувача від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту здобувач має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних та одного практичного запитань, максимальна кількість за кожне із запитань, складає 30+30+40 балів.

Критерії оцінювання знань студента під час іспиту

Задовільно (60-74). Мати уявлення про принципи побудови симетричних (блочних і потокових) криптографічних алгоритмів та протоколів, що використовуються для забезпечення конфіденційності та автентичності і цілісності повідомлень, криптографічні перетворення у відповідності зі схемами симетричного (блочного та потокового), а також проводити порівняльний аналіз крипостійкості симетричних криптографічних систем.

Добре (75-89). Твердо знати характеристику методів і засобів криптографічного перетворення інформації, показники ефективності криптографічних систем, методи забезпечення автентичності користувачів комп'ютерної мережі, виконувати криптографічні перетворення у відповідності зі схемами симетричного (блочного та потокового) шифрування.

Відмінно (90-100). Мати теоретичні знання та практичні навички щодо побудови та використання систем шифрування та обміну ключами.

Таблиця 8.2 – Шкала оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою
	Іспит
90 – 100	Відмінно
75 – 89	Добре
60 – 74	Задовільно
0 – 59	Незадовільно

8. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Інтерактивний характер курсу передбачає обов'язкове відвідування лабораторних занять. Здобувачі, які за певних обставин не можуть регулярно відвідувати лабораторні заняття, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після пропуску. Здобувачі, які станом на початок екзаменаційної сесії мають понад 70% невідпрацьованих пропущених занять, до відпрацювання не допускаються.

Дотримання вимог академічної доброчесності. Під час вивчення навчальної дисципліни здобувачі мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету «Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

9. Методичне забезпечення

Навчально-методичний комплекс дисципліни розміщений у системі управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки та у системі дистанційного навчання «Ментор».

1. Система управління курсами кафедри комп'ютерних систем, мереж і кібербезпеки [Ел. ресурс]. URL: https://elearn.csn.khai.edu .

2. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=5107 .

11. Рекомендована литература

Базова:

1. Горбенко І. Д. ″Криптографічний захист інформації″. Навч. посібник Харків, ХНУРЕ, 2004 р.
2. Вербіцький О. В. Всуп до криптології. - Львів.: Видавництво науково-технічної літератури, 1998. - 247 с.
3. Криптологія: навч. посібник / М.Н. Курко, П.М. Лісовський, Ю.П. Лісовська. — К.: Видавничий дім «Кондор», 2020. — 248 с.
4. Безпека інформаційних систем і технологій: Навч. посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. – Х. : ХНУ імені В. Н. Каразіна, 2013. – 632 с.
5. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування : Монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво “Форт”, 2012. – 880 с.: іл.
6. 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.: іл.
7. Горбенко Ю. І. Побудування та аналіз систем, протоколів и засобів криптографічного захисту інформації: монографія. Харків: Вид. «Форт»- 2015. 900 с.

Допоміжна:

1. Євсеєв С.П. , Король О.Г. , Шматко О.В Кібербезпека: криптографія з PYTHON. Вид. Новий світ-2000. 2021.- 120 с.
2. Клесов О.І., Елементарна теорія чисел та елементи криптографії, 2017, ТВіМС, Київ, 394 стор.
3. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с
4. Кібербезпека: основи кодування та криптографії : навчальний посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Львів : “Новий Світ-2000”, 2025. – 658 с.

12. Інформаційні ресурси

1. Кваліфікаційний центр інформаційних технологій та кібербезпеки ДержНДІ технологій кібербезпеки [Електронний ресурс] – http://dstszi.gov.ua.
2. КАФЕДРА КОМП'ЮТЕРНИХ СИСТЕМ, МЕРЕЖ І КІБЕРБЕЗПЕКИ [Електронний ресурс] – http://www.csn.khai.edu.