Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

РОБОЧА ПРОГРАМА
ОК 8. Методи побудови та аналізу криптосистем

ЗАТВЕРДЖУЮ
Завідувач кафедри

____ ___ Ткач Ю.М.
(підпис) (прізвище та ініціали)

«26» серпня 2025 р.

Розробник: Шелест М.Є., професор, доктор технічних наук; _____
(підпис)

Робочу програму навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання Протокол від « 26 » 08 2025 р. № 6.

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Обов'язкова*
Мова викладання	*Українська*
Рік навчання та семестр	2025-2026 навчальний рік, І семестр, ОП «Кібербезпека» за спеціальністю F5 Кібербезпека та захист інформації галузь знань F Інформаційні технології
Викладач (-і)	Шелест Михайло Євгенович, професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	mishel3141@gmail.com +380674444441 (WhatsApp, Viber)

2. Анотація курсу. «Методи побудови та аналізу криптосистем» є обов'язковою дисципліною

освітньої програми «Кібербезпека» та є фундаментом для майбутньої професійної діяльності. Вивчення дисципліни "*Методи побудови та аналізу криптосистем*" дозволяє студентам оволодіти знаннями та вміннями, які є теоретичним і практичним фундаментом, необхідним для аналізу загроз, що виникають при зберіганні, обробленні та передачі інформації.

Предметом вивчення навчальної дисципліни є методи, алгоритми та засоби криптографічного захисту інформації, методи та засоби криптоаналітичного відтворення захищеної інформації із застосуванням комп'ютерної техніки. Основною метою дисципліни є отримання студентами необхідної компетенції та необхідних знань і умінь щодо оцінки вразливості інформації та інформаційних ресурсів, застосування методів, механізмів, протоколів, алгоритмів та засобів, спрямованих на криптографічний захист інформації на об'єктах інформаційної діяльності, в тому числі в інформаційно-комунікаційних системах, з урахуванням можливих впливів порушників та прогнозу розвитку методів, систем та засобів криптографічного аналізу, стійкості криптографічних систем та безпечності криптографічних протоколів.

Посилання на курс в MOODLE: https://eln.stu.cn.ua/course/view.php?id=2937

3. Мета та цілі курсу. Метою викладання дисципліни є формування компетентності майбутніх спеціалістів в галузі сучасних технологій криптографічного захисту інформації в комп'ютерних системах

Завданнями вивчення навчальної дисципліни є:

· поглиблення теоретичних знань про основні методи криптографічного захисту інформації;
· розгляд математичних моделей симетричних шифрів та їх властивостей;
· удосконалення способів шифрування даних;
· застосування сучасних методів асиметричної криптографії;
· дослідження особливостей криптографічних алгоритмів та криптографічних протоколів;
· ознайомлення з основними положеннями нормативно-правового регулювання у галузі КЗІ;
· розгляд основних напрямків розвитку сучасних систем КЗІ;
· отримати знання про загрози безпеки інформаційних ресурсів, методи та стратегії, що реалізовані для управління процесу усунення несанкціонованого доступу з боку сторонніх користувачів;
· засвоїти методику і напрями використання сучасних криптографічних алгоритмів розподілу ключів і цифрового підпису;
· набути уміння та навички програмування криптографічних алгоритмів.

Під час вивчення дисципліни здобувач вищої освіти (ЗВО) має набути або розширити наступні загальні (КЗ) та фахові (КФ) компетентності, передбачені освітньою програмою спеціальності 125 - Кібербезпека:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.
КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КФ 1. 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.

КФ 8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

4. Результати навчання.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 3 - Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

ПРН 4 - Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

ПРН 5 - 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.

ПРН 13 - 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.

ПРН 20 - Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ПРН 21 - Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

У результаті вивчення навчальної дисципліни ЗВО повинен:

Знати:

- основні криптографічні алгоритми симетричного шифрування;
- основні криптографічні алгоритми асиметричного шифрування та цифрового підпису.
- стандартні криптографічні примітиви та порядок їх застосування при захисті інформації з обмеженим доступом;
- методи аналізу стійкості криптографічних систем та засобів криптографічного захисту інформації;
- типові вимоги до систем та засобів управління ключовими даними;
- базові стандарти в галузі криптографічного захисту інформації.

Вміти:

- працювати з технічною літературою і документацією;
- моделювати (проектувати) алгоритми криптографічних перетворень та елементи криптографічного аналізу на комп'ютері;
- обґрунтувати та пропонувати стандартні криптографічні системи, криптографічні примітиви та протоколи захисту та ресурсів в комп'ютерних системах та комп'ютерних мережах;
- здійснювати загальну оцінку якості криптографічного захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що реалізовані з використанням засобів обчислювальної техніки;
- визначати системи й методи захищеності носіїв інформації;
- створювати засобами стандартного програмного забезпечення елементи захисту інформації.

