



МЕТОДИ КРИПТОАНАЛІЗУ 1 (ПО 1.1)

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>Нормативна</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>1 курс, осінній семестр</i>
Обсяг дисципліни	<i>5 кред. / 150 годин Лекційних занять: 36 год. 36 год. - Лабораторні Самостійна робота студентів: 78 год.</i>
Семестровий контроль/ контрольні заходи	<i>Екзамен/ МКР, ДКР, опитування за темою заняття</i>
Розклад занять	<i>http://rozklad.kpi.ua</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: д.ф.-м.н., професор Савчук Михайло Миколайович Комп'ютерний практикум: асистент Ядуха Дарія Вікторівна</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

У дисципліні «Методи криптоаналізу 1» вивчаються загальні підходи та методи криптоаналізу криптографічних алгоритмів, протоколів, систем захисту інформації, а саме теоретико-інформаційний, кількісний, семантичний, підхід доведеної стійкості та інші. Також у рамках курсу розглядаються основні види криптографічних атак залежно від типу відомої інформації.

Метою вивчення дисципліни є надання майбутнім фахівцям знань щодо основних підходів та методів криптоаналізу систем захисту інформації, здобути вміння і навиків приводити дослідження систем криптографічного захисту інформації, отримувати оцінки їх стійкості та ефективності.

Згідно з вимогами освітньо-наукової програми «Математичні методи криптографічного захисту інформації» спеціальності 113 Прикладна математика другого (магістерського) рівня вищої освіти студенти після засвоєння навчальної дисципліни «Методи криптоаналізу» мають продемонструвати такі результати навчання:

Загальні компетентності

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

Фахові компетентності спеціальності

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, розробляти 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

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

РН 11 Проводити аналіз криптографічних алгоритмів, протоколів та систем

РН 12 Орієнтуватись у останніх досягненнях криптології

РН 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 дисциплін «Симетрична криптографія», «Асиметричні криптографічні системи та протоколи» та поширює і поглиблює відповідні компетентності та результати навчання. Однак матеріал курсу можна вивчати і без прямої прив'язки до зазначених дисциплін. Обов'язковим для опанування курсу є базові знання з лінійної та абстрактної алгебри, теорії чисел, дискретної математики, теорії ймовірностей та математичної статистики, теорії інформації та кодування, а також розуміння основних концепцій криптології.

Головний фокус дисципліни зосереджений на теоретичних засадах криптології як наукової галузі та їх імплементації у статистичних та алгебраїчних методах криптоаналізу. Отримані навички та засвоєнні знання можуть використовуватись для проведення наукових та прикладних досліджень у галузі криптології, а також для розв'язання прикладних задач у галузі криптографічного захисту інформації.

Кредитний модуль «Методи криптоаналізу 1» забезпечує такі дисципліни: «Методи криптоаналізу 2», «Проектування, розробка і реалізація криптографічних систем»; а також науково-дослідну роботу, науково-дослідну практику та виконання магістерської дисертації.

3. Зміст навчальної дисципліни

Розділ 1. Основні задачі і загальні підходи в криптоаналізі. Теоретико-інформаційний підхід в криптоаналізі.

Тема 1.1. Основні задачі криптоаналізу. Умови проведення криптоаналізу. Загальні підходи до визначення стійкості і напрямки криптоаналізу.

Тема 1.2. Басівський підхід в криптоаналізі. Побудова і дослідження детерміністичних та стохастичних розв'язувальних функцій.

Розділ 2. Складнісно-асимптотичний підхід в криптоаналізі. Методи перебору.

Тема 2.1. Кількісна оцінка складності і надійності криптоаналізу методом перебору при атаці на основі відкритого тексту.

Тема 2.2. Статистичні критерії перевірки на змістовний текст.

Тема 2.3. Атака на основі шифрованого тексту. Методи перебору і тотального перебору.

Розділ 3. Складнісно-асимптотичний підхід в криптоаналізі. Аналітичні методи криптоаналізу.

Тема 3.1. Задачі і основні напрямки аналітичних методів криптоаналізу. Знаходження ключа по частинах. Метод зустрічних атак з використанням пам'яті.

