НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

Кафедра комп'ютерних систем, мереж та кібербезпеки

"ЗАТВЕРДЖУЮ"
Декан факультету інформаційних технологій
_____ проф. О.Г.Глазунова
_____ 2023 р.

СХВАЛЕНО
на засіданні кафедри
комп'ютерних систем,
мереж та кібербезпеки
Протокол №10 від «17» травня» 2023р.
Завідувач кафедри
_____ (доц. Касаткін Д.Ю.)

РОЗГЛЯНУТО
Гарант ОП «Комп'ютерна інженерія»
_____ (Нікітенко Є.В.)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ»

Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»
Факультет інформаційних технологій
Розробник: Лахно В.А., професор, д.т.н., професор

Київ – 2023

Опис навчальної дисципліни

Захист інформації в комп'ютерних системах

(назва)

Галузь знань, напрям підготовки, спеціальність, освітньо-кваліфікаційний рівень		
Галузь знань	Інформаційні технології	
Спеціальність	123 – «Комп’ютерна інженерія»	
другий (магістерський) рівень	Бакалавр	
Характеристика навчальної дисципліни		
Вид	Обов’язкова	
Загальна кількість годин	120	
Кількість кредитів ECTS	4	
Кількість змістових модулів	2	
Курсовий проект (робота) (якщо є в робочому навчальному плані)	-	
Форма контролю	Іспит	
Показники навчальної дисципліни для денної та заочної форм навчання		
	денна форма навчання	заочна форма навчання
Рік підготовки	2022-2023	
Семестр	8	
Лекційні заняття	48 год.	
Практичні, семінарські заняття		
Лабораторні заняття	48 год.	
Самостійна робота	24 год.	
Індивідуальні завдання		
Кількість тижневих годин для денної форми навчання: аудиторних	8 год.	

1. Мета та завдання навчальної дисципліни

Мета - є вивчення теоретичних основ проблеми зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення конфіденційної інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності (окрема на підприємствах АПК), способів захисту від несанкціонованого доступу до інформації. Вивчення методологічних, організаційних та наукових основ розробки засобів і систем збору та захисту інформації (ЗІ), забезпечення інформаційної безпеки процесів опрацювання, зберігання та поширення інформації в інформаційно-комунікаційних мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем і засобів здійснення погроз з боку потенційних порушників.

Завдання навчальної дисципліни «Захист інформації в комп'ютерних системах» - є теоретична та практична підготовка здобувачів до розробки та застосування сучасних програмно-апаратних систем захисту інформації в різних установах та на підприємствах, зокрема АПК.

Місце і роль дисципліни в системі підготовки фахівців відповідно до навчального плану. Дана навчальна дисципліна є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області захисту інформації управляючих систем в різних галузях, а також сприяє захисту кваліфікаційної роботи зі спеціальності 123 «Комп’ютерна інженерія» для першого (бакалаврського) рівня вищої освіти.

Вимоги щодо знань і вмінь, набутих внаслідок вивчення дисципліни

Внаслідок вивчення дисципліни студенти повинні:

знати законодавчу та нормативно-правову базу України в галузі інформаційної та /або кібербезпеки; міжнародні стандарти в галузі інформаційної та /або кібербезпеки; моделі загроз та моделі порушника; інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці; основи теорії інформації й сучасних захищених інформаційних технологій; сучасні методи обробки, перетворення та захисту інформації в комп'ютерних системах; теоретичні основи криптології та криптоаналізу; основні принципи, методи й алгоритми експлуатації програмних систем збору, закриття, відновлення і автентифікації інформації; сучасні способи боротьби з несанкціонованим блокуванням, копіюванням, зміною та збором інформації; програмні засоби забезпечення інформаційної безпеки; сучасні уявлення про призначення, структуру та принципи побудови захищених інформаційних і комунікаційних систем; методи та моделі захисту інформації.

вміти практично вирішувати завдання захисту програм та даних ІКС програмно-апаратними засобами та давати оцінку якості прийнятих рішень; практично вирішувати завдання захисту в операційних системах та давати оцінку якості прийнятих рішень; реалізовувати системи захисту інформації в ІКС відповідно до стандартів з оцінки захищених систем; реалізовувати захист інформації в системах передачі даних та системах зв'язку; користуватися науковою та довідковою літературою за напрямком дисципліни.

