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

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

ЗАТВЕРДЖУЮ

Гарант освітньої програми

_____ Дмитро УЗУН
(підпис) (ім'я та ПРІЗВИЩЕ)

«_31_» _серпня_ 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Методи побудови і аналізу криптосистем
(назва навчальної дисципліни)

Галузь знань: F «Інформаційні технології»
(шифр і найменування галузі знань)

Спеціальність: F5 «Кібербезпека та захист інформації»
(код і найменування спеціальності)

Освітньо-професійна програма:
«Кібербезпека та захист інформації»
(найменування освітньої програми)

Рівень вищої освіти: **другий (магістерський)**

Силабус введено в дію з 01.09.2025

Харків – 2025 р.

Розробник (и): Олійников Р.В., професор, д.т.н., професор
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри
комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол № 1 від « 29 » серпня 2025 р.

Завідувач кафедри д.т.н., професор Вячеслав ХАРЧЕНКО
(науковий ступінь і вчене звання) (підпис) (ім'я та ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

(підпис) Іван ОЛЕФІРЕНКО
(ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

ПІБ: Олійников Роман Васильович

Посада: професор

Науковий ступінь: доктор технічних наук

Вчене звання: професор

Перелік дисциплін, які викладає:

Методи побудови і аналізу криптосистем

Напрями наукових досліджень:

Впровадження сучасних технологій автоматизації циклу розробки та забезпечення стану безпеки IT-проектів

Контактна інформація:

r.oliynykov@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	Денна
Семестр	2
Мова викладання	Українська
Тип дисципліни	Обов’язкова
Обсяг дисципліни: кредити ЄКТС/ кількість годин	3 кредити ЄКТС / 90 годин (48 аудиторних, з яких: лекції – 32, лабораторні – 16; СРЗ – 42)
Види навчальної діяльності	Лекції, лабораторні заняття, самостійна робота
Види контролю	Поточний контроль, модульний контроль, семестровий контроль – залік
Пререквізити	Дисципліна є обов’язковим компонентом освітньої програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності

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

Мета дисципліни – формування у здобувачів вищої освіти системи теоретичних знань та практичних умінь у сфері кібербезпеки з розробки, аналізу та оцінки стійкості сучасних криптографічних систем для забезпечення захисту інформації в умовах кіберзагроз.

Завдання:
– сформувати знання про сучасні сервіси безпеки (конфіденційність, цілісність, автентичність) та математичні методи їх забезпечення;
- забезпечити оволодіння теоретичними основами симетричних (блокових, потокових) та асиметричних криптосистем;
- навчити методам ефективної програмної реалізації криптоалгоритмів (на прикладі Калини та AES) з урахуванням особливостей архітектури комп'ютера;
- сформувати навички проведення криптоаналізу (диференціальний, лінійний аналіз, атаки по побічних каналах);
- навчити оцінювати стійкість криптосистем та обґрунтовувати вибір параметрів безпеки (довжина ключів, режими роботи).

Компетентності, які набуваються:

Інтегральна компетентність:
Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

Загальні компетентності (ЗК):
ЗК1. Здатність до адаптації та дій в новій ситуації.
ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК3. Здатність проводити дослідження на відповідному рівні.
ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК5. Здатність генерувати нові ідеї (креативність).
ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
ЗК7. Здатність приймати обґрунтовані рішення.
ЗК8. Здатність спілкуватися іноземною мовою.

Спеціальні компетентності (СК):
СК2. Здатність розробляти, впроваджувати інтегрувати, аналізувати і використовувати кращі світові практики та стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

СК10. Здатність проводити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або

кібербезпеки.

Програмні результати навчання (ПРН):

ПРН1. 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.

ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН5. 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.

ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

ПРН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.

ПРН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН23. 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.

4. Зміст навчальної дисципліни

МОДУЛЬ 1.
Симетрична криптографія та ефективна реалізація

Тема 1. Вступ до криптології. Історія розвитку. Основні сервіси безпеки: конфіденційність, цілісність, доступність, автентичність, незаперечність.
Тема 2. Класичні шифри та досконала секретність. Шифри заміни та перестановки. Принцип Керкгоффза. Умови побудови досконалого шифру (One-time pad).
Тема 3. Блокові шифри: DES та Triple DES. Структура мережі Фейстеля. Особливості реалізації S-блоків та перестановок. Ефективна програмна реалізація через логічні операції.
Тема 4. Advanced Encryption Standard (AES). Структура SPN. Оптимізація реалізації для 32-бітних платформ за допомогою Т-таблиць.
Тема 5. Режими роботи блокових шифрів. ECB, CBC, CFB, OFB, CTR. Рекомендації щодо вибору режимів для забезпечення конфіденційності та цілісності (GCM, CCM).
Тема 6. Блоковий шифр Калина та режими його роботи.
Тема 7. Потокові шифри та LFSR. Регістри зсуву з лінійним зворотним зв'язком. Приклади: A5/1, Snow 3G, ZUC. Малоресурсна криптографія: шифр PRESENT.

