Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 5

КУРСОВИЙ ПРОЕКТ
З ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ
Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Перший (бакалаврський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітньо-професійна програма	*Комп'ютерні системи і технології спеціального зв'язку*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (Денна)*
Рік підготовки, семестр	*IV рік підготовки, весняний семестр*
Обсяг дисципліни	*1,5 Кредитів ECTS*
Семестровий контроль / контрольні заходи	*Захист курсового проекту*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*Керівництво курсовим проектом: Ігор ЯКОВІВ, Дмитро ШАРАДКІН*
Розміщення курсу	*Google Classroom*

Київ 2022

Програма навчальної дисципліни

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

Силабус освітнього компонента «Поектування інформаційних систем - КП» складено відповідно до освітньої програми підготовки бакалаврів «Комп'ютерні системи і технології спеціального зв'язку» спеціальності 122 – Комп'ютерні науки.

Метою навчальної дисципліни є формування та закріплення у студентів наступних компетентностей: (ЗК1) Здатність до абстрактного мислення, аналізу та синтезу; (ЗК2) Здатність застосовувати знання у практичних ситуаціях.; (ЗК3) Знання та розуміння предметної області та розуміння професійної діяльності; (ЗК11) Здатність приймати обґрунтовані рішення; (ЗК12) Здатність оцінювати та забезпечувати якість виконуваних робіт; (СК3) Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем; (СК10) Здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника; (СК14) Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури; (СК18) Здатність до проектування архітектури інформаційно-телекомунікаційних систем державних інформаційних ресурсів (ІТС ДІР), вибору і інтегруванню сертифікованих компонентів технічного і стандартного програмного забезпечення при реалізації технології обробки інформації з обмеженим доступом (ІзОД).

Предмет навчальної дисципліни – основні сучасні методології і методи побудови інформаційних систем та управління ними, основні класи, типи та категорії інформаційних систем, їх функціональні можливості та сфери застосування, сучасні методології, методи, моделі та інструментальні засоби створення і застосування інформаційних систем різних типів.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (ПР1) Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук; (ПР4) Використовувати методи обчислювального інтелекту, машинного навчання, нейромережевої та нечіткої обробки даних, генетичного та еволюційного програмування для розв'язання задач розпізнавання, прогнозування, класифікації, ідентифікації об'єктів керування тощо; (ПР11) Володіти навичками управління життєвим циклом програмного забезпечення, продуктів і сервісів інформаційних технологій відповідно до вимог і обмежень замовника, вміти розробляти проектну документацію (техніко-економічне обґрунтування, технічне завдання, бізнес-план, угоду, договір, контракт); (ПР14) Знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення..

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

Для успішного засвоєння дисципліни студент повинен володіти освітніми компонентами "Проектування інформаційних систем". Компетенції, знання та уміння, одержані в процесі вивчення освітнього компонента є необхідними для подальшого вивчення освітніх компонентів "Переддипломна практика (Військове стажування)", "Дипломне проектування".

3. Зміст навчальної дисципліни

Семестр 8.

Семестровий (кредитний) модуль 1. Проектування інформаційних систем – КП.

3.1. Опис порядку організації виконання курсового проекту.

Завдання на курсової проект складається із двох частин:

- загальна частина завдання на курсовий проект (далі - ЗЧЗ КП);
- індивідуальна частина завдання на курсовий проект (далі – ІЧЗ КП).

ЗЧЗ КП включає в себе:

- загальний опис вихідної ситуації (найменування та завдання державної установи , порядок формування та обробки інформації, організаційно-штатну структуру установи, посадові функції в рамках процесу обробки інформації, плани розміщення приміщень та будівлі установи;
- особливості організації роботи (характеристики інформації, профіль інформаційної взаємодії з іншими установами, перечень обладнання приміщень);
- перелік завдань, що потрібно виконати курсантам.

ІЧЗ КП містить перелік конкретних значінь декількох параметрів, що унікальні для кожного курсанта.

