Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 1

МАТЕМАТИЧНІ МЕТОДИ ПОБУДОВИ ТА АНАЛІЗУ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Другий (магістерський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітньо-професійна програма	*Безпека державних інформаційних ресурсів*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*І рік підготовки, весняний семестр*
Обсяг дисципліни	*4 кредити*
Семестровий контроль/ контрольні заходи	*Залік / Модульна контрольна робота*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	
Розміщення курсу	*Google classroom*

Київ 2023

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус освітнього компонента “Математичні методи побудови та аналізу асиметричних криптосистем” складено відповідно до освітньо-професійної програми підготовки здобувачів вищої освіти магістр, є навчальною дисципліною вибіркової професійної підготовки.

Метою навчальної дисципліни є формування у курсантів теоретичних знань та практичних вмінь, які необхідні для виконання обов'язків на посадах у частинах та підрозділах, що займаються проектуванням, розробкою, сертифікацією та ліцензуванням засобів криптографічного захисту інформації в автоматизованих системах, підготувати курсантів до самостійного освоєння сучасних та перспективних технологій аналізу та синтезу асиметричних криптосистем.

Перелік підсилених компетентностей:

КЗ-1: здатність застосовувати знання у практичних ситуаціях;

КЗ-3: здатність до абстрактного мислення, аналізу та синтезу;

КФ1: 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;

КФ2: здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки;

КФ6: здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації;

КФ8: 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;

КФ13: здатність аналізувати, інтегрувати і використовувати кращі світові практики, міжнародні стандарти при розробці криптографічних систем захисту спеціальних інформаційно-комунікаційних систем.

Предметом навчальної дисципліни є основні державні та зарубіжні стандарти криптографічного захисту інформації, практичне використання отриманих знань для синтезу та аналізу асиметричних криптографічних систем.

Програмні результати навчання, на покращення яких спрямована дисципліна:

РН2: інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах;

РН3: провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі;

РН4: застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки;

РН6: аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення;

РН13: 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;

РН20: ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик;

РН22: планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки;

РН26: проводити аналіз та синтез криптографічних алгоритмів та криптографічних протоколів; розробляти рекомендації впровадження інноваційних проектів, використовуючи базові методи дослідницької діяльності.

2. Пререквізити та постреквізитинавчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Успішне вирішення завдань навчальної дисципліни базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті вивчення навчальної дисципліни "Математичні методи побудови та аналізу симетричних криптосистем".

Навчальна дисципліна, яка забезпечуються цією навчальною дисципліною – "Військове стажування".

3. Зміст навчальної дисципліни

Семестр ІІ

Розділ (змістовий модуль) 1. Математичні методи побудови та аналізу асиметричних криптосистем.

Тема 1. **Асиметричні криптосистеми, що базуються на решітках**.

Заняття 1/1. Постквантові асиметричні криптосистеми.
Заняття 1/2. Кільце зрізаних поліномів.
Заняття 1/3. Обчислення у кільці зрізаних поліномів.
Заняття 1/4. Шифросистема NTRU.
Заняття 1/5. Помилки розшифрування у шифросистемі NTRU.
Заняття 1/6. Практичне застосування шифросистеми NTRU.
Заняття 1/7. Решітки в евклідовому просторі.
Заняття 1/8. Шифросистема NTRU та решітки.
Заняття 1/9. Практичне моделювання атак на шифросистему NTRU.
Заняття 1/10. ДСТУ 8961:2019 «Скеля».
Заняття 1/11. Задача LWE.
Заняття 1/12. Практичне застосування алгоритмів розв'язання задачі LWE.
Заняття 1/13. Нижні оцінки складності алгоритмів розв'язання задачі LWE.
Заняття 1/14. Атака "зустріч посередині" на криптосистему NTRU.
Заняття 1/15. Практичне моделювання атаки "зустріч посередині" на шифросистему NTRU.