МОДУЛЬ 2.
Асиметричні системи та методи криптоаналізу

Тема 8. Протокол Діффі-Геллмана та RSA. Алгоритми генерації ключів, шифрування та цифрового підпису. Інфраструктура відкритих ключів (PKI)
Тема 9. Хеш-функції та коди автентифікації повідомлень (MAC). Властивості хеш-функцій. Структура Меркла-Дамґарда. Атаки подовження повідомлення. CMAC та GMAC. SHA-2, SHA-3, Купина.
Тема 10. Методи криптоаналізу. Класифікація атак (COA, KPA, CPA, CCA). Диференціальний та лінійний криптоаналіз. Атаки на основі передобчислених таблиць.
Тема 11. Атаки по побічних каналах. Аналіз часу виконання, витоки через кеш-пам'ять, споживання енергії та електромагнітне випромінювання.
Тема 12. Рекомендації щодо безпечного застосування криптографії. Вибір довжини ключів. Вимоги до генераторів псевдовипадкових послідовностей (PRNG)

5. Індивідуальні завдання

Не передбачено

6. Методи навчання

Проведення аудиторних лекцій, лабораторних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.11, 12).

7. Методи контролю

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

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Виконання і захист лабораторних робіт	0…8	3	0…24
Модульний контроль	0…26	1	0…26
Змістовний модуль 2			
Виконання і захист лабораторних робіт	0…8	3	0…24
Модульний контроль	0…26	1	0…26
Усього за семестр			**0…100**

Семестровий контроль (іспит) проводиться у разі відмови здобувача освіти від балів підсумкового контролю й за наявності допуску до іспиту. Під час складання семестрового іспиту здобувач освіти має можливість отримати максимум 100 балів.

Білет для іспиту складається з двох теоретичних запитань (максимальна кількість балів за кожне – 25), та практичного запитання (максимальна кількість балів – 25).

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційний залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	

0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи здобувача освіти протягом семестру

Задовільно (60-74) – Показати мінімум знань та умінь. Захистити не менше 50% від усіх завдань лабораторних занять. Знати основні складові дисципліни. Уміти користуватись інструментальними засобами, що розглянуті в курсі.

Добре (75-89) – Знати та розуміти теоретичну частину, захистити не менше 75% завдань лабораторних занять. Знати ключові концепції кожного модуля курсу. Вміти обґрунтовано впроваджувати потрібні інструментальні засоби відповідно до поставленої задачі.

Відмінно (90-100) – Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти їх застосовувати. Вміти обґрунтовано користуватись інструментальними засобами з метою їх інтеграції при проведенні комплексного дослідження стану кібербезпеки ІТ-рішень.

9. Політика навчального курсу

Відвідування занять. Інтерактивний характер курсу передбачає обов'язкове відвідування лабораторних занять. Здобувачі освіти, які за певних обставин не можуть відвідувати лабораторні заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувачі освіти 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 освіти будуть їх оригінальними дослідженнями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів регламентуються Кодексом етичної поведінки в Національному

аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

1. Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: https://mentor.khai.edu/course/view.php?id=1616

11. Рекомендована література

Базова

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія (підручник). — Харків: ХНУРЕ, Форт, 2012 (878 с.).
2. Горбенко І.Д., Горбенко Ю.І. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика. — Харків, 2010.
3. Wong D. Real-world cryptography. – Simon and Schuster, 2021.
4. Boneh D., Shoup V. A graduate course in applied cryptography, 2022.
5. Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography: Revised Third Edition. 2025

Допоміжна

1. Bernstein D. J. Post-quantum cryptography //Encyclopedia of Cryptography, Security and Privacy. – Cham : Springer Nature Switzerland, 2025.
2. ДСТУ 7624:2014 — Симетричний блоковий шифр «Калина».
3. ДСТУ 7564:2014 — Функція гешування «Купина».
4. NIST Special Publications (SP 800-xxx series) — рекомендації щодо криптографії.
5. OWASP Cryptography Cheat Sheet.
6. MITRE ATT&CK (розділ Cryptographic Failures).

12. Інформаційні ресурси

1. OpenSSL — https://www.openssl.org/
2. NVD — https://nvd.nist.gov/
3. MITRE ATT&CK — https://attack.mitre.org/