



ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>F Інформаційні технології</i>
Спеціальність	<i>F1 Прикладна математика</i>
Освітня програма	<i>Математичні методи криптографічного захисту інформації</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>Очна (денна)</i>
Рік підготовки, семестр	<i>1 курс, весняний семестр</i>
Обсяг дисципліни	<i>Загальна кількість: 4 кредитів ЄКТС / 120 годин Лекційних занять: 36 годин Самостійна робота студентів: 84 години</i>
Семестровий контроль/ контрольні заходи	<i>Залік, МКР</i>
Розклад занять	http://schedule.kpi.ua
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>доц. Яковлев Сергій Володимирович, к.т.н. (yasv@rl.kiev.ua)</i>
Розміщення курсу	<i>Google Classroom</i>

Програма навчальної дисципліни

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

Інфраструктури відкритих ключів в наш час є невід'ємною складовою великих інформаційно-телекомунікаційних систем, що використовують криптографічний захист інформації. За декілька десятиліть розробок та впроваджень склалась усталена практика юридичного та технічного імплементації таких систем. В даній дисципліні викладаються основні положення створення та підтримки інфраструктур відкритих ключів як окремої організаційно-технічної одиниці.

При викладенні матеріалу дисципліни виділяються такі аспекти:

- основні задачі інфраструктур відкритих ключів (ІВК);
- технічні специфікації, типи даних та протоколи, що використовуються у ІВК;
- інтеграція систем електронного документообігу із ІВК.

Метою кредитного модуля є формування у студентів здатностей оперування основними поняттями організаційно-адміністративних методів захисту інформації; аналізу наявних засобів та методів організації інфраструктури відкритих ключів, що базуються на міжнародних та міждержавних стандартах, національних стандартах та технічних специфікаціях, спеціальній

літературі; побудови, організації та імплементації інфраструктури відкритих ключів у конкретні інформаційно-телекомунікаційні системи та/або системи електронного документообігу із урахуванням усіх технологічних нюансів; опанування навиками роботи із конкретними інфраструктурами відкритих ключів, реалізованими на практиці.

Студенти після опанування курсу одержать такі результати навчання:

знання:

загальних принципів побудови інфраструктур відкритих ключів, їх переваг та недоліків;
синтаксису ASN.1;

форматів сертифікатів відкритих ключів, списків відкликаних сертифікатів та інших службових типів даних;

процедури перевірки чинності сертифікатів;

протоколів OCSP, TSP, CMP;

форматів електронних цифрових підписів;

уміння:

перевірити коректність типу даних, занотованого у ASN.1;

побудувати модель інфраструктури відкритих ключів для заданої інформаційно-телекомунікаційної системи;

проаналізувати переваги та недоліки застосування тих чи інших типів даних та протоколів інфраструктур відкритих ключів у заданій інформаційно-телекомунікаційній системі;

досвід:

аналіз тематичної технічної документації (RFC, ДСТУ, стандарти ISO/IEC, технічні специфікації ETSI TS та ін.);

побудова моделі інфраструктури відкритих ключів із заданими обмеженнями.

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

Для успішного засвоєння матеріалу дисципліни потрібні ґрунтовні знання з криптології (зокрема, асиметричної криптографії) та базові знання з програмування та основ захисту інформації.

Отримані навички та засвоєнні знання можуть використовуватись для розв'язання прикладних задач у галузі криптографічного захисту інформації та інформаційної безпеки загалом.

3. Зміст навчальної дисципліни

Розділ 1. Загальні поняття про інфраструктури відкритих ключів

Тема 1.1. Інфраструктури відкритих ключів (ІВК): означення, властивості, функції, способи реалізації

Тема 1.2. Моделі ІВК та їх взаємодії

Тема 1.3. Життєвий цикл криптографічного ключа

Розділ 2. Протоколи та формати структур даних, які використовуються в ІВК

Тема 2.1. Мова ASN.1 та способи її кодування

Тема 2.2. Формат сертифікату відкритого ключа X.509v3

Тема 2.3. Протоколи перевіряння статусу сертифікату.

Тема 2.4. Протоколи керування життєвим циклом ключа

Розділ 3. Використання ІВК у системах електронного документообігу

Тема 3.1. Криптографічні структури даних. Формати електронних підписів, часові штемпелі

Тема 3.2. Формати захищених повідомлень.

4. Навчальні матеріали та ресурси

1. Мелашенко А.О., Організація кваліфікованої інфраструктури відкритих ключів / А.О. Мелашенко, О.Л. Перевозчикова. – К.: «Наукова думка», 2010. – 392 стор. – ISBN 978-966-00-1059-8.

2. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. – Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем / За заг. ред. д.т.н., професора І.Д.Горбенка. – Харків: Видавництво «Форт», 2015. -960 с.

Значна частина інформації по курсу викладена у відкритих інтернет-стандартах (RFC), технічних специфікаціях (PKCS, ETSI TS) та українській нормативній документації, посилання на які наводяться у лекціях та супровідному матеріалі.

Відеозаписи більшої частини лекцій викладені на Youtube-каналі кафедри ММЗІ та доступні за посиланням

<https://www.youtube.com/playlist?list=PLhCN8H4P5LvJJsokxSiVwkvZV6MBdyG3z>

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчання здійснюється на основі студентоцентрованого підходу та взаємодії викладачів та студентів для засвоєння матеріалу та опанування практичних навичок. При викладанні дисципліни використовуються пояснювально-ілюстративний метод та метод проблемного викладу.

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань
1	Загальне поняття про інфраструктури відкритих ключів. Класифікація електронних підписів
2	Децентралізовані та централізовані інфраструктури. Різні топології та моделі взаємодії IBK
3	Електронні довірчі послуги. Реалізація IBK в Україні
4	Abstract Syntax Notation One (ASN.1)
5	Правила кодування ASN.1. BER-, CER- та DER-кодування
6	Життєвий цикл криптографічних ключів. Формат сертифікату відкритого ключа X.509v3
7	Розширення сертифікатів. Формат посиленого сертифікату
8	Керування статусами, інфраструктура керування привілеями, атрибути сертифікати
9	МКР, частина 1
10	Протоколи перевіряння статусу сертифікату. Списки відкликаних сертифікатів.
11	Протоколи OCSP та OCSP Lite
12	Процедура перевірки ланцюга сертифікатів (Certificate Path Validation)
13	Формат запиту на сертифікацію PKCS#10. Протокол керування сертифікатами CMP
14	Формати криптографічних повідомлень за CMS (Cryptographic Message Syntax). Формат підписаного повідомлення SignedData
15	Часові штемпелі, протокол TSP. Розширені електронні підписи (CAdES).
16	Формати захищених повідомлень (EncryptedData, EnvelopedData).
17	МКР, частина 2
18	Підсумкове консультативне заняття

6. Самостійна робота студента

Студент повинен завчасно готуватись до лекцій. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Це також необхідне для підготовки до самостійних та модульних контрольних робіт.

Дисципліна передбачає, що студент буде приділяти значну увагу опануванню нормативної документації, яка згадується на лекціях (технічні специфікації, стандарти ДСТУ, ANSI, RFC, PKCS, ETSI тощо). Хоча це не є обов'язковим для успішного складання дисципліни, заглиблення у нормативну базу посилить та закріпить результати навчання, а також дозволить швидко актуалізувати їх у майбутньому.

Розподіл годин самостійної роботи студента

№	Вид самостійної роботи	Годин СРС
1.	Опанування лекційного матеріалу	54
4.	Підготовка до виконання модульної контрольної роботи	24
6.	Підготовка до заліку	6
	Усього	84

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 необхідні навички. Система оцінювання орієнтована на отримання балів за виконання завдань, які здатні розвинути практичні уміння та навички.

Пропущені контрольні заходи

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Якщо пропуск стався з поважних причин (наприклад, хвороби), студент має можливість написати контрольний захід в інший узгоджений з викладачем термін без зниження оцінки. Повторне написання будь-якої частини модульної контрольної роботи не допускається.

Пропущений залік не зараховується незалежно від причин пропуску; у такому випадку студент отримує запис у відомості «не з'явився» та повинен скласти залік на додатковій сесії.

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.

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 разі виявлення порушень норм академічної доброчесності під час виконання контрольного заходу студент одержує за цей захід нуль балів без можливості повторного виконання.

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.	Модульна контрольна робота	100	1	1	100
	Усього				100

Критерії оцінювання контрольних заходів

1) Модульна контрольна робота

Модульна контрольна робота (МКР) складається з декількох частин, які проводяться протягом семестру по мірі опанування теоретичного та практичного матеріалу. МКР складається з тестових питань. Кількість питань та їх вартість у балах визначається викладачами в залежності від складності самої задачі та об'єму винесеного на дану частину МКР матеріалу.

Тестові питання можуть бути відкриті та із мультिवибором відповіді, причому кількість правильних варіантів може бути від 0 до 4.

