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

Кафедра системного проєктування

Захист інформації

Робоча програма навчальної дисципліни (Силабус)

● Реквізити навчальної дисципліни

Рівень вищої освіти	Другий (магістерський)
Галузь знань	12 Інформаційні технології
Спеціальність	122 Комп'ютерні науки
Освітня програма	Комп'ютерні науки
Статус дисципліни	Вибіркова
Форма навчання	очна(денна)/дистанційна/змішана
Рік підготовки, семестр	6 курс, осінній семестр
Обсяг дисципліни	5 кредитів ЄКТС (150 г.): лекції – 36 г., лабораторні роботи – 36 г., СРС – 78 г.
Семестровий контроль/ контрольні заходи	Екзамен / модульна контрольна робота / РГР
Розклад занять	https://cad.kpi.ua/student/rozklad-zanjat/
Мова викладання	Українська
Інформація про керівника курсу / викладачів	Лектор: к.т.н. Кирюша Богдан Анатолійович, bogdankyrysha@gmail.com Лабораторні: к.т.н. Кирюша Богдан Анатолійович
Розміщення курсу	https://ecampus.kpi.ua

● Програма навчальної дисципліни

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

Метою дисципліни є вивчення методів та засобів захисту інформаційних систем персонального та професійного рівня. Вивчення базується на теоретичних відомостях, нормативно-правових актах та відкритому ПО та технічних засобах.

Вивчаються сучасні погрози до персональної та корпоративної інформації, способи протидії атакам, правила, яких мають дотримуватись розробники та користувачі програмного забезпечення. Протоколи авторизації та ідентифікації. Захищені архітектури локальних та розподілених мереж. Типи мережевих атак. Системи ідентифікації вторгнень мережевого та локального рівня. Системи детектування вторгнень хмарного рівня. Класифікація мережевих атак, їх алгоритми та засоби реалізації.

Студенти після засвоєння кредитного модуля мають продемонструвати такі результати навчання:

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

знання:

– технічних та організаційних методів захисту інформації.
– правових аспектів забезпечення захисту інформації.
– методів та засобів пошуку вразливостей інформаційних систем.
– принципів побудови та способів використання сучасних систем захисту інформації.

уміння:

– розробити план заходів з пошуку вразливостей існуючих інформаційних систем;
– розробити політику безпеки для мережевої системи або невеликого підприємства;
– впроваджувати виконання політики безпеки на технічному, програмному та організаційному рівнях;
– впроваджувати існуючи системи захисту інформації для виконання політики безпеки

підприємства.

Згідно з вимогами освітньо-професійної програми, засвоєння навчальної дисципліни сприяє оволодінню здобувачами вищої освіти такими компетентностями та програмними результатами навчання:

Загальні компетентності:

- ЗК 2 Здатність застосовувати знання у практичних ситуаціях;
- ЗК 7 Здатність генерувати нові ідеї (креативність).

Фахові компетентності спеціальності:

- ФК1 Усвідомлення теоретичних засад комп'ютерних наук.,
- ФК4 Здатність збирати і аналізувати дані (включно з великими), для забезпечення якості прийняття проєктних рішень;
- ФК6 Здатність застосовувати існуючі і розробляти нові алгоритми розв'язування задач у галузі комп'ютерних наук;
- ФК7 Здатність розробляти програмне забезпечення відповідно до сформульованих вимог з урахуванням наявних ресурсів та обмежень;
- ФК13 Здатність провадити науково-педагогічну діяльність у закладах вищої освіти;
- ФК16 Здатність до створення і використання сучасних інформаційних систем та технологій різного призначення, сервіс-орієнтованих обчислень і архітектур, туманних обчислень, контекстно-керованих адаптивних обчислень, безсерверних обчислень;

Програмні результати навчання:

- ПРН3 Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію у сфері комп'ютерних наук до фахівців і нефахівців, зокрема до осіб, які навчаються;
- ПРН6 Розробляти концептуальну модель інформаційної або комп'ютерної системи;
- ПРН9 Розробляти алгоритмічне та програмне забезпечення для аналізу даних (включно з великими);
- ПРН10 Проєктувати архітектурні рішення інформаційних та комп'ютерних систем різного призначення.
- ПРН20 Створювати та досліджувати інформаційні та математичні моделі систем і процесів, що досліджуються, зокрема об'єктів автоматизації.