Тема 3.2. Розв'язання систем нелінійних булевих рівнянь над полем $GF(2)$. Метод лінеаризації введенням нових змінних.

Тема 3.3. Методи лінеаризації з опробуванням частини змінних.

Розділ 4. Складнісно-асимптотичний підхід в криптоаналізі. Статистичні методи криптоаналізу.

Тема 4.1. Знаходження ключа по частинам з перевіркою статистичних гіпотез.

Тема 4.2. Зведення нелінійних систем, що описують процес шифрування до лінійних систем зі спотвореннями.

Тема 4.3. Лінійні системи рівнянь над $GF(2)$ зі спотвореними правими частинами. Розв'язок методом повного перебору. Оцінки надійності і складності методу повного перебору.

Тема 4.4. Лінійні системи рівнянь над $GF(2)$ зі спотвореними правими частинами: алгоритм розв'язку Монте-Карло та ітеративний субекспоненційний алгоритм.

Розділ 5. Криптоаналіз асиметричних криптосистем і протоколів.

Тема 5.1. Криптоаналіз асиметричних криптосистем. Криптоаналіз криптосистеми RSA.

Тема 5.2. Атаки на криптосистему RSA.

Тема 5.3. Криптографічні протоколи. Компрометація криптопротоколів.

Розділ 6. Концепції стійкості криптографічних алгоритмів і протоколів.

Тема 6.1. Формалізація поняття стійкості криптосистем. Типи і сценарії зловмисників. Розширення поняття цілком таємної криптосистеми за Шенноном.

Тема 6.2. Теоретичні моделі стійкості криптографічних алгоритмів і протоколів. Семантична і доказова стійкості. Стійкість до атак нерозрізненого шифрування.

4. Навчальні матеріали та ресурси

Базова рекомендована література

1. Сушко С.О., Кузнецов Г.В., Фомичева Л.Я., Кораблев А.В. Математичні основи криптоаналізу. - Д.: Національний гірничий університет, 2010. – 465 с.
2. Konheim A.G. Cryptography: A Primer. – N.Y.: John Wiley & Sons, 1981.
3. Завадская Л.А., Савчук М.М. Математичні методи захисту інформації: курс лекцій. – К.: НТУУ „КПІ”, 2008. - Ч.1. – 128 с.
4. Задірака В.К., Олексюк О.С. Комп’ютерна криптологія. – К.: 2002. – 504 с.
5. Владислав Лещенко, Ніна Пекарчук, Михайло Савчук. Порівняльний аналіз складності методів лінеаризації та перебору розв’язання систем нелінійних булевих рівнянь // Захист інформації, 2020. Т.22, №1. – С. 33-42.

Допоміжна рекомендована література

1. Задірака В.К., Олексюк О.С. Методи захисту фінансової інформації. – К.: Вища школа, 2002. - 457 с.
2. Інформаційна безпека : навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарев [та 8 інших] ; за загальною редакцією Ю.Я. Бобала та І.В. Горбатого. - Львів : Видавництво Львівської політехніки, 2019. – 573 с.
3. Блінцов В.С., Гальчевський Ю.Л. Практикум з криптології: Навчальний посібник. – Миколаїв: НУК, 2005. -172 с.
4. Kovalenko I.N.,Savchuk M.N. On a statistical algorithm to decode heavily corrupted linear codes / Applied Probability and Stochastic Processes. – Berkeley: Kluwer Academic Publishers, 1999. – P. 73-82
5. Коваленко І.М. Про алгоритм субекспоненціальної складності декодування сильно спотворених лінійних кодів// Доповіді АН УРСР. Сер. А. – 1988. – № 10. – С. 16-17.
6. Henk C.A. van Tilborg. Fundamentals of Cryptology. – A Professional Reference and Interactive Tutorial. – Kluwer Academic Publishers, 1999, 2000. Second Printing 2001.
7. Song Y.Yan.Cryptanalytic Attacks on RSA.- Springer.- 2008.- 255 p.
8. Клесов О.І. Елементарна теорія чисел та елементи криптографії: підручник. – Київ: ТВіМС, 2016. – 412 с.