Тема 2. **Асиметричні криптосистеми, що базуються на блокових кодах**.

Заняття 2/1. Блокові коди: основні поняття.
Заняття 2/2. Застосування блокових кодів для виправлення випадкових помилок.
Заняття 2/3. Практичне дослідження лінійних блокових кодів.
Заняття 2/4. Коди Гоппи.
Заняття 2/5. Декодування блокових кодів.
Заняття 2/6. Практичне застосування алгоритму декодування у найближче кодове слово.
Заняття 2/7. Криптосистема Мак-Еліса І.
Заняття 2/8. Криптосистема Мак-Еліса ІІ.

Заняття 2/9. Практичне використання криптосистеми Мак-Еліса.
Заняття 2/10. Криптосистема Нідеррайтера.
Заняття 2/11. Стійкість криптосистем Мак-Еліса Та Нідеррайтера.
Заняття 2/12. Практичне використання криптосистеми Нідеррайтера.
Заняття 2/13. Постквантова криптосистема Classic McEliece.
Заняття 2/14. Модульна контрольна робота.
Залік

4. Навчальні матеріали та ресурси

Основна література:

1. J. Katz and Y. Lindell. Introduction to Modern Cryptography: Principles and Protocols. CRC Press, 2007.
2. Sakshang H. Security analysis of the NTRUEncrypt public key encryption scheme. – Norwegian Univ. of Sci. and Techn., 2007. – 65 p.
3. Nitaj A. The mathematics of the NTRUEncrypt public key cryptosystem, 2012. –16 p.
4. Howgrave-Graham N., Silverman J.H., Singer A., Whyte W. NAEP: provable security choosing parameters for NTRUEncrypt //http://eprint.iacr.org/2003/172.
5. Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch. NTRU Prime // http://eprint.iacr.org/2016/461.
6. Stehlé D. Euclidean lattices: algorithms and cryptography. Lyon, 2011. URL: https://theses.hal.science/tel-00645387/file/HDR_full.pdf.
7. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів.
8. Siim S. Study of McEliece cryptosystem, 2015. – 19 p.
9. Engelbert D., Overbeck R., Schmidt A. A summary of McEliece-type cryptosystems and their security // http://eprint.iacr.org/2006/162.
10. Post-quantum key exchange - a new hope / E. Alkim et al. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2015/1092
11. Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE / J. Bos et al. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2016/659

Додаткова література:

1. Nigel P. Smart. Cryptography Made Simple. Information Security and Cryptography. URL: https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf
2. Guo Q., Johansson T., Nguyen V. A New Sieving-Style Information-Set Decoding Algorithm // https://eprint.iacr.org/2023/247.
3. Zhang X., Zheng Z., Wang X. A detailed analysis of primal attack and its variants. Science China Information Sciences. 2021. Vol. 65, no. 3. DOI: https://doi.org/10.1007/s11432-020-2958-9.
4. Lyubashevsky V., Peikert C., Regev O. On Ideal Lattices and Learning with Errors over Rings. Journal of the ACM. 2013. Vol. 60, no. 6. P. 1–35. DOI: https://doi.org/10.1145/2535925
5. Ігнатенко С. М. Методи розв’язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифроситем : дис. канд. техн. наук : 05.13.21. Харків, 2021. 179 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу	Кількість годин	
	Всього	у тому числі

