



Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий фізико-технічний
інститут
Кафедра математичних методів
захисту інформації

МЕТОДИ КРИПТОАНАЛІЗУ. ЧАСТИНА 2 (ПО 1.2)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>11 Математика та статистика</i>
Спеціальність	<i>113 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Обов'язкова</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>1 курс, весняний семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 3,5 кредити ЄКТС / 105 годин Лекційних занять: 36 годин Практичних занять: 18 годин Лабораторних робіт: 18 годин Самостійна робота студентів: 33 години</i>
Семестровий контроль/ контрольні заходи	<i>Залік, МКР, РР</i>
Розклад занять	http://rozklad.kpi.ua http://ipt.kpi.ua/navchalnij-protses
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: проф. Олексійчук Антон Миколайович, д.т.н. (alex-dtn@ukr.net) Практичні заняття та лабораторні роботи: ас. Курінний Олег Вікторович (ol.kurinnoy@gmail.com)</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

Навчальна дисципліна «Методи криптоаналізу. Частина 2» присвячена методам криптоаналізу (оцінювання та обґрунтування стійкості) потокових шифрів і складається з трьох тем, які присвячено теоретико-автоматним, алгебраїчним та ймовірно-статистичним методам відповідно.

Метою кредитного модуля є забезпечення студентів знаннями, необхідними для проведення самостійних досліджень в галузі криптоаналізу потокових шифрів та їх компонент, а також для розуміння сучасних наукових результатів і основних тенденцій розвитку цієї галузі. Основу курсу складають алгебраїчні та статистичні методи криптоаналізу потокових шифрів, зокрема, методи, що базуються на застосуванні базисів Грьобнера ідеалів кільця булевих функцій, поняття

алгебраїчної імунності булевого відображення, теоретико-автоматні та статистичні методи, пов'язані з побудовою атак на генератори гамми з нерівномірним рухом та кореляційних атак на потокові шифри.

Згідно з вимогами програми навчальної дисципліни студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

знання:

теоретико-автоматних моделей синхронних поточкових шифрів та генераторів гамми, що використовуються у сучасних поточкових шифрах, методів побудови та аналізу (розв'язання) систем рівнянь гаммоутворення синхронних поточкових шифрів, основ теорії булевих базисів Грьбнера, алгоритмів обчислення алгебраїчної імунності булевих відображень, методів оцінювання стійкості поточкових шифрів відносно алгебраїчних і статистичних (кореляційних) атак, швидких алгоритмів розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами.

уміння:

будувати системи рівнянь гаммоутворення синхронних поточкових шифрів;
оцінювати складність розв'язання зазначених систем за допомогою відомих методів;
оцінювати алгебраїчну імунність булевих відображень;
проводити аналіз та оцінювати параметри компонент алгоритмів поточкового шифрування, що визначають їх стійкість відносно відомих алгебраїчних та кореляційних атак;
оцінювати складність розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами з використанням сучасних алгоритмів (BKW та його модифікацій);

досвід:

методика оцінювання та обґрунтування стійкості поточкових шифрів відносно найбільш відомих атак;
побудова оцінок стійкості сучасних поточкових шифрів;
методика дослідження окремих компонент алгоритмів поточкового шифрування;
побудова ймовірно-статистичних моделей генераторів гамми з метою дослідження їх стійкості відносно статистичних атак;
обґрунтування вибору методу (алгоритму) розв'язання прикладної задачі.

Одержані знання та уміння посилюють такі компетентності та результати навчання, визначені освітньою програмою:

Загальні компетентності

ЗК 1 Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми.

Фахові компетентності

ФК 1 Здатність формалізувати та розв'язувати складні задачі й проблеми, які потребують оновлення й інтеграції знань, часто в умовах неповної, неточної чи недостатньої інформації та суперечливих вимог.

ФК 5 Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем.

ФК 7 Здатність проектувати, розроблювати та реалізовувати системи криптографічного захисту з урахуванням сучасних досягнень науки та існуючої правової та нормативної бази.

Програмні результати навчання

РН 1 Використовувати та адаптувати математичні теорії та моделі для забезпечення теоретичного підґрунтя розв'язання наукових та практичних задач.

