Чернівецький національний університет імені Юрія Федьковича

(повне найменування головного закладу вищої освіти)

Відокремлений структурний підрозділ «Фаховий коледж

Чернівецького національного університету імені Юрія Федьковича»

(повна назва відокремленого структурного підрозділу)

Циклова комісія *комп'ютерної інженерії*

(назва циклової/предметної комісії)

"ПОГОДЖЕНО"	"ЗАТВЕРДЖУЮ"
Завідувач	Заступник директора
Природничого відділення	з навчально-методичної роботи
_____ *Христина МЕЛЬНИЧУК*	_____ *Микола ДЕРЕВ'ЯНЧУК*
(підпис) (ім'я та прізвище)	(підпис) (ім'я та прізвище)
"27" 08 20 26 року	"28" 08 20 26 року

ПРОГРАМА

навчальної дисципліни

"Основи кібербезпеки та захист інформації"

(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))

обов'язкова

(вказати: обов'язкова/вибіркова)

Освітньо-професійна програма

"Комп'ютерна інженерія"

(назва освітньо-професійної програми)

Спеціальність

F7 Комп'ютерна інженерія

(код і назва спеціальності)

Галузь знань

F Інформаційні технології

(код і назва галузі знань)

Освітньо-професійний ступінь

фаховий молодший бакалавр

(назва освітньо-професійного ступеня)

Мова навчання

українська

(вказати: на якій мові читається предмет)

Чернівці, 2026

Програма навчальної дисципліни *"Основи кібербезпеки та захист інформації"*

(назва навчальної дисципліни)

складена відповідно до освітньо-професійної програми

"Комп'ютерна інженерія"

(назва освітньо-професійної програми)

затвердженої Вченою радою Чернівецького національного університету імені Юрія Федьковича (Протокол № 13 від « 28 » серпня 2026 року) та введеної в дію наказом ректора № 315 від « 28 » серпня 2026 року.

Розробники: (вказати авторів, їхні посади, наукові ступені та вчені (педагогічні) звання)

викладач першої кваліфікаційної категорії, Х.В. Мельничук,

викладач А.Ю. Мельничук

Профайл викладача

https://ce-college.chnu.edu.ua/tsyklova-komisiia/sklad-tsyklovoi-komisii/melnychuk-khrystyna-volodymyrivna/

https://ce-college.chnu.edu.ua/tsyklova-komisiia/sklad-tsyklovoi-komisii/melnychuk-andrii-yuriiovych/

E-mail h.melnychuk@chnu.edu.ua, a.melnychuk@chnu.edu.ua

Сторінка курсу в Moodle https://moodle.chnu.edu.ua/course/view.php?id=9077

Робоча програма обговорена та узгоджена на засіданні циклової комісії

комп'ютерна інженерія

Протокол № 1 від "27" 08 2026 року

Голова циклової комісії _____ *Олександр ТАЩУК*

(підпис) (ім'я та прізвище)

Схвалена Методичною радою

Протокол № 1 від "27" 08 2026 року

Голова методичної ради _____ *Ольга БІЛОКРИЛА*

(підпис) (ім'я та прізвище)

ПЕРЕЗАТВЕРДЖЕНО

Протокол № ____ від _____, 20 __р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

Протокол № ____ від _____, 20 __р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

Протокол № ____ від _____, 20 __р. _____ _____

(підпис) (ініціали та прізвище голови ЦК)

1. Мета та завдання навчальної дисципліни

Анотація: Дисципліна «Основи кібербезпеки та захист інформації» спрямована на вивчення сучасних методів, засобів і технологій забезпечення конфіденційності, цілісності та доступності інформації.

Мета: формування у студентів теоретичної та практичної бази знань з захисту інформації; навчання принципам захисту облікових записів, операційних систем, побудови комплексних систем захисту інформації; розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні криптографічних алгоритмів, алгоритмів хешування для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій, а також вивчення основ стеганографічного захисту інформації.