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
Розділ 1. Основні задачі і загальні підходи в криптоаналізі. Теоретико-інформаційний підхід в криптоаналізі.	
1	Криптографічна стійкість. Основні задачі криптоаналізу. Теоретична і практична стійкість. Алгебраїчно-ймовірнісні моделі криптосистем. Умови проведення криптоаналізу. Ієрархія криптографічних атак залежно від типу відомої інформації.
2	Рівень розкриття і степінь порушення системи криптографічного захисту. Цінність та час життя різних типів інформації. Зовнішні та внутрішні фактори, які впливають на проведення криптоаналізу.
3	Загальні підходи в визначенні стійкості криптографічних систем та загальні напрями в криптоаналізі. Теоретико-інформаційний підхід в криптоаналізі. Складнісно-асимптотичний криптоаналіз. Системний підхід в визначенні стійкості і криптоаналізі.
4	Доказова стійкість. Семантичне розуміння стійкості. Оцінювання необхідного матеріалу для криптоаналізу та його вартості.
5	Баєсівський теоретико-інформаційний підхід в криптоаналізі. Модель криптосистеми (шифру) Шеннона. Побудова і дослідження детерміністичних та стохастичних розв'язувальних функцій. Властивості детерміністичної розв'язувальної функції.
6	Оптимальна детерміністична розв'язувальна функція. Баєсівська розв'язувальна функція. Баєсівське прийняття рішення за детерміністичною розв'язувальною функцією.
7	Стохастична розв'язувальна функція. Баєсівське прийняття рішення в криптоаналізі стохастичною розв'язувальною функцією.
8	Зв'язок між стохастичними і детерміністичними розв'язувальними функціями. Баєсівська процедура прийняття рішення з урахування теореми Біркгофа.
Розділ 2. Складнісно-асимптотичний підхід в криптоаналізі. Методи перебору.	
9	Метод криптоаналізу послідовним перебором по ключах. Кількісна оцінка складності і надійності криптоаналізу методом перебору при атаці на основі відкритого тексту прямим перебором по ключах без помилок в випробуванні ключів. Асимптотичний аналіз оцінок. Характеристики надійності та трудомісткості методів.
10	Конвеєрний метод розпаралелювання перебору по ключах при атаці на основі відкритого тексту. Розпаралелювання перебору по ключах при атаці на основі відкритого тексту розбиттям простору ключів та розпаралелювання з незалежним і випадковим вибором ключа різними процесорами. Оцінки складності. Надійність і трудомісткість методів.

11	Статистичні критерії перевірки на змістовний текст. Критерії заборонених l – грам. Критерій заборонених знаків і біграм. Критерій, що базується на l -грамах, які часто зустрічаються у змістовному тексті.
12	Критерій на змістовний текст, побудований на індексі відповідності. Критерій пустих ящиків. Лінійний статистичний критерій на роздільних статистиках. Ентропійний і структурний критерії.
13	Атаки на основі шифрованого тексту з помилками при випробуванні ключів. Методи перебору і тотального перебору. Криптоаналіз перебором ключів при атаці на основі шифрованого тексту з використанням статистичного критерію перевірки на змістовний текст.
14	Розрахунки характеристик надійності і трудомісткості методів перебору ключів при атаці на основі шифрованого тексту з використанням статистичного критерію. Часткові випадки для тотального перебору.
Розділ 3. Складнісно-асимптотичний підхід в криптоаналізі. Аналітичні методи криптоаналізу.	
15	Аналітичні методи криптоаналізу. Зведення криптоаналізу до розв'язання нелінійних систем рівнянь. Постановка задачі, головні напрямки. Метод розбиття простору ключів і простору розв'язків системи нелінійних рівнянь на декартовий добуток підпросторів і випробування ключа (невдомих системи) по частинах.
16	Деякі спеціальні методи розв'язання нелінійних систем рівнянь. Розв'язок систем нелінійних рівнянь над полем $GF(2)$, що зводяться до трапецієподібного вигляду. Метод зустрічних атак з використанням пам'яті (зустріч посередині). Характеристики трудомісткості і надійність методів.
17	Зведення нелінійної системи чи її підсистем до лінійної, або до системи суттєво меншого степеня. Метод лінеаризації введенням нових змінних. Алгоритм розв'язку.
18	Ймовірнісні моделі системи нелінійних рівнянь та асимптотичні оцінки. Теоретичні і статистичні порівняльні оцінки середньої складності методів лінеаризації і повного перебору. Рівняння для лінії розмежування відносно складності методів лінеаризації і повного перебору.
19	Лінеаризація опробуванням частини змінних. Зведенням до лінійної системи спеціальним підбором та фіксацією частини змінних (на основі рідкої події). Розв'язання нелінійної системи зведенням до лінійної системи спеціальним підбором та перебором частини змінних.
Розділ 4. Складнісно-асимптотичний підхід в криптоаналізі. Статистичні методи криптоаналізу.	
20	Статистичні методи в криптоаналізі. Побудова статистичних моделей криптосистем. Статистичний аналог. Знаходження ключа по частинах з перевіркою статистичних гіпотез. Статистичний криптоаналіз потокового шифру генератора Джиффі, складність статистичного криптоаналізу.
21	Зведення нелінійних систем, що описують процес шифрування до лінійних систем зі спотвореннями. Ймовірнісна модель постановки задачі про лінійні системи рівнянь над $GF(2)$ зі спотвореннями.