РН 2 Застосовувати існуючий математичний апарат, розробляти нові моделі, методи та алгоритми при вирішенні актуальних практичних задач широкого спектру.

PH 8 Застосовувати методи здобуття знань із даних, методи оцінки та інтерпретації знайдених закономірностей.

PH 11 Провадити аналіз криптографічних алгоритмів, протоколів та систем.

PH 12 Орієнтуватись у останніх досягненнях криптології.

PH 15 Розроблювати та аналізувати алгоритми у класичній та квантовій моделях обчислень.

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

Дана дисципліна є продовженням дисципліни «Методи криптоаналізу. Частина 1». Отримані практичні навички та засвоєнні знання необхідні для опанування дисципліни «Проектування, розробка і реалізація криптографічних систем» та для виконання науково-дослідницької та прикладної діяльності у галузі криптології.

Отримані практичні навички та засвоєнні знання можуть використовуватись у будь-яких дисциплінах, тематика яких пов'язана із алгоритмізацією задач та побудовою їх ефективних розв'язків, обчислювальними методами, криптографічним захистом інформації.

3. Зміст навчальної дисципліни

Розділ 1. Синхронні потокові шифри

Тема 1.1. Скінченні автомати, необоротність скінченного автомата за Гаффманом

Тема 1.2. Генератори гами та синхронні потокові шифри

Тема 1.3. Атака на комбінувальний генератор гами з нерівномірним рухом на основі опробування індексів руху ЛРЗ

Розділ 2. Елементи алгебраїчного криптоаналізу

Тема 2.1. Ідеали кільця булевих функцій. Мономіальні впорядкування

Тема 2.2. Теорема про подільність з остачею у кільці булевих функцій. Базиси Грьобнера

Тема 2.3. Атака Куртуа-Майєра та алгебраїчна імунність булевих функцій

Тема 2.4. Алгебраїчна атака на спрощену версію SNOW 2.0-подібного потокового шифру

Розділ 3. Елементи статистичного криптоаналізу

Тема 3.1. Статистична атака на фільтрувальний генератор гами з лінійним законом формування початкового стану та функцією ускладнення, близькою до алгебраїчно виродженої. Кореляційна атака Зігенталера

Тема 3.2. Алгоритм ВКВ

Тема 3.3. Кореляційна атака на спрощену версію SNOW 2.0-подібного потокового шифру

Тема 3.4. Швидкі алгоритми знаходження лінійних наближень булевих функцій

4. Навчальні матеріали та ресурси

Базова рекомендована література

1. ДСТУ 8845:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення».

2. ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення».

3. Коваленко І. М. Про алгоритм субекспоненціальної складності декодування сильно спотворених лінійних кодів. – Доп. АН УРСР, сер. А, № 10, с. 16–17, 1988.

4. Alekseychuk A. N. Algebraic immunity of vectorial Boolean functions and Boolean Groebner bases. – Theoretical and Applied Cybersecurity: scientific journal, vol. 2, iss. 1, pp. 10-14, 2022.

5. Ars G., Faugere J.-C. Algebraic immunities of functions over finite fields. – Technical Report, INRIA, 2003.
6. Babbage S. A space/time tradeoff in exhaustive search attacks on stream ciphers. – European Convention on Security and Detection, IEE Conference Publication No. 408, May 1995.
7. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. – J. ACM, vol. 50, №3, pp. 506-519, 2003.
8. Canteaut A., Naya-Plasencia M. Correlation attacks on combination generators. – Cryptogr. Commun., vol. 4, №3-4, pp. 147-171, 2012.
9. Courtois N. T., Meier W. Algebraic attacks on stream ciphers with linear feedback. – Boneh D. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 345-359, Springer, Heidelberg, 2003.
10. Golic J. Cryptanalysis of alleged A5 stream cipher. – Fumy W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 239-255, 1997.
11. Huffman D. Canonical forms for information loss less finite state logical machines. – IRE Trans. Circuit Theory, vol. 6, spec. suppl., pp. 41-59, 1959.
12. Katz J., Lindell Y. Introduction to modern cryptography (2nd ed.). – CRC Press, 2015.
13. Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only. – IEEE Trans. Comput., vol. 34, pp. 81-84, 1985.
14. Zenner E. On the efficiency of the clock control guessing attack. – ICISC, pp. 200-212, 2002.

