ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кафедра кібербезпеки та програмного забезпечення

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СПЕЦІАЛЬНІ РОЗДІЛИ МАТЕМАТИКИ ДЛЯ КІБЕРБЕЗПЕКИ

Розглянуто на засіданні кафедри
Протокол № 9 від 9 лютого 2023 року

м. Кропивницький – 2023

ЗМІСТ

1. Загальна інформація

Назва дисципліни	**Спеціальні розділи математики для кібербезпеки**
Рік викладання	2023-2024 навчальний рік
Розробники	Лисенко Ірина Анатоліївна, кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
Викладач	Лисенко Ірина Анатоліївна, кандидат технічних наук, старший викладач кафедри кібербезпеки та програмного забезпечення http://kbpz.kntu.kr.ua/lysenko-irina/ https://scholar.google.com.ua/citations?user=b5TXV7EAAAAJ&hl=ru&authuser=2 https://orcid.org/0000-0003-4394-4960
Контактний телефон	службовий: (0522)390-449 – робочі дні з 8^{30} до 14^{20} Мобільні телефони / Viber / Telegram надано у описі курсу «Спеціальні розділи математики для кібербезпеки» на сервері дистанційної освіти ЦНТУ. – URL: https://moodle.kntu.kr.ua/course/view.php?id=1078
E-mail:	lisenkoia@kntu.kr.ua
Консультації	*Очні консультації* згідно до затвердженого розкладу консультацій. *Онлайн консультації* засобами електронної пошти, мессенджерів (Facebook-Messenger / Viber / Telegram) у робочі дні

2. Анотація дисципліни

Дисципліна «Спеціальні розділи математики для кібербезпеки» призначена для набуття теоретичних знань та практичних навичок розв'язання задач додаткових розділів математики, які не входять до курсу вищої математики, але використовуються у криптографічних засобах захисту інформації. В курсі розглядаються основи теорії чисел, абстрактної алгебри (теорія груп та скінченних полів) та теорія еліптичних кривих. В якості ілюстрації наводяться деякі основні алгоритми асиметричної криптографії.

3. Мета і завдання дисципліни

Метою викладання дисципліни «Спеціальні розділи математики для кібербезпеки» є набуття здобувачами вищої освіти знань основ алгебри множин, порівнянь, обчислень за модулем, елементів теорії чисел, алгебраїчних структур (підгрупи, групи, кільця, поля) та їх властивостей, еліптичних кривих та формування навичок розв'язання задач і побудови алгоритимів на основі теорії чисел, скінченних полів та еліптичних кривих для використання в криптографічних застосуваннях.

Основними **завданнями** вивчення дисципліни є формування наступних **компетенцій**:

– Знання та розуміння предметної області та розуміння професії.

– Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

– Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

4. Формат дисципліни

Для денної форми навчання:

Викладання курсу передбачає для засвоєння дисципліни традиційні лекційні заняття із застосуванням мультимедійних презентацій у поєднанні з лабораторними заняттями.

Формат очний (*Face to face*)

Для заочної форми навчання:

Під час сесії формат очний (*Face to face*), у міжсесійний період – дистанційний (*online*).

5. Результати навчання

У результаті вивчення дисципліни студент повинен забезпечити наступні **програмні результати навчання**:

– Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення;

– Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

6. Обсяг дисципліни

Ознака дисципліни, вид заняття	**Денна форма навчання**	**Заочна форма навчання**
	Кількість годин	**Кількість годин**
Рекомендації щодо семестру вивчення	4 семестр	4 семестр
Спеціальність	125 «Кібербезпека»	125 «Кібербезпека»
Кількість кредитів / годин	3/90	3/90
Кількість змістових модулів	2	2
Нормативна / вибіркова	вибіркова	вибіркова
лекції	28	4
лабораторні	14	2
самостійна робота	48	84
Вид підсумкового контролю : залік	0	0

7. Пререквізити

Враховуючи послідовність накопичення знань та інформації, дисципліна вивчається після викладання наступних дисциплін: «Вища математика», «Основи комп'ютерних технологій», «Вступ до кібербезпеки».