			Лекції	Практичні (семінарські) заняття	Лабораторні заняття (комп'ютерний практикум)	СР
Розділ (змістовий модуль) 1. Математичні методи побудови асиметричних криптосистем						
Тема 1	**Асиметричні криптосистеми, що базуються на решітках**	**56**	**16**	**14**	**0**	**26**
Заняття 1/1	Постквантові асиметричні криптосистеми. 1. Перспективи розвитку асиметричної криптографії на тлі появи квантових комп'ютерів. 2. Сучасні постквантові криптосистеми та математичні задачі, на яких базується їхня стійкість. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/2	Кільце зрізаних поліномів. 1. Означення кільця зрізаних поліномів, оборотні елементи кільця, достатня умова оборотності. 2. Алгоритм обчислення оберненого елемента до заданого оборотного елемента кільця зрізаних поліномів. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/3	Обчислення у кільці зрізаних поліномів. 1. Розв'язання задач на арифметичні обчислення в кільці зрізаних поліномів. 2. Розв'язання задач на обчислення обернених елементів у кільці зрізаних поліномів. Основна література: [1 – 11]	4	-	2	-	2
Заняття 1/4	Шифросистема NTRU. 1. Асиметрична шифросистема NTRU: історія створення, призначення, практичні переваги. 2. Формальне означення шифросистеми. Обґрунтування умов, що забезпечують коректність розшифрування. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/5	Помилки розшифрування у шифросистемі NTRU. 1. Ймовірнісна модель функціонування шифросистеми. Нерівність Гефдінга. 2. Аналітичні оцінки ймовірності помилкового розшифрування у шифросистемі NTRU. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/6	Практичне застосування шифросистеми NTRU.	4	-	2	-	2

	1. Розв’язання задач на зашифрування/розшифрування повідомлень у шифросистемі NTRU. 2. Розв’язання задачі вибору параметрів шифросистеми, які забезпечують потрібне значення помилки розшифрування. Основна література: [1 – 11]					
Заняття 1/7	Решітки в евклідовому просторі. 1. Основні поняття теорії решіток. 2. Обчислювально складні задачі у теорії решіток. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/8	Шифросистема NTRU та решітки. 1. Атака Куперсміта-Шаміра й атаки з відомим шифрованим текстом. 2. Взаємозв’язок між стійкістю шифросистеми NTRU та знаходженням коротких векторів у певних решітках. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/9	Практичне моделювання атак на шифросистему NTRU. 1. Розв’язання задач з моделювання атаки Куперсміта-Шаміра. 2. Розв’язання задач з моделювання атаки з відомим шифрованим текстом на шифросистему NTRU. Основна література: [1 – 11]	4	-	2	-	2
Заняття 1/10	ДСТУ 8961:2019 «Скеля». 1. Алгоритми шифрування та інкапсуляції ключів згідно з ДСТУ 8961:2019. 2. Принципи побудови та вибору параметрів зазначених алгоритмів. Основна література: [1 – 11]	4	-	2	-	2
Заняття 1/11	Задача LWE. 1. Обчислювано складна задача LWE та окремі її варіанти. 2. Огляд алгоритмів розв’язання задачі LWE, її зв’язок з решітками. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/12	Практичне застосування алгоритмів розв’язання задачі LWE. 1. Моделювання первинного алгоритму розв’язання задачі LWE. 2. Моделювання дуального алгоритму розв’язання задачі LWE. Основна література: [1 – 11]	4	-	2	-	2
Заняття	Нижні оцінки складності	4	-	2	-	2

