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 СИМЕТРИЧНИХ 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	*Нормативна*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*І рік підготовки, осінній семестр*
Обсяг дисципліни	*3 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 симетричних криптосистем” складено відповідно до освітньо-професійної програми підготовки здобувачів вищої освіти магістр, є нормативною освітньою компонентою, цикл професійної підготовки.

Метою навчальної дисципліни є формування у курсантів теоретичних знань та практичних вмінь в галузі побудови та аналізу симетричних криптосистем, а також у підготовці їх до подальшого самостійного освоєння перспективних методів криптографічного захисту інформації в інформаційних та телекомунікаційних системах.

Перелік набутих 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 симетричних криптографічних систем.

Програмні результати навчання, на формування та 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)

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

3. Зміст навчальної дисципліни

Семестр I

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

Тема 1. Вступ до методів побудови та аналізу симетричних криптосистем.

Заняття 1/1. Призначення, класифікація та загальні принципи побудови симетричних криптосистем.

Заняття 1/2. Означення та елементарні властивості алгебраїчних моделей шифрів.

Заняття 1/3. Аналіз алгебраїчних властивостей табличних шифрів.

Заняття 1/4. Швидкий алгоритм побудови полінома Жегалкіна булевої функції.

Заняття 1/5. Практичне застосування швидкого алгоритму обчислення поліному Жегалкіна.

Заняття 1/6. Ендоморфні, транзитивні та регулярні шифри.

Тема 2. Загальні методи побудови та аналізу блокових шифрів.

Заняття 2/1. Принципи побудови та основні класи сучасних блокових шифрів.

Заняття 2/2. Криптографічні властивості дискретних відображень.

Заняття 2/3. Алгоритм шифрування "Калина" (ДСТУ 7624:2014).

Заняття 2/4. Алгоритм шифрування Rijndael.

Заняття 2/5. Алгоритми обчислення криптографічних параметрів вузлів заміни блокових шифрів I.

Заняття 2/6. Алгоритми обчислення криптографічних параметрів вузлів заміни блокових шифрів II.

Заняття 2/7. Означення стійкого блокового шифру. Лінійний та різницевий методи криптоаналізу блокових шифрів.

Тема 3. Основні компоненти та загальні принципи побудови потокових шифрів.

Заняття 3/1. Скінченні автомати.

Заняття 3/2. Генератори гами.

Заняття 3/3. Практичне обчислення у скінченних полях.

Заняття 3/4. Синхронні потокові шифри.

Заняття 3/5. Примітивні поліноми над скінченним полем.

Заняття 3/6. Практичні задачі обчислення періоду ЛРП над скінченним полем.

Заняття 3/7. Ефективна програмна реалізація ЛРЗ над скінченним полем великого порядку I.
Заняття 3/8. Ефективна програмна реалізація ЛРЗ над скінченним полем великого порядку II.

Тема 4. Загальні методи побудови та аналізу потокових шифрів.

Заняття 4/1. Атака Беббіджа-Голіча.
Заняття 4/2. Атака Куртуа-Майєра.
Заняття 4/3. Складність розв'язання систем лінійних рівнянь над скінченним полем.
Заняття 4/4. Практичне розв'язання систем нелінійних булевих рівнянь методом лініаризації.
Заняття 4/5. Кореляційна атака Зігенталера.
Заняття 4/6. Перетворення Фур'є псевдобулевих функцій.
Заняття 4/7. Кореляційна атака на спрощену версія SNOW 2.0-подібного потокового шифру.
Заняття 4/8. Модульна контрольна робота.
Залік.

4. Навчальні матеріали та ресурси

Основна література:

1. А. М. Олексійчук, О. В. Курінний. Методи криптоаналізу потокових шифрів [Електронний ресурс] : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2023. – 172 с.
2. Вербицький О.В. Вступ до криптології. – Львів: Видавництво науково-технічної літератори, 1998. – 247 с.
3. Algebraic cryptanalysis of symmetric primitives. ECRYPT summare report / http://www.ecrypt.eu.org/documents/D.STVL.7, 31 Juli, 2008.
4. Український стандарт цифрового підпису ДСТУ 4145/2002.
5. FIPS 197, Advanced Encryption Standard.
6. Конюшок С.М., Олексійчук А.М., Скрипник Л.В. Алгебраїчні методи криптоаналізу симетричних криптосистем: сучасний стан та перспективи розвитку // Спеціальні телекомунікаційні системи та захист інформації. – 2010. – Вип. 2 (18). – С. 5–25.
7. Daemen J., Govaerts R., Vandewalle J. Resynchronization Weaknesses in Synchronous Stream Ciphers // Advances in Cryptology – EUROCRYPT'93, Proceedings. – Springer-Verlag. – 1993. – P. 159 – 167.
8. Armknecht F., Lano J., Preneel B. Extending the resynchronization attack // Selected Areas in Cryptography – SAC'04. – Springer-Verlag. – 2004. – P. 19 – 38.
9. Bardet M., Faugere J.-C., Salvy B. Complexity of Groebner basis computation for semi-regular overdetermined sequences over F_2 with solution in F_2. Technical report, 5049, INRIA, 2003 // http://www.inria.fr/rrrt/rr-5049.html.
10. Billet O., Gilbert H. Resistance of SNOW 2.0 against algebraic attacks // Advanced in Cryptology – CT-RSA 2005. – LNCS 3376. – Springer-Verlag. – P. 19 – 28.
11. Ekdahl P., Johansson T. A new version of the stream cipher SNOW. Selected Areas in Cryptography. SAC 2002. LNCS 2295. Springer-Verlag. 2002. P. 47 – 61.