8. Технічне і програмне забезпечення / обладнання

Для викладання навчальної дисципліни застосовується матеріально-технічна база кафедри кібербезпеки та програмного забезпечення: лекційні заняття проводяться в аудиторії обладнаної мультимедійним проектором Epson EB-X41, лабораторні роботи виконуються у спеціалізованих комп'ютерних лабораторіях з персональними комп'ютерами і мережним устаткуванням (ауд. 501, 507, 508, 517), програмне забезпечення OpenOffice версії 4.1.7 (ліцензія LGPL), онлайновий процесор Google Docs https://docs.google.com/, Google Chrome версії 80.0.3987.162 (ліцензія EULA), система дистанційного навчання Moodle https://moodle.kntu.kr.ua/ версії 4.1.1 (ліцензія GPL), відкрита бездротова мережа Wi-Fi, вільний доступ до Інтернету.

9. Політика дисципліни

Академічна доброчесність:

Очікується, що студенти будуть дотримуватися принципів академічної доброчесності, усвідомлювати наслідки її порушення. Детальніше за посиланням URL : http://www.kntu.kr.ua/doc/dobro.pdf

Відвідування занять

Відвідування занять є важливою складовою навчання. Очікується, що всі студенти відвідають лекції і лабораторні заняття курсу.
Пропущені заняття повинні бути відпрацьовані не пізніше, ніж за тиждень до залікової сесії.

Поведінка на заняттях

Недопустимість: запізнень на заняття, списування та плагіат, несвоєчасне виконання поставленого завдання.

При організації освітнього процесу в Центральноукраїнському національному технічному університеті студенти, викладачі та адміністрація діють відповідно до: Положення про організацію освітнього процесу; Положення про організацію вивчення навчальних дисциплін вільного вибору; Положення про рубіжний контроль успішності і сесійну атестацію студентів ЦНТУ, Кодексу академічної доброчесності ЦНТУ.

10. Навчально-методична карта дисципліни

Тиждень, дата, академічні години	**Тема, основні питання** *(розкривають зміст і є орієнтирами для підготовки до модульного і підсумкового контролю)*	**Форма діяльності (заняття) /формат**	**Матеріали**	**Література, інформаційні ресурси**	**Самостійна робота Завдання, обсяг годин**	**Вага оцінки**	**Термін виконання**
Змістовний модуль 1. Основи модулярної арифметики, теорії чисел, абстрактної алгебри							
Тиж.1 (за розкладом) (2 год.)	**Тема 1. Вступ. Множини, відношення, функції.** Множини. Відношення. Відношення еквівалентності.	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Способи задання множин в мовах програмування (2 год.)	2 бали	Самостійна робота до 1 тижня включно
Тиж.2 (за розкладом) (2 год.)	**Тема 2. Основи теорії подільності цілих чисел.** Позиційна система. числення. Прості числа. Факторизація чисел. Прості числа. Взаємно прості числа. Функція Ейлера. Найбільший спільний дільник двох чисел і алгоритм Евкліда. Найменше спільне кратне. Розширений алгоритм Евкліда	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Гіпотеза Рімана. Функція Мебіуса та її властивості (2 год.)	2 бали	Самостійна робота до 2 тижня включно
Тиж.1,2 (за розкладом) (2 год.)	**Лабораторна робота 1.** НСД. Алгоритм Евкліда та розширений алгоритм Евкліда	Лабораторна робота/ *Face to face*	Методичні рекомендації	[16]	Самостійно опрацювати матеріал до лабораторної роботи 1. (2 год.)	8 балів	Самостійна робота до 2 тижня включно
Тиж.3 (за розкладом) (2 год.)	**Тема 3. Порівняння. Класи лишків.** Повна та зведена система лишків. Теорема Ейлера та теорема Ферма. Модулярні арифметичні операції.	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Алгоритм обчислення генератора мультиплікативної циклічної групи (2 год.)	2 бали	Самостійна робота до 3 тижня включно