3.2.Загальний опис вихідної ситуації.

Державна служба експертного регулювання (*ДСЕР*, далі - *Служба*) здійснює контроль у сфері експорту-імпорту товарів (технологій) військового та подвійного призначення. Контроль здійснюється шляхом експертизи заяв суб'єктів експорту-імпорту на предмет відповідності:

- державній системі нормативно-правового регулювання у цієї сфері;
- міжнародним зобов'язанням держави.

Процедура експертизи складається з наступних етапів:

1) прийом та реєстрація формалізованих заяв від суб'єктів зовнішньоекономічної діяльності;
2) тематична експертиза матеріалів заяви державними експертами;
3) затвердження результатів експертизи профільною комісією Кабінету Міністрів;
4) підготовка і видача державних дозволів на право експорту-імпорту товарів.

З метою підвищення ефективності роботи Служби її керівництво прийняло рішення про створення інформаційної системи забезпечення експертизи (далі - ІСЗЕ), основними завданнями якої є:

- зниження часу підготовки документів експертизи;
- поліпшення якості контролю виконання функціональних завдань;
- підвищення оперативності управління підрозділами;
- інформаційно-аналітичне забезпечення керівництва Служби за рахунок організації доступу до ресурсів WWW;
- інформування клієнтів Служби про порядок оформлення матеріалів заяв шляхом створення свого інформаційного порталу в Інтернет;
- забезпечення безпеки інформаційних ресурсів Служби.

Примітка: ДСЕР відноситься до державного переліку об’єктів критичної інфраструктури.

3.3. Семантика завдання на КП.

Курсант виступаєте в якості *провідного спеціаліста відділу автоматизації і аналітичного забезпечення,* якому доручена підготовка основних вимог до інформаційної системи. За результатами курсового проекту повинні бути представлені:

1) Формалізовані результати аналізу інформаційного середовища установи (перелік інформаційних потоків, інформаційно-функціональні структури потоків; інформаційно-функціональна структура організації).
2) Вербальний опис принципів роботи автоматизованої системи, що забезпечують реалізацію технології обробки інформації на основі бази даних.

a. Структура комп'ютерної системи ІСЗЕ (у вигляді багаторівневої схеми), що відображає компоненти основні сервіси системи та принципи комутації комп'ютерного обладнання.
b. Перелік апаратного та програмного забезпечення, необхідного для реалізації АСЗЕ, схема розміщення ОТСЗ в приміщеннях організації.
c. Схема розміщення обладнання ІСЗЕ (для заданого відділу: ОТСЗ + ДТСЗ).
d. Схему даних для БД "Експертиза".
e. БД "Експертиза".
f. Вимоги до комплексної системи захисту інформації (далі - КСЗІ), отримані у вигляді:

3) Обґрунтування необхідності створення КСЗІ з підтвердженою відповідністю.
4) Модель загроз.
5) Політика безпеки інформації в організації.
6) Аргументовано обрані стандартні функціональні профілі захищеності (СФПЗ).
7) Акт категоріювання відповідно до НД ТЗІ 1.6-005-13 і НД ТЗІ 1.6-006-15 для приміщень заданого відділу.
8) Перелік необхідних заходів захисту від актуальних кіберзагроз. Порядок їх реалізації.
9) Перелік та склад можливих технічних каналів витоку на основі ПЕМВН (у разі необхідності).
   a. Перелік сертифікованих засобів захисту для КСЗІ.
   b. Компоненти КСЗІ та їх взаємозв'язок (у вигляді функціональної структури).

4. Навчальні матеріали та ресурси

Основна література:

1. Проектування інформаційних систем: Загальні питання теорії проектування ІС (конспект лекцій) [Електронний ресурс https://ela.kpi.ua/bitstream/123456789/33651/1/PIS_KL.pdf] : навч. посіб. для студ. спеціальності 122 "Комп'ютерні науки" / КПІ ім. Ігоря Сікорського; уклад.: О. С. Коваленко, Л. М. Добровська. Київ : КПІ ім. Ігоря Сікорського, 2020. 192 с.

