



МОДЕЛІ ТА МЕТОДИ КРИПТОАНАЛІЗУ БЛОКОВИХ ШИФРІВ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>F Інформаційні технології</i>
Спеціальність	<i>F1 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>1 курс, весняний семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 5 кредитів ЕКТС / 150 годин Лекційних занять: 36 годин Практичних занять: 18 годин Комп'ютерних практикумів: 18 годин Самостійна робота студентів: 78 годин</i>
Семестровий контроль/ контрольні заходи	<i>Іспит, МКР, індивідуальне завдання</i>
Розклад занять	http://schedule.kpi.ua
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: доц. Яковлев Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua) Практичні та комп'ютерні практикуми: ас. Паршин Олександр Юрійович</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

Навчальна дисципліна «Моделі та методи криптоаналізу блокових шифрів» розглядає сучасні методи побудови блокових шифрів та їх криптоаналізу. У дисципліні будуть детально розглянуті такі теми:

- 1) будова ітеративних шифрів, схеми блокового шифрування;
- 2) статистичні атаки на раундові ключі;
- 3) формальна теорія диференціального криптоаналізу, теоретична (доказова) та практична стійкість шифрів до диференціального криптоаналізу, методи оцінювання стійкості, криптографічні параметри, які впливають на стійкість;

4) модифікації та узагальнення диференціального криптоаналізу: аналіз неможливих диференціалів, аналіз диференціалів вищого порядку, атаки бумерангів та прямокутників, атаки на пов'язаних ключах;

5) формальна теорія лінійного криптоаналізу, теоретична (доказова) та практична стійкість шифрів до лінійного криптоаналізу, методи оцінювання стійкості, криптографічні параметри, які впливають на стійкість;

6) модифікації та узагальнення лінійного криптоаналізу: білінійний криптоаналіз, узагальнений лінійний криптоаналіз на довільних абелевих групах, аналіз нульових кореляцій, диференціально-лінійні розпізнавачі;

7) методи автоматизованого пошуку високоімовірних та неможливих диференціалів, високоімовірних лінійних апроксимацій;

8) інтегральний криптоаналіз та його узагальнення: аналіз лінійних підпросторів, властивості подільності.

Основною метою дисципліни є формування у студентів глибинного розуміння сучасних статистичних методів криптоаналізу. Для досягнення мети передбачається опрацювання значної кількості розрахункових та аналітичних задач, які ілюструють та розширюють лекційний матеріал, виконання розрахункової роботи та двох комп'ютерних практикумів.

У результаті вивчення курсу студент повинен:

а) знати моделі та методи криптоаналізу блокових шифрів, параметри стійкості до криптоаналітичних атак та їх поведінку;

б) вміти будувати статистичні атаки на ітеративні блокові шифри та одержувати аналітичні чи розрахункові оцінки стійкості до таких атак.

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

Головний фокус дисципліни зосереджений на статистичних та алгебраїчних методах криптоаналізу і безпосередньо демонструє застосування математичної статистики та алгебри на практиці. Отримані навички та засвоєнні знання можуть використовуватись для проведення наукових та прикладних досліджень у галузі симетричної криптографії, а також для розв'язання прикладних задач у галузі криптографічного захисту інформації.

3. Зміст навчальної дисципліни

Розділ 1. Диференціальний криптоаналіз ітеративних блокових шифрів

Тема 1.1. Ітеративні шифри та їх класифікація. Статистичні атаки на ітеративні шифри.

Тема 1.2. Диференціальний криптоаналіз: формальна теорія, побудова атак та оцінювання стійкості.

Тема 1.3. Узагальнення та модифікації диференціального криптоаналізу

Розділ 2. Лінійний криптоаналіз ітеративних блокових шифрів

Тема 2.1. Лінійний криптоаналіз: формальна теорія, побудова атак та оцінювання стійкості.

Тема 2.2. Узагальнення та модифікації лінійного криптоаналізу

Розділ 3. Інтегральний криптоаналіз ітеративних блокових шифрів

Тема 3.1. Інтегральний криптоаналіз: формальна теорія, побудова атак та оцінювання стійкості.

