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

Кафедра цифрових технологій в енергетиці

БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	**Перший (бакалаврський)**
Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки
Освітня програма	Цифрові технології в енергетиці
Статус дисципліни	Нормативна
Форма навчання	Очна (денна)
Рік підготовки, семестр	3 курс 5 семестр
Обсяг дисципліни	4 кредити (120 год.) (лекцій 36 год., лаб. 18 год., 66 СРС)
Семестровий контроль/ контрольні заходи	Екзамен, МКР
Розклад занять	*http://schedule.kpi.ua*
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: доцент,к.в.н., доцент Онисько Андрій Ілліч, *email: oniskoandrij2020@gmail.com* Практичні заняття: доцент, к.в.н., доцент Онисько Андрій Ілліч, *email: oniskoandrij2020@gmail.com*, асістент Пасічнюк Антон Олександрович *email: _____@gmail.com*
Розміщення курсу	Google classroom, е-Кампус

Програма навчальної дисципліни

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

Метою кредитного модуля є формування у студентів **компетентностей** у відповідності до освітньо-професійної програми.

ЗК 02	Здатність застосовувати знання у практичних ситуаціях.
ЗК 06	Здатність вчитися й оволодівати сучасними знаннями.
ЗК 12	Здатність оцінювати та забезпечувати якість виконуваних робіт.
ФК 14	Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

В результаті засвоєння кредитного модуля студенти мають продемонструвати такі програмні результати навчання:

ПРН 15	Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

2. Пререквізити та постреквізити дисципліни

Вивчення дисципліни спирається на знання, отримані за програмою попереднього семестру навчання за спеціальністю F3 "Комп'ютерні науки".

У структурно-логічній схемі навчання, зазначена дисципліна розміщена у другому семестрі 1 курсу, тобто тоді, коли студенти продовжують вивчати "Алгоритмізація та програмування", "Дискретна математика", "Операційні системи", "Об'єктно-орієнтоване програмування" та набули певного досвіду у програмуванні і можуть виконати лабораторні роботи.

З іншого боку, викладений матеріал може бути використаний при вивченні дисциплін "Системи баз даних", "Комп'ютерні мережі", "Технологіїї розробки програмного забезпечення", які викладаються при підготовці бакалаврів.

3. Зміст навчальної дисципліни

В дисципліні вивчаються такі теми:

Розділ 1. Криптографічні засоби захисту інформації з симетричним ключем.

Тема 1.1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки.

Тема 1.2. Традиційні криптографічні системи.

Тема 1.3. Криптографічна стійкість шифрів.

Тема 1.4. Блокові шифри як основа сучасних криптосистем.

Тема 1.5. Криптосистема DES (Data Encryption Standard).

Тема 1.6. Сучасні симетричні криптосистеми.

Розділ 2. Криптографічні засоби захисту інформації з відкритим ключем.

Тема 2.1. Модель асиметричної системи.

Тема 2.2. Протоколи розподілення ключів на основі центрів довіри.

Тема 2.3. Протоколи асиметричного шифрування.

Тема 2.4. Криптосистема RSA.

Тема 2.5. Цифрові підписи.

Тема 2.6. Програмна реалізація цифрового підпису засобами .NET.

Тема 2.7. Криптографічні геш-функції.

4. Навчальні матеріали та ресурси

Базова література

1. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 2011. – 248 с.
2. Клінцв Л.М. Безпека програм і даних / Л.М. Клінцв Л.М. – Чернігов: ВСП Чернігівський інститут інформації, бізнесу і права, 2017. – 81 с.
3. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 162 с.
4. Яковенко Є. Інформаційна безпека / Є. Яковенко, І. Журавель, І. Горбатий, А. Бондарєв – Львів. : "Львівська політехніка", 2019. – 580 с.

Додаткова література

1. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых.-К.: Изд. «Политехника», 2004. – 224с.
2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: Підручник. – К.: ДУТ, 2015. – 449 с.
3. Вербіцький О.В. Вступ до криптології / О.В. Вербіцький. – Львів: Науково-техн.літ., 1998. – 248с.
4. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с. 2. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
5. Задірака В.К. Методи захисту фінансової інформації / В.К. Задірака, О.С. Олексюк. – К.: Вища школа, 2009. – 460 с.
6. Задірака В.К., Олексюк О.С.,.Недашковський М.О. Методи захисту фінансової інформації. Навчальний посібник. К.: Вища школа, 2000. – 460 с
7. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.
8. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
9. Мухачев В.А., Хорошко В.А. Методы практической криптографии. К.: ООО Полиграф-Консалдинг, 2005. – 209 с.
10. Остапов С.Е. Основи криптографії: Навчальний посібник / С.Е. Остапов, Л.О. Валь. – Чернівці: Книги – XXI, 2008. – 188 с.
11. Скобелєв В.Г. Основи захисту інформації. Навчальний посібник. − Донецьк, ДонНТУ, 2006 − 173 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Розділ 1. Криптографічні засоби захисту інформації з симетричним ключем.

