НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних наук

«ЗАТВЕРДЖУЮ»
Декан факультету інформаційних технологій

_____ О. Г. Глазунова

«_____» _____ 20 ____ р.

РОЗГЛЯНУТО І СХВАЛЕНО

на засіданні кафедри комп'ютерних наук

Протокол № ___від «___» _____ 20__ р.
Завідувач кафедри
_____ Б. Л. Голуб

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРОФЕСІЙНА ПРАКТИКА ПРОГАМНОЇ ІНЖЕНЕРЕЇ

Спеціальність – 121 «Інженерія програмного забезпечення»

Факультет інформаційних технологій

Розробник: д.т.н., професор кафедри комп'ютерних наук, Хлапонін Ю.І.

Київ – 2019 р.

1. Опис навчальної дисципліни

_____Професійна практика програмної інженерії_____
(назва дисципліни)

Галузь знань, спеціальність, освітній ступінь	
Галузь знань	12 "Інформаційні технології"
Спеціальність	121 «Інженерія програмного забезпечення»
Освітній ступінь	"Бакалавр"
Характеристика навчальної дисципліни	
Вид	Обов’якова
Загальна кількість годин	120
Кількість кредитів ECTS	4
Кількість змістових модулів	3
Курсовий проект (робота) (якщо є в робочому навчальному плані)	
Форма контролю	Іспит
Показники навчальної дисципліни для денної та заочної форм навчання	
	денна форма навчання
Рік підготовки	3
Семестр	6
Лекційні заняття	12 год
Практичні, семінарські заняття	
Лабораторні заняття	24 год.
Самостійна робота	84 год.
Індивідуальні завдання	
Кількість тижневих годин для денної форми навчання: - аудиторних - самостійної роботи студента	4 год.

2. Мета та завдання навчальної дисципліни

Метою професійної практики програмної інженерії є ознайомлення з процесом проектування, розробки, тестування та експлуатації елементів інформаційних управляючих систем і технологій та власна участь студентів у цьому процесі.

Завдання:

- освоєння сучасних інструментальних засобів проектування та розробки інформаційних технологій;
- проектування та розробка елементів інформаційних технологій;
- тестування розроблених програмних модулів;
- підготовка елементів технічної проектної та експлуатаційної документації.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- структуру, організацію та виробничу діяльність установи або організації з профілю інформаційних технологій;
- плани науково – технічних досліджень, тематику задач та їх використання;
- обов'язки та коло задач, які розв'язує інженер – програміст і при цьому надавати допомогу базі практики в якості інженера – програміста;

вміти:

проектувати та розроблювати елементи комплексної системи захисту інформації в умовах підприємств профілю інформаційних технологій або в умовах реально діючих підприємств. Значне місце в індивідуальних завданнях на проектування та розробку елементів комплексної системи захисту інформації повинно надаватися використанню засобів системного аналізу предметної області.

3. Програма та структура навчальної дисципліни для:

– повного терміну денної (заочної) форми навчання;

– скороченого терміну денної (заочної) форми навчання.

Назви змістових модулів і тем	Кількість годин												
	денна форма							Заочна форма					
	тижні	усього	у тому числі					усього	у тому числі				
			л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13	14
Змістовий модуль 1. Загальні принципи побудови систем захисту.													
Тема 1. Загальні принципи побудови систем захисту.	1,2	8	4		4		12						
Тема 2. Аналіз середовища функціонування ІС.	3,4	8	4		4		12						
Тема 3. Аналіз складу аппаратного та программного забезпечення.	5,6	8	4		4		12						
Разом за змістовим модулем 1	24		12		12		36						
Змістовий модуль 2. Назва													
Тема 1. Аналіз обчислювальної мережі. Акт обстеження середовища функціонування ІС.	7,8	8	4		4		12						
Тема 2. Аналіз підходів до формування моделей загроз та порушника.	9,10	8	4		4		12						
Тема 3. Основні складові політики безпеки. Види політик безпеки та підходи до її формування.	11,12	8	4		4		12						
Разом за змістовим модулем 2	24		12		12		36						

Усього годин												
Курсовий проект (робота) з _____ _____ _____ (якщо є в робочому навчальному плані)		-	-	-		-		-	-	-		-
Усього годин		24		24		72						

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Не передбачено	
2		
...		

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Не передбачено	
2		

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Аналіз середовища функціонування ІС. Розробка акту обстеження на прикладі ІС НУБіП.	8
2	Аналіз підходів до формування моделей загроз та порушника. Розробка моделі загроз для інформації та моделі порушника на прикладі реальної ІС.	8
3	Основні складові політики безпеки. Розробка політики безпеки на прикладі реального підприємства та ІС.	8

7. Контрольні питання, комплекти тестів для визначення рівня засвоєння знань студентами.

1. Поняття інформаційної системи, її призначення.
2. Завдання і функції ІС. Класифікація ІС. Корпоративні ІС. Еволюція корпоративних інформаційних систем. Стандарти корпоративних ІС.
3. Особливості сучасних інформаційних систем як об’єкту захисту.\
4. Основні загрози безпеці інформації в інформаційних системах.
5. Поняття захищених інформаційних систем. Забезпечення захисту інформації в захищених інформаційних системах.
6. Побудова систем захисту даних.
7. Основні підсистеми систем захисту даних
8. Поняття життєвого циклу системи.