Тема 3.2. Узагальнення та модифікації інтегрального криптоаналізу

4. Навчальні матеріали та ресурси

Даний курс побудовано на основі наукових публікацій у галузі симетричної криптографії та криптоаналізу за останні тридцять років. На жаль, наразі немає одного (чи навіть декількох) джерел, які б систематично та глибоко викладали усі необхідні матеріали; більш того, кожного року зміст курсу оновлюється, оскільки постійно публікуються нові наукові результати за тематикою курсу. Через наведені причини головним джерелом навчальних матеріалів є лекції та практичні заняття, а також власне наукові публікації, на яких ґрунтується курс. Нижче наводиться перелік основних таких публікацій.

1. Biham E. Cryptanalysis of Skipjack Reduced to 31 Round using Impossible Differential / E. Biham, A. Biryukov, A. Shamir // *Advances in Cryptology – EUROCRYPT'99*. – Prague: Springer-Verlag, 1999. – pp. 12–23.
2. Biham, E. Enhancing differential-linear cryptanalysis / E. Biham, O. Dunkelman, N. Keller // In: Zheng, Y. (ed.) *ASIACRYPT 2002*. – LNCS, vol. 2501. – Heidelberg: Springer, 2002. – pp. 254-266.
3. Biham E. Differential cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // *Journal of Cryptology*. – 1991. – V. 4. – № 1. – P. 3 – 72.
4. Biham E. Differential cryptanalysis of the full 16-round DES / E. Biham, A. Shamir // *Advances in Cryptology – CRYPTO'92, Proceedings*. – Springer Verlag, 1993. – P. 487 – 496.
5. Chabaud Florent. Links between Differential and Linear Cryptanalysis [електронний ресурс] / Florent Chabaud, Serge Vaudenay. – Режим доступу : <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.48.2675>
6. Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis. – Doctoral Dissertation, 1995.
7. Daemen J. The Design of Rijndael / J. Daemen, V. Rijmen // *AES – The Advanced Encryption Standard*. – Berlin: Springer-Verlag, 2002.
8. Daemen J. Probability distributions of Correlation and Differentials in Block Ciphers [електронний ресурс] / J. Daemen, V. Rijmen. – Режим доступу : <https://eprint.iacr.org/2005/212.pdf>
9. Daemen J. Statistics of Correlation and Differentials in Block Ciphers [електронний ресурс] / J. Daemen, V. Rijmen. – Режим доступу : <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.59.4898>
10. Hawkes Philip. Asymptotic Bounds of Differential Probabilities [електронний ресурс] / Philip Hawkes, Luke O'Connor. – Режим доступу : <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.20.2383>
11. Heys Howard M. A Tutorial on Linear and Differential Cryptanalysis [електронний ресурс] / Howard M. Heys. – Режим доступу : http://www.engr.mun.ca/~howard/PAPERS/ldc_tutorial.pdf
12. Hong S. Provable security against differential and linear cryptanalysis for the SPN structure / S. Hong, S. Lee, J. Lim, J. Sung, D. Cheon // *Fast Software Encryption. – FSE'00, Proceedings*. – Springer Verlag, 2001. – P. 273 – 283.
13. Kaneko Y. On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions / Y. Kaneko, F. Sano, K. Sakurai // *Proc. of SAC'97*. – Springer, 1997.
14. Kang J.-S. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks / J.-S. Kang, S. Hong, S. Lee, O. Yi, C. Park, J. Lim // *ETRI Journal*. – #23. – 2001. – pp. 158-167.
15. Knudsen L.R. Integral Cryptanalysis (extended abstract) [електронний ресурс] / L.R. Knudsen, D. Wagner. – Режим доступу : www.cs.berkeley.edu/~daw/papers/integrals-fse02.ps
16. Knudsen L.R. Truncated and higher order differentials. / L.R. Knudsen // In: Preneel, B. (ed.) *FSE 1994*. – LNCS, vol. 1008. – Heidelberg: Springer, 1995. – pp. 196-211.
17. Lai X. Markov ciphers and differential cryptanalysis / X. Lai, J.L. Massey, S. Murphy. // *Advances in Cryptology – EUROCRYPT'91, Proceedings*. – Springer Verlag, 1991. – pp. 17-38.
18. Langford, S.K. Differential-linear cryptanalysis. / S.K. Langford, M.E. Hellman // In: Desmedt, Y. (ed.) *CRYPTO 1994*. – LNCS, vol. 839. – Heidelberg: Springer, 1994. – pp. 17-25.