1/13	алгоритмів розв’язання задачі LWE. 1. Програмна реалізація нижніх оцінок складності первинного алгоритму розв’язання задачі LWE. 2. Програмна реалізація нижніх оцінок складності дуального алгоритму розв’язання задачі LWE. Основна література: [1 – 11]					
Заняття 1/14	Атака “зустріч посередині” на шифросистему NTRU. 1. Сутність атаки “зустріч посередині”. 2. Швидкі алгоритми сортування та пошуку. Застосування цих алгоритмів до реалізації атаки “зустріч посередині” на шифросистему NTRU. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 1/15	Практичне моделювання атаки “зустріч посередині” на шифросистему NTRU. 1. Розв’язання задач на застосування швидких алгоритмів сортування та пошуку. 2. Розв’язання задач на реалізацію атаки “зустріч посередині” на шифросистему NTRU. Основна література: [1 – 11]	4	-	2	-	2
Тема 2	**Асиметричні криптосистеми, що базуються на блокових кодах**	**56**	**14**	**14**	**-**	**28**
Заняття 2/1	Блокові коди: основні поняття. 1. Означення та способи задання блокових кодів. 2. Метрика Гемінга. Числові параметри блокових кодів. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 2/2	Застосування блокових кодів для виправлення випадкових помилок. 1. Модель системи зв’язку із застосуванням блокових кодів. Поняття двійкового симетричного каналу зв’язку. 2. Поняття коригувальної здатності блокового коду. Взаємозв’язок між кількістю помилок, що виправляє код, та його мінімальною відстанню. Основна література: [1 – 11]	3,5	2	-	-	1,5
Заняття 2/3	Практичне дослідження лінійних блокових кодів. 1. Розв’язання задач на визначення кодів за допомогою твірних та перевірочних матриць. 2. Розв’язання задач на	4	-	2	-	2

	знаходження мінімальної відстані лінійного коду. Основна література: [1 – 11]					
Заняття 2/4	Коди Гоппи. 1. Означення кодів Гоппи, співвідношення між параметрами кодів. 2. Алгоритм реалізації кодування кодами Гоппи. Основна література: [1 – 11]	4	2	-	-	2
Заняття 2/5	Декодування блокових кодів. 1. Поняття алгоритму декодування блокових кодів. 2. Обчислювальна складність задачі декодування кодів загального вигляду. Основна література: [1 – 11]	4	-	2	-	2
Заняття 2/6	Практичне застосування алгоритму декодування у найближче кодове слово. 1. Знаходження найближчих кодових слів за допомогою швидкого перетворення Адамара. 2. Розв'язання практичних задач на декодування за допомогою швидкого перетворення Адамара. Основна література: [1 – 11]	4	-	2	-	2
Заняття 2/7	Криптосистема Мак-Еліса I. 1. Криптосистема Мак-Еліса: історичний огляд та сучасний стан. 2. Формальне означення криптосистеми. Основна література: [1 – 11]	4	2	-	-	2
Заняття 2/8	Криптосистема Мак-Еліса II. 1. Алгоритми формування ключів у криптосистемі Мак-Еліса на основі кодів Гоппи. 2. Алгоритми зашифровування та розшифровування повідомлень у криптосистемі Мак-Еліса на основі кодів Гоппи. Основна література: [1 – 11]	4	2	-	-	2
Заняття 2/9	Практичне використання криптосистеми Мак-Еліса. 1. Розв'язання задач на обчислення відкритих ключів за секретними у криптосистемі Мак-Еліса. 2. Розв'язання задач на зашифрування/розшифрування повідомлень у криптосистемі Мак-Еліса. Основна література: [1 – 11]	4	-	2	-	2
Заняття 2/10	Криптосистема Нідеррайтера. 1. Означення криптосистеми Нідеррайтера. 2. Взаємозв'язок між криптосистемами Мак-Еліса та	3	2	-	-	2

	Нідеррайтера. Основна література: [1 – 11]					
Заняття 2/11	Стійкість криптосистем Мак-Еліса Та Нідеррайтера. 1. Обчислювально складні задачі теорії кодування. 2. Зведення задачі про зламування кодової криптосистеми до задачі декодування певних блокових кодів. Основна література: [1 – 11]	3	2	-	-	2
Заняття 2/12	Практичне використання криптосистеми Нідеррайтера. 1. Розв'язання задач на обчислення відкритих ключів за секретними у криптосистемі Нідеррайтера. 2. Розв'язання задач на зашифрування/розшифрування повідомлень у криптосистемі Нідеррайтера. Основна література: [1 – 11]	4	-	2	-	2
Заняття 2/13	Постквантова криптосистема Classic McEliece. 1. Формальне означення криптосистеми. 2. Принципи вибору параметрів криптосистеми для забезпечення її належної стійкості відносно відомих атак. Основна література: [1 – 11]	4	-	2	-	2
Заняття 2/14	Модульна контрольна робота.	5	-	2	-	3
Разом за розділом		112	30	28	-	54
Залік		8	-	2	-	6
Всього годин		**120**	**30**	**30**	**0**	**60**

