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

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

АСИМЕТРИЧНІ КРИПТОСИСТЕМИ ТА ПРОТОКОЛИ 2 (ПО 7.2)

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*11 Математика та статистика*
Спеціальність	*113 Прикладна математика*
Освітня програма	*Математичні методи криптографічного захисту інформації*
Статус дисципліни	*Обов'язкова (нормативна) (цикл професійної підготовки)*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*4 курс, весняний семестр*
Обсяг дисципліни	*Загальна кількість: 2 кредити ЄКТС / 60 год., з них* *Лекційних занять: 18 год.* *Лабораторних занять: 18 год.* *Самостійна робота студентів: 24 год.*
Семестровий контроль/ контрольні заходи	*залік, МКР, поточний контроль*
Розклад занять	*http://ipt.kpi.ua/navchalnij-protses*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Лектор: к.т.н., Кучинська Наталія Вікторівна (kuchynskanv-ipt@lll.kpi.ua)* *к.ф.-м.н., Фесенко Андрій В'ячеславович (fesenko.andrii@lll.kpi.ua)* *Лабораторні: к.т.н., Кучинська Наталія Вікторівна (kuchynskanv-ipt@lll.kpi.ua)* *к.ф.-м.н., Фесенко Андрій В'ячеславович (fesenko.andrii@lll.kpi.ua)*
Розміщення курсу	*Google Classroom*

Програма навчальної дисципліни

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

Навчальна дисципліна "Асиметричні криптосистеми та протоколи 2" присвячена дослідженню різноманітних криптографічних протоколів та їхнього застосуванням у сучасних системах обміну інформації.

Метою навчальної дисципліни "Асиметричні криптосистеми та протоколи 2" є ознайомлення студентів з формалізацією криптографічних протоколів, особливостями їхньої побудови та методами аналізу; формування у студентів навичок використання методів аналізу криптографічних протоколів.

Предметом навчальної дисципліни є формальні моделі криптографічних протоколів, методи аналізу протоколів, особливості побудови сучасних криптографічних протоколів.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі результати навчання:

1) Знання:

- класифікації криптографічних протоколів;
- формальних моделей функціонування криптографічних протоколів;
- методів аналізу протоколів;

– сучасних протоколів встановлення ключа та інших криптографічних протоколів.

2) Уміння:

– аналізувати криптографічні протоколи;
– використовувати сучасні методи побудови протоколів у відповідності до необхідних властивостей.

3) Досвід: побудови криптографічних протоколів та методів аналізу протоколів.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні компетентності та результати навчання за освітньою програмою::

Загальні компетентності

ЗК 1 — Здатність учитися і оволодівати сучасними знаннями.
ЗК 3 — Здатність генерувати нові ідеї (креативність).
ЗК 7 — Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК 8 — Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК 10 — Навички у використанні інформаційних і комунікаційних технологій.
ЗК 13 — Навички міжособистісної взаємодії.

Фахові компетентності

ФК 1 — Здатність використовувати й адаптувати математичні теорії, методи та прийоми для доведення математичних тверджень і теорем.
ФК 2 — Здатність виконувати завдання, сформульовані у математичній формі.
ФК 3 — Здатність обирати та застосовувати математичні методи для розв'язання прикладних задач, моделювання, аналізу, проектування, керування, прогнозування, прийняття рішень.
ФК 7 — Здатність експлуатувати та обслуговувати програмне забезпечення автоматизованих та інформаційних систем різного призначення.
ФК 9 — Здатність до проведення математичного і комп'ютерного моделювання, аналізу та обробки даних, обчислювального експерименту, розв'язання формалізованих задач за допомогою спеціалізованих програмних засобів.
ФК 13 — Здатність зрозуміти постановку завдання, сформульовану мовою певної предметної галузі, здійснювати пошук та збір необхідних вихідних даних.
ФК 14 — Здатність сформулювати математичну постановку задачі, спираючись на постановку мовою предметної галузі, та обирати метод її розв'язання, що забезпечує потрібні точність і надійність результату.
ФК 17 — Здатність проектувати, розробляти, реалізовувати та провадити первинний аналіз криптографічних алгоритмів різного профілю.
ФК 18 — Навички розв'язування специфічних математичних та комп'ютерних задач, які виникають при розробці, реалізації та аналізі криптографічних систем.