Завдання:

- формування в студентів бази знань, умінь і навичок, необхідних для кваліфікованого та ефективного використання сучасних технологій захисту даних у навчально-пізнавальній діяльності та повсякденному житті;
- розвиток навичок захисту інформації в різних станах: при передачі, при опрацюванні і зберіганні, вміння виявити та уникнути, усунути загрози інформаційній безпеці;
- набуття знань про криптографічні алгоритми, системи автентифікації, управління доступом, захист мереж і даних від несанкціонованого втручання з метою ефективного розв’язання різноманітних завдань, які пов’язані з майбутньою професійною діяльністю в умовах інформаційного суспільства.

Предмет навчальної дисципліни: Принципи, методи та технології захисту інформації в комп’ютерних системах і мережах, основи криптографії, шифрування, хешування, стеганографія, методи автентифікації користувачів, управління доступом, виявлення та запобігання несанкціонованим діям, захист даних від шкідливого програмного забезпечення, побудова комплексних систем безпеки та нормативно-правові аспекти у сфері інформаційної безпеки.

Пререквізити: Дисципліна «Основи кібербезпеки та захист інформації» може вивчатись разом або після набуття окремих компетентностей з дисциплін «Операційні системи», «Комп’ютерні системи та мережі», «Об’єктно-

орієнтоване програмування».

Дисципліна «Основи кібербезпеки та захист інформації» є складовою циклу професійної підготовки фахового молодшого бакалавра з комп'ютерної інженерії. Набуті знання можуть бути використанні при проходженні переддипломної практики та написанні кваліфікаційних робіт.

Студент повинен **знати**:

- види загроз інформації;
- канали витоку інформації;
- технології несанкціонованого витоку інформації;
- методи та засоби захисту інформації;
- технології захисту об'єктів;
- технології захисту мереж зв'язку;
- технології програмного захисту;
- технології криптографічного захисту;
- технології стеганографії.

Студент повинен **вміти**:

- систематизувати і аналізувати розрізнену технічну інформацію;
- працювати із довідковою технічною літературою;
- ставити завдання, давати порівняльну характеристику різним варіантам рішень захисту інформації;
- використовувати ПК та спеціальні програми для тестування, пошуку основних проблем та захисту даних в комп'ютерних системах, мережах та програмах;
- розробляти алгоритми криптографічного перетворення;
- використовувати різні інформаційні джерела для пошуку та усунення різних загроз інформаційній;
- самостійно презентувати власні і колективні результати аналізу проблем кібербезпеки;
- самостійно шукати альтернативні рішення у професійній діяльності.

Компетентності:

ЗК3. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК4. Здатність застосовувати знання у практичних ситуаціях.

ЗК5. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК7. Здатність працювати в команді.

ЗК8. Здатність вчитися і оволодівати сучасними знаннями.

СК2. Здатність застосовувати на практиці фундаментальні концепції, парадигми і основні принципи функціонування апаратних, програмних та інструментальних засобів комп'ютерної інженерії.

СК3. Здатність вільно користуватись сучасними комп'ютерними та інформаційними технологіями, прикладними та спеціалізованими комп'ютерно інтегрованими середовищами для розробки, впровадження та обслуговування апаратних та програмних засобів комп'ютерної інженерії.

СК5. Здатність забезпечувати захист інформації в комп'ютерних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

СК7. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

СК8. Здатність здійснювати організацію робочих місць з урахуванням вимог охорони праці, їх технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

СК9. Здатність оформляти отримані робочі результати у вигляді презентацій, науково-технічних звітів.

СК10. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати прийняті рішення.

СК11. Здатність здійснювати вибір, розгортати, інтегрувати, діагностувати, адмініструвати та експлуатувати комп'ютерні системи та мережі, мережеві ресурси, сервіси та інфраструктуру організації.

СК13. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їх компонентів шляхом використання аналітичних методів і методів моделювання.

СК15. Здатність проектувати, розробляти та обслуговувати websастосунки з динамічним контентом, використовуючи webтехнології, технології комп'ютерної графіки та анімації.

СК16. Здатність генерувати нові ідеї (креативність).

СК17. Здатність до абстрактного мислення, аналізу і синтезу.

Програмні результати навчання

РН02. Знати і розуміти теоретичні положення, що лежать в основі функціонування апаратних та програмних засобів комп'ютерної інженерії.