5. Пререквізити. Дисципліна є складовою частиною Обов'язкових дисциплін циклу професійної підготовки. Вивчення курсу передбачає наявність систематичних та ґрунтовних

знань із курсу – «Основи криптографічного захисту інформації» та «Математичні основи криптографії»

6. Обсяг курсу. Зазначте загальну кількість кредитів, кількість занять та годин самостійної роботи.

Вид заняття	Загальна кількість годин
Лекції	16
Лабораторні заняття	16
Самостійна робота	88
Індивідуальне завдання – розрахункова графічна робота	
Всього кредитів – *вказати кількість кредитів*	4

Форма проведення занять*: лекційні, лабораторні заняття, самостійна робота – з використанням системи дистанційного навчання Moodle, літератури.*

7. Тематика курсу.

Змістовний модуль 1. Основи криптографії: шифри, ключі, криптостійкість

Тема 1. Еволюція криптографії: від класичних шифрів до постквантової доби.

Історія розвитку криптографії: від шифрів Цезаря до Enigma. Основні етапи становлення сучасної криптографії. Поява стандартів: DES, 3DES, AES, роль NIST, NSA. Поява та мотивація постквантової криптографії. Поняття стеганографії та клептографії як суміжних напрямів кібербезпеки безпеки.

Тема 2. Криптостійкість, випадковість і моделі атак.

Поняття криптостійкості. Моделі оцінювання стійкості. Криптоаналітичні атаки: класифікація, моделі зловмисника. Теоретично стійкі шифри. Джерела ключової інформації: випадковість, псевдовипадковість, ентропія. Методи генерування і тестування ПВП.

Тема 3. Симетричні шифри: алгоритми та режими роботи.

Блокові та потокові симетричні шифри. Стандарти AES та ChaCha. Режими шифрування блочних шифрів: порівняння переваг і недоліків, приклади застосування в системах захисту. Типові атаки на симетричні шифри.

Тема 4. Асиметричне шифрування та цифровий підпис: RSA і Ель-Гамаля.

Основи асиметричної криптографії. Алгоритм RSA. Цифровий підпис. Система шифрування Ель-Гамаля. Типові вразливості та атаки на асиметричні схеми.

Змістовний модуль 2. Прикладна криптографія: від ECC до безпечних месенджерів

Тема 5. Еліптичні криві в криптографії: ECC та сучасні алгоритми.

Вступ до еліптичних кривих: базові поняття, рівняння кривої, група точок. Основні операції над точками: додавання, множення. Переваги ECC над RSA: розмір ключів, продуктивність, енергоспоживання. Криптографічні алгоритми на основі ECC: ECDSA, ECDH. Стандарти та реалізації: Curve25519, secp256k1, бібліотеки (OpenSSL, libsodium тощо). Типові атаки на слабкі, нестійкі або неправильно реалізовані криві.

Тема 6. Хешування, автентифікація та контроль цілісності.

Хеш-функції (SHA-2, SHA-3, BLAKE2) — призначення, властивості, приклади. MAC та HMAC: принципи побудови та застосування. Контроль цілісності даних у системах захисту. Атаки на хеш-функції: колізії, атака дня народження, атаки з передзаданим хешем (preimage attacks). Контроль автентичності повідомлень: коди автентифікації, перевірка джерела. Автентичне шифрування: принципи та реалізації (GCM, ChaCha20-Poly1305).

Тема 7. Криптографічні протоколи та приклади впровадження (Diffie–Hellman, TLS, PKI).

Принципи обміну ключами без попереднього секрету. Протоколи узгодження ключів (Diffie–Hellman, Ephemeral DH, ECDH). Аутентифікація сторін у протоколах. Сертифікати X.509. Захист сесій і forward secrecy. Протокол TLS 1.3. Уразливості реалізацій (приклади атак). Верифікація сертифікатів і trusted anchors. Поняття PKI (Public Key Infrastructure). Принципи довіри: ієрархія, "ланцюжок довіри".

Тема 8. Криптографія на практиці: OpenSSH, WireGuard, Signal.

Реальні приклади застосування криптографії в системах захисту: **OpenSSH:** ключовий обмін, алгоритми шифрування, автентифікація користувачів. **WireGuard:** сучасний VPN-протокол, використання Curve25519, обмін ключами, мінімалістична архітектура. **Signal Protocol:** архітектура, криптографічна модель, forward secrecy, self-healing, triple ratchet. Порівняння безпечних месенджерів (Signal, WhatsApp, Telegram): архітектура, шифрування, загрози. Демонстрація базових налаштувань і практичних аспектів використання.

Теми лабораторних робіт

№	Назва теми	Кількість годин
1	Класичні шифри	2
2	Генерація та тестування випадкових послідовностей	2
3	Симетричні алгоритми та режими роботи блочних шифрів	2
4	Асиметрична криптографія: RSA	2
5	Криптографія на еліптичних кривих	2
6	Хешування	2
7	Протоколи узгодження ключів та PKI	2
8	Прикладна криптографія: OpenSSH, GPG, WireGuard, Signal	2
РАЗОМ		**16**

8. Система оцінювання та вимоги (Бажано з прив’язкою до мети курсу. Кожен результат навчання повинен оцінюватися окремо).