Тема 1.1. Лекція 1. Захист інформації, його складові і рівні формування режиму інформаційної безпеки. Основні поняття та визначення. Правові аспекти захисту інформації. Властивості інформації з точки зору її захисту. Рівні формування режиму інформаційної безпеки.

Тема 1.2. Лекція 2.Традиційні криптографічні системи. Криптографія і її основні поняття. Модель симетричної криптографічної системи. Принцип Керкхоффса. Етапи розвитку криптографічних систем. Види історичних шифрів.

Тема 1.3. Лекція 3. Криптографічна стійкість шифрів. Поняття криптографічної стійкості шифру. Обчислювальна складність алгоритму, основні класи складності. Межі застосування «грубої сили» до атак на шифри. Абсолютна криптостійкість шифрів, шифр Вернама. Поняття квантової криптографії.

Тема 1.4. Лекція 4. Блокові шифри як основа сучасних криптосистем. Блокові алгоритми і режими шифрування. Режим електронної кодової книги. Режим зціплення блоків по криптотексту. Режим зціплення блоків по криптотексту. Режим з оберненим зв’язком по виходу. Режим з лічильником. Схема Фейстеля.

Тема 1.5. Криптосистема DES (Data Encryption Standard). Загальна характеристика DES. Алгоритм шифрування/розшифрування DES. Структура функції шифрування. Криптографічна стійкість DES. Криптосистеми DESX, 3DES. DES і шифрована файлова система EFS. Програмна реалізація симетричних криптографічних алгоритмів DES і 3DES засобами .NET.

Тема 1.6. Сучасні симетричні криптосистеми. Алгоритми блокового симетричного шифрування ДСТУ ГОСТ 28147:2009. Міжнародний стандарт симетричного шифрування AES (Advanced Encryption Standard). Загальноєвропейський стандарт шифрування IDEA (International Data Encryption Algorithm). Програмна реалізація симетричних криптографічних алгоритмів AES засобами .NET.

Розділ 2. Криптографічні засоби захисту інформації з відкритим ключем

Тема 2.1. Модель асиметричної системи. Передумови виникнення асиметричних систем. Модель ДіффіХеллмана криптосистеми з публічними ключами. Поняття односторонньої функції-пастки. Асиметрична криптосистема на основі використання «задачі рюкзака».

Тема 2.2. Протоколи розподілення ключів на основі центрів довіри. Проблема розподілення ключів симетричної криптосистем. Протокол широкоротої жаби. Протокол Нідхейма-Шредера. Протокол ОтвейРіса. Протокол Цербер. Протокол мережної аутентифікації Kerberos 5 і аутентифікація в Windows.

Тема 2.3. Протоколи асиметричного шифрування. Протокол Діффі-Хеллмана. Шифр Шаміра. Шифр ЕльГамаля. Програмна реалізація алгоритму Діффі-Хеллмана засобами .NET.

Тема 2.4. Криптосистема RSA.Принцип шифрування в RSA. Генерація пари ключів шифрування. Алгоритм шифрування/розшифрування RSA. Програмна реалізація алгоритму RSA засобами .NET.

Тема 2.5. Цифрові підписи. Схема застосування цифрового підпису. Цифровий підпис на основі шифру RSA. Цифровий підпис на основі шифру Ель-Гамаля. Алгоритм цифрового підпису DSA (Digital Signature Algorithm). Стандарт ГОСТ Р34.10-94.

Тема 2.6. Програмна реалізація цифрового підпису засобами .NET. Реалізація цифрового підпису на основі RSA. Використання криптопровайдера цифрового підпису на основі DSA.

Тема 2.7. Криптографічні геш-функції. Геш-функції і їх призначення. Ключові геш-функції. Безключові геш-функції. Програмна реалізація алгоритмів геширування в .NET.

