НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних наук

«ЗАТВЕРДЖУЮ»
Декан факультету інформаційних технологій
_____ О. Г. Глазунова
«_____» _____ 20 ____ р.

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

«РОЗГЛЯНУТО»
Гарант ОП «Інженерія програмного забезпечення»
_____доцент, к.ф.-м.н. Лялецький О.В.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

Спеціальність – 121 «Інженерія програмного забезпечення»

Освітня програма – «Інженерія програмного забезпечення»

Факультет інформаційних технологій

Розробник: д.т.н., професор кафедри комп'ютерних наук Семко В.В.

Київ 2021

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 (НСД);
- засвоєння принципів функціонування засобів захисту інформації;
- засвоєння порядку застосування КЗЗ при побудові комплексних систем захисту інформації КСЗІ.

У результаті вивчення навчальної дисципліни студент повинен

знати:

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

вміти:

- обирати нормативні документи системи технічного захисту інформації (ТЗІ), які регламентують функціональні вимоги політики безпеки інформації щодо захисту ресурсів інформаційних (ІС) і інформаційно-комунікаційних систем (ІКС) та об'єктів інформаційної діяльності (ОІД) від НСД;
- використовувати технічні засоби захисту інформації від НСД в системах автоматизованої обробки інформації;
- використовувати програмні засоби захисту інформації при реалізації політики безпеки інформації в ІС, ІКС при створенні КЗЗ ОІД.

Загальні компетентності (ЗК)

К05. Здатність вчитися і оволодівати сучасними знаннями.

Фахові компетентності спеціальності (ФК)

К17. Здатність дотримуватися специфікацій, стандартів, правил і рекомендацій в професійній галузі при реалізації процесів життєвого циклу.

К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).

К23. Здатність реалізовувати фази та ітерації життєвого циклу програмних систем та інформаційних технологій на основі відповідних моделей і підходів розробки програмного забезпечення.

К25. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення, враховуючи специфіку природоохоронної галузі та сільського господарства.

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. Класифікація засобів захисту інформації.	1, 2	2	2		4		6						
Тема 2. Класифікація засобів захисту інформації.	3, 4	2	2		4		2						
Тема 3. Визначення і абстрактні моделі управління безпекою в інформаційних системах.	5, 6	2	2		4		2						
Тема 4. Моделі управління безпекою в інформаційних системах.	7, 8	2	2		4		2						
Разом за змістовим модулем 1	60		8		16		39						
Змістовий модуль 2. Комплекси засобів захисту інформації для АС класу 2													
Тема 1. Принципи функціонування програмних систем криптографічних перетворень інформації. Основні алгоритми.	9, 10	2	2		4		12						
Тема 2. Методи захисту програм і даних в системах електронної взаємодії.	11, 12	2	2		4		12						
Тема 3. Методи захисту програм і даних в системах обміну голосовими повідомленнями.	13, 14	2	2		4		12						
Тема 4. Методи захисту програм і даних в системах	15	1	2		2		12						

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
захищеного обміну повідомленнями електронної пошти.													
Разом за змістовим модулем 2	60		7		14		36						
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	

