



ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ 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	Вибіркова
Форма навчання	Очна (денна)
Рік підготовки, семестр	4 курс 7 семестр
Обсяг дисципліни	4 кредити (120 год) (лекцій 36 год., лаб. 18 год., СРС 66 год.)
Семестровий контроль/ контрольні заходи	м.к.р., залік
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 , асистент Тітов Владислав Миколайович, email: _____@gmail.com
Розміщення курсу	https://campus.kpi.ua

Програма навчальної дисципліни

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

Метою дисципліни є теоретичні підходи, принципи, закономірності, технології та обладнання сучасних комп'ютерних систем та формування у студентів здатностей формалізації задачі інформаційного забезпечення, вибору методів рішення безпеки комп'ютерних систем та аналізу результатів.

Згідно з вимогами програми навчальної дисципліни студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

знання: основних понять і загальних принципів побудови мереж; моделей системного опису мережевої архітектури; комутація каналів; основних типів мережевих архітектур, топології та апаратних компонентів комп'ютерних систем;

вміти: працювати з організацією налаштування та інформування споживачів комп'ютерних мереж; розробляти комплекс заходів для забезпечення захисту комп'ютерних систем; обирати та використовувати інформацію щодо безпеки комп'ютерних систем.

2. Пререквізити та постреквізити дисципліни

У структурно-логічній схемі навчання зазначена дисципліна розміщена на 4 курсі, тобто тоді, коли студенти вже прослухали дисципліни “Архітектура комп’ютера”, “Безпека інформаційних систем”, “Комп’ютерні мережі” та набули певного досвіду у програмуванні і можуть виконати складні лабораторні роботи.

Матеріал курсу є основою для виконання курсових робіт з дисциплін, де необхідне враховувати захист комп’ютерних систем.

Отримані знання при вивченні дисципліни “Інформаційне забезпечення безпеки комп’ютерних систем” формує базові знання для вивчення дисциплін, пов’язаних з моделюванням комп’ютерних мереж, комп’ютерне моделювання систем, захист інформації в комп’ютерних мережах.

3. Зміст навчальної дисципліни

Розділ 1. Мережні технології.

Тема 1.1. Типи комп’ютерних мереж. Моделі OSI і TCP / IP.

Тема 1.2. Загальні принципи побудови комп’ютерних мереж.

Тема 1.3. Загальні проблеми безпеки мереж.

Тема 1.4. Політики безпеки.

Тема 1.5. Адміністративна підсистема комп’ютерної мережі.

Тема 1.6. Безпека даних у комп’ютерних мережах.

Розділ 2. Технології захисту міжмережевого обміну даними

Тема 2.1. Забезпечення безпеки операційних систем.

Тема 2.2. Фільтрація трафіку. Виконання функцій посередництва.

Тема 2.3. Функції міжмережевих екранів.

Тема 2.4. Особливості функціонування міжмережевих екранів на різних рівнях моделі OSI.

Тема 2.5. Схеми мережевого захисту на базі міжмережевих екранів.

Розділ 3. Захист на каналному та сеансовому рівнях

Тема 3.1. Протоколи формування захищених каналів на каналному рівні.

Тема 3.2. Протоколи PPP та L2TP.

Тема 3.3. Протоколи формування захищених каналів на сеансовому рівні.

Тема 3.4. Протоколи SSL/TLS. Протокол SOCKS.

Тема 3.5. Захист бездротових мереж.

Розділ 4. Захист на мережевому рівні - протокол IPSec

Тема 4.1. Архітектура засобів безпеки IPSec.

Тема 4.2. Захист передаваних даних за допомогою протоколів АН та ESP.

Тема 4.3. Протокол захисту заголовку АН для аутентифікації. Протокол захист ESP.

Тема 4.4. Алгоритми аутентифікації та шифрування у IPSec.

4. Навчальні матеріали та ресурси

1. Комп’ютерні мережі: навчальний посібник [Електронне видання] / О. В. Задерейко, Н. І. Логінова, А. А. Толокнов. – Одеса: Фенікс, 2022. – 249 с. URL: <http://dspace.onua.edu.ua/handle/11300/19423>

2. Карпенко М. Ю. Конспект лекцій з курсу «Комп’ютерні мережі» (для студентів усіх форм навчання спеціальностей 122 – Комп’ютерні науки, 151 – Автоматизація та комп’ютерно-інтегровані технології, 126 – Інформаційні системи та

технології) / М. Ю. Карпенко, Н. В. Макогон; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків : ХНУМГ ім. О. М. Бекетова, 2019. – 99 с.

3. Полторак, В. П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах [Електронний ресурс]: навчальний посібник для студентів спеціальності 126 «Інформаційні системи та технології» / В. П. Полторак; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 1,77 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 79 с. URL: <https://ela.kpi.ua/handle/123456789/38326>

4. Микитишин А.Г., Митник М.М., Стухляк П.Д. Комп'ютерні мережі, книга 1. Навчальний посібник для технічних спеціальностей ВНЗ (рекомендовано МОН України). – Львів: “Магнолія 2006”, 2021. – 256 с.