Додаткова література:

1. Швидкий імовірнісний алгоритм оцінювання відстані між зрівноваженою булевою функцією та множиною k-вимірних функцій / С. М. Конюшок, А. М. Олексійчук, А. Ю. Сторожук // Прикладная радиоэлектроника. - 2014. - Т. 13, № 3. - С. 186-191. - Режим доступу: http://nbuv.gov.ua/UJRN/Prre_2014_13_3_4/.
2. Олексійчук А.М., Поремський М.В Метод обґрунтування стійкості SNOW 2.0-подібних потокових шифрів відносно кореляційних атак над полями порядку 2^r // Науково-практичної конференція «Сучасні інформаційні технології та кібербезпека». 15-16 листопада 2018 р., К., 2018, с. 41-43.

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 та аналізу симетричних криптосистем						
Тема 1	**Вступ до методів побудови та аналізу симетричних криптосистем**	**16,5**	**6**	**6**	**0**	**4,5**
Заняття 1/1	Призначення, класифікація та загальні принципи побудови симетричних криптосистем. 1. Призначення та класифікація криптосистем (КС). Симетричні криптосистеми; прикладні задачі, що розв'язуються з їхним використанням. 2. Загальні принципи побудови симетричних КС. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 1/2	Означення та елементарні властивості алгебраїчних моделей шифрів. 1. Формальне означення поняття шифру та пов'язаних з ним понять. 2. Табличний спосіб визначення шифрів. Табличні шифри гамування. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 1/3	Аналіз алгебраїчних властивостей табличних шифрів. 1. Розв'язання простіших задач криптоаналізу табличних шифрів. 2. Розв'язання задач з перевірки транзитивності шифрів. Основна література: [1 – 11]	3	-	2	-	1
Заняття 1/4	Швидкий алгоритм побудови полінома Жегалкіна булевої функції. 1. Рекурсивний алгоритм обчислення полінома Жегалкіна за вектором значень булевої функції. Оцінка складності алгоритму. 2. Розв'язання практичних задач знаходження поліномів Жегалкіна та обчислення степенів нелінійності булевих функцій. Основна література: [1 – 11]	3	-	2	-	1
Заняття 1/5	Практичне застосування швидкого алгоритму обчислення поліному Жегалкіна.	3	-	2	-	1

	1. Особливості програмної реалізації швидкого алгоритму обчислення полінома Жегалкіна БФ. 2. Практичне обчислення степенів нелінійності булевих функцій з використанням зазначеного алгоритму. Основна література: [1 – 11]					
Заняття 1/6	Ендоморфні, транзитивні та регулярні шифри. 1. Означення понять ендоморфного, транзитивного та регулярного шифру. 2. Найважливіші властивості транзитивних та регулярних шифрів. Основна література: [1 – 11]	2,5	2	-	-	0,5
Тема 2	**Загальні методи побудови та аналізу блокових шифрів**	**19,5**	**8**	**6**	**-**	**5,5**
Заняття 2/1	Принципи побудови та основні класи сучасних блокових шифрів. 1. Формальне означення ітераційного блокового шифру та пов'язаних з ним понять. 2. Основні принципи побудови сучасних блокових шифрів. Шифри SPN та шифри Фейстеля. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 2/2	Криптографічні властивості дискретних відображень. 1. Найважливіші криптографічні параметри та властивості булевих функцій. 2. Найважливіші криптографічні параметри підстановок на множині двійкових векторів. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 2/3	Алгоритм шифрування "Калина" (ДСТУ 7624:2014). 1. Алгоритм шифрування "Калина": принципи побудови та математична модель. 2. Аналіз криптографічних властивостей компонент алгоритму шифрування "Калина". Основна література: [1 – 11]	3	-	2	-	1
Заняття 2/4	Алгоритм шифрування Rijndael. 1. Історія створення та загальні принципи побудови алгоритму Rijndael. 2. Опис та криптографічні властивості алгоритму Rijndael. Основна література: [1 – 11]	2,5	2	-	-	0,5