Критерії оцінювання одного тестового питання з відкритою відповіддю:

- Правильна відповідь 100% оцінки
- Відкрита відповідь містить суттєві неточності 50% оцінки
- Відкрита відповідь є неправильною 0% оцінки

Правила оцінювання одного тестового питання з мультिवибором відповіді:

- Кожен правильний варіант відповіді має вагу, яка дорівнює кількості правильних варіантів, поділений на максимальну кількість балів за дане питання.
- Кожен правильний варіант відповіді має вагу, яка дорівнює кількості правильних варіантів, поділений на максимальну кількість балів за дане питання, зі знаком мінус.
- Студент одержує за питання кількість балів, яка дорівнює сумі ваг усіх варіантів відповіді, які він обрав.

- Якщо студент не обрав жодного варіанту відповіді і питання не містило правильних варіантів відповіді, студент одержує за це питання максимальну кількість балів за дане питання; в усіх інших випадках якщо студент не обрав жодної відповіді у питанні, він одержує за нього 0 балів.

Під час виконання МКР дозволяється користуватись власними рукописними конспектами лекцій.

Максимальна кількість балів, яку можна одержати за модульну контрольну роботу, дорівнює 70. Загальна кількість балів, яку студент одержує за одну частину модульної контрольної, дорівнює сумі балів за кожне завдання у відповідності до їх вартості та наведених критеріїв оцінювання, але не менше 0 балів. Загальна кількість балів, яку студент одержує за модульну контрольну роботу, дорівнює сумі балів за виконання усіх її частин.

Студент, який без поважних причин пропустив частину МКР, одержує за неї нуль балів без можливості перескладання. Виконання частини МКР, пропущеної з поважних причин, врегульовується за домовленістю з викладачем в індивідуальному порядку.

Заохочувальні бали

Студент, який протягом семестру виступив на науковій конференції із публікуванням доповіді (у вигляді матеріалів чи доповідей конференції) за тематикою дисципліни або подав таку доповідь та одержав підтвердження про включення в програму конференції, одержує 10 бонусних балів.

Загальна кількість заохочувальних балів, які можна одержати за дисципліну: 10 балів.

Умови одержання проміжної атестації

Проміжна атестація студентів (далі – атестація) є календарним рубіжним контролем та проводиться двічі за семестр, на 7-му та 13-му навчальному тижнях семестру. Для одержання кожної атестації поточний рейтинг студента повинен бути не менше половини від суми максимальних балів за усі контрольні заходи, які були проведені на момент атестації.

Умови одержання семестрової оцінки

Необхідною умовою одержання семестрової оцінки є семестровий рейтинг не менше 60 балів.

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, виконують залікову роботу. При цьому їх семестровий рейтинг анулюється, а рейтингова оцінка виставляється по результату виконання залікової роботи.

Студенти, які набрали від 50 до 60 балів за семестр, за бажанням замість написання залікової роботи можуть пройти усну співбесіду із викладачем за матеріалами курсу. На співбесіді, відповідаючи на теоретичні питання (до десяти питань, одне питання = один бал), студент може підвищити свій семестровий рейтинг до мінімальної позитивної оцінки.

Студенти, які протягом семестру одержали менше 10 балів, вважаються такими, що не виконали умови одержання семестрової оцінки, та рекомендуються кафедрі на відрахування або повторне переслуховування дисципліни.

Умови проведення залікової роботи

Право писати залікову роботу мають:

- а) студенти, семестровий рейтинг яких складає 10-59 балів;
- б) студенти, семестровий рейтинг яких складає 60-100 балів, але які не згодні з одержаною семестровою оцінкою.

Студентам, які пишуть залікову роботу, анулюється семестровий рейтинг. Оцінка, яку вони одержують за дисципліну, формується за результатами складання залікової роботи.

Залікова робота проводиться на заліковому тижні в кінці семестру.

Залікова робота складається з 20 тестових питань задач, які сумарно оцінюються в 100 балів. Критерії оцінювання питань співпадають з критеріями оцінювання питань МКР.

Під час виконання залікової роботи дозволяється користуватись власними рукописними конспектами лекцій.

Перескладання дисципліни

Перескладання дисципліни проходить у такій само формі, як і залікова робота. Для допуску до перескладання студент повинен одержати не менше 10 рейтингових балів (з урахуванням складання залікової роботи). Рейтингова оцінка студента визначається результатами перескладання.

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

Підсумкова оцінка з дисципліни

Рейтингова оцінка складається з результатів виконання семестрових контрольних заходів (включно з заохочувальними) або за результатами виконання залікової роботи чи перескладання. Оцінка за стобальною шкалою переводиться до університетської шкали оцінок за наведеною таблицею відповідності.

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, к.т.н. Яковлев Сергій Володимирович

Ухвалено кафедрою математичних методів захисту інформації (протокол №6/2 від 25.06.2025 р.).

Затверджено Методичною комісією НН ФТІ (протокол №6 від 30.06.2025 року)