6. Самостійна робота курсанта

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до екзамену.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
Розділ (змістовий модуль) 1. Асиметричні криптосистеми, що базуються на решітках		
1	Тема 1. Асиметричні криптосистеми, що базуються на решітках 1. Означення та способи представлення елементів кілець зрізаних поліномів. 2. Означення та алгоритми виконання алгебраїчних операцій у кільцях зрізаних поліномів. 3. Алгоритм обчислення оберненого елементу до заданого оборотного елементу кільця. 4. Алгоритм формування ключів у криптосистемі NTRU. 5. Основні поняття теорії цілочисельних решіток. 6. Важкорозв'язні обчислювальні задачі у теорії решіток. 7. Неформальний взаємозв'язок між стійкістю криптосистеми NTRU та знаходженням коротких векторів у певних решітках. 8. Доведення теореми про зв'язок криптосистеми NTRU з відповідними	28

	решітками. 9. Поняття редукованого базису решітки. 10. Алгоритми LLL та BKZ обчислення редукованих базисів решіток. Оцінки обчислювальної складності алгоритмів. 11. Загальна схема побудови решіточних атак. Обчислювальна складність решіточних атак на NTRU, рекомендації щодо вибору параметрів криптосистеми. 12.Сутність атаки “зустріч посередині”. 13.Можливі варіанти реалізації атаки та нижня межа її обчислювальної складності. 14. Швидкі алгоритми сортування та пошуку. Оцінки складності алгоритмів. 15.Застосування алгоритмів сортування та пошуку при реалізації атаки “зустріч посередині” на криптосистему NTRU. Основна література: [1 – 11]. Додаткова література: [1 – 5].	
2	Тема 2. Асиметричні криптосистеми, що базуються на блокових кодах 1. Означення та способи задання блокових кодів. 2. Метріка Гемінга. Числові параметри блокових кодів. 3. Модель системи зв’язку із застосуванням блокових кодів. Поняття двійкового симетричного каналу зв’язку. 4. Означення кодів Гоппи, співвідношення між параметрами кодів. 5. Алгоритм реалізації кодування кодами Гоппи. 6. Поняття алгоритму декодування блокових кодів. 7. Обчислювальна складність задачі декодування кодів загального вигляду. 8. Формальне означення криптосистеми. 9. Алгоритми формування ключів у криптосистемі Мак-Еліса на основі кодів Гоппи. 10.Алгоритми зашифровування та розшифрування повідомлень у криптосистемі Мак-Еліса на основі кодів Гоппи. 11.Означення криптосистеми Нідеррайтера. 12.Взаємозв’язок між криптосистемами Мак-Еліса та Нідеррайтера. 13.Важкорозв’язні обчислювальні задачі теорії кодування. 14.Зведення задачі про зламування кодової криптосистеми до задачі декодування певних блокових кодів. 15.Підготовка до модульної контрольної роботи. Основна література: [1 – 11]. Додаткова література: [1 – 5].	26
5	Залік	6
6	Всього	60

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Правила поведінки та відвідування навчальних занять передбачають: оволодівати теоретичними знаннями і практичними навичками за обраною спеціальністю; дотримуватися графіка навчального процесу та вимог навчального плану; відвідувати навчальні заняття і виконувати у встановлені терміни усі види завдань, передбачені навчальними планами і програмами; у разі хвороби, несення служби в наряді або у виняткових випадках курсант може бути відсутній на заняттях (з подальшим відпрацюванням пропущеного матеріалу).