Заняття 2/5	Алгоритми обчислення криптографічних параметрів вузлів заміни блокових шифрів І. 1. Особливості програмної реалізації алгоритму обчислення степеня нелінійності вузла заміни. 2. Практичне застосування зазначеного алгоритму до аналізу алгебраїчних властивостей вузлів заміни шифру “Калина”. Основна література: [1 – 11]	3	-	2	-	1
Заняття 2/6	Алгоритми обчислення криптографічних параметрів вузлів заміни блокових шифрів ІІ. 1. Швидкі алгоритми побудови таблиць різниць та лінійних апроксимацій вузлів заміни. 2. Практичне застосування зазначених алгоритмів до аналізу різницевих та кореляційних властивостей вузлів заміни шифру “Калина”. Основна література: [1 – 11]	3	-	2	-	1
Заняття 2/7	Означення стійкого блокового шифру. Лінійний та різницевий методи криптоаналізу блокових шифрів. 1. Формальне означення стійкого блокового шифру. Розрізнювальні атаки, обґрунтована та практична стійкість блокових шифрів. 2. Лінійний та різницевий методи криптоаналізу блокових шифрів. Аналітичні співвідношення для параметрів, що характеризують стійкість шифрів відносно зазначених методів. Основна література: [1 – 11]	3	2	-	-	1
Тема 3	**Основні компоненти та загальні принципи побудови потокових шифрів**	**23**	**6**	**10**	**-**	**7**
Заняття 3/1	Скінченні автомати. 1. Означення скінченного автомату. Основні види автоматів. 2. Поняття графу скінченного автомату. Необоротність автомату за Гаффманом. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 3/2	Генератори гами. 1. Формальне означення генератора гами. Псевдовипадкові генератори. 2. Основні види генераторів гами (комбінувальні, фільтрувальні, з нерівномірним рухом). Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття	Практичне обчислення у	3	-	2	-	1

3/3	скінченних полях. 1. Виконання операцій додавання та множення в скінченному полі. 2. Виконання операції обернення у скінченному полі. Основна література: [1 – 11]					
Заняття 3/4	Синхронні потокові шифри. 1. Означення та принцип функціонування синхронного потокового шифру. 2. Стійкі потокові шифри, класифікація атак на них. Основна література: [1 – 11]	3	2	-	-	1
Заняття 3/5	Примітивні поліноми над скінченним полем. 1. Означення та критерій примітивності поліному над скінченним полем. 2. Взаємозв'язок між незвідністю та примітивністю полінома. Основна література: [1 – 11]	3	-	2	-	1
Заняття 3/6	Практичні задачі обчислення періоду лінійних рекурент над скінченним полем. 1. Практична перевірка незвідності та примітивності поліномів над скінченним полем. 2. Обчислення періодів лінійних рекурент над скінченним полем. Основна література: [1 – 11]	3	-	2	-	1
Заняття 3/7	Алгоритмічна реалізація лінійних регістрів зсуву (ЛРЗ) над скінченним полем великого порядку I. 1. Алгоритм вибору поліномів та передобчислень для реалізації ЛРЗ над полем великого порядку. 2. особливості програмної реалізації ЛРЗ на основі заздалегідь створених таблиць множення на фіксовані елементи поля. Основна література: [1 – 11]	3	-	2	-	1
Заняття 3/8	Алгоритмічна реалізація лінійних регістрів зсуву (ЛРЗ) над скінченним полем великого порядку II. 1. Особливості програмної реалізації ЛРЗ, який використовується в алгоритмі шифрування SNOW 2.0. 2. Особливості програмної реалізації ЛРЗ для SNOW 2.0-подібних потокових шифрів. Основна література: [1 – 11]	3	-	2	-	1
Тема 4	**Загальні методи побудови та аналізу потокових шифрів**	**23**	**10**	**6**	**-**	**7**