Програмні результати навчання

РН 1 — Демонструвати знання й розуміння основних концепцій, принципів, теорій прикладної математики і використовувати їх на практиці.
РН 3 — Формалізувати задачі, сформульовані мовою певної предметної галузі; формулювати їх математичну постановку та обирати раціональний метод вирішення; розв'язувати отримані задачі аналітичними та чисельними методами, оцінювати точність та достовірність отриманих результатів.
РН 7 — Вміти проводити практичні дослідження та знаходити розв'язок некоректних задач.
РН 11 — Вміти застосовувати сучасні технології програмування та розроблення програмного забезпечення, програмної реалізації чисельних і символьних алгоритмів.
РН 13 — Використовувати в практичній роботі спеціалізовані програмні продукти та програмні системи комп'ютерної математики.
РН 14 — Виявляти здатність до самонавчання та продовження професійного розвитку.
РН 15 — Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.
РН 16 — Демонструвати навички взаємодії з іншими людьми, уміння працювати в команді.
РН 19 — Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми.
РН 22 — Володіти основними принципами та методами побудови симетричних та асиметричних криптографічних систем у різних моделях обчислення, а також методами їх аналізу.
РН 23 — Використовувати у професійній діяльності криптографічні примітиви та протоколи.

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

Для засвоєння матеріалу дисципліни "Асиметричні криптосистеми та протоколи 2" студент повинен успішно та вчасно опановувати дисципліну "Асиметричні криптосистеми та протоколи 1", попередньо засвоївши термінологію та поняття з дисципліни "Симетрична криптографія". Дисципліна "Асиметричні криптосистеми та протоколи 2" є продовженням дисципліни "Асиметричні криптосистеми та протоколи 1", однак за наявності необхідних навичок може опановуватись студентами незалежно.

Отримані практичні навички та засвоєні знання будуть корисними для проходження переддипломної практики та дипломного проектування.

3. Зміст навчальної дисципліни

Розділ 1. Базові криптографічні протоколи.
Тема 1.1. Загальні характеристики протоколів.
Тема 1.2. Протоколи встановлення ключа.
Тема 1.3. Протоколи захищених обчислень.
Розділ 2. Побудова сучасних криптографічних протоколів.
Тема 2.1. Протоколи систем обміну повідомленнями.
Тема 2.2. Криптографічні протоколи захищеної передачі даних в інтернеті.

4. Навчальні матеріали та ресурси

Базова рекомендована література:

1. *Вербіцький О.В.* Вступ до криптології // Львів: Науково-технічна література, 1998. 248 с.

2. *Кузнецов Г.В., Фомичев В.В., Сушко С.О. Фомичова Л.Я.* Математичні основи криптографії // Дніпропетровськ: Національний гірничій університет, 2004. Ч. 1. 391 с.

3. *Задірака В.К., Олексюк О.С.* Комп'ютерна криптологія // К.: 2002. 504 с.

4. *Dan Boneh, Victor Shoup* A Graduate Course in Applied Cryptography [Електронний ресурс] // Режим доступу: https://toc.cryptobook.us/book.pdf

Допоміжна рекомендована література:

1. *Wenbo Mao* Modern Cryptography: Theory and Practice // Prentice Hall Professional Technical Reference, 2003. — 740 pp. — ISBN13: 9780130669438.

2. *Alfred Menezes, Paul van Oorschot, Scott Vanstone* Handbook of Applied Cryptography // — CRC Press, 2001. — 810 pp. — ISBN-13: 978-1-133-18779-0.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та стратегії взаємодії викладача та студентів для засвоєння студентами матеріалу та опанування практичних навичок. Для лекційних занять використовуються пояснювально-ілюстративний метод та метод проблемного викладу, для проведення лабораторних занять — частково-пошуковий та дослідницький методи, щоб спонукати студентів до самостійного дослідницького процесу. За джерелом передачі змісту для проведення лекційних занять застосовуються словесний метод.

Дистанційна форма навчання: платформа дистанційного навчання «Сікорський» на основі системи Google Classroom та платформа для проведення онлайн-зустрічей Zoom, електронна пошта, канали Telegram.

Лекційні заняття

Перелік лекційних занять наводиться у послідовності їхнього викладання та опанування. Кожне заняття займає дві академічні години аудиторного часу та вимагає в середньому дві години самостійної роботи.

