НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних наук

«ЗАТВЕРДЖУЮ»
декан факультету інформаційних технологій
_____ Глазунова О.Г.
«25» ____05____ 2022 р.

«СХВАЛЕНО»
на засіданні кафедри комп'ютерних наук
Протокол № ____ від «___» _____ 20____ р.
Завідувач кафедри
_____ Б. Л. Голуб

«РОЗГЛЯНУТО»
Гарант ОП 121 «Інженерія програмного забезпечення»
гарант ОП
_____ Лялецький О.В.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Інженерія програмного забезпечення»

за спеціальністю 121 «Інженерія програмного забезпечення»

галузі знань **12 «Інформаційні технології»**

Факультет інформаційних технологій

Розробники: доцент кафедри комп'ютерних наук , к.т.н. Сватко В.В.

Київ 2022

1. Опис навчальної дисципліни

Безпека програм та даних

(назва дисципліни)

Галузь знань, спеціальність, освітній ступінь	
Галузь знань	12 «Інформаційні технології»
Спеціальність	121 – «Інженерія програмного забезпечення»
Освітня програма	«Інженерія програмного забезпечення»
Освітній ступінь	Бакалавр
Характеристика навчальної дисципліни	
Вид	Обов’язкова
Загальна кількість годин	120
Кількість кредитів ECTS	4
Кількість змістових модулів	2
Курсовий проект (робота) (за наявності)	
Форма контролю	*Екзамен*
Показники навчальної дисципліни для денної та заочної форм навчання	
	денна форма навчання
Рік підготовки (курс)	4
Семестр	7
Лекційні заняття	*15 год.*
Практичні, семінарські заняття	
Лабораторні заняття	*30 год.*
Самостійна робота	*75 год.*
Індивідуальні завдання	
Кількість тижневих аудиторних годин для денної форми навчання	*3 год.*

2. Мета та завдання навчальної дисципліни

Метою вивчення дисципліни є засвоєння студентами практичних основ, принципів побудови, класифікації засобів технічного забезпечення автоматизованої обробки інформації.

Завдання:

- засвоєння структури нормативно-правової бази, яка регламентує використання технічних засобів забезпечення автоматизованої обробки інформації;
- засвоєння принципів побудови комплексів засобів захисту (КЗЗ) інформації від несанкціонованого доступу;
- засвоєння принципів функціонування засобів захисту інформації;
- засвоєння порядку застосування КЗЗ при побудові КСЗІ .

У результаті вивчення навчальної дисципліни студент повинен

знати:

- структуру нормативно-правової бази, яка регламентує використання технічних засобів забезпечення автоматизованої обробки інформації;
- принципи побудови комплексів засобів захисту (КЗЗ) інформації від несанкціонованого доступу
- принципи функціонування засобів захисту інформації та порядок їх застосування при побудові КСЗІ.

вміти:

- обирати нормативні документи, які регламентують використання технічних засобів забезпечення автоматизованої обробки інформації, встановлювати програмне забезпечення КЗЗ на комп'ютер, проводити налаштування КЗЗ.

3. Програма та структура навчальної дисципліни для:

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. Комплекси засобів захисту інформації для АС класу 1													
Тема 1. Вимоги законодавства України та нормативно-правових документів системи ТЗІ, які регламентують використання засобів технічного забезпечення автоматизованої обробки інформації.	1,2	4	1		2		7						

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
Тема 2. Комплекс засобів захисту «Лоза-1». Порядок роботи системи. Користувачі системи. Обєкти доступу. Правила розмежування доступу. Перевірка цілісності програмного забезпечення. Реєстрація подій.	3,4,5	6	2		4		12						
Тема 3. Комплекс засобів захисту «Гриф-ХР». Функції комплекса. Функціональний профіль захищеності інформації та гарантії. Політика послуг безпеки, які реалізує КЗЗ. Розмежування повноважень користувачів.	6,7,8	6	2		4		10						
Тема 4. Комплекс засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу 1 «Рубіж-РСО». Структура КЗЗ «Рубіж-РСО». Використання КЗЗ “Рубіж-РСО” для обробки інформації з обмеженим доступом.	9,10	6	2		4		10						
Разом за змістовим модулем 1	60		7		14		39						

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 2. Комплекси засобів захисту інформації для АС класу 2													
Тема 1. Комплекс засобів захисту «Лоза-2». Порядок роботи системи. Сервер та робочі станції. Правила розмежування доступу. Забезпечення цілісності програмного забезпечення. Реєстрація подій.	11,12	6	2		4		12						
Тема 2. Комплекс засобів захисту «Гриф-Мережа». Склад та архітектура комплексу. Функціональний профіль захищеності інформації та гарантії. Політика послуг безпеки, які реалізує КЗЗ.	13	6	2		4		12						
Тема 3. Комплекс програмних засобів реалізації інфраструктури відкритих ключів «Тайфун-РКІ». Призначення, склад та функції комплексу. Порядок управління сертифікатами відкритих ключів.	14	6	2		4		12						
Тема 4. Система «Захищена електронна пошта» «Бриз». Призначення, склад та функції системи.	15	6	2		4		12						
Разом за змістовим модулем 2	60		8		16		36						