Тиж.4 (за розкладом) (2 год.)	**Тема 4. Розв'язання порівнянь першого степеня та систем порівнянь.** Мультиплікативні обернені за модулем. Китайська теорема про залишки. Алгоритм Рівеста-Штайна-Адельмана	Лекція / *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Розв'язання порівнянь із складеним модулем (2 год.)	2 бали	Самостійна робота до 4 тижня включно
Тиж.3,4 (за розкладом) (2 год.)	**Лабораторна робота 2.** Алгоритм RSA	Лабораторна робота / *Face to face*	Методичні рекомендації	[16]	Самостійно опрацювати матеріал до лабораторної роботи 2. (2 год.)	8 балів	Самостійна робота до 4 тижня включно
Тиж.5 (за розкладом) (2 год.)	**Тема 5. Квадратичні порівняння.** Символ Лежандра. Символ Якобі. Квадратичні порівняння за складеним модулем.	Лекція / *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Алгоритм Тонеллі-Шенкса (2 год.)	2 бали	Самостійна робота до 5 тижня включно
Тиж.6 (за розкладом) (2 год.)	**Тема 6. Первісні корені. Індекси (дискретні логарифми).** Експонента. Первісні корені. Індекси за модулями p^n, 2p^n	Лекція / *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Індекси за будь-яким складеним модулем (4 год.)	2 бали	Самостійна робота до 6 тижня включно
Тиж.5,6 (за розкладом) (2 год.)	**Лабораторна робота 3.** Квадратичні лишки	Лабораторна робота / *Face to face*	Методичні рекомендації	[16]	Самостійно опрацювати матеріал до лабораторної роботи 3. (2 год.)	8 балів	Самостійна робота до 6 тижня включно
Тиж.7 (за розкладом) (2 год.)	**Тема 7. Основи алгебри.** Групи. Підгрупи. Абелеві групи. Циклічні групи. Гомоморфізми груп. Нормальні групи. Класи суміжності. Фактор-групи. Теорема Лагранжа	Лекція / *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Групи підстановок (2 год.)	2 бали	Самостійна робота до 7 тижня включно
Тиж.7	**Змістовний контроль №1**	Тест	Тест		Виконати тестові завдання	8 балів	До 7 тижня включно
Максимальна кількість балів за змістовим модулем 1						50 балів	

Змістовний модуль 2. Скінченні поля. Еліптичні криві							
Тиж.8 (за розкладом) (2 год.)	**Тема 8. Кільця. Поля.** Кільце поліномів. Ідеали	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Лінійний векторний простір. Гратка (2 год.)	2 бали	Самостійна робота до 8 тижня включно
Тиж.7,8 (за розкладом) (2 год.)	**Лабораторна робота 4.** Операції над многочленами	Лабораторна робота / *Face to face*	Методичні рекомендації	[16]	Самостійно опрацювати матеріал до лабораторної роботи 4. (2 год.)	8 балів	Самостійна робота до 8 тижня включно
Тиж.9 (за розкладом) (2 год.)	**Тема 9. Скінченні поля.** Скінченні розширення полів. Скінченні поля. Поля незвідних многочленів. Будова скінченних полів. Мінімальні многочлени. Ізоморфізми скінченних полів	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Кругові многочлени. Алгоритм факторизації на кругові многочлени (2 год.)	2 бали	Самостійна робота до 9 тижня включно
Тиж.10 (за розкладом) (2 год.)	**Тема 10. Основні алгоритми для скінченних полів.** Алгоритм Евкліда для многочленів. Розширений алгоритм Евкліда для многочленів. Мультиплікативні обернені. Модулярний степінь для многочленів. Тестування на незвідність.	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Генерування випадкового незвідного многочлена. Обчислення генератора скінченної скінченної циклічної групи. (4 год.)	2 бали	Самостійна робота до 10 тижня включно
Тиж.9,10 (за розкладом) (2 год.)	**Лабораторна робота 5.** Алгоритми для скінченних полів	Лабораторна робота/ *Face to face*	Методичні рекомендації	[16]	Самостійно опрацювати матеріал до лабораторної роботи 5. (2 год.)	8 балів	Самостійна робота до 10 тижня включно
Тиж.11 (за розкладом) (2 год.)	**Тема 11. Еліптичні криві. Класифікація еліптичних кривих.** Еліптичні криві над полем дійсних чисел. Додавання точок еліптичної кривої. Абелева група точок. Порядок групи і порядок точки	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Суперсингулярні еліптичні криві (2 год.)	2 бали	Самостійна робота до 11 тижня включно