№ з/п	Назва теми лекції та перелік основних питань
	Розділ 1. Базові криптографічні протоколи.
1	*Загальні характеристики протоколів.* Класифікація криптографічних протоколів.
2	*Протоколи встановлення ключа.* Протоколи встановлення ключа з використанням симетричних криптографічних методів.
3	Протоколи встановлення ключа з використанням асиметричних криптографічних методів.
4	*Протоколи захищених обчислень.*
	Розділ 2. Побудова сучасних криптографічних протоколів.
5	*Протоколи систем обміну повідомленнями.*
6	*Криптографічні протоколи захищеної передачі даних в інтернеті.*
7	Криптографічні протоколи HTTP/TLS.
8	Криптографічні протоколи бездротового з'єднання.
9	Особливості побудови сучасних криптографічних протоколів та їхнього застосування. МКР.

Лабораторні роботи

Для закріплення теоретичних знань та формування необхідних практичних навичок студенти повинні виконати дві лабораторні роботи:

1. застосування систем автоматичної перевірки протоколів до обраних протоколів встановлення ключа;
2. застосування програмних застосунків аналізу мережевих пакетів для розпізнання структури мережевих протоколів (аналізу мережевих пакетів та їх полів).

Лабораторні роботи можуть виконуватись самостійно або у парі. У другому випадку виконання задач лабораторних робіт розподіляється між учасниками на власний розсуд, а оцінка за виконання ставиться обом учасникам однакова, за фактичне виконання поставлених задач.

Індивідуальне завдання

Для закріплення теоретичних знань студенти повинні виконати індивідуальне завдання. Виконання цього завдання передбачає створення звіту на обрану тему, яка узгоджується з викладачем.

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях.

З метою кращого засвоєння матеріалу дисципліни, а також формування навичок самостійної роботи студентам пропонується виконати індивідуальне завдання за обраними темами, погодженими з викладачем, а також дві лабораторні роботи. Для підготовки до виконання індивідуального завдання слід скористатися рекомендованою літературою та записами лекцій. Кінцевий термін виконання індивідуального завдання оголошується викладачем.

Політика та контроль

7. Політика навчальної дисципліни освітнього компонента

Форми організації освітнього процесу, види навчальних занять і оцінювання результатів навчання регламентуються *Положенням про організацію освітнього процесу в Національному технічному університеті України "Київському політехнічному інституті імені Ігоря Сікорського"*.

Відвідування занять

Студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання лабораторних робіт та модульної контрольної роботи. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, які здатні розвинути практичні уміння та навички.

Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно.

Оголошення результатів контрольних заходів

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 теоретичного тесту вказуються на бланках для теоретичних тестів (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.

Політика академічної поведінки та доброчесності

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.

Конфліктні ситуації мають відкрито обговорюватись в академічних групах з викладачем, необхідно бути взаємно толерантним, поважати думку іншого. Плагіат та інші форми нечесної роботи є неприпустимими.

Всі індивідуальні завдання студент має виконати самостійно із використанням рекомендованої літератури й отриманих знань та навичок. Цитування в письмових роботах допускається тільки із відповідним посиланням на авторський текст. Недопустимими є підказки і списування у ході теоретичних опитувань, на контрольних роботах і тестах, та на заліку.

У разі порушення принципів академічної доброчесності студентом він може бути не допущеним до основного складання заліку. Бали семестрового рейтингу, набрані з порушенням принципів академічної доброчесності, будуть анульовані.

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.

Зокрема, необхідно дотримуватися моральних норм, правил етичної поведінки, принципів та правил академічної доброчесності. Повага один до одного дає можливість ефективніше досягати поставлених командних результатів. Тому необхідно дотримуватись таких норм академічної етики як дисциплінованість, дотримання субординації, чесність, відповідальність, робота в аудиторії з вимкненими мобільними телефонами. При використанні свого ноутбука або телефону (чи інших пристроїв) для аудіо- чи відеозапису під час лекційних або практичних занять, необхідно заздалегідь отримати дозвіл викладача.

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 наведених зауважень.

Правила призначення заохочувальних балів

Передбачено заохочувальні бали за
– розв'язання додаткових додаткових завдань при виконанні лабораторних робіт(до 10 заохочувальних балів).

Загальна кількість зароблених заохочувальних балів для одного студента за семестр не може перевищувати 10 балів. Заохочувальні бали виставляються виключно наприкінці курсу і не впливають на проміжні атестації.

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

№ з/п	Контрольний захід	Макс. бал	Ваговий бал	Кіл-ть	Усього
1.	Модульна контрольна робота	20	1	1	20
2.	Теоретичний тест	10	1	3	30
3.	Лабораторні роботи	20	1	2	40
4.	Індивідуальне завдання	10	1	1	10
	Усього				100

Поточний контроль

Поточний контроль здійснюється шляхом проведення теоретичних тестів та контролю виконання лабораторних робіт.