Набуття компетентностей:

Відповідно до освітньої програми підготовки фахівців за спеціальністю 123 «Комп'ютерна інженерія» навчальна дисципліна забезпечує формування загальних і фахових компетентностей:

Загальні компетентності:

ЗК1. Здатність до абстрактного і системного мислення, аналізу та синтезу.

ЗК2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК3. Здатність застосовувати знання у практичних ситуаціях.

ЗК6. Навички міжособистісної взаємодії.

Фахові компетентності:

СК4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

СК5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

СК13. Здатність вирішувати проблеми у галузі комп'ютерних та інформаційних технологій, визначати обмеження цих технологій.

СК10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

СК14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

В результаті вивчення навчальної дисципліни студент набуде певні програмні результати, а саме

ПРН1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

ПРН2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.

ПРН7. Вміти застосовувати знання для розв'язування задач аналізу та синтезу засобів, характерних для спеціальності.

ПРН13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

ПРН15. Вміти виконувати експериментальні дослідження за професійною

тематикою.

ПРН16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

ПРН21. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

В контексті зазначених вище компетентностей та програмних результатів навчання задачі викладання дисципліни визначають необхідний комплекс знань і вмінь, що отримують студенти під час вивчення дисципліни.

Навчальна програма розрахована на здобувачів вищої освіти, які навчаються за освітньою програмою підготовки бакалаврів за спеціальністю 123 «Комп'ютерна інженерія».

Робоча програма побудована за вимогами кредитно-модульної системи організації навчального процесу у закладах вищої освіти і використанням академічної системи оцінювання досягнень студентів та шкали оцінок Європейської кредитно-трансферної системи (ECTS).

Навчальна програма з курсу «Захист інформації в комп'ютерних системах» є основним документом, що охоплює всі види навчальної роботи при вивченні курсу студентами та відбиває основні методичні настанови кафедри.

Навчальна програма характеризує шляхи перетворення інформації, що одержується студентом впродовж вивчання курсу, і відбиває зміст курсу, розподілення його на розділи та їх обсяги, дані про форми вивчення та контролю знань.

Теоретичною базою для вивчення курсу «Захист інформації в комп'ютерних системах» є курси «Комп'ютерні системи»; «Комп'ютерні мережі».

2. Програма навчальної дисципліни

Змістовий модуль №1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки. Основні поняття політики інформаційної безпеки та захисту інформації.

Тема лекційного заняття 1. Властивості інформації з точки зору проблематики її захисту.

Криза забезпечення безпеки інформації в сучасних інформаційно- телекомунікаційних системах (ІТКС). Проблеми теорії захисту інформації. Властивості інформації з точки зору ЗІ. Мова, об'єкти, суб'єкти. Ієрархічний метод. Інформаційні потоки на підприємствах АПК.

Тема лекційного заняття 2. Ризики порушення політики інформаційної безпеки об'єкту інформатизації.

Цінність інформації. Використання поняття ризику. Моделювання доступу в ІТКС, зокрема на прикладах підприємств АПК.

Тема лекційного заняття 3. Вимоги щодо безпеки системи, ризики безпеки.

Основні поняття та визначення безпеки в ІКС. Роль захисту інформації в ІКС, умови функціонування підсистеми безпеки в комп'ютерних мережах та системах. Вимоги щодо безпеки системи, ризики безпеки. Послуги безпеки: конфіденційність, цілісність, автентичність, причетність, спостереженість.

Тема лекційного заняття 4. Механізми реалізації послуг безпеки.

Механізми і політики розмежування прав доступу в ІКС. Засоби забезпечення захисту інформації в ІКС. Засоби ідентифікації й автентифікації об'єктів баз даних, управління

доступом. Засобу контролю цілісності інформації, організація аудиту. Скасування прав доступу. Видача прав доступу до об’єктів ІКС.

Тема лекційного заняття 5. Поняття загрози інформації.

Поняття загрози інформації. Види загроз ІБ, на прикладах ОБІ (зокрема підприємств АПК). Дестабілізуючі факторі. Модель загроз для середовищ опрацювання інформації. Узагальнений підхід щодо побудови моделі загроз. Аналітичні моделі загроз. Емпіричні моделі загроз.

Тема лекційного заняття 6. Політика інформаційної безпеки.

Поняття політики інформаційної безпеки (ІБ). Основна теорема ІБ. Дискреційна політика безпеки. Мандатна політика безпеки. Рольова політика безпеки. Монітор безпеки. Доказовий підхід.