РН03. Знати сучасні методи та технології для розв'язання прикладних задач комп'ютерної інженерії.

РН06. Тестувати, діагностувати та обслуговувати апаратні та програмні засоби комп'ютерної інженерії.

РН07. Застосовувати знання для формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

РН08. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації апаратних та програмних засобів комп'ютерної інженерії для вирішення технічних задач у професійній діяльності.

РН10. Здійснювати пошук інформації з різних джерел для розв'язання задач комп'ютерної інженерії.

РН11. Ідентифікувати, класифікувати та описувати роботу програмнотехнічних засобів комп'ютерної інженерії.

РН12. Поєднувати теорію і практику, знаходити та обґрунтовувати шляхи рішення типових задач у професійній діяльності з урахуванням виробничих інтересів.

РН13. Обґрунтовувати прийняті рішення, оцінювати, оформляти та представляти результати професійної діяльності згідно з діючою нормативною документацією.

РН14. Використовувати сучасні інтегровані середовища, методи і технології розробки, впровадження, адміністрування комп'ютерних систем та мереж, баз даних і знань.

РН15. Проводити інсталяцію та налаштування системного та прикладного програмного забезпечення, у тому числі програмних засобів захисту інформації з метою реалізації встановленої політики інформаційної безпеки.

РН18. Системно мислити та застосовувати творчі здібності до формування нових та нестандартних рішень при розв'язуванні задач комп'ютерної інженерії.

2. Опис навчальної дисципліни

2.1. Загальна інформація

Назва навчальної дисципліни *Основи кібербезпеки та захист інформації*												
Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсумкового контролю**
			кредитів	**годин**	**змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**підготовка до екзамену**	
Денна	4	8	3	90	2	24	-	-	24	42	-	залік

2.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
Теми лекційних занять	**Змістовий модуль 1. Основні поняття захисту інформації**					
Тема 1. Захист інформації та його головні завдання	5	2	-	-	-	3
Тема 2. Тріада: конфіденційність, цілісність, доступність. Стани даних	8	2	-	2	-	4
Тема 3. Механізми і політики розмежування прав доступу	7	2	-	2	-	3
Тема 4. Шифрування/дешифрування даних	11	2	-	4	-	5
Тема 5. Протоколи автентифікації	7	2	-	2	-	3
Тема 6. Цифрові підписи	7	2	-	2	-	3
Разом за ЗМ1	45	12	-	12	-	21
Теми лекційних занять	**Змістовий модуль 2. Захист даних**					
Тема 1. Основні види атак, принципи криптоаналізу.	12	4	-	2	-	6
Тема 2. Методи та пристрої забезпечення інформаційної безпеки	8	2	-	2	-	4
Тема 3. Моделі захисту. Захист пам’яті	6	2	-	-	-	4
Тема 4. Захист операційних систем	12	2	-	6	-	4
Тема 5. Використання паролів і механізмів контролю за доступом	7	2	-	2	-	3
Разом за ЗМ 2	45	12	-	12	-	21
Усього годин	**90**	**24**	-	**24**	-	**42**

3. Теми лекційних занять

№	Назва теми	Кількість годин
	Змістовий модуль 1. Основні поняття захисту інформації	
1	**Тема 1.** Захист інформації та його головні завдання **План** 1. Поняття захисту інформації. 2. Інформація з обмеженим доступом. 3. Політика безпеки	2
2	**Тема 2.** Тріада: конфіденційність, цілісність, доступність. Стани даних **План** 1. Конфіденційність. 2. Цілісність. 3. Доступність. 4. Стани даних	2
3	**Тема 3.** Механізми і політики розмежування прав доступу **План** 1. Доступ до інформації 2. Принципи розмежування доступу. 3. Політики безпеки та моделі контролю доступу. 4. Механізми реалізації політик доступу	2
4	**Тема 4.** Шифрування/дешифрування даних **План** 1. Криптографія. 2. Основні вимоги до сучасних криптосистем. 3. Класифікація сучасних криптосистем. 4. Симетричне шифрування 5. Асиметричне шифрування	2
5	**Тема 5.** Протоколи автентифікації **План** 1. Хешування 2. Класифікація хеш-функцій 3. Алгоритми MD 4. Алгоритми SHA	2
6	**Тема 6.** Цифрові підписи **План** 1. Поняття цифрового підпису 2. Основні алгоритми ЕЦП 3. Стандарти ЕЦП	2
	Змістовий модуль 2. Захист даних	
7	**Тема 1.** Основні види атак, принципи криптоаналізу. **План** 1. Типові загрози 2. Атаки на застосунки 3. Атаки на бездротові мережі та мобільний зв’язок 4. Атаки на симетричні алгоритми 5. Атаки на асиметричні алгоритми 6. Криптоаналіз	4
8	**Тема 2.** Методи та пристрої забезпечення інформаційної безпеки **План** 1. Пристрої захисту інформації 2. Принципи захисту інформації при підключенні до мережі Інтернет	2

