



Проектування, розробка і реалізація криптографічних систем

ПО-6

Робоча програма навчальної дисципліни (Силабус)

• Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>11 Математика і 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>II курс, осінній семестр</i>
Обсяг дисципліни	<i>120 годин (4 кредити) 36 год. лекції, 18 год. лабораторні роботи, срс 66 год</i>
Семестровий контроль/ контрольні заходи	<i>Іспит, модульна контрольна робота</i>
Розклад занять	<i>Rozklad.kpi.ua</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: д.т.н., Кудін Антон Михайлович, pplayshner@gmail.com Лабораторні: Селюх Поліна Валентинівна,</i>
Розміщення курсу	<i>Посилання на дистанційний ресурс pplayshner@gmail.com</i>

• Програма навчальної дисципліни

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

Широке впровадження криптографічних систем в практику електронного бізнесу та електронного урядування вимагає від фахівців в галузі інформаційних технологій глибокого розуміння правил застосування криптосистем в автоматизованих системах загального призначення, побудови прикладних криптографічних протоколів з відомих базових криптографічних механізмів і примітивних протоколів. Ці фактори приводять до актуалізації проблеми адекватного застосування криптосистем, їх реалізації на основі базових криптографічних примітивів та протоколів, вміння практичного застосування методів побудови та аналізу криптографічних протоколів захисту систем електронної комерції та електронного документообігу. Цим питанням присвячена дисципліна „Проектування, розробка і реалізація криптографічних систем”. Теоретичні знання та практичні навички, отримані під час вивчення матеріалу курсу можуть бути використані при створенні та експлуатації систем електронного документообігу, електронної комерції та електронного урядування, а також при проведенні сертифікації та експертизи засобів захисту інформації.

Мета: *ознайомлення студентів з сучасними прикладними криптографічними протоколами, які використовуються в системах електронного документообігу, електронної комерції та*

електронного урядування, їх практичними реалізаціями та застосуванням криптосистем для вирішення прикладних задач захисту інформації.

Завданням дисципліни є засвоєння студентами вміння адекватно оцінювати стійкість прикладних криптографічних протоколів, здійснювати вибір криптографічного протоколу та криптосистеми відповідно до специфіки конкретної ситуації, розробляти правила практичного використання криптосистем.

Загальні компетентності:

ЗК2 – Здатність генерувати нові ідеї та нестандартні підходи до їх реалізації, адаптуватись та діяти в нових ситуаціях, виявляти ініціативу, інноваційність та підприємливість.

Фахові компетентності:

ФК5 – Здатність провадити теоретичний та практичний аналіз сучасних криптографічних систем

ФК6- Здатність розробляти новітні механізми криптографічного захисту

ФК7 – Здатність проектувати, розроблювати та реалізовувати системи криптографічного захисту з урахуванням сучасних досягнень науки та існуючої правової та нормативної бази

ФК8 – Здатність використовувати та впроваджувати існуючі механізми, протоколи та системи криптографічного захисту інформації

Програмні результати¹ навчання:

РН2 – Застосовувати існуючий математичний апарат, розробляти нові моделі, методи та алгоритми при вирішенні актуальних практичних задач широкого спектру

РН9- Здійснювати математичне і комп'ютерне моделювання складних систем та процесів, обчислювальні експерименти з використанням сучасних методів інтелектуального аналізу даних та комп'ютерних технологій

РН11-Проводити аналіз криптографічних алгоритмів, протоколів та систем

РН12-Орієнтуватись у останніх досягненнях криптології

РН13-Розроблювати нові криптографічні алгоритми, механізми та системи захисту

РН14- Керуватись законами, стандартами, технічними специфікаціями та нормативними документами у галузі

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

Дисципліна «Проектування, розробка і реалізація криптографічних систем» частково використовує знання та вміння, набуті у «Методи реалізації криптографічних механізмів захисту інформації», «Методи криптоаналізу 1,2», «Науково-дослідна практика» та спрямовує їх у напрямку розв'язання відповідних прикладних задач математики із використанням сучасних криптосистем.

3. Зміст навчальної дисципліни

Лекції.

Тема 1.