6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Введення класифікації автоматизованих систем і стандартних функціональних профілів захищеності.	4
2.	Дослідження програмного засобу захисту інформації “Лоза-1”.	4
3.	Використання концепції ієрархічної декомпозиції при побудові систем захисту.	4
4.	Дослідження функціонування злоякісного програмного коду (комп’ютерного вірусу в обчислювальному середовищі під управлінням операційної системи Windows.	4
5.	Організаційні засади забезпечення безпеки мережевої інфраструктури.	4
6.	Дослідження технології криптографічного захисту інформації в системах електронної взаємодії.	4
7.	Дослідження технології захисту від несанкціонованого доступу в системах обміну голосовими повідомленнями.	4
8.	Дослідження технології захисту від несанкціонованого доступу в системах обміну повідомленнями електронної пошти..	2
	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. Вимірювання шуму та вібрацій на об'єкті інформаційної діяльності.
9. Аналіз існуючих систем захисту інформації від НСД
10. Засоби оброблення інформації, які за принципом дії не створюють технічні канали витоку
11. Архітектура і технології сучасних систем контролю доступу.
12. Безпека об'єктів критичної інфраструктури.
13. Ситуаційні центри управління та контролю служб оперативного реагування.
14. Програмно-апаратні засоби забезпечення безпеки на обєктах мережевої інфраструктури.
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. Основні складові політики безпеки.
22. Види політик безпеки та підходи до її формування.
23. Формування базових положень політики безпеки.
24. Оцінка ефективності систем захисту.
25. Загальна методологія оцінювання.
26. 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. Богуш В.М., Давидьков О.А. Теоретичні основи захищених інформаційних технологій. – К.: ДУІКТ, 2010. – 414 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности ынформационных систем. – М.: Горячая линия, Телеком, 2000. – 452 с.
3. Шарыгин В.Ф. Информационная безопасность компьютерных систем и сетей учебное пособие. – М.: ИД “Форум”, 2011. – 416с.
4. Мамченко С.М. Комплексні системи захисту інформації: Навч. посіб. / С.М. Мамченко, В.Д. Козюра, В.Д. Бровко. – Київ: Нац. Акад. СБУ, 2018. – 372 с.
5. Довгань О.Д. Методологія захисту інформації: навч.-метод. посіб. / О.Д.Довгань, Г.М.Гулак, А.К.Гринь, С.В.Мельник. – К.: Наук.-вид. центр НА СБ України, 2012. – 184 с.
6. Ленков С.В. Методы и средства защиты информации / Ленков С.В., Перегудов Д.А., Хорошко В.А., / под. ред. В.А. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность, – 344 с.
7. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. 608 с.
8. Юдін О.К., Корченко О.Г., Конахович В.Г. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ НВП “ІНТЕРСЕРВІС”, 2009. 716 с.

Додаткові рекомендовані джерела

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.
16. 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 р. № 22 із змінами згідно наказу Адміністрації Держспецзв’язку від 28.12.2012 №806.

17. 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 р. № 22.
18. ГОСТ 34.601-90. Информационные технологии. Комплекс стандартов на автоматизированные систеиы. Автоматизированные системы стадии создания.
19. РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.
20. ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення".
21. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT) "Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри".
22. ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования".
23. ДСТУ ISO/IEC 10116:2019 (ISO/IEC 10116:2017, IDT) "Інформаційні технології. Методи захисту. Режими роботи n-бітних блокових шифрів".
24. ДСТУ 8845:2019 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення".
25. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, ЮТ) "Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 4. Потокові шифри".
26. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння".
27. ДСТУ ISO/IEC 9796-2:2015 (ISO/IEC 9796-2:2010, IDT) "Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел".
28. ДСТУ ISO/IEC 9796-3:2015 (ISO/IEC9796-3:2006, IDT) "Інформаційні технології. Методи захисту. Схеми цифрового підпису, які забезпечують відновлення повідомлення. Частина 3. Механізми, що ґрунтуються на дискретному логарифмі".
29. ДСТУ ISO/IEC 14888-2:2015 (ISO/IEC 14888-2:2008, IDT) "Інформаційні технології. Методи захисту, Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел".
30. ДСТУ ISO/IEC 14888-3:2019 (ISO/IEC 14888-3:2018, IDT) "Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 3. Механізми, що ґрунтуються на дискретному логарифмуванні".
31. ДСТУ ISO/IEC 15946-5:2019 (ISO/IEC 15946-5:2017) "Інформаційні технології. Методи захисту. Криптографічні методи на основі еліптичних кривих. Частина 5. Генерування еліптичних кривих".
32. ДСТУ ISO/IEC 18033-2:2015 (ISO/IEC 18033-2:2006, IDT) "Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 2. Асиметричні шифри".