Заняття 4/1	Атака Беббіджа-Голіча. 1. Сутність та алгоритм реалізації атаки. 2. Оцінка складності атаки. Необхідна умова стійкості синхронного потокового шифру, що випливає із зазначеної атаки. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 4/2	Атака Куртуа-Майєра. 1. Сутність та оцінка складності атаки. 2. Алгебраїчна імунність булевих функцій, її властивості та вплив на стійкість шифрів до зазначеної атаки. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 4/3	Складність розв'язання систем лінійних рівнянь над скінченним полем. 1. Зв'язок між задачами розв'язання систем лінійних рівнянь та множення матриць над скінченним полем. Результат Банча-Хопкрофта. 2. Особливості практичного використання алгоритмів розв'язання систем лінійних рівнянь над скінченним полем. Основна література: [1 – 11]	3	-	2	-	1
Заняття 4/4	Практичне розв'язання систем нелінійних булевих рівнянь за допомогою лінеаризації. 1. Розв'язання систем гамоутворення фільтрувальних генераторів гами методом введення нових змінних. 2. Розв'язання систем гамоутворення фільтрувальних генераторів гами методом фіксації частини змінних. Основна література: [1 – 11]	3	-	2	-	1
Заняття 4/5	Кореляційна атака Зігенталера. 1. Опис атаки. Ймовірнісні припущення, що використовуються для аналізу її ефективності. 2. Вивід оцінки часової складності атаки Зігенталера. Основна література: [1 – 11]	2,5	2	-	-	0,5
Заняття 4/6	Перетворення Фур'є псевдобулевих функцій. 1. Означення та важливіші властивості перетворення Фур'є. Коефіцієнти Фур'є та Уолша-Адамара булевої функції. 2. Лінійні статистичні аналоги булевої функції. Алгоритм	2,5	2	-	-	0,5

	швидкого перетворення Адамара. Основна література: [1 – 11]					
Заняття 4/7	Кореляційна атака на спрощену версія SNOW 2.0-подібного потокового шифру. 1. Формальне означення SNOW 2.0-подібних потокових шифрів. Шифри SNOW 2.0 та “Струмок”. 2. Опис та аналіз ефективності кореляційної атаки на спрощену версія SNOW 2.0-подібного потокового шифру.	3	2	-	-	1
Заняття 4/8	Модульна контрольна робота.	4	-	2	-	2
Разом за розділом		82	**30**	28	-	24
Залік		**8**	**-**	**2**	**-**	**6**
Всього годин		**90**	**30**	**30**	**-**	**30**

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. Математичні методи побудови та аналізу симетричних криптосистем		
1	Тема 1. Вступ до методів побудови та аналізу симетричних криптосистем 1. Диференційний та лінійний криптоаналіз. 2. Розв’язування задач на побудову поліному Жегалкіна за допомогою швидкого рекурсивного методу. 3. Програмна реалізація швидкого алгоритму обчислення полінома Жегалкіна булевої функці\ї. 4. Прикладні задачі, що розв’язуються за допомогою симетричних криптографічних систем. 5. Властивості регулярних, транзитивних та ендоморфних шифрів. Розв’язання задач на визначення властивостей шифрів. Основна література: [1 – 11] Додаткова література: [1 – 2]	4,5
2	Тема 2. Загальні методи побудови та аналізу блокових шифрів 1. Відмінності алгоритмів ДСТУ 7624:2014 та Rijndael. 2. Режими роботи ДСТУ 7624:2014. 3. Обґрунтована та практична стійкість блокових шифрів. 4. Лінійний та різницевий методи криптоаналізу блокових шифрів. 5. Аналіз алгебраїчних властивостей вузлів заміни шифру “Калина”. Основна література: [1 – 11] Додаткова література: [1 – 2]	5,5
3	Тема 3. Основні компоненти та загальні принципи побудови потокових шифрів 1. Види скінченних автоматів. 2. Принцип роботи комбінувальних та фільтрувальних генераторів гами. 3. Взаємозв’язок між незвідністю та примітивністю полінома. 4. Перевірка незвідності та примітивності поліномів над скінченним полем. 5. Класифікація атак на синхронні потокові шифри. 6. Особливості програмної реалізації ЛРЗ для SNOW 2.0-подібних потокових шифрів. Основна література: [1 – 11]	7

	Додаткова література: [1 – 2]	
4	Тема 4. Загальні методи побудови та аналізу потокових шифрів 1. Алгоритм реалізації атаки Беббіджа-Голіча. 2. Оцінка складності атаки Куртуа-Майєра. 3. Розв'язання систем нелінійних булевих рівнянь за допомогою лінеаризації. 4. Алгоритм швидкого перетворення Адамара. 5. ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення». 6. Підготовка до модульної контрольної роботи. Основна література: [1 – 11] Додаткова література: [1 – 2]	7
5	Залік	6
6	Всього	30

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 симетричних криптосистем” вивчається курсантами на 1-ому курсі магістратури у 1-ому семестрі навчання.

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

Навчальна дисципліна “Математичні методи побудови та аналізу симетричних криптосистем” вивчає фундаментальні загальнотеоретичні та практичні принципи і методи синтезу та аналізу криптографічних схем симетричних криптосистем, в тому числі – методи проектування вузлів та блоків симетричних криптосистем з використанням сучасної елементної бази.

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 симетричних криптосистем.

Самостійна робота курсантів проводиться без керівництва викладача з метою самостійного закріплення (розширення) знань та поглиблення навичок.