Лекція 1. Моделі криптосистем та комп'ютерних систем.

Лекція 2. Особливості проектування криптографічних систем захисту з'єднань.

¹ Для нормативних дисциплін зазначається згідно матриці відповідності програмних компетентностей та результатів навчання в освітній програмі.

Лекція 3. Особливості проектування криптографічних систем захисту інформаційних сховищ.

Тема 2.

Лекція 4. Примітивні криптографічні протоколи та типові атаки на них.

Лекція 5. Методи побудова прикладних криптографічних протоколів захисту з'єднань (конфіденційність та цілісність) з примітивних криптографічних протоколів.

Лекція 6. Базові примітивні протоколи. Доведення із нульовим розголошенням.

Тема 3

Лекція 7. Загальні особливості побудови захисту систем електронного документообігу (СЕД).

Лекція 8. Протоколи захисту електронних документів.

Лекція 9. Формати даних в СЕД та їх захист.

Лекція 10. Захист «мобільних» та специфічних форматів даних СЕД.

Тема 4.

Лекція 11. Загальні особливості побудови захисту систем електронної комерції.

Лекція 12. Криптографічні протоколи захисту систем електронної комерції.

Тема 5.

Лекція 13. Криптографічні протоколи захисту систем електронних платежів (СЕП).

Лекція 14. Криптографічні протоколи захисту систем мікроплатежів.

Лекція 5. Електронні та цифрові гроші.

Тема 6.

Лекція 16. Криптографічні протоколи електронного урядування.

Лекція 17. Криптографічні протоколи захисту комп'ютерної телефонії.

Тема 7.

Лекція 18. Розробка правил використання криптосистем в сучасних інформаційних технологіях.

4. Навчальні матеріали та ресурси

Базова література.

1. Задірака В.К. , Олексюк О.С. Комп'ютерна криптологія: Підручник. – Київ: 2002. – 504 с
2. Вербіцький О.В. Вступ до криптології. – Львів:Науково-технічна література, 1998.- 248 с.
3. Koblitz N. A course in number theory and cryptography.- N.Y.: Springer-Verlag, 1987. – 312 p.
4. Goldreich O. Foundation of cryptography (fragments of a book).-1995.
5. Goldwasser S., Bellare M. Lecture notes on cryptography. – 1997.
6. Bellare M., Rogaway P. Optimal asymmetric encryption – how to encrypt with RSA / Advances in cryptology-Eurocrypt94 proceedings, LNCS.-V.950.-A.De Santis ed., Springer-Verlag, 1994.

● Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Найменування розділів, тем	Розподіл за видами занять				
	Разом	Лекції	Лабораторні роботи	МКР	СРС
Тема 1. Моделі інформаційно-телекомунікаційних систем та особливості проектування криптосистем для них.	8	6			2

Тема 2. Примітивні криптографічні протоколи та методи побудови на їх основі прикладних криптографічних протоколів.	16	6	4		6
Тема 3. Криптографічні протоколи для захисту електронного документообігу.	10	8			2
Тема 4. Криптографічні протоколи для захисту електронної комерції.	12	4	4		4
Тема 5. Фінансові криптографічні протоколи.	14	6	4		4
Тема 6. Криптографічні протоколи для захисту електронного урядування та комп'ютерної телефонії.	16	4	6		6
Тема 7. Розробка правил використання криптосистем в сучасних інформаційних технологіях.	6	2			4
Підготовка до іспиту	36				38
Разом в семестрі:	120	36	18	2	66

6. Самостійна робота студента/аспіранта

Самостійна робота студента складається з:

- підготовки до МКР та екзамену шляхом опанування лекційного матеріалу;
- підготовки до захисту лабораторних робіт.