Тема лекційного заняття 7. Аналіз моделей безпеки ІКС.

Модель Белла-Лападула. Приклади використання.

Тема лекційного заняття 8. Загальні моделі ІБ.

Модель процесу захисту. Модель системи захисту. Модель функцій захисту. Модель з повним перекриттям. Інформаційно-аналітична модель з оцінки захисту інформації від загроз НСД. Модель виявлення порушень. Вартісна модель. Модель функціонального профілю. Об'єктно-концептуальна модель обчислювальної системи і РПЗ. Модель взаємодії об'єктів обчислювальної системи з погляду безпеки.

Тема лекційного заняття 9. Аналіз безпеки програмного забезпечення.

Задача аналізу безпеки ПЗ. Методи аналізу безпеки ПЗ. Нелегітимне використання ресурсів. Нелегітимний доступ до даних. Нелегітимний запуск програм. Нелегітимне виконання програм. Нелегітимна відмова в обслуговування (порушення доступності).

Тема лекційного заняття 10. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

Організаційно-технічні заходи відновлення функціонування ІКС. Журнал аудиту подій.

Тема лекційного заняття 11. Політики резервного копіювання даних.

Тема лекційного заняття 12. Механізми безпеки комп'ютерних мереж.

Віртуальні приватні мережі (VPN). Протоколи автентифікації RADIUS. Протоколи SSL/TLS.

Змістовий модуль № 2. Моделювання та аналіз безпеки об’єктів захисту інформації.

Тема лекційного заняття 13. Модель архітектури безпеки інформаційно-телекомунікаційних систем.

Модель архітектури безпеки сучасних ІТКС. Тенденції систем захисту розвитку ІТКС. Канали витоку інформації в ІКС та мережах. Класифікація засобів технічного захисту інформації в каналах загального користування.

Тема лекційного заняття 14. Методи захисту інформації в ІТКС.

Методи захисту інформації в ІТКС. Категорії уразливостей ІТКС. Мережеві уразливості і загрози для інформаційного та програмного продукту. Класи атак. Рівень антивірусного захисту шлюзів. Захист шлюзів. Можливі схеми захисту. Міжмережеві екрани. Керовані комутатори. Мережеві фільтри. Шлюзи сеансового рівня. Інспектори стану. Міжмережеві екрани прикладного рівня. Міжмережеві екрани з пакетною

фільтрацією. Криптографічний захист інформації. Блокові шифри: DES, AES, ГОСТ 28147, DSTU7624. Потокові шифри: RC4, STRUMOK. Асиметричні криптосистеми. Шифри RSA, EG. Електронний цифровий підпис DSA. Тенденції розвитку систем криптографічного захисту інформації.

Тема лекційного заняття 15. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу.

Система візуалізації та управління подіями (SIEM).

Тема лекційного заняття 16. Концептуальна схема оцінки ІБ.

Концептуальна схема оцінки ІБ. Кількісна та якісна оцінки ІБ.

Тема лекційного заняття 17. Виявлення технічних каналів витоку інформації.

Акустичний (мовний) канал витоку інформації. Електричний канал витоку інформації. Електромагнітний канал витоку інформації. Оптичний та оптоелектронний канал витоку інформації. Параметричний канал витоку інформації.

Тема лекційного заняття 18. Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами.

Пасивні заходи захисту інформації на підприємствах спрямовані на підвищення звукоізоляції огороджувальних конструкції. Активні заходи захисту інформації спрямовані на зниження співвідношення сигнал/завада.

Тема лекційного заняття 19. Управління кіберінцидентами.

Дослідження інцидентів. Надання допомоги та рекомендацій з питань протидії кіберзагрозам. Моніторинг і виявлення інцидентів. Накопичення та проведення аналізу даних про кіберзагрози.

Тема лекційного заняття 20. Розслідування кіберінцидентів / кібератак (зокрема, на прикладі підприємств АПК).

Тема лекційного заняття 22. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.

Проведення аудиту ІБ та визначення на основі звіту з аудиту ризиків ІБ. Вибір методів та засобів забезпечення необхідного рівня ІБ.

Тема лекційного заняття 23. IDS.

Система виявлення атак (вторгнень) (Intrusion Detection System, IDS). Виявлення фактів несанкціонованого доступу в комп'ютерну систему або мережу або несанкціонованого управління ними.

Тема лекційного заняття 24. IPS.