.

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

Забезпечуючі дисципліни бакалаврського та магістерського рівня підготовки: «Архітектура обчислювальних систем», «Безпека інформаційних систем»», «Дискретна математика», «Алгоритми і структури даних», «Технології створення програмних сервісів», «Операційні системи». Знання та уміння, отримані при вивченні дисципліни "Захист інформації" можуть використовуватись при написанні магістерської дисертації а також в подальшій професійній діяльності.

3. Зміст навчальної дисципліни

Тема 1. Мета, завдання та зміст курсу.
Тема 2. Авторизація користувача.
Тема 3. Забезпечення безпеки інформації в відкритих мережах
Тема 4. Системи автоматизованого пошуку погроз
Тема 5. Класифікація вірусів, та відповідних засобів протидії.
Тема 6. Системи виявлення вторгнень
Тема 7. Нормативно-правові акти, що регулюють права та обов'язки громадян.
Тема 8. Пояснення до термінології та правил використання громадянського кодексу
Тема 10. Політика безпеки

4. Навчальні матеріали та ресурси

Базова література:

1. Писарчук О.О. Основи захисту інформації : навчальний посібник / О.О. Писарчук, Ю. Г. Даник,

С. Г. Вдовенко та ін. – Житомир : ЖВІ ДУТ, 2015.
2. Корченко О. Г. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014.
3. Писарчук О.О. Захист інформації в комп'ютерних системах»: Навч. посібник. [Електронний ресурс] / Писарчук О.О.–Електронні текстові дані (1 файла: 1,8байт). – Київ : КПІ ім. Ігоря https://ela.kpi.ua/handle/123456789/48296
4. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г.Король. – Х. : Вид. ХНЕУ, 2013.
5. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С.П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с. (Укр. мов.)
6. Дронюк І. М. Технології захисту інформації на матеріальних носіях Монографія. Львів :Видавництво Львівської політехніки, 2017. 200 с.
7. Тарнавський, Ю.А. Технології захисту інформації [Електронний ресурс] : підручник для студентів спеціальності 122 «Комп'ютерні науки», спеціалізацій «Інформаційні технології моніторингу довкілля», «Геометричне моделювання в інформаційних системах» / Ю. А. Тарнавський ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с.

Додаткова література:

1. Вітер С.А. Захист облікової інформації та кібербезпека підприємства / С.А. Вітер, І.І. Світлишин // Економіка і суспільство: електронне фахове видання. – 2017.
2. Эл Свейгарт. Криптография и взлом шифров на Python / Эл Свейгарт, К.:«ДИАЛЕКТИКА», 2020, 512 с.
3. Бойченко О. Моделювання сучасних систем захисту інформаційних ресурсів / О. Бойченко // Комп'ютерні технології друкарства : зб. наук. пр. / М-во освіти і науки України, Укр. акад. друкарства ; [редкол.: Б. В. Дурняк та ін.]. – Львів, 2011. – № 26. – С. 269–275.
4. Кононова В. О. Оцінка засобів захисту інформаційних ресурсів / В. О. Кононова, О. В. Харкянен, С. В. Грибков // Вісник Національного університету "Львівська політехніка" / М-во освіти і науки України, Нац.ун-т "Львівська політехніка" ; відп. ред. А. О. Мельник. – Львів, 2014. – №806 : Комп'ютерні системи та мережі. – С. 99–105.
5. Шатило Я. Л. Підвищення ефективності функціонування комплексів технічного захисту інформації / Я. Л. Шатило // Імперативи розвитку цивілізації : [матеріали міжнар. наук.-практ. конф. «Інформаційна безпека у воєнній сфері. Сучасний стан та перспективи розвитку», Київ, 31 берез. 2015 р.] / М-во оборони України, Нац. ун-т оборони України ім. І. Черняховського, Глобал. орг. союзн. лідерства ; [орг. ком.: Б. Й. Семон та ін.]. – Київ, 2015. – № 2. – С. 116–119.
6. Лисенко С. М. Аналіз методів виявлення шкідливого програмного забезпечення в комп'ютерних системах / С. М. Лисенко, Р. В. Щука // Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 2. – С. 101-107.
7. Аналіз апаратної підтримки криптографії у пристроях інтернету речей / Я.Р. Совин [та ін.] // Безпека інформації. – 2018. – Т. 24, № 1. – С. 36–48.

● Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань *(перелік дидактичних засобів, завдання на СРС з посиланням на літературу)*
1	**Лекція 1**. Мета, завдання та зміст курсу. Визначення основних понять та питань, що використовуються в системах ЗІ мережевого та протокольного рівня. Завдання на СРС: Повторення лекційного матеріалу. Ідентифікація користувача. Паролі, смарт-карти, біометрика, хендшейк. Завдання на СРС: Повторення лекційного матеріалу. *Література: 1(1), 5(1).*
2	**Лекція 2**. Ідентифікація та авторизація в відкритих мережах. Завдання на СРС: Повторення лекційного матеріалу. Авторизація користувача. Алоритм Діфі-Хелмана. Поняття ЦРК. Протоколи авторизації з ЦРК. Завдання на СРС: Повторення лекційного матеріалу. Вивчити основні етапи проектування і класифікацію моделей ЦРК.

№ з/п	Назва теми лекції та перелік основних питань *(перелік дидактичних засобів, завдання на СРС з посиланням на літературу)*
	Література: 1(1), 5(1).
3	**Лекція 3**. Забезпечення безпеки інформації в відкритих мережах: обладнання. Класифікація та характеристики основних апаратних засобів, які використовуються в ЗІ на мережевому рівні. Завдання на СРС: Повторення лекційного матеріалу. Вивчити основні типи моделей елементів мережі, зв'язків і протоколів. *Література: 4(1), 0(1), (1.3,4).*
4	**Лекція 4**. Класифікації погроз в відкритих мережах та стратегії їх застосування. Завдання на СРС: Повторення лекційного матеріалу. Вивчити основні типи погроз. *Література: 4(1), 0(1), (1.3,4).*
5	**Лекція 5.** Забезпечення безпеки інформації в відкритих мережах: архітектури. Способи використання мережевого обладнання для подолання загроз різного типу. Завдання на СРС: Повторення лекційного матеріалу. Вивчити основні типи загроз і їх протидії. *Література: 3(1),4(13)*
6	**Лекція 6.** Особливості вразливостей мобільних пристроїв. Завдання на СРС: Повторення лекційного матеріалу. Вивчити основні типи загроз мобільних пристроїв. *Література: 3(1),4(13)*
7	**Лекція 7.** Особливості вразливостей елементів розумного будинку. Завдання на СРС: Повторення лекційного матеріалу. Вивчити основні типи загроз елементів розумного будинку. *Література: 3(1),4(13)*
8	**Лекція 8.** Системи автоматизованого пошуку погроз. Аналіз бездротових мереж за допомогою Kali Linux. Завдання на СРС: Повторення лекційного матеріалу. Повторення практичних дій з тестування, виконаних на лекції в умовах домашньої мережі. *Література: 1(13), 4(3.5)*
9	**Лекція 9.** Системи автоматизованого пошуку погроз з використанням елементів штучного інтелекту та хмарних сервісів. Завдання на СРС: Повторення лекційного матеріалу. Повторення практичних дій з тестування, виконаних на лекції в умовах домашньої мережі. *Література: 1(13), 4(3.5)*
10	**Лекція 10**. Класифікація вірусів, та відповідних засобів протидії. Склад сучасної системи комплексного захисту інформації. Пояснення відмінностей між професійними системами комплексного захисту інформації та персональними системами. Завдання на СРС: Виконати пошук прикладу персональної та професійної системи захисту інформації. *Література: 1(13), 4(3.5)*
11	**Лекція 11**. Системи виявлення вторгнень локального типу, їх архітектура та налаштування. Засоби автоматизації обробки файлів-протоколів. Завдання на СРС: Виконати пошук прикладу персональної та професійної системи виявлення вторгнень. *Література: 2 (2.2)*
12	**Лекція 12**. Системи виявлення вторгнень мережевого типу, їх архітектура та налаштування. Засоби автоматизації обробки файлів-протоколів. Завдання на СРС: Виконати пошук прикладу персональної та професійної системи виявлення вторгнень. *Література: 2 (2.2)*
13	**Лекція 13**. Класифікація засобів ТЗІ (технічного захисту інформації). *Література: 1(9),2(1.5).*
14	**Лекція 14**. Поняття матриці безпеки. Способи побудови та перевірки матриці безпеки.

