



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

Фізико-технічний інститут
Математичних методів захисту
інформації

КУРСОВА РОБОТА

Проектування, розробка і реалізація криптографічних систем (ПО- 11) 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>2 курс, осінній семестр</i>
Обсяг дисципліни	<i>Загальна кількість: (1 кредит)30 год Самостійна робота студентів: 30 год</i>
Семестровий контроль/ контрольні заходи	<i>Залік</i>
Розклад занять	<i>http://rozklad.kpi.ua</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор:д.т.н., с.н.с., професор Кудін Антон Михайлович</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

Курсова робота виконується на заключному етапі вивчення навчальної дисципліни «Проектування, розробка і реалізація криптографічних систем» присвячена формуванню у студентів компетентностей у галузі криптосистем, які використовуються в системах електронного документообігу, електронної комерції та електронного урядування, їх практичними реалізаціями та застосуванням криптосистем для вирішення прикладних задач захисту інформації

ЗНАННЯ:

- основних криптографічних протоколів та правил їх реалізації

УМІННЯ:

- практично реалізовувати та проводити аналіз криптосистем.

ДОСВІД:

- проводити оцінку стійкості криптосистем, здійснювати налаштування їх параметрів.

Після засвоєння навчальної дисципліни студенти мають продемонструвати такі програмні компетентності та результати навчання за освітньо-професійною програмою «Проектування, розробка і реалізація криптографічних систем» (див. на сайті <https://osvita.kpi.ua/op>):

Загальні компетентності:

ЗК1 – Здатність до самонавчання, пошуку, оброблення та інтелектуального аналізу інформації з різних джерел, вміння виявляти, ставити та вирішувати проблеми.

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

Фахові компетентності:

ФК2- Здатність проводити наукові дослідження з розроблення нових та адаптацією існуючих математичних та комп'ютерних моделей для дослідження різноманітних процесів, явищ і систем, проводити відповідні чисельні експерименти з аналізом одержаних результатів.

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 результати навчання:

РН11 – Проводити аналіз криптографічних алгоритмів, протоколів та систем

РН12 – Орієнтуватись у останніх досягненнях криптології

РН13- Розробляти нові криптографічні алгоритми, механізми та системи захисту

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

Вивчення навчальної дисципліни «Курсова робота проектування, розробка і реалізація криптографічних систем» частково використовує знання та вміння, набуті у «Методи реалізації криптографічних механізмів захисту інформації», «Науково-дослідна практика» та спрямовує їх у напрямку розв'язання відповідних прикладних задач математики із використанням сучасних криптосистем..

3. Зміст навчальної дисципліни

Перелік тематик для курсових робіт.

1. Криптографічні протоколи інтерактивних доведень з нульовими знаннями та нульовою аргументацією: огляд, аналіз та порівняння.
2. Криптографічні протоколи неінтерактивних доведень з нульовими знаннями: огляд та аналіз.
3. SNARK та STARK протоколи та їх застосування.
4. Практичне застосування протоколів розподілу секрету із забуванням.
5. Identity-based протоколи автентифікації: практичні застосунки та обмеження.
6. Криптосистеми реалізації концепції «електронних грошей».
7. Криптосистеми реалізації концепції «криптовалюти».
8. Криптосистеми реалізації концепції «електронні довірчі послуги».
9. Криптосистеми реалізації концепції «електронні вибори».
10. Криптосистеми реалізації концепції «електронне урядування».
11. Криптосистеми реалізації захищених месенджерів.

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)

Для проведення занять застосовуються частково-пошуковий та дослідницький методи навчання, при яких студенти вирішують поставлену викладачем або самостійно визначену задачу, шляхом творчого пошуку та перевірки власних ідей, підбираючи для цього необхідні джерела інформації.

Курсова робота виконується протягом останнього місяця семестра, коли студентами засвоєні основні положення дисципліни «Проектування, розробка і реалізація криптографічних систем». Кожен студент отримує індивідуальне завдання. Курсова робота виконується у вигляді аналітичного есе на обрану тему (перелік тематик наведений у розділі 3). Сенс аналітичного викладення матеріалу – в стислому, але достатньому для повного розуміння висвітлення стану і перспектив розвитку проблематики, яка досліджується. Обов'язковим є аналіз публікацій на задану тематику та висновки про перспективи розвитку питання, яке освітлюється.

6. Самостійна робота студента

Робота виконується самостійно кожним студентом з поданням викладачеві результатів виконання етапів відповідно до завдання.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

Не передбачається.

Пропущені контрольні заходи

Подання результатів етапів курсової є обов'язковим.

Оголошення результатів контрольних заходів

Результати виконання самостійних робіт оголошуються кожному студенту окремо у присутності або у дистанційній формі та супроводжуються оціночними листами, в яких студенти можуть побачити свою оцінку за певними критеріями, а також позначення основних помилок та коментарі до них.

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 поставити 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)

Рейтингова оцінка має дві складові. Перша (стартова) характеризує роботу студента під час курсового проектування та її результат – якість пояснювальної записки та графічного матеріалу. Друга складова характеризує якість захисту студентом курсової роботи.

Розмір шкали стартової складової дорівнює 50 балів, а складової захисту – 50 балів.

1. Стартова складова:

- своєчасність виконання графіка роботи – 5...10 балів;
- правильність викладення матеріалу – 10...20 балів;
- якість оформлення, виконання вимог нормативних документів – 5...10 балів;
- якість графічного матеріалу і дотримання вимог стандартів – 5...10 балів.

2. Складова захисту курсової роботи:

- якість доповіді – 5...10 балів;
- ступінь володіння матеріалом – 10...15 балів;
- ступінь обґрунтування прийнятих рішень – 5...10 балів;
- вміння захищати свою думку – 10...15 балів.

3. Сума балів двох складових переводиться до залікової оцінки згідно з таблицею:

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):

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

Ухвалено кафедрою ММЗІ (протокол № 6 від 22.06.2022 р.)

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