Система запобігання вторгненням (Intrusion Prevention System, IPS). IPS як розширення систем виявлення вторгнень (IDS)

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	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
Змістовий модуль 1. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки. Основні поняття політики інформаційної безпеки та захисту інформації.												

Тема 1. Властивості інформації з точки зору проблематики її захисту.	3	2				1						
Тема 2. Ризики порушення політики інформаційної безпеки об'єкту інформатизації.	7	2		4		1						
Тема 3. Вимоги щодо безпеки системи, ризики безпеки.	7	2		4		1						
Тема 4. Механізми реалізації послуг безпеки.	3	2				1						
Тема 5. Поняття загрози інформації.	3	2				1						
Тема 6. Політика інформаційної безпеки.	3	2				1						
Тема 7. Аналіз моделей безпеки ІКС.	7	2		4		1						
Тема 8. Загальні моделі ІБ.	3	2				1						
Тема 9. Аналіз безпеки програмного забезпечення.	7	2		4		1						
Тема 10. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	7	2		4		1						
Тема 11. Політики резервного копіювання даних.	7	2		4		1						
Тема 12. Механізми безпеки комп'ютерних мереж.	3	2				1						
Разом за змістовим модулем 1	**60**	**24**		**24**		**12**						
Змістовий модуль 2. Моделювання та аналіз безпеки об'єктів захисту інформації.												
Тема 13. Модель архітектури безпеки ІКС.	7	2		4		1						
Тема 14. Методи захисту інформації в ІКС.	3	2				1						
Тема 15. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу. Система візуалізації та управління подіями (SIEM).	3	2				1						
Тема 16. Концептуальна схема оцінки ІБ. Кількісна та якісна оцінки ІБ.	3	2				1						
Тема 17. Виявлення технічних каналів витоку інформації.	7	2		4		1						
Тема 18. Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами.	7	2		4		1						
Тема 19. Управління кіберінцидентами (зокрема, на прикладі підприємств АПК).	7	2		4		1						
Тема 20. Розслідування кіберінцидентів / кібератак	7	2		4		1						

(зокрема, на прикладі підприємств АПК).												
Тема 21. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.	3	2				1						
Тема 22. Вибір методів та засобів забезпечення необхідного рівня ІБ (зокрема, на прикладі підприємств АПК).	7	2		4		1						
Тема 23. IDS.	3	2				1						
Тема 24. IPS.	3	2				1						
Разом за змістовим модулем 2	**60**	**24**		**24**		**12**						
Усього годин за курс	**120**	**48**		**48**		**24**						

7. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1.	Аналіз ризиків порушення політики інформаційної безпеки об'єкта інформатизації (ОБІ) (зокрема, на прикладі підприємства АПК).	4
2.	Аналіз вимог щодо безпеки ОБІ (зокрема, на прикладі підприємств АПК).	4
3.	Планування заході що до впровадження механізмів реалізації послуг безпеки (зокрема, на прикладі підприємств АПК).	4
4.	Аналіз моделей безпеки ІКС для конкретного ОБІ (зокрема, на прикладі підприємств АПК).	4
5.	Аналіз безпеки програмного забезпечення для ОБІ (зокрема, на прикладі підприємств АПК).	4
6.	Побудова концептуальної моделі архітектури безпеки ІКС ОБІ.	4
7.	Планування методів захисту інформації в ІКС, зокрема, на прикладі підприємств АПК.	4
8.	Автентифікація користувачів у ІКС ОБІ.	4
9.	Застосування криптографічного захисту інформації у ІКС ОБІ, (зокрема, на прикладі підприємств АПК).	4
10.	Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.	4
11.	Виявлення технічних каналів витоку інформації.	
12.	Управління кіберінцидентами (зокрема, на прикладі підприємств АПК).	
	Разом за семестр	**48**
	Разом	**48**

8. Самостійна робота

№ з/п	Назва теми	Кількість годин
1.	Властивості інформації з точки зору проблематики її захисту об'єкту інформатизації (ОБІ) на прикладі підприємств АПК.	1
2.	Ризики порушення політики інформаційної безпеки ОБІ (зокрема, на прикладі підприємств АПК).	1
3.	Сучасні вимоги щодо безпеки системи, ризики безпеки ОБІ (зокрема, на прикладі підприємств АПК).	1