№ з/п	Назва теми лекції та перелік основних питань *(перелік дидактичних засобів, завдання на СРС з посиланням на літературу)*
	Література: 1(9),2(1.5).
15	**Лекція 15**. Нормативно-правові акти, що регулюють права та обов'язки громадян України, що до захисту інформації. Державні установи, які керують виконанням вимог до захисту інформації в Україні. Відносини між замовниками, розробниками та користувачами інформаційних систем. *Література: 1(9,10), 2(1.5,3.4).*
16	**Лекція 16**. Пояснення до термінології та правил використання громадянського кодексу України до порушень в сфері інформаційної безпеки. Завдання на СРС: Запропонувати власні приклади до розглянутих статей кодексу. *Література: 1(10).*
17	**Лекція 17**. Політика безпеки: поняття, складові, процедура розробки та впровадження. *Література: 1(13), 4(3.5)*
18	**Лекція 18**. Автоматизація створення політик безпеки та їх впровадження. *Література: 1(13), 4(3.5)*

Лабораторні заняття

№ з/п	Назва лабораторної роботи	Кількість годин
1	Простий клієнт-серверний додаток на сокетах	8
2	Розробка клієнт-сервера видаленого доступу до захищених даних	6
3	Аналіз мережевого трафіку засобами KaliLinux	6
4	Імітація мережевих атак	8
5	Протидія мережевим атакам	8
	Загалом	36

Розрахунково-графічна робота

Розробка матриці безпеки типового підприємства з розташуванням в окремо розташованому будинку. В якості альтернативи, допускається розробка політики безпеки або впровадження мережевої системи виявлення вторгнень.

6. Самостійна робота студента

№ з/п	Види робіт, що виносяться на самостійне опрацювання	Кількість годин
1 2	Підготовка до лекційних занять Підготовка до лабораторних занять	9 10
3	Виконання РГР	15
4	Вивчення питань, що винесені на самостійну роботу,робота з літературними джерелами	10
5	Підготовка до контрольної роботи	4
6	Підготовка до іспиту	30
	Загалом	78

● Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Вимоги, яких має дотримуватися студент в рамках даної дисципліни:

- доповнювати відвідування лекцій вивченням електронних матеріалів з онлайн класу;
- заохочувальні бали можуть призначатися за активність на лекціях;
- штрафні бали можуть призначатися за несвоєчасне виконання лабораторних робіт;
- обов'язковим є самостійне та доброчесне виконання робіт.

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.

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

Семестрова атестація проводиться у виді екзамену. Для оцінювання результатів навчання застосовується 100-бальна рейтингова система і університетська шкала оцінювання.

Поточні індивідуальні рейтинги студентів оновлюються після кожного лекційного заняття і у будь-який момент доступні для студентів на навігаційній сторінці кредитного модулю в електронному кампусі НТУУ «КПІ».

Атестація студентів базується на поточній рейтинговій оцінці, яка враховує активність на заняттях, виконання лабораторних робіт , МКР і розрахунково-графічну роботу. Умовою позитивної атестації є значення поточного рейтингу студента не менше, ніж 50% від максимально можливого на час атестації.

Рейтинг студента з дисципліни складається з балів, що він отримує за:

1. виконання та захист 5 лабораторних робіт;
2. одну розрахунково-графічну роботу;
3. модульну контрольну роботу.

Система рейтингових (вагових) балів та критерії оцінювання

1. Лабораторні роботи

Вагові бали лабораторних робіт:

Лаб. роб.	1	2	3	4	5
Бали	8	8	8	8	8

Оцінюється повнота, якість виконання завдань і якість відповідей на контрольні запитання. Максимальна кількість балів за всі лабораторні роботи дорівнює 40 балам.