По прибутті на навчальні заняття курсанти повинні відключати мобільні телефони; входити і виходити з аудиторії тільки з дозволу керівника заняття і тільки у виняткових випадках; уважно слухати пояснення керівника заняття та відповіді одногрупників; не розмовляти і не займатися сторонніми справами; виконувати всі вказівки керівника навчального заняття, мати на заняттях всі необхідні підручники, зошити, приладдя; підтримувати чистоту і порядок в приміщеннях, дотримуватися морально-етичних правил поведінки і спілкування.

Штрафні та заохочувальні бали.

Сума як штрафних, так і заохочувальних балів не має перевищувати 10 балів:

– за умови гарної підготовки і активної роботи на практичному занятті +1 бал. Одному або двом кращим курсантам на кожному практичному занятті може додаватися як заохочування 1 бал;

– активність на заняттях і систематична робота протягом семестру +1 ... +10;

– участь в олімпіадах, а також ВНО і наукових конференціях +1…+10;

– несвоєчасне виконання або невиконання завдання на самопідготовку –1 бал.

– неготовність, пасивність на заняттях і несистематична робота протягом семестру –1…–10.

Дотримання академічної доброчесності курсантами передбачає: самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання; посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; дотримання норм законодавства про авторське право і суміжні права; надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даної дисципліни можна здійснювати віддалено з використанням технологій дистанційного навчання. В цьому випадку з курсантів вимагається обов'язково наявність справних відеокамери та мікрофону, які мають бути увімкнені на кожному дистанційному занятті.

Навчальна література кредитного модуля є відкритою, не містить відомостей з обмеженим доступом і може бути оприлюднена з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Видами контролю якості навчання курсантів є: поточний, календарний та семестровий контроль.

Оцінювання результатів навчання курсантів здійснюється у відповідності до Методичних рекомендацій до розроблення і застосування рейтингових систем оцінювання курсантів (курсантів) в ІСЗЗІ КПІ ім. Ігоря Сікорського.

Рейтинг курсанта з навчальної дисципліни складається з балів, які він отримує за:

1) МКР (максимальна кількість рейтингових балів: 30 б.);

2) 2 експрес-контролі, кожен з яких оцінюється у 10 балів (максимальна кількість рейтингових балів: 2х10=20);

3) 2 усні відповіді, кожна з яких оцінюється у 10 балів (максимальна кількість рейтингових балів: 2х10=20);

4) 2 індивідуальні доповіді, кожна з яких оцінюється у 15 балів (максимальна кількість рейтингових балів 2х15=30).

Система рейтингових (вагових) балів і критерії оцінювання

1. Модульна контрольна робота.

– "відмінно", повна відповідь (не менше 90% потрібної інформації) – 27-30 балів;

– "добре", достатньо повна відповідь на задачу (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 22-25 балів;

– "задовільно", завдання виконані з помилками та незначні помилки (не менше 60% потрібної інформації) – 18-21 балів;

– "незадовільно", не відповідає вимогам до "задовільно"– 0 балів.

2. Експрес-контроль.

– “відмінно”, виконані всі вимоги до роботи – 9-10 балів;

– “добре”, виконані майже всі вимоги до роботи, або є несуттєві помилки – 7-8 балів;

– “задовільно”, є недоліки щодо виконання вимог до роботи і певні помилки – 1-6 балів;

– “незадовільно”, не відповідає вимогам до “задовільно”– 0 балів.

3. Усна відповідь.

– “відмінно”, повна відповідь (не менше 90% потрібної інформації) – 9-10 балів;

– “добре”, достатньо повна відповідь на задачу (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 7-8 балів;

– “задовільно”, завдання виконані з помилками та незначні помилки (не менше 60% потрібної інформації) – 1-6 балів;

– “незадовільно”, не відповідає вимогам до “задовільно”– 0 балів.

4. Індивідуальна доповідь.