4.	Механізми реалізації послуг безпеки ОБІ (зокрема, на прикладі підприємств АПК).	1
5.	Політика інформаційної безпеки ІКС або ОБІ. Поняття загрози інформації.	1
6.	Моделі безпеки ІКС.	1
7.	Проблематика безпеки програмного забезпечення.	1
8.	Модель архітектури безпеки ІКС.	1
9.	Інноваційні методи захисту інформації в ІКС.	1
10.	Автентифікація користувачів на ОБІ та у ІКС підприємств АПК.	1
11.	Криптографічний захист інформації. Криптографічні протоколи.	1
12.	Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу. Система візуалізації та управління подіями (SIEM).	1
13.	Концептуальна схема оцінки безпеки інформації. Кількісна та якісна оцінки безпеки інформації.	1
14.	Виявлення технічних каналів витоку інформації. Акустичний (мовний) канал витоку інформації. Електричний канал витоку інформації. Електромагнітний канал витоку інформації. Оптичний та оптоелектронний канал витоку інформації. Параметричний канал витоку інформації.	2
15.	Методи та засоби технічного захисту інформації. Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами.	2
16.	Управління кіберінцидентами (зокрема, на прикладі підприємств АПК).	2
17.	Поняття кіберінцидента/кібератаки. Розслідування кіберінцидентів / кібератак (зокрема, на прикладі підприємств АПК).	2
18.	Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ. Вибір методів та засобів забезпечення необхідного рівня ІБ (зокрема, на прикладі підприємств АПК).	3
	Разом	**24**

9. Індивідуальні завдання (ПЕРЕЛІК ПИТАНЬ ДЛЯ САМОСТІЙНОЇ РОБОТИ)

1. Проблеми теорії захисту інформації.
2. Властивості інформації з точки зору ЗІ.
3. Використання поняття ризику.
4. Моделювання доступу в ІТКС.
5. Механізми реалізації послуг безпеки.
6. Стандарт ISO-7498-2.
7. Побудова та впровадження СЗІ.
8. Механізми і політики розмежування прав доступу в ІКС.
9. Засоби забезпечення захисту інформації в ІКС.
10. Засоби ідентифікації й автентифікації об’єктів баз даних, управління доступом.
11. Засобу контролю цілісності інформації, організація аудиту.
12. Види загроз для інформаційної безпеки (ІБ).
13. Дестабілізуючі факторі.
14. Модель загроз для середовищ опрацювання інформації.
15. Аналітичні моделі загроз ІБ.
16. Емпіричні моделі загроз ІБ.
17. Основна теорема ІБ.
18. Дискреційна політика безпеки.
19. Мандатна політика безпеки.
20. Рольова політика безпеки.
21. Монітор безпеки.
22. Модель ADEPT-50.
23. Модель HRU.
24. Модель Take-Grant.

25. Модель Белла-Лападула.
26. Модель з повним перекриттям.
27. Інформаційно-аналітична модель з оцінки захисту інформації від загроз НСД.
28. Модель виявлення порушень.
29. Вартісна модель.
30. Модель функціонального профілю.
31. Об'єктно-концептуальна модель обчислювальної системи і РПЗ.
32. Модель взаємодії об'єктів обчислювальної системи з погляду безпеки.
33. Методи аналізу безпеки ПЗ.
34. Нелегітимне використання ресурсів.
35. Нелегітимний доступ до даних.
36. Нелегітимний запуск програм.
37. Нелегітимне виконання програм.
38. Нелегітимна відмова в обслуговування (порушення доступності).
39. Тенденції розвитку систем захисту ІТКС.
40. Канали витоку інформації в ІКС та мережах.
41. Класифікація засобів технічного захисту інформації в каналах загального користування.
42. Категорії уразливостей ІТКС.
43. Класи атак.
44. Захист шлюзів.
45. Міжмережеві екрани.
46. Розробка конфігурації міжмережевих екранів.
47. Симетричне шифрування даних.
48. Криптографічні примітиви й типи структур симетричного шифрування.
49. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, ГОСТ-28147.
50. Алгоритми Rijndael (AES).
51. Архітектура блочних симетричних шифрів.
52. Режим гама шифрування. Режим шифрування зі зворотним зв’язком за виходом. Режим вироблення імітовставки.
53. Потокові шифри. Математичні положення теорії скінченних полів та систем класів лишків.
54. Асиметричні алгоритми шифрування даних RSA та Ель Гамаля.
55. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри.
56. Основні напрями розвитку асиметричних криптоалгоритмів.
57. Криптографія на еліптичних кривих.
58. Теоретико-чисельні задачі, складність арифметики точок ЕК в різних формах і представленнях.
59. Цифрова стеганографія з відкритим ключем.
60. Симетричні та несиметричні методи автентифікації суб’єкта.
61. Протоколи автентифікації.
62. Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки.
63. ЗУ про інформацію, про науково-технічну інформацію.
64. ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах».
65. ЗУ «Про доступ до публічної інформації».
66. ЗУ «Про державну таємницю».
67. ЗУ «Про основні засади забезпечення кібербезпеки України».
68. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури».
69. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки.
70. Регламенти ЄС в галузі кібербезпеки.
71. ДСТУ ISO 27001.
72. Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці.
73. Мережева модель OSI. Основні протоколи стеку TCP/IP.
74. Віртуалізація (принципи, гіпервізори).
75. Архітектура комп’ютерів.