5. Микитишин А.Г., Митник М.М., Стухляк П.Д. Комп'ютерні мережі, книга 2. Навчальний посібник для технічних спеціальностей ВНЗ (рекомендовано МОН України). – Львів: “Магнолія 2006”, 2021. – 328с.

Навчальний контент

1. Методика опанування навчальної дисципліни (освітнього компонента)

Розділ 1. Мережні технології

Предмет та завдання курсу. Типи комп'ютерних мереж. Технології доступу в Інтернет. Вимоги до мережі. Сервісна модель мережі Інтернет. Рівнева архітектура та еталонна модель взаємодії відкритих систем OSI. Методи доступу до середовища. Способи комутації. Дейтаграмний та віртуальний принципи передачі пакетів. Структуризація мереж. Модель ISO/OSI і стек протоколів TCP/IP. Аналіз загроз мережевої безпеки. Загрози і уразливості дротових корпоративних мереж. Загрози і уразливості безпроводних мереж. Рівні керування в комп'ютерній мережі. Призначення та функції адміністративної системи. Загальна характеристика способів організації моніторингу в комп'ютерних мережах. Захист мережі з використанням брандмауерів та серверів-посередників. Розподілені архітектури мережевих обчислень. Аналіз ризиків та основні принципи забезпечення інформаційної безпеки.

Розділ 2. Технології захисту міжмережевого обміну даними

Забезпечення безпеки операційних систем. Загрози безпеки операційних систем. Поняття захищеної системи. Архітектура підсистеми захисту операційної системи. Функції міжмережевих екранів. Фільтрація трафіку. Виконання функцій посередництва. Додаткові функції міжмережевих екранів. Особливості функціонування міжмережевих екранів на різних рівнях моделі OSI. Схеми мережевого захисту на базі міжмережевих екранів.

Розділ 3. Захист на каналному та сеансовому рівнях

Протоколи формування захищених каналів на каналному рівні. Протоколи PPTP та L2TP. Протоколи формування захищених каналів на сеансовому рівні. Протоколи SSL/TLS. Протокол SOCKS. Захист бездротових мереж.

Розділ 4. Захист на мережевому рівні - протокол IPSec

Архітектура засобів безпеки IPSec. Захист передаваних даних за допомогою протоколів AH та ESP. Протокол захисту заголовку AH для аутентифікації. Протокол захист ESP. Алгоритми аутентифікації та шифрування у IPSec.

Протоколи PPTP та L2TP. Протоколи формування захищених каналів на сеансовому рівні. Протоколи SSL/TLS. Протокол SOCKS. Захист бездротових мереж. Захист на мережевому.

6. Самостійна робота

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

Розподіл годин СРС: підготовка до заліку – 24 години; підготовка до лекцій – 22 години; підготовка до лабораторних робіт – 14 годин; підготовка до МКР – 6 годин.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

- Відвідування лекцій, а також відсутність на них, не оцінюються. 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 (PCO)

1. Поточний контроль (виконання робіт в семестрі) оцінюється у 100 балів. Розподіл балів наведено в таблиці:

Роботи	Максимальна кількість балів за виконання однієї роботи	Σ
Лабораторні роботи 1 - 6	10	60
Модульна контрольна робота	40	40
		100

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.

2. 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 14-15
Умови отримання позитивної оцінки	≥ 12 балів	≥ 24 бали

3. Умови допуску до заліку: відсутність заборгованостей з лабораторних робіт 1 - 6.

Студенти, які виконали умови допуску до заліку та мають рейтингову оцінку 60 і більше балів, отримують відповідну до набраного рейтингу оцінку без додаткових випробувань.

Зі студентами, які виконали умови допуску до заліку та мають рейтингову оцінку менше 60 балів, а також з тими студентами, хто бажає підвищити свою рейтингову оцінку, на останньому за розкладом занятті з дисципліни в семестрі проводиться семестровий контроль у вигляді заліку.

4. Відповідь на заліку оцінюється у 100 балів. Залікова робота складається з одного теоретичного питання та одного практичного завдання. Ваговий бал теоретичного питання – 50 балів, завдання – 50 балів.

Теоретична частина оцінюється таким чином:

- правильна чітко викладена, повна відповідь – (не менше 90% потрібної інформації) – 45-50 балів;
- достатньо повна відповідь (не менше 75% потрібної інформації) – 38-44 бали;
- неповна відповідь (не менше 60% потрібної інформації) – 30-37 балів;
- незадовільна відповідь – 0 балів.

Практичне завдання оцінюється таким чином:

- повне, безпомилкове розв'язування завдання – 45-50 балів;
- повне, розв'язування завдання із несуттєвими невідповідностями – 38-44 бали;
- завдання виконане з певними недоліками – 30-37 балів;
- завдання не виконано – 0 балів.

5. Рейтингова оцінка за освітній компонент за бажанням студента визначається одним з таких способів:

- 1) кількість балів, отриманих за поточний контроль, або
- 2) результат виконання залікової контрольної роботи (тоді не враховуються бали, отримані в семестрі).

Таблиця 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 Ониськом Андрієм Іллічем асистентом кафедри Кардашовим Олександром Вадимовичем

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.).