2. Пономаренко В. С., Пушкар І. О., Мінухін С. В. Проектування інформаційних систем. К.: ВС "Академія" , 2002. 486 с.

3. Недашківський О. М.. Планування та проектування інформаційних систем. Київ, 2014. 215 с.

4. Ушакова І. О. Основи системного аналізу об'єктів і процесів комп'ютеризації. Частина 2. Харків: Вид. ХНЕУ, 2008. 308 с.

5. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. ТР ЕОТ–95.

6. Пономаренко В.С., Пушкар І.О., Мінухін С.В. Проектування інформаційних систем.- К.: ВС "Академія" , 2002.- 486 с.

7. Закон України "Про інформацію".

8. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

9. Закон України " Про основні засади забезпечення кібербезпеки України".

10. Закон України "Про доступ до публічної інформації".

11. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".

12. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. ЗАТВЕРДЖЕНО постановою Кабінету Міністрів України від 29 березня 2006 р. N 373.

13. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. ЗАТВЕРДЖЕНО постановою Кабінету Міністрів України від 19 червня 2019 р. N 518.

14. Яковів І.Б. Основи побудови комплексної системи захисту інформації для інформаційно-телекомунікаційної системи. Навчальний посібник. Київ: Вид-во ІСЗЗІ НТУУ "КПІ імені Ігоря Сікорського", 2016. 88с.

15. НД ТЗІ 2.6-001-11. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах.

16. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. ТР ЕОТ–95.

17. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

18. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 №22.

19. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04.12.2000 № 53.

20. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 №22.

21. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

22. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

23. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

24. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено Указом Президента України від 07 березня 2016 року № 242/2016.

25. Яковів І.Б. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. Збірник наукових праць "Інформаційні технології і безпека". Том 5, № 2. К.: ІССЗІ, 2017.

26. Положення "Про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в інформаційно-телекомунікаційних системах". Затверджено постановою Кабінету Міністрів України від 16 лютого 1998 р. N 180.

27. НД ТЗІ 2.5-010-05: Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 02.04.2003,№ 33.

28. НД ТЗІ 1.6-005-13. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. Затверджено Адміністрацією Держспецзв'язку наказом від 15.04.2013 №215.

29. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено наказом Адміністрації Держспецзв'язку від 04.07.2008 №112.

30. Положення про державний контроль за станом технічного захисту інформації. Затверджено наказом Адміністрації Держспецзв'язку від 10.07.2007 №87.

Додаткова література:

1. Проектування інформаційних систем: навчальний посібник / В. С. Авраменко, А. С. Авраменко. Черкаси: Черкаський національний університет ім. Б.Хмельницького, 2017. 434 с.

2. Табунщик Г.В. Інженерія якості програмного забезпечення: навчальний посібник / Г. В. Табунщик, Р. К. Кудерметов, Т. І. Каплієнко. 2-ге видання. Запоріжжя: Дике Поле, 2016. 176 с.

3. Реєстр вразливостей MITRE Corporation CVE List (https://cve.mitre.org/cve/).

4. М. В. Грайворонський, О. М. Новіков. "Безпека інформаційно-комунікаційних систем". Київ: Видавнича група BHV, 2009, 608 с.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Графік виконання курсового проекту

Тиждень семестру	Назва етапу роботи	Навчальний час	
		Ауд.	СРК
1	Отримання теми та завдання .	-	2
1-2	Підбор та вивчення літератури .	-	4
3-4	Виконання розділу 1. Формалізований аналіз інформаційного середовища державної установи.	-	6
5-6	Виконання розділу 2. Розробка принципів обробки інформації комп'ютерною системою.		6
7-8	Виконання розділу 3. Розробка прототипу базі даних "Експертиза"		12
9	Виконання розділу 4. Формування вимог до комплексної системи захисту інформації.		9
10-11	Подання курсового проекту на перевірку.		2
11-13	Захист курсового проекту.		4
	Разом:	-	**45**