76. Методи і засоби обробки інформації.

77. Алгоритмізація та програмування (без прив'язки до конкретної мови програмування).

78. Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Делегати, Узагальнення).

79. Методи сортування та пошуку даних.

80. Кількісна міра інформації. Завадостійкі коди.

81. Операційні системи.

82. Архітектура операційних систем. Процеси і потоки в операційних системах. Керування пам'яттю в операційних системах.

83. Файлові системи.

84. Захисні механізми операційних систем.

85. Моделі безпеки в інформаційній та/або кібербезпеці.

86. Модель порушника.

87. Модель загроз.

88. Модель вразливостей.

89. Захист інформації, що обробляється та зберігається в ІКС.

90. Процедури ідентифікації, автентифікації, авторизації користувачів.

91. Резервування інформації та компонентів ІКС.

92. Програмні та програмно-апаратні комплекси ЗЗІ.

93. Антивіруси, міжмережеві екрани.

94. IPS, IDS.

95. Системи контролю та управління доступом.

96. Відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

97. Організаційно-технічні заходи відновлення функціонування ІКС.

98. Журнал аудиту подій.

99. Політики резервного копіювання даних.

100. Моніторинг процесів функціонування ІКС.

101. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу.

102. Система візуалізації та управління подіями (SIEM).

103. Аналіз подій.

104. Механізми безпеки комп'ютерних мереж.

105. Віртуальні приватні мережі (VPN).

106. Протоколи автентифікації RADIUS.

107. Протоколи SSL/TLS.

108. Проєктування, створення, супровід КСЗІ.

109. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.

110. Вибір методів та засобів забезпечення необхідного рівня ІБ.

111. Моделі загроз та моделі порушника.

112. Загрози цілісності.

113. Загрози доступності.

114. Загрози конфіденційності.

115. Загрози через технічні канали.

116. Загрози через соціальну інженерію.

117. Оцінка захищеності інформації в ІКС.

118. Концептуальна схема оцінки безпеки інформації.

119. Кількісна та якісна оцінки безпеки інформації.

120. Управління кіберінцидентами.

121. Поняття кіберінцидента / кібератаки.

122. Розслідування кіберінцидентів / кібератак.

123. Управління ризиками в інформаційній та / або кібербезпеці.

124. Ризики інформаційної безпеки.

125. Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику.

126. Аудит інформаційної та/або кібербезпеки.

127. Етапи проведення аудиту.

128. Аудит на основі аналізу ризиків.
129. Аудит на основі стандартів ІБ.
130. Аудит на основі експериментальних досліджень ІС.
131. Забезпечення безперервності бізнес-процесів.
132. Поняття бізнес-процесу.
133. Модель бізнес-процесу.
134. Математичні основи криптографії та стеганографії.
135. Модулярні обчислення.
136. Елементи теорії чисел. Алгоритм Евкліда. Теорема Ейлера. Теореми Ферма. Обчислення у скінченних полях.
137. Умови стійкості шифрів.
138. Однонаправлені функції, функції гешування.
139. Псевдовипадкові послідовності в криптосистемах.
140. Обчислення в системі чисел з плаваючою точкою.
141. Симетричні криптосистеми.
142. Модель симетричної криптосистеми.
143. Класичні методи шифрування. Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування.
144. Блокові шифри. DES, AES, ГОСТ 28147, DSTU7624.
145. ДСТУ ГОСТ 28147-2009
146. ДСТУ 7624:2014 (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість).
147. Потокові шифри. RC4, STRUMOK.
148. ДСТУ 8845:2019 (довжина ключів, крипостійкість).
149. Асиметричні криптосистеми.
150. Модель асиметричної криптосистеми.
151. Шифри RSA, EG.
152. Генерація спільних секретів DH.
153. Електронний цифровий підпис DSA.
154. Криптографічні протоколи.
155. Протоколи захисту мережевого трафіку IPSec.
156. Протоколи безпечної передачі даних прикладного рівня: https.
157. Цифрова стеганографія.
158. Поняття цифрової стеганографії.
159. Модель стеганосистеми. Основні вимоги до стеганосистеми.
160. Відкриті, напівзакриті, закриті стеганосистеми.
161. Поняття ЦВЗ, класифікація.
162. Метод модифікації найменшого значущого біта.
163. Атаки на стеганосистеми.
164. Технічні канали витоку інформації.
165. Акустичний (мовний) канал витоку інформації.
166. Електричний канал витоку інформації.
167. Електромагнітний канал витоку інформації.
168. Оптичний та оптоелектронний канал витоку інформації.
169. Параметричний канал витоку інформації.
170. Методи та засоби технічного захисту інформації.
171. Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами.
172. Системи відеоспостереження.

