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

Силабус
ОК 8. Методи побудови та аналізу криптосистем

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю. М._____
(підпис) (прізвище та ініціали)

«26» серпня 2024р.

Розробник (-и): ; Шелест М.Є., професор, доктор технічних наук;
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «26»_серпня_2024 р._№__7__

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	2024-2025 навчальний рік, І семестр, ОПП «Кібербезпека» за спеціальністю 125 Кібербезпека та захист інформації галузь знань 12 Інформаційні технології
Викладач (-і)	Шелест Михайло Євгенович, професор кафедри кібербезпеки та математичного моделювання, доктор технічних наук. професор
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	mishel3141@gmail.com +380674444441 (WhatsApp, Viber) +38099 518 1852 E-mail: mara.a.snnk@gmail.com

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.

КЗ 4. Здатність оцінювати та забезпечувати якість оцінюваних робіт.

КЗ 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

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 3. Здатність досліджувати розробляти і супроводжувати методи та засоби інформаційної безпеки та/ або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

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.

КФ 10. 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.

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

ПРН 8 - Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

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 денна/заочна
Лекції	16/6
Лабораторні заняття	16/6
Самостійна робота	88/108
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.

Змістовий модуль 1. Опис сучасних симетричних систем

Тема 1. Основи теорії секретних систем (конфіденційності).

Основні поняття криптології. Криптографічні перетворення, класифікація та основні властивості. Основні послуги криптографічних систем захисту інформації. Математичні моделі джерел відкритих повідомлень та криптограм. Загальні умови реалізації та класифікація крипто аналітичних атак. Теоретично (безумовно) стійкі криптографічні системи (шифри) та умови їх реалізації.

Тема 2. Симетричні криптографічні перетворення та їх властивості.

Симетричні перетворення, класифікація та їх властивості. Методи оцінки криптографічної стійкості симетричних крипто перетворень. Блокові симетричні шифри та їх властивості. Потокові симетричні шифри та їх властивості. Сучасні шифри (AES, ChaCha), шрифти Східної Європи (ГОСТ 28147, «Калина», «Струмок». Модель криптографічної захищеної телекомунікаційної системи на основі застосування блокових симетричних шифрів. Модель криптографічної захищеної інформаційно-телекомунікаційної системи на основі застосування потокових симетричних шифрів.

Тема 3. Джерела ключів та ключової інформації, вимоги до них.

Джерела ключів та ключової інформації, вимоги до них. Випадкові та псевдовипадкові послідовності та їх властивості. Генерування випадкових та псевдовипадкових послідовностей. Критерії та показники оцінки властивостей випадкових послідовностей. Вимоги відносно необоротності, непередбачуваності, нерозрізнюваності та складності генерування ключів та ключової інформації.

Змістовний модуль 2. Асиметричні криптосистеми

Тема 4. Вступ в теорію асиметричних криптоперетворень.

Асиметричні крипто перетворення. Класифікація та загальна характеристика.

Асиметричні перетворення в групі точок еліптичних кривих та гіпереліптичних кривих, їх основні властивості. Направлені шифри, що реалізуються в групі точок еліптичних кривих. Оцінка стійкості та складності криптографічних перетворень в групі точок еліптичних кривих.

Тема 5.

Джерела ключів асиметричних криптосистем та вимоги до них. Двох ключові криптографічні (асиметричні) перетворення. Інфраструктура відкритих ключів (PKI). PKI для забезпечення шифрування між клієнтом та сервером в інтернеті. Безпека транспортного рівня для захисту з'єднання між клієнтом і сервером. Центри сертифікації. Ієрархічний принцип довіри в ланцюгах сертифікатів. Джерела ключів асиметричних криптосистем та вимоги до них.

Тема 6. Прикладна криптографія: OPENSSH, WIREGUARD, SIGNAL.

Застосування криптоалгоритмів у реальних протоколах. Особливості протоколу SSH,Wireguard та Signal, який лежить в основі більшості сучасних безпечних месенджерів: Signal, Facebook Messenger, WhatsApp, Google Messages. Налаштування Wireguard VPN.

Тема 7. Квантові комп'ютери та постквантова криптографія.

Принципи квантових обчислень. Загроза квантового комп'ютера. Постквантова криптографія (алгоритми, стандартизація, впровадження та практичне застосування).

Тема 8. Криптографічний аналіз симетричних та асиметричних криптосистем

Методи крипто аналізу в симетричних криптосистемах. Методи брутальної сили та на основі створення колізій. Алгебраїчні методи. Статистичні та ймовірнісні методи.

Методи та алгоритми крипто аналізу асиметричних криптосистем в кільцях, полях та групах точок еліптичних і гіпереліптичних кривих. Оцінка складності та вартості.

Теми лабораторних робіт

№	Назва теми	Кількість годин
1	Лінійний генератор псевдовипадкових чисел. Методика тестування ПВП.	2
2	Симетричні шифри.	4
3	Режими роботи симетричних шифрів.	2
4	Криптографія на еліптичних кривих	2
5	Інфраструктура публічних ключів	2
6	Прикладна криптографія: OpenSSH, Signal, WireGuards	2
7	Частотний криптоаналіз	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

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	Відмінно	Зараховано
82-89	**B** (*дуже добре*)	Добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

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.

1. Галкін О.В., Шкільняк О.С. Основи криптології: навчальний посібник / Галкін О.В., Шкільняк О.С. – Київ, 2023. – 119 с.
2. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
3. Євсеєв С.П. Кібербезпека: основи кодування та криптографії: навчальний посібник / С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 658 с.
4. Євсеєв С.П Кібербезпека: Криптографія з Python: навчальний посібник/ Євсеєв С.П. , Король О.Г. , Шматко О.В.- Харків: Вид. “Новий Світ-2000”, 2021. – 120с.

5. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. – Житомир: Державний університет «Житомирська політехніка», 2021. 120 с.
6. Wong D. Real-World Cryptography. – Manning, 2021. – 400 p.

Допоміжна

1. Stallings W. Cryptography and Network Security: Principles and Practice, 8th edition. Global edition. – Pearson, 2023. – 832 p.
2. Гребенніков В. В. Історія криптології та секретного зв'язку / Гребенніков В. В. — Київ: Вид. «КНТ», 2023. — 800 с.
3. Стасюк, Марта. Елементи математичних основ криптографії: навчальний посібник / Марта Стасюк – Львів : ЛДУ БЖД, 2021. – 216 с.

Інформаційні ресурси

1. http://www.rsasecurity.com
2. http://www.nist.gov
3. http://www.eprint.iacr.org
4. http://www.citeseer.ist.psu.edu
5. http://www.ansi.org
6. http://www.cryptography.org
7. http://www.iso.org
8. http://www.linuxiso.org
9. http://www.cryptography.com
10. http://www.springerlink.com
11. http://www.cacr.math.uwaterloo.ca