Тиж.12 (за розкладом) (2 год.)	**Тема 12. Властивості еліптичних кривих.** Проективні координати. Стистнення точок. Дискримінант та j-інваріант еліптичної кривої	Лекція / *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Несуперсингулярні еліптичні криві (2 год.)	2 бали	Самостійна робота до 12 тижня включно
Тиж.11,12 (за розкладом) (2 год.)	**Лабораторна робота 6**. Еліптичні криві над полем дійсних чисел	Лабораторна робота/ *Face to face*	Методичні рекомендації	[16]	Самостійно опрацювати матеріал до лабораторної роботи 6. (2 год.)	8 балів	Самостійна робота до 12 тижня включно
Тиж.13 (за розкладом) (2 год.)	**Тема 13. Еліптичні криві над простими полями Галуа p>3 та над розширеними полями характеристики 2.** Межі Хассе для порядку кривої. Побудова кривої із заданим порядком. Методи розв'язання проблеми дискретного логарифмування в групі точок еліптичної кривої	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Криптосистеми на еліптичних кривих над числовим скінченним полем. Система Ель-Гамаля (2 год.)	2 бали	Самостійна робота до 13 тижня включно
Тиж.14 (за розкладом) (2 год.)	**Тема 14. Поняття про квантові комп'ютери та квантову криптографію**	Лекція/ *Face to face*	Конспект лекції. Презентація	[1, 3, 4 ,16]	Самостійно опрацювати матеріал: Фізичні основи квантової криптографії (4 год.)	2 бали	Самостійна робота до 14 тижня включно
Тиж.13,14 (за розкладом) (2 год.)	**Лабораторна робота 7**. Еліптичні криві над полем GF(2^n)	Лабораторна робота/ *Face to face*	Методичні рекомендації	[16]	Самостійно опрацювати матеріал до лабораторної роботи 7. (2 год.)	8 балів	Самостійна робота до 14 тижня включно
Тиж.14	**Змістовний контроль №2**	Тест	Тест		Виконати тестові завдання	8 балів	До 14 тижня включно
Максимальна кількість балів за змістовим модулем 2						50 балів	
Максимальна кількість балів за залік						0 балів	

11. Система оцінювання та вимоги

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю, усне опитування, письмовий контроль, тестовий контроль.

Форма підсумкового контролю: залік.

Контроль знань і умінь (поточний і підсумковий) з дисципліни «Спеціальні розділи математики для кібербезпеки» здійснюється згідно з кредитною трансферно-накопичувальною системою організації навчального процесу. Рейтинг студента із засвоєння дисципліни визначається за 100-бальною шкалою. Він складається з рейтингу навчальної роботи (засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи, виконання лабораторних робіт), для оцінювання якої призначається 100 балів, та заліку, максимальна оцінка за який складає 0 балів.