Допоміжна рекомендована література

1. Abdouli A. S., Dumer I., Kabatiansky G., Tavernier C. The Goldreich-Levin algorithm with reduced complexity. – Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory (ACCT 2012), pp. 7-14, Pomorie, Bulgaria, June 15-21, 2012.
7. Bardet M., Faugere J.-C., Salvy B. On the complexity of Groebner basis computation for semi-regular overdetermined sequences over F_2 with solutions in F_2 . – Technical Report 5049, INRIA, 2003.
8. Berbain C., Gilbert H. On the security of IV dependent stream ciphers. – Biryukov A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 254-273, Springer, Heidelberg, 2007.
9. Billet O., Gilbert H. Resistance of SNOW 2.0 against algebraic attacks. – Menezes A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 19-28, Springer, Heidelberg, 2005.
10. Bshouty N., Jackson J., Tamon C. More efficient PAC-learning of DNF with membership queries under the uniform distribution. – Proc. of COLT'99, pp. 286-295, 1999.
11. Berlekamp E. R., McEliece R. J., van Tilborg H. On the inherent intractability of certain coding problems. – IEEE Trans. Inform. Theory, vol. 24, № 3, pp. 384-386, 1978.
12. Bogos S., Tramer F., Vaudenay S. On solving LPN using BKW and variants. Implementation and analysis. – Cryptology ePrint Archive, report 2015/049, <http://eprint.iacr.org/2015/049>.
13. Daemen J., Govaerts R., Vandewalle J. Resynchronization weaknesses in synchronous stream ciphers. – Hellesteth T. (ed.) EUROCRYPT 1993. LNCS, pp. 159-167, Springer-Verlag, 1993.
14. Goldreich O., Levin L. A. A hard core predicate for all one-way functions. – Proc. 21 ACM Sympos. of Theory of Computing, pp. 25-32, 1989.
15. Hoeffding W. Probability inequalities for sums of bounded random variables. – J. Amer. Statist. Assoc., vol. 58, № 301, 1963.
16. Ovchinnikov A., Zobnin A. Classification and applications of monomial orderings and the properties of differential orderings. – Ganzha V., Mayer E. and Vorozhtsov E. (ed.) Proc. CASC'02, pp. 237-252, 2002.
17. Semaev I., Mikus M. Methods to solve algebraic equations in cryptanalysis. – Tatra Mt. Math. Publ., vol. 45, pp. 107-136, 2010.

18. Semaev I., Tenti A. Probabilistic analysis on Macaulay matrices over finite fields and complexity of constructing Groebner bases. – J. Algebra, vol. 565, pp. 651-674, 2021.

Відеозаписи лекцій викладені на Youtube-каналі кафедри ММЗІ та доступні за посиланням https://www.youtube.com/playlist?list=PLhCN8H4P5Lvg0jAzaN_iiWaBibQMMI2vy.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Для проведення занять застосовується практичний метод. Для лекційних та практичних занять використовуються пояснювально-ілюстративний метод та метод проблемного виконання, для проведення лабораторних робіт та виконання розрахунково-графічної та домашньої контрольної робіт використовуються метод проблемного виконання та частково-пошуковий метод.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Поняття скінченного автомату, основні класи автоматів. Генератори гами, найважливіші види генераторів гами.
2	Граф скінченного автомата. Необоротність скінченного автомата за Гаффманом.
3	Означення та класифікація поточкових шифрів, синхронні поточкові шифри. Формальне означення стійкості та практична стійкість СПШ. Класифікація атак на синхронні поточкові шифри.
4	Атака на комбінувальний генератор гами з нерівномірним рухом на основі опробування індексів руху ЛРЗ.
5	Поняття ідеалу кільця булевих функцій, пов'язаного із системою рівнянь. Співвідношення між вимірністю та числом нулів ідеалу.
6	Мономіальні впорядкування на множині невід'ємних цілочисельних векторів. Приклади впорядкувань, лексикографічне та степеневе лексикографічне впорядкування. Старший член булевого поліному. Леми про старші члені суми та добутку поліномів.
7	Мономіальні ідеали. Теорема про подільність з остачею в кільці булевих функцій. Алгоритм ділення з остачею.
8	Поняття базису Грьобнера ідеалу кільця булевих функцій. Приклади: базиси Грьобнера мономіальних ідеалів. Необхідні та достатні умови, за якими система булевих функцій утворює базис Грьобнера породжуваного їй ідеалу. Загальна методика застосування базисів Грьобнера для побудови алгебраїчних атак на СПШ.
9	Мінімальний степінь ідеалу кільця булевих функцій. Атака Куртуа-Майєра та алгебраїчні імунітет булевих функцій.
10	Алгебраїчна атака на спрощену версію SNOW 2.0-подібного поточкового шифру.
11	Атака Бєбіджа-Голіча. Опис та ймовірно-статистична модель атаки.
12	Статистична атака на фільтрувальний генератор гами з лінійним законом формування початкового стану та функцією ускладнення, близькою до алгебраїчно виродженої.
13	Кореляційна атака Зігенталера. Загальна кореляційна задача.
14	Перетворення Фур'є псевдобулевих функцій. Алгоритм швидкого перетворення Адамара. Перетворення Уолша-Адамара та афінні наближення булевих функцій.
15	Системи рівнянь зі спотвореними правими частинами. Застосування швидкого перетворення Адамара до розв'язання систем лінійних рівнянь зі спотвореними правими частинами. Алгоритм ВКВ.