№	Вид самостійної роботи	Кількість годин СРС
1	Підготовка до лекційних занять	5
2	Підготовка до лабораторних робіт	20
3	Підготовка до МКР	11
4	Підготовка до екзамену	30
	всього	66

7. Політика навчальної дисципліни (освітнього компонента)

- **Порушення термінів виконання завдань та заохочувальні бали**

Заохочувальні бали		Штрафні бали	
Критерій	Ваговий бал, додається до рейтингу	Критерій	Ваговий бал, віднімається від базового балу
Активність на заняттях	+2 бали	Невчасний захист лабораторної роботи	-2 бали

- **Відвідування занять**

Відвідування лекцій, практичних та лабораторних занять, а також відсутність на них, не оцінюється. Однак, студентам рекомендується відвідувати заняття, оскільки на них викладається теоретичний матеріал, розв'язуються супутні задачі, необхідні для виконання лабораторних робіт та успішного написання МКР. В разі великої кількості пропусків студент може бути недопущений до заліку, якщо не встигне виконати навчальний план по лабораторних роботах та МКР.

- **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.

- **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 контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами (згідно “Положення про систему забезпечення якості вищої освіти у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського”, “Положення про організацію навчального процесу”).

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

● Рейтингова система оцінювання

№ з/п	Контрольний захід	Максимальна кількість балів	Кіл-ть	Всього
1.	МКР	20	1	20
2.	Лабораторні роботи	10	4	40
3.	Екзамен	40	1	40
	Всього			100

● Умови допуску до екзамену

Обов'язкова умова допуску до іспиту	Критерій
Поточний рейтинг	$RD \geq 36$
Модульна контрольна робота	Набрано не менше ніж 12 балів
Лабораторні роботи	Виконано 4 лабораторні роботи, за кожену набрано не менше 6 балів

● Таблиця переведення рейтингових балів до оцінок за університетською шкалою ²

Рейтингові бали, RD	Оцінка за університетською шкалою	Можливість отримання оцінки «автоматом»
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	-

● Екзамен

Підсумковим контролем є екзамен. У цьому разі рейтингова оцінка роботи за семестр складається з результатів роботи в семестрі (RD) (в рамках 60 балів). На екзамені студент одержує білет, в якому містяться два теоретичних питання, кожне з яких оцінюється на 10 балів та практична задача, правильний та повний розв'язок якої оцінюється на 20 балів, відповідно повні та правильні розв'язки всіх завдань білету оцінюються в 40 балів.

9. Додаткова інформація з дисципліни (освітнього компонента)

- Сертифікати проходження дистанційних чи онлайн курсів за відповідною тематикою можуть бути зараховані, якщо в програмі курсу розглянуто всі питання, які входять до змісту навчальної дисципліни (п.3) ;
- Перелік питань до іспиту повністю відповідає змісту дисципліни.

² Оцінювання результатів навчання здійснюється за рейтинговою системою оцінювання відповідно до рекомендацій Методичної ради КПІ ім. Ігоря Сікорського, ухвалених протоколом №7 від 29.03.2018 року.

Нижче наведений орієнтовний перелік теоретичних питань до екзамену. Цей перелік може корегуватись якщо якісь теми були зменшені або збільшені в обсязі.

1. Автоматизованою системою є окрема ПЕОМ, яка призначена для обробки інформації декількома користувачами. Наведіть алгоритм проектування КЗЗ для системи та особливості реалізації криптографічних механізмів.
2. Автоматизованою системою є локальна обчислювальна мережа. Наведіть алгоритм проектування КЗЗ для системи та особливості реалізації криптографічних механізмів.
3. Автоматизованою системою є корпоративна обчислювальна мережа. Наведіть алгоритм проектування КЗЗ для системи та особливості реалізації криптографічних механізмів.
4. Автоматизованою системою є обчислювальна мережа, орендована у провайдера послуг хмарних обчислень. Наведіть алгоритм проектування КЗЗ для системи та особливості реалізації криптографічних механізмів.
5. Опишіть відомі вади протоколу SSL.
6. Поясніть принцип роботи та існуючі атаки на протокол SET.
7. Наведіть відміни протоколів доказів із нульовим та частковим розкриттям секрету. Надайте приклади протоколів.
8. Наведіть типові атаки на примітивні протоколи. Надайте приклади.
9. Наведіть відміни протоколів для мікроплатежів від протоколів для електронних грошей. Наведіть приклади.
10. Поясніть особливості реалізації протоколів вироблення загального випадкового числа. Наведіть приклади.
11. Поясніть особливості реалізації та застосування протоколів «із забуванням інформації». Наведіть приклади

Лабораторні роботи

Цикл лабораторних робіт дозволяє студентам придбати такі навички та уміння:

- практичне використання криптосистем для захисту СЕДО, СЕП та інших прикладних систем;
- аналіз практичних аспектів безпечного використання криптографічних протоколів;
- практичні навички роботи із програмними засобами криптографічного захисту інформації;
- дослідження практичної ефективності та стійкості криптографічних протоколів.