Лабораторні роботи

№ з/п	Назва лабораторних робіт	Кільк. ауд.год
1	Класичні і історичні шифри. Шифр Цезаря, Шифр Тритеміуса.	2
2	Класичні і історичні шифри. Шифр Гамування.	2
3	Класичні і історичні шифри. Шифр Книжковий.	2
4	Симетричні криптосистеми. Алгоритм DES.	2
5	Шифрування з відкритим ключем на основі задачі рюкзака.	2
6	Асиметричні криптосистеми. Алгоритм RSA.	2
7	Електронно-цифровий підпис на основі алгоритму RSA.	4
8	Геш функція на основі RSA .	2

6. Самостійна робота студента

Самостійна робота студента (66 годин) передбачає підготовку до аудиторних занять та контрольних заходів.

Розподіл годин СРС: підготовка до екзамену – 24 години; підготовка до лекцій – 18 годин; підготовка до лабораторних робіт – 18 годин; підготовка до МКР – 6 годин.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- Відвідування лекцій, а також відсутність на них, не оцінюється. Відвідування лабораторних занять є обов'язковою складовою вивчення матеріалу;
- При захисті лабораторних робіт студент має продемонструвати розроблений програмний код та результати його виконання на тестах, як заздалегідь підготованих, так і запропонованих викладачем. У випадку дистанційної форми навчання захист відбувається на відповідній конференції шляхом демонстрації екрана.
- 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.

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

1. Виконання завдань лабораторних робіт

Завдання лабораторної роботи являє собою індивідуальне виконання робіт, що пов'язані з рішенням на ЕОМ заданої задачі комп'ютерного моделювання. Вагові бали завдань наведено у таблиці.

Види завдань	**Внесок до семестрового рейтингу балів**
Виконання лабораторних робіт	
Завдання №1. Класичні і історичні шифри. Шифр Цезаря, Шифр Тритеміуса	5
Завдання №2. Класичні і історичні шифри. Шифр Гамування	5
Завдання №3. Класичні і історичні шифри. Шифр Книжковий	5
Завдання №4. Симетричні криптосистеми. Алгоритм DES.	5
Завдання №5. Шифрування з відкритим ключем на основі задачі рюкзака	5
Завдання №6. Асиметричні криптосистеми. Алгоритм RSA.	5
Завдання №7. Електронно-цифровий підпис на основі алгоритму RSA	6
Завдання №8. Хеш функція на основі RSA	6

2. Стартовий рейтинг (виконання робіт в семестрі) оцінюється у 50 балів. Розподіл балів наведено в таблиці:

Роботи	**Максимальна кількість балів за виконання однієї роботи**	∑
Лабораторні роботи 1 - 8	5	42
Модульна контрольна робота	8	8
		50

Штрафні бали віднімаються за:

1) неоптимальний алгоритм – 10% від максимальної кількості балів;
2) неоптимальні структури представлення інформації – 10% від максимальної кількості балів;
3) ненадану або невірну відповідь на запитання – 20% від максимальної кількості балів при захисті лабораторної роботи або 100% – на контрольній роботі.

3. Календарний контроль проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу:

Критерій	**Перший календарний контроль**	**Другий календарний контроль**
Термін календарного контролю	Тиждень 7-8	Тиждень 13-14
Умови отримання позитивної оцінки	≥ 12 балів	≥ 24 балів

4. Умови допуску до екзамену: відсутність заборгованостей з лабораторних робіт 1 – 8 та стартовий рейтинг не менше 30 балів.

5. Екзаменаційний рейтинг (відповідь на екзамені) оцінюється в 50 балів. Екзаменаційний білет складається з двох теоретичних питань та одного практичного завдання. Ваговий бал кожного теоретичного питання – 15 балів, завдання – 20 балів.

Теоретична частина оцінюється таким чином:
- правильна чітко викладена, повна відповідь – (не менше 90% потрібної інформації) – 13-15 балів;
- достатньо повна відповідь (не менше 75% потрібної інформації) – 11-12 балів;
- неповна відповідь (не менше 60% потрібної інформації) – 9-10 балів;
- незадовільна відповідь – 0 балів.

Практичне завдання оцінюється таким чином:
- повне, безпомилкове розв'язування завдання – 18-20 балів;
- повне, розв'язування завдання із несуттєвими невідповідностями – 15-17-балів;
- завдання виконане з певними недоліками – 12-14 балів;
- завдання не виконано – 0 балів.

6. Рейтингова оцінка за освітній компонент розраховується як сума балів стартового та екзаменаційного рейтингів (50 + 50 = 100 балів) і визначається згідно з таблицею переведення рейтингових балів у оцінку 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):

Складено доцентом, к.військ.н., доцентом Ониським Андрієм Іллічем

Ухвалено кафедрою ЦТЕ (протокол № 22 від 25.06.2025 р.).

Погоджено Методичною комісією НН ІАТЕ КПІ ім. Ігоря Сікорського (протокол № 9 від 27.06.2025 р.).