19. Lu Jiqiang . New Methodologies for Differential-Linear Cryptanalysis and Its Extensions [електронний ресурс] / Jiqiang Lu. – Режим доступу : <https://eprint.iacr.org/2010/025.pdf>
20. Matsui M. Linear cryptanalysis methods for DES cipher / M. Matsui // Advances in Cryptology – EUROCRYPT’93, Proceedings. – Springer Verlag, 1994. – P. 386 – 397.
21. Matsui M. On a Structure of Block Ciphers with Provable Security against Differential and Linear Analysis / M. Matsui // IEICE Trans. Fundamentals. – Vol. E82-A. – #1. – 1999. – pp. 117-122.
22. Nyberg K. Provable Security Against a Differential Attack / K. Nyberg, L.R. Knudsen // Journal of Cryptology. – Vol.8. – No.1. – 1995.
23. Nyberg Kaisa. Linear Approximation of Block Ciphers / Kaisa Nyberg // EUROCRYPT’94. – Lecture Notes in Computer Science, vol. 950. – Springer Verlag, 1994.
24. Vaudenay S. On the security of CS-cipher / S. Vaudenay // Fast Software Encryption. – FSE’99, Proceedings. – Springer Verlag, 1999. – P. 260-274.
25. Vaudenay S. Decorrelation: a theory for block cipher security / S. Vaudenay // Journal of Cryptology. – 2003. – V. 16. – № 4. – pp. 249-286.
26. Wagner D. The Boomerang Attack / D. Wagner // in: L. R. Knudsen, editor, FSE’99. – LNCS, vol. 1636. – 1999. – pp. 156-170.
27. Ковальчук Л.В. Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів шифрування до методів різницевого криптоаналізу / Л.В. Ковальчук, С.В. Пальченко, Л.В. Скрипник // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні – К.: НДЦ «Тезіс», 2009 – №2 (19) – стор. 45-56.
28. Ковальчук Л.В. Дослідження різницевої характеристики раундової функції блочних шифрів MISTY1 та MISTY2 / Л.В. Ковальчук, А.О. Шерстюк // Прикладная радиоэлектроника. – №3. – 2009. – С. 15–27.
29. Яковлев С.В. Методика обґрунтування стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу / С.В. Яковлев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – №1(25). – С. 73-80.

Відеозаписи більшої частини лекцій викладені на Youtube-каналі кафедри ММЗІ та доступні за посиланням

<https://www.youtube.com/playlist?list=PLhCN8H4P5LvhdD8oXciqd4-sIPwmMhVNR>

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та взаємодії викладачів та студентів для засвоєння матеріалу та опанування практичних навичок. При викладанні дисципліни використовуються такі методи навчання: для лекційних занять – пояснювально-ілюстративний метод та метод проблемного викладу; для практичних занять – пояснювально-ілюстративний метод, репродуктивний метод та метод проблемного викладу. Захист розрахункової роботи та комп’ютерних практикумів передбачає використання дискусійного методу.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Модель ітеративного шифру. Схеми блокового шифрування, їх класифікація
2	Статистичні атаки на ключі останнього раунду. Вступ до диференціального криптоаналізу
3	Формальна теорія диференціального криптоаналізу ітеративних шифрів. Марковські та немарковські шифри
4	Доказова стійкість схеми Фейстеля та SP-мереж до диференціального криптоаналізу

5	Доказова стійкість каскадних та AES-подібних SP-мереж до диференціального криптоаналізу
6	Узагальнення та модифікації диференціального криптоаналізу: аналіз усічених диференціалів, аналіз диференціалів високого порядку
7	Аналіз неможливих диференціалів та методи оцінювання стійкості до нього
8	Атака бумерангів та її узагальнення. Атаки на пов'язаних ключах
9	Вступ до лінійного криптоаналізу. Алгоритми Мацуї
10	Формальна теорія лінійного криптоаналізу. Доказова стійкість схем блокового шифрування до лінійного криптоаналізу
11	Узагальнений лінійний криптоаналіз небінарних шифрів
12	Узагальнення лінійного криптоаналізу: аналіз нульових кореляцій, білінійний криптоаналіз, аналіз узагальнених збалансованих апроксимацій, аналіз I/O-сум, атака інтерполяції
13	Диференціально-лінійні розпізнавачі
14	Інтегральний криптоаналіз: вступ та формальна теорія
15	Побудова інтегральної атаки на шифр AES
16	Властивості подільності Тодо та їх застосування в інтегральному криптоаналізі
17	Аналіз лінійних підпросторів
18	Підсумкове консультативне заняття