Розподіл балів, які отримують студенти при вивченні дисципліни «Спеціальні розділи математики для кібербезпеки»

Поточний контроль та самостійна робота																													Залік	Сума
Змістовий модуль 1															Змістовий модуль 2															
Т1		Т2		Т3		Т4		Т5		Т6		Т7		ЗК1	Т8		Т9		Т10		Т11		Т12		Т13		Т14		ЗК2		
Л1	ЛР1	Л2	ЛР1	Л3	ЛР2	Л4	ЛР2	Л5	ЛР3	Л6	ЛР3	Л7	ЛР4		Л8	ЛР4	Л9	ЛР5	Л10	ЛР5	Л11	ЛР6	Л12	ЛР6	Л13	ЛР7	Л14	ЛР7			
2	4	2	4	2	4	2	4	2	4	2	4	2	4	8	2	4	2	4	2	4	2	4	2	4	2	4	2	4	8		
50															50														0	100

Примітка: Т1, Т2,…,Т14 – тема, Л1, Л2,..., Л14 – теоретичні (лекційні) заняття; ЛР1, ЛР2,..., ЛР7 – лабораторні заняття; ЗК1, ЗК2 – змістовний модульний контроль

Відповідність шкали оцінювання ЄКТС національній системі оцінювання в Україні та ЦНТУ

Оцінка за шкалою ЄКТС	Визначення	Оцінка		
		За національною системою (екзамен, диф. залік, курс. проект, курс. робота, практика)	За національною системою (залік)	За системою ЦНТУ
A	ВІДМІННО - відмінне виконання лише з незначною кількістю помилок	5 (відмінно)	Зараховано	90-100
B	ДУЖЕ ДОБРЕ - вище середнього рівня з кількома помилками	4 (добре)	Зараховано	82-89
C	ДОБРЕ - в загальному правильна робота з певною кількістю грубих помилок			74-81
D	ЗАДОВІЛЬНО - непогано, але зі значною кількістю недоліків	3 (задовільно)	Зараховано	64-73
E	ДОСТАТНЬО - виконання задовольняє мінімальні критерії			60-63
FX	НЕЗАДОВІЛЬНО - потрібно попрацювати перед тим, як перескласти	2 (незадовільно)	Незараховано	35-59
F	НЕЗАДОВІЛЬНО - необхідна серйозна подальша робота			1-34

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, лабораторні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті:

оцінку «відмінно» (90-100 балів, A) – заслуговує студент, який:

– всебічно, систематично і глибоко володіє навчально-програмовим матеріалом;

– вміє самостійно виконувати завдання, передбачені програмою, використовує набуті знання і вміння у 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, виявив творчі здібності і використовує їх при вивченні навчально-програмового матеріалу, проявив нахил до наукової роботи.

оцінку «добре» (82-89 балів, B) – заслуговує студент, який:

– повністю опанував і вільно (самостійно) володіє навчально-програмовим матеріалом, в тому числі застосовує його на практиці, має системні знання 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 виправляє, добирає переконливі аргументи на підтвердження вивченого матеріалу;

оцінку «добре» (74-81 бал, C) – заслуговує студент, який:

– в загальному роботу виконав, але відповідає на заліку з певною кількістю помилок;

– вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому 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 студент, який:

– знає основний навчально-програмовий матеріал в обсязі, необхідному для подальшого навчання і використання його у майбутній професії;

– виконує завдання, але при рішенні допускає значну кількість помилок;

– ознайомлений з основною літературою, яка рекомендована програмою;

– допускає на заняттях чи заліку помилки при виконанні завдань, але під керівництвом викладача знаходить шляхи їх усунення.

оцінку «задовільно» (60-63 бали, E) – заслуговує студент, 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 студенту, який:

– виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.

оцінку «незадовільно» (35 балів, F) – виставляється студенту, 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.