22	Алгоритм знаходження розв'язку методом повного перебору лінійної системи рівнянь над $GF(2)$ зі спотвореними правими частинами. Знаходження імовірнісного розподілу нев'язки при випробуванні вектору рішення. Оцінка складності і надійності алгоритму повного перебору знаходження розв'язку лінійної системи рівнянь зі спотвореними правими частинами.
23	Метод Монте-Карло розв'язку системи лінійних рівнянь над скінченним полем $GF(2)$ зі спотвореними правими частинами. Трудомісткість і надійність методу. Експериментальні оцінки складності та надійності алгоритмів розв'язку системи лінійних рівнянь над полем $GF(2)$ зі спотвореними правими частинами.
24	Субекспоненціальний ітеративний метод І. Н. Коваленка знаходження розв'язку системи лінійних рівнянь над полем $GF(2)$ зі спотвореними правими частинами (або знаходження інформаційного слова сильно спотворених лінійних кодів).
Розділ 5. Криптоаналіз асиметричних криптосистем і протоколів.	
25	Основні односторонні функції асиметричної криптографії та складність їх обернення. Криптоаналіз асиметричних криптосистем. Загальні вимоги до параметрів при побудові криптосистем на основі односторонніх функцій Діффі-Геллмана, RSA та Рабіна.
26	Деякі атаки на криптосистему RSA при неякісному виборі параметрів. Атака на криптосистему RSA з відомою або малою різницею $ p-q $ дільників модуля $n=pq$. Атака на основі шифрованого тексту з малою експонентою з використанням китайської теореми про лишки. Атака безключового читання на основі шифрованого тексту з використанням спільного модуля.
27	Атаки на шифрування і на цифровий підпис RSA за допомогою вибраного тексту, з використанням підпису іншого повідомлення та неявного використання секретного ключа.
28	Атака зі зв'язаними повідомленнями з малим відкритим ключем. Криптоаналіз RSA методом зустрічних атак. Циклічна атака на алгоритми шифрування для асиметричних та симетричних криптосистем.
29	Атаки з використанням інформації зі стороннього каналу. Атака на RSA по часу обчислень. Атака з використанням помилок при обчисленнях в реалізації асиметричних алгоритмів шифрування та цифрового підпису.
30	Аналіз криптографічних протоколів асиметричної криптографії. Задачі і цілі атак на криптографічні протоколи. Атаки на протокол зв'язку абонентів мережі з використанням криптосистеми RSA з «пасивним» та з «активним» перехопленням даних з каналів зв'язку одним з учасників мережі або додатковими учасниками. Компрометація протоколу відкритого розподілу ключів Діффі і Геллмана атакою «супротивник посередині».
Розділ 6. Концепції стійкості криптографічних систем і протоколів.	
31	Формалізація поняття стійкості криптосистем. Типи і сценарії зловмисників.
32	Розширення поняття цілком таємної криптосистеми за Шенноном з урахуванням можливостей і способу використання криптоаналітиком отриманої в результаті криптоаналізу інформації. Ієрархія різних класів досконалих шифрів.
33	Теоретичні моделі семантичної і доказової стійкості. Стійкість до атак нерозрізненого шифрування. Формальні методи аналізу протоколів.