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Диференціали S-блоків та їх алгебраїчні та ймовірнісні властивості
2	Диференціали та диференціальні характеристики блокових шифрів та їх алгебраїчні та ймовірнісні властивості
3	Оцінювання доказової стійкості блокових шифрів до диференціального криптоаналізу, побудова аналогів теореми Ніберг-Кнудсена
4	Аналіз неможливих диференціалів слово-орієнтованих шифрів, застосування UID-методу
5	МКР, частина 1
6	Лінійні апроксимації, лінійні потенціали та лінійні характеристики блокових шифрів, їх алгебраїчні та ймовірнісні властивості
7	Оцінювання доказової стійкості блокових шифрів до лінійного криптоаналізу, побудова аналогів теореми Ніберг
8	Побудова інтегралів для слово-орієнтованих шифрів
9	МКР, частина 2

Комп'ютерні практикуми

Для закріплення теоретичних знань та формування необхідних практичних навичок студенти повинні виконати два комп'ютерних практикуми:

1) проведення диференціального криптоаналізу та побудова диференціальної атаки на шифр Хейса;

2) проведення лінійного криптоаналізу та побудова відповідної атаки на шифр Хейса.

Комп'ютерні практикуми можуть виконуватись самостійно або у парі. У другому випадку виконання задач практикумів розподіляється між учасниками на власний розсуд, а оцінка за виконання ставиться обом учасникам однакова, за фактичне виконання задач практикумів.

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал.

Обов'язковим є виконання домашніх завдань, які необхідно виконувати до наступного практичного заняття. Виконання та ревізія виконаних домашніх завдань також необхідні для підготовки до самостійних та модульних контрольних робіт.

Виконання комп'ютерного практикуму сприяє формуванню навичок самостійної та творчої роботи (пошуку додаткових матеріалів, формалізація поставлених задач, реалізація алгоритмів їх розв'язування); також, при виконанні практикуму в бригаді, формуються навички колективної роботи над розробницькими проектами.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати індивідуальне завдання за темою побудови доказових оцінок стійкості блокових шифрів до відомих методів криптоаналізу. Для підготовки до виконання індивідуального завдання слід скористатися рекомендованою літературою, конспектом та/або відеозаписами лекцій. Студенту надається не менше місяця на виконання індивідуального завдання.

Розподіл годин самостійної роботи студента

№	Вид самостійної роботи	Годин СРС
1.	Опанування лекційного матеріалу	12
2.	Підготовка до практичних занять	10
3.	Підготовка до виконання комп'ютерних практикумів	12
4.	Підготовка до виконання модульної контрольної роботи	4
5.	Виконання індивідуального завдання	10
6.	Підготовка та складання іспиту	30
	Усього	78

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються необхідні навички. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно.

Відвідування занять з комп'ютерних практикумів є обов'язковим тільки для захисту поставлених на практикумі завдань, а також для одержання консультацій викладачів щодо виконання завдань.

Пропущені контрольні заходи

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Якщо пропуск стався з поважних причин (наприклад, хвороби), підтверджених відповідними документами, студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини модульної контрольної роботи не допускається.

Пропущений іспит не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості «не з'явився» та повинен складати іспит на додатковій сесії.

Оголошення результатів контрольних заходів

Результати виконання домашніх завдань оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються коментарями, в яких студенти можуть побачити свою оцінку за певними критеріями, а також виокремлення основних помилок та зауваження.

Результати модульної контрольної роботи вказуються на бланках для модульної контрольної роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо.

Результати письмової частини заліку вказуються на бланках для письмової залікової роботи (завдання, які виконували студенти) з позначенням усіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Результати усної частини заліку оголошуються наприкінці її проходження.

Академічна доброчесність

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

У разі виявлення порушень норм академічної доброчесності під час виконання контрольного заходу студент одержує за цей захід нуль балів без можливості повторного виконання.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами.

Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

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

№	Контрольний захід	Макс бал	Кіл-ть	Усього
1.	Модульна контрольна робота	24	1	24
2.	Комп'ютерні практикуми	13	2	26
3.	Індивідуальне завдання	10	1	10
4.	Іспит	40	1	40
	Усього			100

Критерії оцінювання контрольних заходів

1) Модульна контрольна робота

Модульна контрольна робота (МКР) складається з декількох частин, які проводяться протягом семестру по мірі опанування теоретичного та практичного матеріалу. Кількість задач та їх вартість у балах визначається викладачами в залежності від складності самої задачі та об'єму винесеного на дану частину МКР матеріалу.