33. ДСТУ ISO/IEC 9797-2:2015 (ISO/IEC 9797-2:2011, ЮТ) "Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми що використовують спеціалізовану геш-функцію".
34. ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція ґешування".
35. ДСТУ ISO/IEC 10118-2:2015 (ISO/IEC 10118-2:2010; Cor 1:2011, IDT) "Інформаційні технології. Методи захисту. Геш-функції. Частина 2. Геш~ функції j що використовують n-бітний блоковий шифр".
36. ДСТУ ISO/IEC 10118-3:2005 (ISO/IEC 10118-3:2004; Cor 1:2011, IDT) "Інформаційні технології. Методи захисту. Геш-функції. Частина 3. Спеціалізовані геш-функції".
37. ДСТУ ISO/IEC 10118-4:2015 (ISO/IEC 10118-4:1998; Cor 1:2014; Amd 1:2014, IDT) "Інформаційні технології. Методи захисту. Геш-функції.
38. ГОСТ 34.311-95 "Информационная технология. Криптографическая защита информации. Функция хэширования".
39. ДСТУ ISO/IEC 9798-2:2015 **(ISO/IEC** 9798-2:2008; Cor 3:2013, IDT) "Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 2. Механізми, що використовують симетричні алгоритми шифрування".
40. ДСТУ ISO/IEC 9798-3:2002 (ISO/IEC 9798-3:1998; Cor 1:2009; Cor 2:2012) "Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з використанням методу цифрового підпису".
41. ДСТУ ISO/IEC 9798-4:2015 (ISO/IEC 9798-4:1999; Cor 1:2009; Cor 2:2012, IDT) "Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 4. Методи, що використовують криптографічну перевірочну функцію".
42. ДСТУ ISO/IEC 9798-5:2015 (ISO/IEC 9798-5:2009, IDT) "Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 5. Механізми, що використовують методи нульової обізнаності".
43. ДСТУ ISO/IEC 9798-6:2015 (ISO/IEC 9798-6:2010, IDT) "Інформаційні технології. Методи захисту. Автентифікація об'єктів. Частина 6. Механізми, що використовують ручне передавання даних".
44. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів".
45. ДСТУ ISO/IEC 11770-3:2015 (ISOAEC 11770-3:2008; Cor 1:2009, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів".
46. ДСТУ ISO/IEC 11770-4:2015 (ISO/IEC 11770-4:2008; Cor 1:2009, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 4. Механізми , засновані на нестійких секретах".
47. ДСТУ ISO/IEC 11770-5:2015 (ISO/IEC 11770-5:2008, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 5. Керування груповими ключами".
48. ДСТУ ISO/IEC 18031:2015 (ISO/IEC 18031:2011; Cor 1:2014, IDT) "Інформаційні технології. Методи захисту. Генерування випадкових бітів".

49. ДСТУISO/IEC 20543 "Інформаційні технології. Методи захисту. Методи тестування та аналізу для генерування випадкових бітів".
50. ДСТУ ISO/IEC 11770-2:2015 (ISO/IEC 11770-2:2008; Cor 1:2009, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів".
51. ДСТУ ISO/IEC 11770-3:2015 (ISO/IEC 11770-3:2008; Cor 1:2009, IDT) "Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми з використанням асиметричних методів",
52. ДСТУ ISO/IEC 20085-1 "Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом'якшення неінвазійних атак на криптографічні модулі. Частина 1. Методи та засоби тестування".
53. ДСТУ ISO/IEC 20085-2 "Методи захисту ІТ. Вимоги до засобів тестування та методів калібрування засобів тестування для застосування у методах тестування пом'якшення неінвазійних атак на криптографічні модулі. Частина 2. Методи та прилади тестового калібрування".

12. Інформаційні ресурси

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