Загальна система оцінювання курсу	● Оцінювання курсу відбувається за 100 бальною шкалою. Протягом семестру здобувач вищої освіти може набрати 60 балів: практичні/лабораторні оцінюється в 40 балів, модульні контрольні - 15 балів, відповіді – 5 балів, іспит – 40 балів. Допоміжні бали виставляються за виступи на конференціях, написання тез та статей.
Вимоги до РГР, КР, КП тощо	● Виконання модульних контрольних робіт ● Щонайменше за результатами контролю протягом семестру ЗВО повинен одержати 25 балів
Практичні (лабораторні) заняття	● Модуль за тематичним планом дисципліни та форма контролю: ● Кількість балів - 0…60: ● 1. Виконання практичних/лабораторних робіт 0…40 ● 2. Модульне контрольне завдання 0…8 ● 3. Повнота відповідей на запитання на лекціях 0…2
Умови допуску до підсумкового контролю	Оцінювання курсу відбувається за 100 бальною шкалою. Протягом семестру здобувач вищої освіти може набрати 60 балів: практичні/лабораторні оцінюється в 30 балів, модульні контрольні - 15 балів, відповіді – 5 балів, іспит – 40 балів. Допоміжні бали виставляються за виступи на конференціях, написання тез та статей.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1.		
1	**Повнота відповідей на запитання на лекціях**	**0…2**
2	Результати захисту лабораторних робіт	**0…20**
3	Модульне контрольне завдання	**0…8**
Змістовий модуль 2.		
1	Повнота відповідей на запитання на лекціях	**0…2**
2	Результати захисту лабораторний робіт	**0…20**
3	Модульне контрольне завдання	**0…8**
Усього поточний і проміжний модульний контроль		**0…60**
Семестровий контроль (Екзамен/диференційований залік/залік)		**0…40**
Разом		**0…100**

Шкала оцінювання результатів навчання

<table>
<tr><th rowspan="2">Оцінка в балах</th><th rowspan="2">Оцінка ECTS</th><th colspan="2">Оцінка за національною шкалою (диференційований залік)</th></tr>
<tr><th>для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації</th><th>для заліку</th></tr>
<tr><td>90 – 100</td><td>A (відмінно)</td><td>Відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82-89</td><td>B (дуже добре)</td><td rowspan="2">Добре</td></tr>
<tr><td>75-81</td><td>C (добре)</td></tr>
<tr><td>66-74</td><td>D (задовільно)</td><td rowspan="2">задовільно</td></tr>
<tr><td>60-65</td><td>E (достатньо)</td></tr>
<tr><td>0-59</td><td>FX (незадовільно)</td><td>незадовільно з можливістю повторного складання</td><td>незараховано з можливістю повторного складання</td></tr>
</table>

9. Обладнання та програмне забезпечення (за необхідності**).**

10. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання іспиту під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ "Чернігівська політехніка"». Повторне складання іспиту з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання екзамену всі набрані протягом семестру бали анулюються.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Основна література

1. Козіна Г. Л. Криптографія від історії до сучасних стандартів (2020)
2. Євсєєв С. П. та ін. Кібербезпека: основи кодування та криптографії (2025)
3. Katz, J., Lindell, Y. Introduction to Modern Cryptography (3rd ed., 2025)
4. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
5. Галкін О.В., Шкільняк О.С. Основи криптології: навчальний посібник / Галкін О.В., Шкільняк О.С. – Київ, 2023. – 119 с.

Додаткова література

1. Dholakia, S. Modern Cryptography: The Practical Guide (2024)
2. Boneh, D., Shoup, V. A Graduate Course in Applied Cryptography (2023, draft)

Інформаційні ресурси

1. Laurens Van Houtven, Crypto 101. – [Електронний ресурс]. – Режим доступу: https://www.crypto101.io/
2. Crypto StackExchange. – [Електронний ресурс]. – Режим доступу: https://crypto.stackexchange.com/
3. Ivan Ristić, Cryptography & Security Newsletter. – [Електронний ресурс]. – Режим доступу: https://www.feistyduck.com/newsletter/
4. Cryptography.org. – [Електронний ресурс]. – Режим доступу: https://cryptography.org/
5. Офіційний сайт National Institute of Standards and Technology (NIST) . – [Електронний ресурс]. – Режим доступу: http://www.nist.gov/
6. http://www.rsasecurity.com
7. http://www.eprint.iacr.org
8. http://www.citeseer.ist.psu.edu
9. http://www.ansi.org
10. http://www.cryptography.org
11. http://www.iso.org
12. http://www.linuxiso.org
13. http://www.cryptography.com
14. http://www.springerlink.com
15. http://www.cacr.math.uwaterloo.ca