Критерії оцінювання однієї задачі МКР:

- | | |
|---------------------------------------------------------------------------------------------------|---------------|
| • Правильне повне розв'язання без помилок | 100% оцінки |
| • Розв'язання з несуттєвими помилками та/або описками | 90-99% оцінки |
| • Розв'язання з деякими неточностями | 70-89% оцінки |
| • Розв'язання із правильною ідеєю, але грубими помилками | 50-69% оцінки |
| • Наявність правильної ідеї розв'язку з неправильним її застосуванням або незакінченим розв'язком | 30-49% оцінки |
| • Розв'язок повністю неправильний або відсутній | 0% оцінки |

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Виконання частини МКР, пропущеної з поважних причин, врегульовується за домовленістю з викладачем в індивідуальному порядку.

Максимальна кількість балів, яку можна одержати за модульну контрольну роботу, дорівнює 24. Загальна кількість балів, яку студент одержує за одну частину модульної контрольної, дорівнює сумі балів за кожне завдання у відповідності до їх вартості та наведених критеріїв оцінювання. Загальна кількість балів, яку студент одержує за модульну контрольну роботу, дорівнює сумі балів за виконання усіх її частин.

2) Індивідуальне завдання (розрахункова робота)

Розрахункова робота (РР) складається з декількох завдань. Кожен студент одержує своє індивідуальне завдання для виконання. Кількість задач та їх вартість у балах визначається викладачами та наводиться у завданні на РР. Оцінювання РР складається з двох етапів: безпосереднього виконання студентом індивідуального завдання та його захист у викладача; кожна частина дає до 50% від оцінки за кожну задачу РР.

Критерії оцінювання одного завдання РР:

- | | |
|--------------------------------------------------------------------------------------------|---------------|
| • Повне розв'язання без помилок, правильна відповідь | 50% оцінки |
| • Правильне розв'язання із неправильною відповіддю через неточності та арифметичні помилки | 25-49% оцінки |
| • Розв'язання із правильною ідеєю, але грубими помилками | 10-24% оцінки |
| • Розв'язок повністю неправильний або відсутній | 0% оцінки |

Критерії оцінювання захисту одного завдання РР:

- | | |
|-----------------------------------------------------------------------------------------------------|---------------------|
| • Студент демонструє вичерпне розуміння наведеного розв'язку та відповідного теоретичного матеріалу | 50% оцінки |
| • Студент відповідає з неточностями та помилками | 30-49% оцінки |
| • Відповідь студента містить окремі вірні положення | 10-29% оцінки |
| • Студент демонструє повне нерозуміння теоретичного матеріалу та наведеного розв'язку | 0 балів за завдання |

Максимальна кількість балів, яку можна одержати за виконання та захист РР, дорівнює 10.

Здача РР після призначеного терміну виконання без поважної причини приводить до зниження оцінки за неї на 0,25 балу за кожен день запізнення; максимальне зниження оцінки за пропуск дедлайну – 2 бали. АЛЕ: якщо РР була здана через вісім днів після призначеного терміну, вона автоматично оцінюється у 0 балів.

3) Комп'ютерні практикуми

Комп'ютерні практикуми виконуються самостійно, бригадами по два студенти або одноосібно. Кожен комп'ютерний практикум оцінюється в 13 бали. Оцінка за комп'ютерний практикум формується з таких складових:

- практична частина (програмний код): 50% від оцінки;
- протокол виконання практикуму: 25% від оцінки;
- захист (теоретична частина): 25% від оцінки.

Зданий протокол та захист практикуму є необхідними умовами його зарахування.

Здача комп'ютерного практикуму після призначеного терміну виконання без поважної причини приводить до зниження оцінки за нього на 0,5 бал за кожен тиждень запізнення; максимальне зниження оцінки за пропуск дедлайну – 2 бали.

Через чотири тижні після призначеного терміну виконання комп'ютерні практикуми перестають прийматись. Можливість здати та захистити такі комп'ютерні практикуми буде надана один раз перед перескладанням дисципліни.