	3. Міжмережеві екрани 4. Захист інформації на мережевому рівні	
9	**Тема 3.** Моделі захисту. Захист пам'яті **План** 1. Аналіз умов функціонування та загроз інформації в комп'ютерних системах і мережах. 2. Побудова моделі загроз в сучасних комп'ютерних системах і мережах. 3. Побудова моделі порушника в сучасних комп'ютерних системах і мережах. 4. Захист пам'яті на ПК.	2
10	**Тема 4.** Захист операційних систем **План** 1. Аналіз захищеності сучасних ОС. 2. Підсистема захисту в ОС Windows. 3. Порівняння архітектури Windows та Linux. 4. Інші ОС.	2
11	**Тема 5.** Використання паролів і механізмів контролю за доступом **План** 1. Ідентифікація та автентифікація користувачів. 2. Парольна автентифікація. 3. Політика управління паролями. 4. Механізми контролю за доступом. 5. Сучасні тенденції в автентифікації та контролі доступу.	2
Всього:		**24**

4. Теми лабораторних занять

№	Назва теми	Кількість годин
Змістовий модуль 1. Основні поняття захисту інформації		
1	Оцінка дії загрози в інформаційній системі	2
2	Cisco Packet Tracer. Налаштування контролю доступу. Налаштування аутентифікації та авторизації в Linux	2
3	Шифрування і дешифрування даних за допомогою різних інструментів	4
4	Криптоаналіз. Стеганографія	2
5	Створення та використання ЕЦП	2
Змістовий модуль 2. Захист даних		
6	Онлайн-інструменти для дослідження шкідливих програм	2
7	Налаштування брандмауера зональної політики	2
8	Дослідження можливостей захисту ОС Windows	4
9	Дослідження можливостей захисту ОС Linux	2

10	Відновлення паролів	2
	Всього:	**24**

5. Самостійна робота

№	Назва теми	Кількість годин
Змістовий модуль 1. Основні поняття захисту інформації		
1	Активні та пасивні загрози	3
2	Поняття п’яти дев’яток (доступності)	4
3	Загрози, що порушують кожен із компонентів тріади	
4	Матриця доступу, ACL	3
5	Методи захисту від підміни чи модифікації зашифрованих даних	5
6	Стеганографія	
7	Основні протоколи автентифікації (Kerberos, CHAP, EAP, OAuth 2.0)	3
8	Різниця між ЕЦП та КЕП	3
Змістовий модуль 2. Захист даних		
9	Атаки на криптографічні алгоритми (brute-force, dictionary, side-channel)	6
10	Різниця між атаками на шифри та на протоколи	
11	Захист від перехоплення й підміни повідомлень	
12	Системи виявлення/запобігання вторгнень (IDS/IPS)	4
13	Загрози для оперативної пам’яті (buffer overflow, code injection)	4
14	Захист даних в пам’яті	
15	Принципи безпеки операційних систем	4
16	Принцип роботи сервера AAA	3
	Всього:	**42**

6. Методи навчання

При вивченні дисципліни передбачене проведення лекцій та лабораторних занять. Самостійна робота, пов’язана з опрацюванням відповідного теоретичного матеріалу, може супроводжуватись підготовкою конспектів, написанням домашніх чи самостійних робіт, підготовкою проєктів.