16	Застосування функції сліду до розв'язання систем лінійних рівнянь зі спотвореними правими частинами над двійковими полями. Кореляційна атака на спрощену версію SNOW 2.0- подібного потокового шифру.
17	Швидкі алгоритми знаходження лінійних наближень булевих функцій.
18	Залік.

Практичні заняття

№ з/п	Назва теми заняття та перелік основних питань
1	Необоротність за Гаффманом, достатня умова необоротності. Задачі оцінювання числа розв'язків СР гамоутворення ГГ з нерівномірним рухом.
2	Задачі побудови та аналізу систем рівнянь, що описують функціонування ГГ з нерівномірним рухом.
3	Розв'язання задач на властивості базисів Грьобнера ідеалів кільця булевих функцій та побудови редукованих базисів Грьобнера.
4	Розв'язання задач обчислення алгебраїчної імунності функцій ускладнення генераторів гами СПШ за допомогою методу Гаусса.
5	Розв'язання задач побудови функцій найменшого степеню, які належать анулятору заданої булевої функції, та оцінювання алгебраїчної імунності булевих функцій за допомогою базисів Грьобнера.
6	Розв'язання задач на алгебраїчну виродженість та несуттєві вектори; аналіз кореляційних властивостей булевих функцій.
7	Розв'язання задач на застосування апарату перетворення Фур'є булевих функцій.
8	Розв'язання задач на властивості булевих функцій.
9	МКР.

Лабораторні роботи (комп'ютерні практикуми)

Для закріплення теоретичних знань та формування необхідних практичних навичок студенти повинні виконати дві лабораторні роботи (комп'ютерні практикуми):

- 1) побудова алгебраїчної атаки на генератор гами;
- 2) побудова статистичної атаки на генератор гами;

Лабораторна робота може виконуватись самостійно або у парі. У другому випадку виконання задач лабораторної розподіляється між учасниками на власний розсуд, а оцінка за виконання ставиться обом учасникам однаково, за фактичне виконання задач лабораторної роботи.

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.

З метою кращого засвоєння матеріалу курсу, а також формування навичок самостійної роботи студентам пропонується виконати розрахункову роботу за темою «Дослідження криптографічних властивостей функції ускладнення фільтрувального генератора гами». Для

підготовки до виконання розрахункової роботи слід скористатися рекомендованою літературою, конспектом та/або відеозаписами лекцій. Студенту надається не менше двох тижнів на виконання розрахункової роботи, після чого в узгоджений із викладачем час студент повинен захистити виконану роботу.

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

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 навички, необхідні для виконання домашніх завдань, контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички.

Пропущені контрольні заходи

Студент, який пропустив частину МКР має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини модульної контрольної роботи не допускається.

Студент, який без поважних причин пропустив тестове завдання на практичному занятті, одержує за нього нуль балів без можливості перескладання. Якщо пропуск стався з поважної причини, студенту буде надана можливість виконати тестове завдання у інший узгоджений із викладачем час.