Лабораторна робота № 1

Тема: „Дослідження реалізацій протоколу SSL”.

Мета роботи: „Дослідження особливостей реалізації криптографічних механізмів протоколу SSL/TLS ”.

Завдання на лабораторну роботу

Група 1. Дослідити реалізації під протоколів протоколу SSL, а також особливості роботи із сертифікатами відкритих ключів.

Група 2. Розробити програмний засіб захисту логічного каналу зв'язку на базі бібліотеці OpenSSL.

Група 3. Дослідити реалізацію протоколу SSL в браузері Mozilla Firefox.

Оформлення результатів роботи

Група 1. Опис криптографічних механізмів.

Група 2. Тексти програм на мові C++.

Група 3. Детальний опис особливостей реалізації. Аналіз пакетів, які передаються між абонентами.

Лабораторна робота № 2.

Тема: „Дослідження реалізацій протоколів IPSec”.

Мета роботи: „Дослідження особливостей реалізації криптографічних механізмів протоколів IPSec”.

Завдання на лабораторну роботу

Група 1. Дослідити реалізації під протоколів протоколу IPSec.

Група 2. Розробити програмний засіб захисту логічного каналу зв'язку на базі будь-якої бібліотеки з відкритим кодом.

Група 3. Дослідити реалізацію протоколу IPSec в будь-якому додатку прикладного рівня.

Оформлення результатів роботи

Група 1. Опис криптографічних механізмів.

Група 2. Тексти програм на мові C++.

Група 3. Детальний опис особливостей реалізації. Аналіз пакетів, які передаються між абонентами.

Лабораторна робота № 3.

Тема: „Дослідження криптографічних протоколів систем WebMoney, PayPal”.

Мета роботи: „Дослідження особливостей реалізації криптографічних механізмів платіжних систем”.

Завдання на лабораторну роботу

Група 1. Дослідити особливості реалізації криптографічних протоколів, а також особливості роботи із електронними гаманцями.

Група 2. Розробити власну систему електронних грошей із спрощеними функціями.

Група 3. Вивчити можливості пакетів розробки власних підсистем під платіжні системи.

Оформлення результатів роботи

Група 1. Опис криптографічних механізмів.

Група 2. Тексти програм на мові C++.

Група 3. Детальний опис особливостей реалізації.

Лабораторна робота № 4.

Тема: „Дослідження систем захисту захищених месенджерів типу Skype, Viber, WhatsApp, Signal”.

Мета роботи: „Дослідження особливостей реалізації криптографічних механізмів протоколів захисту мультимедійної інформації типу SIP”.

Завдання на лабораторну роботу

Група 1. Проаналізувати існуючу інформацію про систему та її криптографічні механізми. Довести теоретично можливість існування в системі виявлених протоколів

Група 2. Розробити інструкції користувачеві для використання усіх можливостей системи Skype, Viber, WhatsApp, Signal та запропонувати організаційні міри для підвищення її стійкості.

Група 3. Експериментально дослідити захищений протокол встановлення зв'язку між абонентами.

Оформлення результатів роботи

Група 1. Опис криптографічних механізмів.

Група 2. Інструкції, нормативні документи.

Група 3. Детальний опис особливостей реалізації. Аналіз пакетів, які передаються між абонентами.

Робочу програму навчальної дисципліни (силабус):

Складено професором кафедри ММЗІ, д.т.н., с.н.с. Кудін Антон Михайлович

Ухвалено кафедрою ММЗІ (протокол № 6 від 19.06.2024 р.)

Погоджено Методичною комісією ФТІ (протокол № 6 від 27.06.2024)