Викладання дисципліни передбачає поєднання основних традиційних та інноваційних методів навчання з елементами електронного консультування, що передбачає використання сучасних інформаційних технологій, платформ та забезпечує засвоєння програмних результатів навчання.

Для досягнення освітньої мети й прогнозованих результатів навчання у дисципліні «Основи кібербезпеки та захист інформації» використовуються такі технології та методи навчання:

1. Пояснювально-ілюстративний метод (виклад теоретичного матеріалу на лекціях, ілюстрація методів розв’язання завдань та прикладів застосування в професійній сфері, показ презентацій).

2. Метод проблемного навчання, що передбачає засвоєння студентами фундаментальних знань з дисципліни та пошуку способів розв'язання поставлених на лекції завдань.

3. Репродуктивний метод, що передбачає безпосереднє застосування набутих базових знань до демонстрації практичних умінь та навичок при розв'язуванні поставлених завдань.

4. Частково-пошуковий метод – організація пошуку об’єктів дослідження, розв'язування запропонованих викладачем завдань.

5. Дослідницький метод, що передбачає пошук розв'язку практичних завдань дисципліни з можливістю консультацій з викладачем.

6. Використання мультимедійних та хмарних технологій при організації комунікації з викладачем чи при онлайн-навчанні.

7. Індивідуальні методи роботи на лабораторних заняттях та при виконанні завдань самостійної роботи.

8. Застосування електронних ресурсів, а також платформи для електронного навчання Moodle (https://moodle.chnu.edu.ua).

Отримані навички та знання в подальшому будуть використані під час виконання завдань практичного характеру, а також при виконанні кваліфікаційних робіт.

7. Система контролю та оцінювання

Методи контролю

Методи та засоби оцінювання та демонстрування результатів навчання даної дисципліни наступні:

- модульні контрольні роботи з використанням різнорівневих завдань та стандартизованих тестів у системі дистанційного навчання Moodle;
- лабораторні роботи;
- презентації результатів виконаних завдань;
- захист лабораторних робіт;
- інші види індивідуальних та групових завдань.

У разі проведення навчального процесу та оцінювання в дистанційній формі використовуються засоби Moodle (у тому числі тестування).

Контроль самостійної роботи і оцінка її результатів включає:

- самоконтроль і самооцінку студента;
- контроль і оцінку з боку викладача, циклової комісії, державних кваліфікаційних комісій та ін.

Основними формами контролю самостійної роботи є:

- проведення заліку;
- тестування;
- проведення модульних контрольних робіт;
- письмові чи усні опитування студентів;
- захист лабораторних робіт.

Форми контролю

Даною дисципліною передбачені наступні форми поточного контролю:

- усне опитування (фронтальне, індивідуальне та комбіноване), захист лабораторних робіт студентів;
- письмове опитування (модульні контрольні, тестування).

Форма підсумкового контролю – залік.

Політика академічної доброчесності

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні освітнього компонента регламентовано чинними документами ВСП «Фаховий коледж ЧНУ»:

- Етичний кодекс Відокремленого структурного підрозділу «Фаховий коледж Чернівецького національного університету імені Юрія Федьковича»

- Положенням про виявлення та запобігання академічному плагіату у Відокремленому структурному підрозділі «Фаховий коледж Чернівецького національного університеті імені Юрія Федьковича»
- Політика використання штучного інтелекту в Чернівецькому національному університету імені Юрія Федьковича

Використання здобувачами фахової передвишої освіти інструментів штучного інтелекту (ШІ) під час виконання навчальних завдань:

- *допускається за умови* дотримання принципів академічної доброчесності (здобувач освіти несе відповідальність за зміст, достовірність і результати поданої роботи, а у разі використання ШІ зобов'язаний зазначити факт і спосіб його застосування);
- *не допускається* використання ШІ як заміни самостійного виконання завдань або з порушенням інших вимог академічної доброчесності.