34	Інші концепції стійкості криптоалгоритмів і підходів до криптоаналізу.
35	Модульна контрольна робота.

Комп'ютерний практикум - лабораторні.

№ з/п	Назва теми заняття
1-2	Комп'ютерний практикум №1. Баєсівський підхід в криптоаналізі: побудова і дослідження детерміністичних вирішуючих функцій.
3	Комп'ютерний практикум №1. Баєсівський підхід в криптоаналізі: побудова і дослідження стохастичних вирішуючих функцій.
4-5	Комп'ютерний практикум №2. Статистичні критерії на відкритий текст.
6	Комп'ютерний практикум №3. Криптоаналіз асиметричних криптосистем на прикладі RSA. Атака з малою експонентою на основі китайської теореми про лишки.
7-8	Комп'ютерний практикум №3. Криптоаналіз асиметричних криптосистем на прикладі RSA. Атака «зустріч посередині».
9	Підведення підсумків

6. Самостійна робота студента

Завданням самостійної роботи студентів є навчити студентів самостійно працювати з літературою, творчо сприймати навчальний матеріал і осмислювати його та формування навичок до щоденної роботи з метою одержання та узагальнення знань, умінь і навичок. На самостійну роботу відводяться наступні види завдань:

- обробка і осмислення інформації, отриманої безпосередньо на заняттях;
- робота з відповідними підручниками та особистим конспектом лекцій;
- самостійне розв'язання лекційних запитань;
- виконання підготовчої роботи до лабораторних (комп'ютерних практикумів);
- підготовка до модульної контрольної роботи;
- виконання домашньої контрольної роботи;
- підготовка до складання семестрового контролю.

Студент повинен завчасно готуватись до лекцій та лабораторних (комп'ютерного практикуму). Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед здачею комп'ютерного практикуму на занятті студенту необхідно самостійно або в бригаді з двох людей виконати відповідний згідно з календарним планом комп'ютерний практикум. Студенту надається не менше місяця на виконання ДКР.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- **Відвідування занять.** Відвідування лекцій та практичних занять рекомендується згідно Положення про організацію освітнього процесу КПІ ім. Ігоря Сікорського. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опанувати самостійно. У будь-якому випадку студентам рекомендується відвідувати усі види

занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання лабораторних (комп'ютерних практикумів) та ДКР. Система оцінювання орієнтована на отримання балів за виконання завдань, які спрямовані на опанування теоретичних знань та розвиток практичних умінь та навичок.