– “відмінно”, повністю розкрите питання та надані повні відповіді на запитання (не менше 90% потрібної інформації) – – 13-15 балів;

– “добре”, достатньо повно розкрите питання та надані відповіді на запитання (не менше 75% потрібної інформації) – 10-12 бали;

– “задовільно”, недостатньо розкрито питання та надані неповні відповіді на запитання (не менше 60% потрібної інформації) – 1-9 бали;

– “незадовільно”, відсутня доповідь та відповіді на запитання – 0 балів.

Залікова контрольна робота оцінюється з 100 балів. Контрольне завдання цієї роботи складається з трьох питань (два теоретичних та одного практичного).

Система оцінювання теоретичного запитання:

– “відмінно”, повна відповідь – 27-30 балів;

– “добре”, достатньо повна відповідь – 22-26 балів;

– “задовільно”, неповна відповідь – 18-21 балів;

– “незадовільно”, незадовільна відповідь – 0 балів.

Система оцінювання практичного запитання:

– “відмінно”, повне, безпомилкове розв’язування завдання – 36-40 балів;

– “добре”, достатньо повне розв’язування завдання – 30-35 балів;

– “задовільно”, завдання виконане з певними недоліками – 24-29 балів;

– “незадовільно”, завдання не виконано – 0 балів.

Умовою атестації є отримання не менше 50% від кількості балів, яку курсант може отримати на час проведення атестації.

Умовою допуску до заліку є: виконання усіх видів робіт та завдань, що передбачені силабусом зазначеного кредитного модуля.

Сума рейтингових балів, отриманих курсантом протягом семестру, переводиться до підсумкової оцінки згідно з таблицею. Якщо сума балів ***менша за 60***, курсант виконує залікову контрольну роботу.

Курсант, який набрав протягом семестру необхідну кількість балів (***$R_c \geq 60$***), отримує залікову оцінку (залік) так званим «автоматом» відповідно до набраного рейтингу. В такому разі до заліково-екзаменаційної відомості вносяться бали R_c та відповідні оцінки.

Курсант, який у семестрі отримав більше 60 балів, може взяти участь у заліковій контрольній роботі з метою підвищення оцінки. У цьому разі бали, отримані ним на заліковій контрольній роботі, є остаточними.

Якщо оцінка за залікову контрольну роботу більша ніж за рейтингом, курсант отримує оцінку за результатами залікової контрольної роботи.

Якщо оцінка за залікову контрольну роботу менша, ніж за рейтингом, викладач застосовує жорстку РСО – попередній рейтинг курсанта з кредитного модуля скасовується і він отримує оцінку з урахуванням результатів залікової контрольної роботи.

Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею 1.

Таблиця 1. Переведення рейтингових балів до оцінок за університетською шкалою

Рейтингові бали, RD, Оцінка за університетською шкалою

Кількість балів	Оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше ніж 60	Незадовільно

9. Додаткова інформація з навчальної дисципліни

Навчальна дисципліна “Математичні методи побудови та аналізу асиметричних криптосистем” складена відповідно до освітньо-професійної програми підготовки здобувачів вищої освіти магістр, є навчальною дисципліною вибіркової професійної підготовки.

Видами навчальних занять є лекції, практичні заняття та самостійна робота.

Навчальна дисципліна “Математичні методи побудови та аналізу асиметричних криптосистем” вивчає фундаментальні загальнотеоретичні та практичні принципи і методи синтезу та аналізу криптографічних схем асиметричних криптосистем.

Лекції є початковими заняттями в темах дисципліни. В них формулюється головне завдання теми та викладаються основні напрямки його вирішення, вивчається конкретизований теоретичний матеріал. Практичні заняття проводяться з метою закріплення знань та поглиблення навичок. На практичних заняттях курсанти отримують навички практичного застосування алгоритмів асиметричних криптосистем а також спеціальних бібліотек для роботи з алгоритмами. Самостійна робота курсантів проводиться без керівництва викладача з метою самостійного закріплення (розширення) знань та поглиблення навичок.