6. Самостійна робота курсанта

Всі завдання курсового проекту виконуються під час самостійної роботи курсанта. Проблемність виконання практичних завдань КП із застосуванням ПЕОМ досягається шляхом комплексного застосування знань і вмінь, отриманих на заняттях навчальних дисциплін "Технології розробки програмного забезпечення", "Системний аналіз", "Моделювання систем", "Безпека інформаційних систем", "Основи створення КСЗІ та аудит кібербезпеки", "Проектування інформаційних систем". Для формування вмінь в рамках практичних завдань курсового проекту застосовуються складові і функції CSIRT-ED та ситуаційного центру Держспецзв'язку, електронні інформаційні ресурси реєстру вразливостей MITRE Corporation CVE List (https://cve.mitre.org/cve/), бази даних вразливостей NIST NVD (https://nvd.nist.gov/).

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни визначає наступну систему вимог:

- виконання курсантами завдань курсового проекту проводиться розкладу, що визначає час самостійної роботи;

- курсант зобов'язаний опрацювати навчальний матеріал із якістю, що забезпечує формування професійних здатностей, які визначені метою навчальної дисципліни;

- поведінка курсанта під час виконання КП не повинна заважати ефективному засвоєнню навчального матеріалу та виконанню своїх обов'язків всіма учасниками навчального процесу;

- курсант забезпечує своєчасне та якісне виконання всіх завдань КП із дотриманням вимог академічної доброчесності.

Відвідування занять є обов'язковим. Відсутність на занять з будь яких причин не вважається поважною причиною невиконання відповідного домашнього завдання.

Всі робочі оголошення та необхідні матеріали курсу будуть розміщуватися на вказаній сторінці. Очікується, що студенти перевірятимуть свою електронну пошту і сторінку дисципліни в Google Class та реагуватимуть своєчасно. Результат виконання домашніх завдань також мають бути викладені на сторінці Google Class у форматі, який буде вказаний викладачем. Також через сторінку Google Class курсанти можуть надіслати у вигляді відкритого чи приватного листа викладачу питання, що виникли під час виконання завдань, або інші питання стосовно курсу, який вивчається.

Кожний курсант зобов'язаний дотримуватися принципів академічної доброчесності. Письмові завдання з використанням часткових або повнотекстових запозичень з інших робіт без зазначення авторства – це плагіат. Використання будь-якої інформації (текст, фото, ілюстрації тощо) мають бути правильно процитовані з посиланням на автора. До студентів, у роботах яких буде виявлено списування, плагіат чи інші прояви недоброчесної поведінки можуть бути застосовані різні дисциплінарні заходи.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даного кредитного модуля можна здійснювати віддалено з використанням технологій дистанційного навчання.

Навчальні матеріали та ресурси, зазначені у розділі 4 цієї робочої програми навчальної дисципліни (силабус) є відкритою, не містить відомостей з обмеженим доступом і може бути оприлюднена з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

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

8.1. Види контролю. Основні види контролю, які застосовуються в процесі курсового проектування:

- поточна перевірка матеріалів КП;
- підсумковий контроль (захист курсового проекту).

Оцінювання результатів навчання курсантів здійснюється у відповідності до Методичних рекомендацій до розроблення і застосування рейтингових систем оцінювання курсантів (студентів) в ІСЗЗІ КПІ ім. Ігоря Сікорського.

8.2. Рейтингова система оцінювання результатів навчання.

Шкала РСО з кредитного модуля R дорівнює 100 балів ($R=100$). Шкала РСО з кредитного модуля R дорівнює 100 балів ($R=100$).Рейтингова оцінка з курсового проекту RD матиме дві складові:

- перша (стартова) складова r_1 характеризує роботу курсанта з курсового проектування та її результат – якість пояснювальної записки та графічного матеріалу;
- друга (фінальна) складова r_2 характеризує якість захисту курсантом курсового проекту.