9. Базові стадії та етапи життєвого циклу інформаційних систем та систем захисту.
10. Моделі життєвого циклу систем. Каскадна модель. Каскадно - зворотня модель. Спіральна модель.
11. **RUP** – методологія реалізації етапів ЖЦ захищених систем.
12. Загальні принципи побудови систем захисту.
13. Вихідні дані для проектування систем захисту.
14. Сутність створення систем захисту.
15. Аналіз середовища функціонування ІС.
16. Аналіз складу аппаратного та программного забезпечення.
17. Аналіз обчислювальної мережі.
18. Аналіз технології та процесів реалізації функцій ІС.
19. Аналіз підходів до формування моделей загроз та порушника.
20. Засоби аналізу захищеності
21. Створення анкет для оцінки складу загроз та аналізу ризиків.
22. Підходи для оцінки витрат на розробку систем захисту.
23. Основні складові політики безпеки.
24. Види політик безпеки та підходи до її формування.
25. Формування базових положень політики безпеки.
26. Оцінка ефективності систем захисту.
27. Загальна методологія оцінювання.
28. Міжнародний стандарт ISO/IEC 15408.

8. Методи навчання.

При проходженні професійної практики програмної інженерії використовуються словесний, інформаційно-ілюстративний, наочний та практичний, проблемний та пошуковий методи навчання із застосуванням лекцій, задач, ситуаційних завдань, моделювання конкретних ситуацій, комплексних розрахункових завдань, реферативних оглядів, провокаційних вправ і запитань, ділових ігор, мозкових атак.

9. Форми контролю.

Контрольні заходи передбачають проведення вхідного (за необхідності), поточного, модульного та семестрового контролю. Вхідний, поточний, модульний контроль здійснюється під час проведення лабораторних та індивідуальних занять з викладачем. Семестровий контроль виконується за окремим графіком, складеним деканатом факультету.

10. **Розподіл балів, які отримують студенти.** Оцінювання студента відбувається згідно положенням «Про екзамени та заліки у НУБіП України» від 27.02.2019р. протокол №7

Оцінка національна	Рейтинг здобувача вищої освіти, бали
Відмінно	**90-100**
Добре	**74-89**
Задовільно	**60-73**
Незадовільно	**0-59**

Для визначення рейтингу студента (слухача) із засвоєння дисципліни $\mathbf{R_{ДИС}}$ (до 100 балів) одержаний рейтинг з атестації (до 30 балів) додається до рейтингу студента (слухача) з навчальної роботи $\mathbf{R_{НР}}$ (до 70 балів): $\mathbf{R_{ДИС} = R_{НР} + R_{АТ}}$.

11. Методичне забезпечення
Рекомендована література

1. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення від 01.07.1997.
2. Державний стандарт України ДСТУ 3396.1 -96. Захист інформації. Технічний захист інформації. Порядок проведення робіт від 01.07.1997.
3. Державний стандарт України ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. від 01.07.1997.
4. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.99р. № 22.
5. НД ТЗІ 1.1-005-07 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення.

6. НД ТЗІ 2.1-002-07. Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення.
7. НД ТЗІ 3.1-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи.
8. НД ТЗІ 3.3-001-07. Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.
9. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі від 08.11.2005 р. №125.
10. НД ТЗІ 2.2-005-08 Технічний захист інформації. Захист інформації, яку обробляють засобами електронної обчислювальної техніки на об’єктах інформаційної діяльності, від витоку інформації за рахунок побічних електромагнітних випромінювань і наводів. Норми ефективності захисту.
11. НД ТЗІ 2.2-006-08 Захист інформації на об’єкті інформаційної діяльності. Норми протидії технічній розвідці в акустичному і віброакустичному каналах витоку інформації.
12. НД ТЗІ 2.4-001-06 Протидія технічним розвідкам. Рекомендації з протидії засобам радіотехнічної розвідки.
13. НД ТЗІ 2.4-002-06 Протидія технічним розвідкам. Рекомендації із захисту параметрів лазерного випромінювання від оптико-електронної розвідки.
14. НД ТЗІ 2.7-008-08 Захист інформації на об’єктах інформаційної діяльності. Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами. Методичні вказівки.
3.1.1. НД ТЗІ 4.7-002-2001 Визначення захищеності мовної інформації від витоку акустичним і віброакустичним каналами. Методичні вказівки. Затверджено наказом ДСТСЗІ СБ України від 21.12.2001 р. № 012. Чинний з 01.01.2002 р.

Додаткові рекомендовані джерела

3.1.19. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. 608 с.

3.1.20. Юдін О.К., Корченко О.Г., Конахович В.Г. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ НВП “ІНТЕРСЕРВІС”, 2009. 716 с.

13. Інформаційні ресурси

http://www.dsszzi.gov.ua/dsszzi/control/uk/index