12. Рекомендована література

Базова

1. Задірака В.К. Комп'ютерна криптологія: Підручник / В.К. Задірака, О.С. Олексюк. – Київ – Тернопіль: Збруч, 2002. – 504 с.
2. Богуш В.М. Криптографічні застосування елементарної теорії чисел: Навч. посібник / В.М. Богуш, В.А. Мухачов – К.: ДУІКТ, 2006. – 126 с.
3. Nigel P. Smart. Cryptography: An Introduction. ISBN 978-0077099879. Publisher: Mcgraw-Hill College (December 30, 2004); eBook (3rd Edtion, 2013), 424 Pages. URI: https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
4. Lidl R., Pilz G. Applied Abstract Algebra. Undergraduate Texts in Mathematics (Second Edition). ISBN 9781475729429, Springer New York, 2013, 488 Pages. URI: https://books.google.com.ua/books?id=8bYUswEACAAJ&hl

Допоміжна

5. Задірака В.К. Комп’ютерна арифметика багаторозрядних чисел у послідовній та паралельній моделях обчислень / В.К. Задірака, А.М. Терещенко. – К.: Наукова думка, 2021. – 152 с.
6. Клесов О.І. Елементарна теорія чисел та елементи криптографії: Підручник. – Київ: ТВіМС, 2016. – 393 с.
7. Математичні основи криптоаналізу: навч. посіб. / С. О. Сушко, Г. В. Кузнецов, Л. Я. Фомичова, А. В. Корабльов ; – Дніпропетровськ: НГУ, 2010. – 465 с.
8. Lidl R., Niederreiter H. Finite Fields: Encyclopedia of Mathematics and Its Applications (Vol. 20). ISBN 9781306148122, Cambridge University Press, 2014, 737 Pages. URI: https://books.google.com.ua/books?id=GcSsoAEACAAJ; https://books.google.com.ua/books?id=xqMqxQTFUkMC&pg=PR3&hl=ru&source=gbs_selected_pages&cad=3#v=onepage&q&f=false.
9. Judson T. W. Abstract Algebra: Theory and Applications. ISBN 9781944325107. Orthogonal Publishing L3c, 2019, 424 Pages. URI: https://books.google.com.ua/books?id=ubcpywEACAAJ
10. Metcalf, L., & Casey, W. (2016). Cybersecurity and Applied Mathematics ([edition missing]). Elsevier Science. Retrieved from https://www.perlego.com/book/1827336/cybersecurity-and-applied-mathematics-pdf (Original work published 2016)
11. Mathematics in Cyber Research Edited By Paul L. Goethals, Natalie M. Scala, Daniel T. Bennett. ISBN 9780367374679. Published February 7, 2022 by Chapman & Hall. 524 Pages. 115 B/W Illustrations: https://www.routledge.com/Mathematics-in-Cyber-Research/Goethals-Scala-Bennett/p/book/9780367374679
12. FIPS 197. [Electronic resource] Advanced encryption standard, 2001. URI: http://csrc.nist.gov/publications/.
13. Kim, Y.-S.; Jang, J.-W.; No, J.-S.; Helleseth, T. On p-ary bent functions defined on finite fields. Mathematical Properties of Sequences and Other Combinatorial Structures. The Springer International Series in Engineering and Computer Science, vol. 726. Springer, Boston, MA, 2002, P. 65–76. DOI: https://doi.org/10.1007/978-1-4615-0304-0_8.
14. Mister, S.; Adams, C. Practical S-box design. Proc. of Workshop in Selected Areas of Cryptography, SAC’96, 1996. P. 61-76. URI: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.40.7715&rep=rep1&type=pdf.
15. Nyberg, K. Differentially uniform mappings for cryptography. Advances in cryptology. Proc. of EUROCRYPT’93, Lecture Notes in Computer Science, Vol. 765, P. 55–65, 1994. DOI: https://doi.org/10.1007/3-540-48285-7_6

Інформаційні ресурси

16. Курс "Спеціальні розділи математики для кібербезпеки" в системі дистанційної освіти ЦНТУ Moodle. Режим доступу: https://moodle.kntu.kr.ua/course/view.php?id=1078
17. Додавання та множення точок на еліптичній кривій https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html