Розмір шкали першої складової дорівнює 50 балів, а другої складової – 50 балів.

Рейтингова оцінка (RD) формуються як сума балів успішності підготовки матеріалів курсового проектування (стартовий рейтинг) r_1 та захисту курсового проекту (фінальний рейтинг) r_2 :

$$RD = r_1 + r_2.$$

1. Стартова складова (r_1) формується з наступних п’яті якостей:
– своєчасність виконання графіку роботи з курсового проектування (КП);
– сучасність та обґрунтування прийнятих рішень;
– правильність застосування методів аналізу і розрахунку;
– якість оформлення, виконання вимог нормативних документів;
– якість текстового та графічного матеріалу із дотриманням вимог ДСТУ .
Кожна якість оцінюється за чотирма оцінками – 0 (незадовільно), 3 (задовільно), 4 (добре), 5 (відмінно). Вага одної одиниці оцінки – 2 бали шкали *R*.

Критерії оцінювання	Оцінка
курсант своєчасно виконує графік КП, показав глибоке знання, що забезпечують повноту виконя завдань, правильно і акуратно оформив результати у вигляді текстового та графічного матеріалу, показав здатність вільно застосовувати свої знання в ході прийняття рішень.	5
курсант своєчасно виконує графік КП, показав рівень знань, що забезпечують повноту виконя завдань, правильно і акуратно оформив результати у вигляді текстового та графічного матеріалу, показав здатність вільно застосовувати свої знання в ході прийняття рішень, але була потрібна допомога викладача у вигляді поправок та додаткових питань.	4
курсант показав знання предмету, виконав завдання, оформив результати, але: - результати мають недоліки непринципового характеру; - знання предмету є правильними, але неповними; - матеріали результатів оформлені неохайно; - була потрібна допомога викладача у вигляді поправок та додаткових питань.	3
В інших випадках	0

2. Складова захисту курсового проекту (r_2):
– ступінь володіння матеріалом;
– повнота аналізу можливих варіантів;
– повнота та ступінь обґрунтування прийнятих рішень;
– рівень актуальності рішень;
– вміння захищати свою позицію;
Кожна якість оцінюється за чотирма оцінками – 0 (незадовільно), 3 (задовільно), 4 (добре), 5 (відмінно). Вага одної одиниці оцінки – 2 бали шкали *R*.

Критерії оцінювання	**Оцінка**
курсант показав високий рівень знань предмету, повно виконав завдання, правильно і акуратно оформив результати, показав здатність вільно застосовувати свої знання в ході захисту прийнятих рішень.	5
курсант показав високий рівень знань предмету, повно і чітко виконав завдання, правильно і акуратно оформив результати, показав здатність застосовувати свої знання в ході захисту прийнятих рішень, але була потрібна допомога викладача у вигляді поправок та додаткових питань.	4
курсант показав знання предмету, виконав завдання, оформив результати, але: - результати мають недоліки непринципового характеру; - знання предмету є правильними, але неповними; - матеріали результатів оформлені неохайно;	3

- була потрібна допомога викладача під час захисту КП у вигляді поправок та додаткових питань.	
В інших випадках	0

Сума балів двох складових переводиться до залікової оцінки згідно з таблицею:

Бали $RD=r_1+r_2$	Оцінка
95-100	відмінно
85-94	дуже добре
75-84	добре
65-74	задовільно
60-64	достатньо
Менше 60	незадовільно

Необхідні додаткові умови допуску до захисту КП:

- здана пояснювальна записка;
- виконані та письмово оформлені результати всіх завдань КП;
- наданий працездатний прототип бази даних організації.

При отриманні курсантом $r_1 < 40$ та невиконанні додаткової умови допуск до захисту КП забороняється.