10. Методи навчання

Проведення лекцій з використанням технічних засобів навчання. Проведення лабораторних робіт та самостійної роботи засобами інформаційно-комунікаційних технологій в освіті. Використовується електронний навчальний курс на платформі Moodle «Захист інформації в комп'ютерних системах».

11. Форми контролю

Наприкінці кожного змістовного модуля проводиться контрольна робота у вигляді тесту, що створений у комп'ютерному навчальному середовищі. Підсумкова атестація: іспит.

12. Розподіл балів, які отримують студенти

Оцінювання знань студента відбувається за 100-бальною шкалою і переводиться в національні оцінки згідно з табл.1 «Положення про екзамени та заліки у НУБіП України» (наказ про уведення в дію від 26.04.2023 р. №10):

Рейтинг здобувача вищої освіти, бали	**Оцінка національна за результати складання екзаменів заліків**	
	Екзамен	**Залік**
90-100	Відмінно	зараховано
74-89	Добре	
60-73	Задовільно	
0-59	незадовільно	не зараховано

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

Оцінка виконання та захисту лабораторних робіт за кожний модуль здійснюється у наступній відповідності:

№ лабораторної роботи	**Кількість балів**	**Загальна кількість балів**
1 модуль		
Лабораторна робота № 1	10	70
Лабораторна робота № 2	10	
Лабораторна робота № 3	10	
Лабораторна робота № 4	10	
Лабораторна робота № 5	10	
Лабораторна робота № 6	10	
Самостійна робота	10	
Модульна контрольна		30
2 модуль		
Лабораторна робота № 7	10	70
Лабораторна робота № 8	10	
Лабораторна робота № 9	10	
Лабораторна робота № 10	10	
Лабораторна робота № 11	10	
Лабораторна робота № 12	10	
Самостійна робота	10	
Модульна контрольна		30

13. Методичне забезпечення

1. Електронний навчальний курс на платформі Moodle вміщує повне методичне забезпечення включаючи: лекції, презентації до лекцій, методичні вказівки до виконання лабораторних робіт, глосарій термінів тощо.

14. Рекомендована література

Базова

1. Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Василіу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ЦП «Компринт» О.В., 2020. – 444 с

2. Проєктування комплексних систем захисту інформації. Підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць. Львів : Видавництво Львівської політехніки, 2020. 320 с.

3. Сагун А.В., Лахно В.А., Бобков В.Б., Касаткін Д.Ю., Хайдуров В.В. навчальний посібник «Спеціалізовані комп'ютери» / А.В.Сагун, В.А.Лахно, В.Б.Бобков, Д.Ю.Касаткін, В.В.Хайдуров // НУБіП України, - Київ, Видавничий центр Компринт 2021, 24 у.д.а.

4. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.].Вінниця : ВНТУ, 2018. - 118 с.

Допоміжна

1. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S., ... & Florov, S. (2021). Synergy of building cybersecurity systems.

15. Інформаційні ресурси

1. АДМІНІСТРАЦІЯ ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=81998&cat_id=38835

16. Нормативна література

1. ДСТУ ISO/IEC 11770-3:2002 «Інформаційні технології. Методи захисту».

2. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

3. НД ТЗІ 1.4-001-00. Типове положення про службу захисту інформації в автоматизованій системі.