



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	Комп'ютерний моніторинг та геометричне моделювання процесів і систем
Статус дисципліни	Вибіркова
Форма навчання	Очна (денна)
Рік підготовки, семестр	4 курс осінній 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://rozklad.kpi.ua
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: к.в.н., доцент, Онисько Андрій Ілліч, oniskoandrij2020@gmail.com тел. 096-374-84-20 Лабораторні: к.в.н., доцент, Онисько Андрій Ілліч, oniskoandrij2020@gmail.com тел. 096-374-84-20
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 в комп'ютерних мережах; розробляти комплекс заходів для забезпечення захисту комп'ютерних систем; обирати та використовувати інформацію щодо безпеки комп'ютерних систем.

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

У структурно-логічній схемі навчання зазначена дисципліна розміщена на 4 курсі, тобто тоді, коли студенти вже прослухали "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 PPTP 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 AH та ESP.
- Тема 4.3. Протокол захисту заголовку AH для аутентифікації. Протокол захист ESP.
- Тема 4.4. Алгоритми аутентифікації та шифрування у IPSec.

4. Навчальні матеріали та ресурси

Основна література

1. Комп’ютерні мережі та телекомунікації: навч. посібник / В. А. Ткаченко, О. В. Касілов, В. А. Рябик. – Харків: НТУ “ХПІ”, 2011. – 224 с.
2. Абрамов В. О., Клименко С. Ю. Базові технології комп’ютерних мереж: навчальний посібник. – К.: Київ, 2011. – 291 с.
3. Кулаков Ю. А., Луцький Г. М. – Комп’ютерні мережі. Підручник – Київ: “Юніор”, 2005. – 400 с.
4. Жуков І. А., Гуменюк В. О., Альтман І.Є. Комп’ютерні мережі та технології.– К.: НАУ, 2004. – 276 с.
5. Бурко Н. Г., Безугла Г. Є., Комп’ютерні мережі. Навч. посібник – ХНУРЕ, 2002 – 200 с.
6. Gim Geier. Wireless Networks. First Step – Cisco Press, 2005. – 192 p.

7. William Stallings. High Speed Networks and Internet. Performance and Quality of Service. 2nd Edition – Prentice Hall PTR, 2002. – 783 p.

8. Комп'ютерні мережі. Книга.1. [Навчальний посібник] /Микитишин А.Г., Митник М.М., Стухляк П.Д., В.В. Пасічник . – Львів, «Магнолія 2006», 2013. – 256 с.

9. Комп'ютерні мережі. Книга.2. [Навчальний посібник] /Микитишин А.Г., Митник М.М., Стухляк П.Д., В.В. Пасічник . – Львів, «Магнолія 2006», 2013. – 328 с.

10. Зайченко Ю.П. Комп'ютерні мережі. Навчальний посібник для ВНЗ / – К.; Слово. – 2003. – 256 с.

Навчальний контент

5. 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 захисту 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

На самостійну роботу студента відведено 66 годин.

Перелік питань, що виносяться на самостійне опрацювання:

1. Проблеми передавання даних в мережі.
2. Моделі передавання даних в мережі

3. Передавання даних на нижніх рівнях мережі
4. Передавання даних на верхніх рівнях мережі
5. Взаємодія між рівнями мережі передавання даних
6. Проблеми забезпечення якості сервісів мережі Інтернет
7. Віртуалізація мереж
8. Безпека передавання даних в мережі
9. Принципи реагування на зміни топології мережі

6. Самостійна робота

Самостійна робота студента (66 годин) передбачає підготовку до аудиторних занять та контрольних заходів, проведення розрахунків та підготовка вхідних даних до роботи.

Розподіл годин СРС: підготовка до заліку – 30годин; підготовка до лабораторної роботи – 2 години; підготовка до МКР – 6 годин; підготовка до лекції – 1 година.

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)

- Рейтинг студента з освітнього компонента розраховується зі 100 балів, з них 50 балів складає стартова шкала. Стартовий рейтинг (протягом семестру) складається з балів, що студент отримує за виконання лабораторних робіт (6 робіт) та МКР;

- Критерії нарахування балів за виконання лабораторних робіт.

Ваговий бал за виконання завдань лабораторних робіт складає 5 балів. Максимальна кількість балів за всі завдання дорівнює

$$5 \text{ балів} \times 6 = 30 \text{ балів.}$$

Виконання кожного завдання оцінюється за наступними критеріями:

1. правильність отриманих результатів – від 1 до 4 балів;
2. зручний інтерфейс користувача – 0.3 бали;
3. інтерактивне введення параметрів методу – 0.3 бали;
4. динамічні зміни на екрані – 0.4 бали;

Мінімальна кількість для зарахування лабораторної роботи складає 3 бали (60%)

Максимальна кількість балів за контрольну роботу дорівнює 10 балів. На модульну контрольну роботу виноситься одне теоретичне питання та два практичних.

Контрольна робота оцінюється наступним чином:

1. правильність написання теоретичного питання - 5 балів;
2. надання прикладу на вказані завдання – 1 бал;
3. правильність розв'язання практичного завдання - 2 бали;

- За активність на лекціях та виконання домашніх робіт нараховується максимум – 5 балів.

- Умови допуску до заліку: зарахування всіх лабораторних робіт. Мінімальна кількість набраних балів – 30 (60%).

- На заліку студенти виконують письмову роботу. Екзаменаційний білет складається з двох теоретичних питань та одного практичного завдання. Ваговий бал кожного теоретичного питання – 15. Ваговий бал практичного завдання – 20. Максимальна кількість балів за складання екзамену дорівнює

$$15 \text{ балів} \times 2 + 20 \text{ балів} = 50 \text{ балів.}$$

Теоретична частина оцінюється наступним чином:

- «відмінно» , правильна чітко викладена, повна відповідь – (не менше 90 % потрібної інформації) – 14-15 балів;
- «добре», достатньо повна відповідь (не менше 75% потрібної інформації) – 11-13 балів;
- «задовільно», неповна відповідь (не менше 60% потрібної інформації) – 9-10 балів;
- «незадовільно», незадовільна відповідь - 0 балів.

Практичне завдання оцінюється наступним чином:

- «відмінно» , повне, безпомилкове розв'язування завдання– 18-20 балів;
- «добре», повне, розв'язування завдання із несуттєвими неточностями – 15-17 балів;
- «задовільно», завдання виконане з певними недоліками – 12-14 балів;
- «незадовільно завдання невиконано.

5. Сума стартових балів і балів за залік переводиться за освітній компонент 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 доцентом, к.в.н., доц. Ониськом Андрієм Іллічем

Ухвалено кафедрою ЦТЕ (протокол № 01 від 01.07.2022 р.)

Погоджено Методичною комісією НН ІАТЕ КПІ ім. Ігоря Сікорського (протокол № 10 від 04.07.2022 р.)