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
Усього годин	120		15		30		75						
Курсовий проект (робота) з _____ _____ (якщо є в робочому навчальному плані)			-	-	-		-		-	-	-		-
Усього годин	120		15		30		75						

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.	Налаштування комплексу засобів захисту «Лоза-1». Порядок роботи системи. Користувачі системи. Обєкти доступу. Правила розмежування доступу. Перевірка цілісності програмного забезпечення. Реєстрація подій.	2
2.	Налаштування комплексу засобів захисту «Гриф-ХР». Функції комплекса. Функціональний профіль захищеності інформації та гарантії. Політика послуг безпеки, які реалізує КЗЗ. Розмежування повноважень користувачів.	4
3.	Налаштування комплексу засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу 1 «Рубіж-РСО». Структура КЗЗ «Рубіж-РСО». Використання КЗЗ “Рубіж-РСО” для обробки інформації з обмеженим доступом.	2
4.	Налаштування комплексу засобів захисту «Лоза-2». Порядок роботи системи. Сервер та робочі станції. Правила розмежування доступу. Забезпечення цілісності програмного забезпечення. Реєстрація подій.	2
5.	Налаштування комплексу засобів захисту «Гриф-Мережа». Склад та архітектура комплексу. Функціональний профіль захищеності інформації та гарантії. Політика послуг безпеки, які реалізує КЗЗ.	6
6.	Налаштування системи «Захищена електронна пошта» «Бриз». Призначення, склад та функції системи.	4

7.	Налаштування комплексу програмних засобів реалізації інфраструктури відкритих ключів «Тайфун-РКІ». Призначення, склад та функції комплексу. Порядок управління сертифікатами відкритих ключів.	2
8.	Комплексні засоби захисту інформації від несанкціонованого доступу. Інсталяція КЗЗ “Гриф V.3”	8
	Разом	***30***

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. Розрахунок звукоізоляції приміщень та вибір заходів щодо її підвищення
9. Вимірювання шуму та вібрацій на об’єкті інформаційної діяльності.
10. Система контролю доступу на основі аналізу геометрії обличчя
11. Аналіз існуючих систем захисту інформації від НСД
12. Засоби оброблення інформації, які за принципом дії не створюють технічні канали витоку
13. Лабораторна робота “Порядок налаштування системи “Гриф-ХР”
14. Лабораторна робота “Обробка інформації в системі “Гриф-ХР”
15. Архітектура і технології сучасних систем контролю доступу.
16. Технології радіочастотної ідентифікації (RFID) у різних сферах застосування.
17. Безпека об’єктів критичної інфраструктури.
18. Системи пожежної сигналізації, оповіщення та управління евакуацією людей.
19. Можливості відеоаналітики в системах охорони об’єктів.
20. Ситуаційні центри управління та контролю служб оперативного реагування.
21. “Хмарна” відеоаналітика.
22. Відеоаналітичні системи для безпечного міста.
23. Програмно-апаратні засоби забезпечення безпеки в місцях великого скупчення людей.
24. Програмно-апаратні засоби забезпечення безпеки на обєктах транпортної інфраструктури.
25. Архітектура VSAAS рішень .
26. Використання нейронних мереж в галузі відеоаналітики

27.IP-відеонагляд.
28.Аналіз середовища функціонування ІС.
29.Аналіз складу аппаратного та программного забезпечення.
30.Аналіз обчислювальної мережі.
31.Аналіз технології та процесів реалізації функцій ІС.
32.Аналіз підходів до формування моделей загроз та порушника.
33.Засоби аналізу захищеності
34.Основні складові політики безпеки.
35.Види політик безпеки та підходи до її формування.
36.Формування базових положень політики безпеки.
37.Оцінка ефективності систем захисту.
38.Загальна методологія оцінювання.
39.Міжнародний стандарт ISO/IEC 15408.

8. Методи навчання.

При викладанні навчальної дисципліни 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 20.02.2015 р. протокол № 6 з табл. 1.

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	екзаменів	**заліків**
90-100	відмінно	зараховано
74-89	добре	
60-73	задовільно	
0-59	незадовільно	не зараховано

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.
15. 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

1. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. 608 с.
2. Юдін О.К., Корченко О.Г., Конахович В.Г. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ НВП “ІНТЕРСЕРВІС”, 2009. 716 с.
3. «Гриф – Мережа» Комплекс средств защиты информации с ограниченным доступом в локальних вычислительных сетях от несанкционированного доступа. *версия 2.01*. Описание комплекса. *редакция 2*. Киев.
4. Комплекс программных средств реализации инфраструктуры открытых ключей «Тайфун-PKI». *Версия 1.01* Руководство по установке и эксплуатации

13. Інформаційні ресурси

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