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.

Тестові завдання виконуються студентами на практичних заняттях. Студенту надається тестове завдання, яке складається з тестових питань та/або завдань, які потребують короткої відповіді. Тестове завдання виконується письмово або за допомогою відповідної платформи (наприклад, <https://www.classtime.com/>) в залежності від форми навчання. При виконанні тестового завдання оцінка оголошується після перевірки, і студент може одержати розгорнуте пояснення щодо виставленої оцінки та зауваження по своїх відповідях.

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>.

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	Ваговий бал	Кіл-ть	Усього
1.	Домашнє завдання	3	1	≥4	24
2.	Тестове завдання	3	1	≥4	24
3.	Модульна контрольна робота	12	1	1	12
4.	Лабораторна робота	12	1	2	24
5.	Розрахункова робота	16	1	1	16
	Усього				100

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 8-му та 14-му навчальному тижнях кожного семестру. Для одержання першої атестації поточний рейтинг студента повинен бути не менше 12 балів, другої – не менше 30 балів.

Система оцінювання дисципліни не передбачає штрафних балів. Також студент може одержати до 10 заохочувальних балів протягом семестру. Ці бали він отримує за відповіді на практичних заняттях. Відповідь на одному практичному занятті максимально оцінюється в 0.8 балів. Загальна кількість балів, яку студент одержує за відповіді на практичних заняттях, дорівнює сумі балів за кожне практичне заняття. Окрім цього, заохочувальні бали студент може одержати і за інші типи завдань, наприклад, студенти за бажанням можуть отримувати дослідницькі задачі протягом семестру за узгодженням із викладачем.

Рейтингова оцінка студента складається з результатів роботи в семестрі та заохочувальних балів. Якщо одержана за підсумками семестру сума перевищує 100 балів, вона встановлюється у 100 балів. Якщо виконано такі умови:

- семестровий рейтинг складає не менше 60 балів;
- виконано лабораторні роботи (комп'ютерні практикуми);
- виконано розрахункову роботу,

то студенту виставляється відповідна оцінка, крім випадку, коли студент не погоджується із нею.

Студенти, які набрали від 50 до 60 балів за семестр, за бажанням замість заліку можуть пройти усну співбесіду із викладачем за матеріалами курсу. На співбесіді, відповідаючи на теоретичні та/або практичні питання, студент може підвищити свій семестровий рейтинг до мінімальної позитивної оцінки у 60 балів. Однак якщо відповіді студента незадовільні і семестровий рейтинг не було збільшено до 60 балів, студент йде на перескладання дисципліни.

Студенти, які не одержали позитивну оцінку за результатами роботи у семестрі (але при цьому їх семестровий рейтинг складає не менше 10 балів), та студенти, які не погоджуються із такою оцінкою, на останньому лекційному занятті повинні скласти залік. При цьому їхній семестровий рейтинг анулюється, а рейтингова оцінка виставляється по результату виконання залікової роботи. Залікова робота може включати в себе як теоретичні так і практичні завдання.

Студенти, які не одержали позитивної оцінки за результатами заліку, йдуть на перескладання дисципліни. Перескладання проводиться у такій само формі, як і залікова робота. На перескладанні семестровий рейтинг та результати виконання залікової роботи анулюються, а рейтингова оцінка виставляється за результатами виконання роботи на перескладанні. Студенти, які після першого перескладання не одержали позитивної оцінки, йдуть на повторне перескладання дисципліни спеціалізований атестаційній комісії. Формат повторного перескладання визначається комісією. Студенти, які протягом семестру одержали менше 10 балів, не допускаються до складання семестрової атестації та рекомендуються кафедрі на відрахування або повторне проходження дисципліни.

Критерії оцінювання контрольних заходів, форми проведення іспиту/заліку та інші деталі рейтингової системи наведено у Положеннях про рейтингову систему, які є додатками до даного силабусу.

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, д.т.н. Олексійчук Антон Миколайович;
ас. Курінний Олег Вікторович.

Ухвалено кафедрою математичних методів захисту інформації (протокол № 6 від 22.06.2022 р.).

Затверджено Методичною комісією ФТІ (протокол № 6 від 30.06.2022 року).