4) Семестрова атестація (іспит)

Семестрова атестація (іспит) проводиться усно зі студентами, які були допущені за результатами роботи протягом семестру. Іспит включає в себе

- практичну частину (2 задачі, 20 балів);
- теоретичну частину (2 теоретичне питання із розгорнутою відповіддю, 20 балів);

Критерії оцінювання задач практичної частини співпадають з критеріями оцінювання задач МКР.

Критерії оцінювання теоретичного питання із розгорнутою відповіддю:

- | | |
|----------------------------------------------------------------|---------------|
| • Студент демонструє вичерпне розуміння теоретичного матеріалу | 100% оцінки |
| • Студент відповідає з незначними неточностями | 90-99% оцінки |
| • Студент відповідає з суттєвими неточностями | 60-89% оцінки |
| • Відповіді студента лише частково вірні | 30-59% оцінки |
| • Відповіді студента містять лише окремі вірні положення | 10-29% оцінки |
| • Студент демонструє повне незрозуміння теоретичного матеріалу | 0 балів |

Під час іспиту забороняється використання будь-яких додаткових довідкових матеріалів.

Заохочувальні бали

Модульна контрольна робота може включати в себе додаткові задачі, правильне розв'язання яких оцінюється бонусними (заохочувальними) балами поза шкалою семестрового рейтингу.

Студенти, які склали іспит не менш ніж на 36 балів, мають право одержати бонусне завдання, розв'язання якого також надасть до 6 заохочувальних балів.

Загальна кількість заохочувальних балів, які можна одержати за дисципліну: 10 балів.

Умови одержання проміжної атестації

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 7-му та 13-му навчальному тижнях семестру. Для одержання кожної атестації поточний рейтинг студента повинен бути не менше половини від суми максимальних балів за усі контрольні заходи, які були проведені на момент атестації.

Умови допуску до семестрової атестації

Необхідною умовою допуску до семестрової атестації є

- семестровий рейтинг не менше 25 балів;
- виконані та здані усі комп'ютерні практикуми;
- виконана та здана розрахункова робота.

Студенти, які протягом семестру отримали від 10 до 25 балів, але виконали інші умови допуску, не допускаються до складання іспиту. Замість іспиту такі студенти виконують письмову допускну роботу (10 задач, 20 балів), результати якої додають до семестрового рейтингу; якщо після виконання допускну роботи семестровий рейтинг стає більшим 30 балів, студент допускається до семестрової атестації на перескладанні, а його семестровий рейтинг вважається таким, що дорівнює 30 балів; в іншому випадку результати допускну роботи анулюються, а на перескладанні студент повторно виконує допускну роботу.

Студенти, які не виконали розрахункову роботу та/або комп'ютерні практикуми, не допускаються до складання іспиту. Таким студентам буде надана можливість здати та захистити розрахункову роботу та/або комп'ютерні практикуми перед додатковою сесією, щоб одержати допуск до перескладання дисципліни.

Студенти, які протягом семестру одержали менше 10 балів, не допускаються до складання чи перескладання семестрової атестації та рекомендуються кафедрі на відрахування або повторне переслуховування дисципліни.

Перескладання дисципліни

Перескладання дисципліни проходить у такій само формі, як і іспит. Для допуску до перескладання студент повинен одержати не менше 30 рейтингових балів (з урахуванням першої спроби складання іспиту або допускну роботи), виконати і захистити розрахункову роботу, виконати і захистити усі комп'ютерні практикуми. На перескладанні результати основного іспиту анулюються, а рейтингова оцінка складатиметься із семестрового рейтингу та результатів перескладання.

Студенти, які після першого перескладання не одержали позитивної оцінки, йдуть на повторне перескладання дисципліни спеціалізованій атестаційній комісії. Формат повторного перескладання визначається комісією.

Підсумкова оцінка з дисципліни

Рейтингова оцінка складається з результатів виконання семестрових контрольних заходів (включно з заохочувальними) та результатів усного іспиту або його перескладання. Оцінка за стобальною шкалою переводиться до університетської шкали оцінок за наведеною таблицею відповідності.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

<i>Кількість балів</i>	<i>Оцінка</i>
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Склав: доцент кафедри ММЗІ, к.т.н. Яковлев Сергій Володимирович

Ухвалено кафедрою математичних методів захисту інформації (протокол №6/2 від 25.06.2025 р.).

Затверджено Методичною комісією НН ФТІ (протокол №6 від 30.06.2025 року)