2. Розрахунково-графічна робота

Вагові бали завдання:

1. Правильність формування проектних завдань - 5
2. Правильність програмування 5
3. Розуміння дій, що виконуються вибраними процедурами - 5

Максимальна кількість балів дорівнює 15 балам.

3. Модульна контрольна робота.

Складається з 2 завдань, з тем, що розглядались на лекційних заняттях. Кожне питання оцінюється максимум в 5 балів.

Максимальна кількість балів дорівнює 10 балів.

4. Екзамен.

Максимальна кількість балів дорівнює 35 балів.

Штрафні та заохочувальні бали за:

- Здача лабораторної роботи пізніше встановленого терміну -1 бал.
- Несвоєчасне подання РГР (пізніше ніж на тиждень) -2 бали.
- За участь у модернізації лабораторних робіт, удосконалення дидактичних матеріалів з дисципліни надається від +3-5 заохочувальних балів.
- За відвідування ≥ 80% лекційних занять 4- 10 бали.

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

9. Додаткова інформація з дисципліни (освітнього компонента)

Перелік питань, які виносяться на семестровий контроль (екзамен):

1. Яке призначення механізму хендшейк?
2. Які переваги та недоліки має використання списку паролів?
3. Що таке двостороння авторизація та чим вона відрізняється від односторонньої?
4. В чому полягає ідея введення додаткових перевірок особи користувача? Наведіть приклади такої перевірки.
5. Поясніть призначення алгоритму Діфі-Хелмана. Чи можна його вважати алгоритмом двосторонньої авторизації?
6. Наведіть приклад процедури авторизації з ЦРК та симетричним шифруванням. Алгоритм шифрування та хендшейку обрати за власним бажанням.
7. Наведіть приклад процедури авторизації з ЦРК та асиметричним шифруванням. Алгоритм шифрування та хендшейку обрати за власним бажанням.
8. Наведіть приклад процедури авторизації з ЦРК та симетричним шифруванням та часовими позначками. Алгоритм шифрування та хендшейку обрати за власним бажанням.
9. Наведіть приклад процедури авторизації з ЦРК та асиметричним шифруванням та часовими позначками. Алгоритм шифрування та хендшейку обрати за власним бажанням.
10. Від яких типів атак захищає брандмауер початкового рівня?
11. Від яких типів атак захищає брандмауер експертного рівня?
12. Від яких типів атак захищає побудова мережі з демілітаризованою зоною (дворівневий брандмауер)?
13. Від яких типів атак захищає мережева система виявлення вторгнень?
14. Від яких типів атак захищає система виявлення вторгнень на комп’ютері користувача?
15. Від яких типів атак захищає антивірус?
16. Від яких типів атак не захищає брандмауер початкового рівня?
17. Від яких типів атак не захищає брандмауер експертного рівня?
18. Від яких типів атак не захищає побудова мережі з демілітаризованою зоною (дворівневий брандмауер)?
19. Від яких типів атак не захищає мережева система виявлення вторгнень?
20. Від яких типів атак не захищає система виявлення вторгнень на комп’ютері користувача?
21. Від яких типів атак не захищає антивірус?
22. З яких етапів складається формування матриці безпеки?
23. Які службі входять в зону найщільнішого захисту та які технічні засоби в цій зоні застосовуються?
24. Перерахуйте технічні засоби авторизації та розподіліть їх серед зон матриці безпеки.
25. Перерахуйте технічні засоби визначення присутності/проникнення та розподіліть їх серед зон матриці безпеки.
26. Які засоби допустимо застосовувати для затримки/уповільнення вторгнення.

Робочу програму навчальної дисципліни (силабус):
Складено доцент, к. т. н. Кирюша Богдан Анатолійович
Ухвалено кафедрою системного проектування (протокол № 13 від 17.06.2024)
Погоджено методичною комісією НН ІПСА (протокол № 10 від 24.06.2024)
Погоджено науково-методичною комісією КПІ ім. Ігоря Сікорського зі спеціальності 122 Комп'ютерні науки (протокол №11 від 28.06.2024)