- **Лабораторні (Комп'ютерні практикуми).** Комп'ютерні практикуми виконуються студентом самостійно, або в бригаді з двох студентів. При виконанні комп'ютерного практикуму не дозволяється використовувати готові реалізації та програмний код, створений іншими особами. Здача комп'ютерного практикуму складається з двох частин: практичної та теоретичної. Здача практичної частини виконується студентом самостійно або в бригаді з двох студентів (залежно від обраного типу виконання завдання). При складанні практичної частини комп'ютерного практикуму студенти зобов'язані продемонструвати процес та результати застосування створеної програмної реалізації, а також відповісти на питання стосовно створеного програмного коду. Теоретична частина комп'ютерного практикуму складається кожним студентом індивідуально (навіть якщо практична частина комп'ютерного практикуму виконувалась в бригаді). При складанні теоретичної частини комп'ютерного практикуму студенту потрібно відповісти на теоретичні питання за темою комп'ютерного практикуму.
- **ДКР.** Виконується кожним студентом індивідуально. Для його виконання студенту необхідно опрацювати основну\допоміжну рекомендовану літературу та\або інші доступні студенту наукові джерела за темою теоретичного завдання.
- **Поточний контроль:** експрес-опитування, опитування за темою заняття, **модульна контрольна робота.**
- **Пропущені контрольні заходи.** Результат модульної контрольної роботи для студента(-ки), який не з'явився на контрольний захід, є нульовим. У такому разі, студент(-ка) має можливість написати модульну контрольну роботу, але максимальний бал за неї буде дорівнювати 50% від загальної кількості балів. Повторне написання модульної контрольної роботи не допускається.
- **Оголошення результатів контрольних заходів.** Захист лабораторних робіт (комп'ютерних практикумів), ДКР, МКР проводиться у формі співбесіди з викладачем. Під час захисту студент зобов'язаний вміти розповісти про порядок виконання завдань відповідного комп'ютерного практикуму, та завдань вказаних викладачем і відповісти на теоретичні питання за темами задач. Результати виконання робіт 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 екзамену вказуються на бланках (завдання, які виконували студенти) з позначенням всіх помилок, коректної або некоректної відповіді, а також з коментарями, зауваженнями тощо. Усна частина екзамену проводиться у форматі співбесіди зі студентом. Студент зобов'язаний вміти розповісти про розв'язування вказаних викладачем задач та відповісти на теоретичні питання за темами курсу.
- **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 випадку, якщо в результаті перевірки програмного коду студента виявлено плагіат більше 30%, студент зобов'язаний виконати завдання повторно, отримає штраф -10 балів до рейтингу та не матиме можливість скласти іспит на основній сесії. У випадку, коли плагіат програмного коду студента становить більше 10%, але менше 30%, студент отримає штраф -10 балів до рейтингу та зобов'язаний виконати завдання повторно в визначені викладачем терміни.

- **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 оцінювального листа та/або зауважень.

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

- 1) Комп'ютерний практикум №1. Баєсівський підхід в криптоаналізі: побудова і дослідження детерміністичної та стохастичної вирішуваних функцій: 12 балів.
- 2) Комп'ютерний практикум №2. Статистичні критерії на відкритий текст»: 12 балів.
- 3) Комп'ютерний практикум №3. Криптоаналіз асиметричних криптосистем на прикладі RSA»: 12 балів.
- 4) Модульна контрольна робота: 14 балів.
- 5) ДКР 10 балів.
- 6) Екзамен: 40 балів.

Поточний контроль: комп'ютерні практикуми №1, №2, №3; розрахункова робота, експрес-опитування, опитування за темою заняття.

Календарний контроль. Для отримання відмітки «атестовано» при першому календарному контролі необхідно здати теоретичну та практичну частину комп'ютерного практикуму №1. Для отримання відмітки «атестовано» при другому календарному контролі необхідно здати теоретичну та практичну частину комп'ютерних практикумів №1 та №2.

Семестровий контроль: екзамен, що складається з письмової та усної складових.

Умови допуску до семестрового контролю. Зараховані комп'ютерні практикуми №1, №2 та №3, а також зарахована розрахункова робота, причому у жодній з цих робіт не виявлено плагіату більше 10%. Кількість отриманих студентом балів за семестр має не менше 20.

№ з/п	Контрольний захід	Макс бал	Ваговий бал	Кількість	Всього
1	Комп'ютерний практикум	12	1	3	36

2	ДКР	10	1	1	10
3	Модульна контрольна робота	14	1	1	14
4	Екзамен	40	1	1	40
5					100