Календарний контроль

Проміжна атестація студентів (далі — атестація) є календарним рубіжним контролем поточного стану виконання вимог силабусу та проводиться двічі за семестр, на 8-му та 14-му навчальному тижнях кожного семестру. Для одержання першої атестації (на 8-му навчальному тижні) та другої атестації (на 14-му навчальному тижні) поточний рейтинг студента повинен бути щонайменше 60% від максимуму балів, які студент може отримати за всі контрольні заходи, що відбулися на час атестації.

Зауважимо, що оцінювання виконання індивідуальних завдань відбувається наприкінці семестру, як і виставлення загальної кількості заохочувальних балів, а, отже, на проміжну атестацію студентів впливають виключно результати всіх теоретичних тестів, оцінених до моменту виставлення проміжної атестації, а також результати першої лабораторної роботи.

Таким чином на результат першої атестації впливають тільки оцінки за перший теоретичний тест (максимальна кількість балів за який дорівнює 10) і першу лабораторну роботу (максимальна кількість балів за яку дорівнює 20). На результат другої атестації впливають додатково оцінки за другий теоретичний тест (максимальна кількість балів за який дорівнює 10) і другу лабораторну роботу (максимальна кількість балів за яку дорівнює 20).

Таблиця необхідної кількості балів для отримання проміжних атестацій

Проміжна атестація	*Максимально можлива кількість балів*	*Необхідна кількість балів*
перша атестація	30	18
друга атестація	60	36

Семестровий контроль

Рейтингова оцінка студента складається з результатів роботи в семестрі і є сумою всіх балів, які він отримує:
– за виконання модульної контрольної роботи;
– за написання теоретичних тестів;
– за виконання лабораторних робіт;
– за виконання індивідуального завдання;
– як заохочувальні бали.

Рейтингова оцінка з урахуванням заохочувальних балів не може перевищувати 100 балів.

Якщо семестровий рейтинг складає не менше 60 балів і зараховані всі лабораторні роботи й індивідуальне завдання, студенту виставляється відповідна оцінка, окрім випадку, коли студент не погоджується із нею.

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

Студенти, які набрали від 50 до 60 балів за семестр, і в яких є зарахованими всі лабораторні роботи й індивідуальне завдання, за бажанням замість складання заліку можуть пройти усну співбесіду із викладачем за матеріалом дисципліни. На співбесіді, ставиться до 10 теоретичних питань, кожне з яких оцінюється в 1 бал. Студент може підвищити свій семестровий рейтинг до мінімальної позитивної оцінки. Якщо кількості правильних відповідей не вистачило для отримання мінімальної позитивної оцінки, то студент йде на перескладання заліку.

Студенти, які не одержали позитивну оцінку за результатами роботи у семестрі (але при цьому їхній семестровий рейтинг складає не менше 30 балів і зараховані всі лабораторні роботи й індивідуальне завдання), та студенти, які не погоджуються із такою оцінкою, на останньому практичному занятті виконують залікову роботу. При цьому їхній семестровий рейтинг анулюється, включно із заохочувальними балами, а рейтингова оцінка виставляється за результатом виконання залікової роботи. Залікова робота містить тест з теоретичного матеріалу та практичну частину. Максимальна кількість балів за залікову роботу складає 100 балів.

Студенти, які не одержали позитивної оцінки за результатами заліку, йдуть на складання заліку на додатковій сесії. До складання заліку на додатковій сесії допускаються тільки студенти, усі лабораторні роботи яких є зарахованими включно з індивідуальним завданням до дати складання заліку на додатковій сесії, і семестровий рейтинг був не меншим за 10 балів. Робота на перескладанні має той самий вигляд, як і залікова робота. На перескладанні семестровий рейтинг та результати виконання залікової роботи анулюються, а рейтингова оцінка виставляється за результатами виконання роботи на перескладанні. Максимальна кількість балів за залікову роботу на додатковій сесії також складає 100 балів.

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

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
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):

Склали: ст. викладач кафедри ММЗІ, к.ф.-м.н. Фесенко Андрій В'ячеславович,
доцент кафедри ММЗІ, к.т.н. Кучинська Наталія Вікторівна

Ухвалено кафедрою математичних методів захисту інформації (протокол №2 від 16.02.2022).

Погоджено Методичною комісією НН ФТІ (протокол №6 від 30.06.2022).