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

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль

- 1) Задачі криптоаналізу. Криптографічна стійкість. Ієрархія атак на криптосистеми в залежності від типу відомої інформації та інших характеристик шифрів і вимог до інформації, що підлягає захисту. Підходи та загальні методи в криптоаналізі.
- 2) Шеннонівська модель симетричних криптосистем. Баєсівський підхід у криптоаналізі. Детерміністичні розв'язувальні функції.
- 3) Баєсівський підхід у криптоаналізі. Стохастичні розв'язувальні функції.
- 4) Складніший підхід в криптоаналізі. Криптоаналіз методами перебору. Постановка задачі при атаці на основі відкритого тексту, визначення характеристик надійності та трудомісткості (складності). Алгоритм криптоаналізу, оцінки надійності та складності.
- 5) Методи розпаралелювання перебору без помилок в випробуванні ключів при атаці на основі ВТ: алгоритми криптоаналізу, оцінки надійності та складності різних алгоритмів.
- 6) Критерії на відкритий (змістовний) текст.
- 7) Методи перебору при атаці на основі ШТ з помилками при випробуванні ключів. Постановка задачі при атаці на основі ШТ для симетричних і асиметричних криптосистем. Загальний опис та кроки алгоритму, надійність та складність. Розрахунки надійності та трудомісткості.
- 8) Аналітичні методи криптоаналізу. Постановка задачі. Метод розбиття простору ключів і простору розв'язків системи нелінійних рівнянь на декартовий добуток підпросторів і випробування ключа (невідомих системи) по частинам. Оцінка трудомісткості.
- 9) Аналітичні методи. Розв'язання нелінійних систем булевих рівнянь приведенням їх до трапецоїдного виду. Оцінка трудомісткості. Зведення нелінійних систем до систем меншого степеню як підхід в криптоаналізі. Оцінки складності алгоритмів розв'язку систем лінійних рівнянь над скінченними полями.

- 10) Розв'язання нелінійних систем булевих рівнянь методами лінеаризації за допомогою введення нових змінних. Оцінка трудомісткості і надійності.
- 11) Розв'язання нелінійних систем булевих рівнянь методами лінеаризації за допомогою випробування частини змінних та використовуючи рідкісні події. Оцінка трудомісткості та надійності.
- 12) Криптоаналіз методом зустрічних атак. Алгоритм атаки. Оцінка трудомісткості.
- 13) Статистичні методи. Побудова статистичних моделей криптосистем. Статистичний аналог. Знаходження ключа по частинам перевіркою статистичних гіпотез. Криптоаналіз генератора Джиффі.
- 14) Статистичні методи. Постановка задачі знаходження ключа з допомогою побудови системи лінійних систем рівнянь зі спотвореними правими частинами. Метод повного перебору розв'язання лінійних систем булевих рівнянь зі спотвореними правими частинами. Опис алгоритму знаходження розв'язку.
- 15) Метод повного перебору розв'язання лінійних систем булевих рівнянь зі спотвореними правими частинами: знаходження імовірнісного розподілу нев'язки при випробуванні вектора рішення, оцінки надійності та складності.
- 16) Метод Монте-Карло розв'язання лінійних систем булевих рівнянь із спотвореними правими частинами: опис алгоритму знаходження розв'язку, оцінки ймовірності помилок і складності.
- 17) Субекспоненціальний ітеративний метод І. Н. Коваленка розв'язання лінійних систем булевих рівнянь зі спотвореними правими частинами.
- 18) Основні односторонні функції асиметричної криптографії та складність їх обернення. Доказова стійкість. Загальні вимоги до параметрів при побудові криптосистем на основі односторонніх функцій Діффі-Геллмана, RSA та Рабіна.
- 19) Атака на RSA на основі ШТ: з «малою» експонентою; зі застосуванням спільного модуля.
- 20) Атака на RSA з відомою або малою різницею, атака зі зв'язаними повідомленнями і з «малою» експонентою.
- 21) Циклічна атака для асиметричних та симетричних криптосистем. Криптоаналіз RSA методом зустрічних атак («зустріч посередині»).
- 22) Атаки на шифрування і на цифровий підпис RSA за допомогою вибраного тексту та неявного використання секретного ключа.
- 23) Атака на RSA за побічними каналами. Приклади атак на RSA за часом обчислення та з використанням помилок - атака «мікрохвильовкою».
- 24) Атаки на криптографічні протоколи. Атака на протокол розподілу ключів в мережі з використанням третьої сторони (зі зговором двох легальних користувачів).
- 25) Концепції стійкості криптографічних алгоритмів, протоколів і систем.

Робочу програму навчальної дисципліни (силабус):

Склали: *д.ф.-м.н., професор Савчук Михайло Миколайович; асистент Ядуха Дарія Вікторівна.*

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

Погоджено Методичною комісією ННФТІ (протокол № 6 від 30.06.2022)