Розподіл балів, які отримують студенти

Поточне оцінювання (*аудиторна та самостійна робота*)												Кількість балів (залік)	Сумарна кількість балів
Змістовий модуль №1						Змістовий модуль № 2							
Лаб1	Лаб2	Лаб3	Лаб4	Лаб5	М КР	Лаб6	Лаб7	Лаб8	Лаб9	Лаб 10	М КР	50	100
3	3	3	3	3	10	3	3	3	3	3	10		

Кількість балів за роботу студента при здійсненні поточного контролю залежить від дотримання таких вимог:

- якість виконання навчальних завдань;
- повний обсяг їх виконання;
- повнота та послідовність відповідей;
- наявність нормативного та наукового обґрунтування;
- рівень вмінь застосовувати знання для аналізу практичних завдань чи
- проблемних питань;
- можливість поєднання теоретичного матеріалу в реальній проблемній
- ситуації;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- своєчасність виконання навчальних завдань;
- ініціативність у навчальній діяльності.

Критерії оцінювання поточних завдань

Рівень знань	Бали	Критерії оцінювання відповіді
Високий	90-100% від максимальної кількості встановлених балів	Завдання виконане відповідно до поставлених вимог; містить розгорнутий виклад матеріалу з поставленого питання; відслідковується знання основних понять і категорій та взаємозв'язку між ними; вказує на вміння давати змістовний та логічний аналіз питань, аргументувати власну відповідь, робити висновки; прослідковується творчий підхід та самостійність.
Достатній	70-89% від максимальної кількості встановлених балів	Завдання виконане відповідно до поставлених вимог; містить достатній виклад матеріалу з поставленого питання з незначними неточностями; відслідковується знання основних понять і категорій, але наявні прогалини при встановленні взаємозв'язку між ними; окремі формулювання при аналізі питань є нечіткими або неаргументованими; алгоритм розв'язку задачі є правильним, однак допущені помилки при розрахунках.
Середній	50-69 % від максимальної кількості встановлених балів	Завдання виконане відповідно до поставлених вимог; містить достатній виклад матеріалу з поставленого питання з незначними неточностями; відслідковується знання основних понять і категорій, але наявні прогалини при встановленні взаємозв'язку між ними; окремі формулювання при аналізі питань є нечіткими або неаргументованими; порушено алгоритм розв'язку задачі і/або присутні помилки при розрахунках.
Початковий	0-49 % від максимальної кількості встановлених балів	Завдання виконане з недотриманням вимог; відповідь відсутня або неправильна, тобто містить грубі змістовні помилки; аналіз, аргументація, висновки відсутні або помилкові. Завдання розв'язане неправильно.

8. Критерії оцінювання навчальних досягнень студентів під час проведення підсумкового контролю

В кінці вивчення дисципліни «Основи кібербезпеки та захист інформації» студенти згідно із навчальним планом складають залік. Залік проводиться в усній формі. Залікове завдання може бути у вигляді залікового білету, яке включає 2 теоретичні питання та 1 практичне завдання. Підсумкова оцінка знань студентів з дисципліни «Основи кібербезпеки та захист інформації» здійснюється на основі проведення заліку, результати якого оцінюються за 50-бальною шкалою.

На оцінювання впливають такі моменти:

- рівень опанування основних проблемних питань відповідно до програми дисципліни та до завдань білетів;
- знання студентом ключових термінів і категорій;
- вміння вирішувати ситуаційні завдання та робити висновок;
- ступінь ознайомлення із основною та додатковою науковою літературою відповідно до програми дисципліни;
- вміння пов’язати теоретичні положення з практикою;
- здатність студента відстоювати власні погляди;
- вміння логічно у відведений час викласти основні положення запропонованих в заліковому завданні питань і зробити відповідні висновки і узагальнення.

50,0-45,0 балів ставиться у випадках, коли студент має систематичні та глибокі знання навчального матеріалу, вміє без помилок виконувати практичні завдання, передбачені програмою дисципліни, засвоїв основу та ознайомився з додатковою літературою, викладає матеріал у логічній послідовності, робить узагальнення і висновки, наводить практичні приклади у контексті тематичного теоретичного матеріалу.

44,9-40,0 балів ставиться, якщо студент повністю засвоїв навчальний матеріал, знає основну літературу, вміє виконувати практичні завдання, викладає матеріал у логічній послідовності, робить певні узагальнення і висновки, але не наводить практичних прикладів у контексті тематичного теоретичного матеріалу або допускається незначних помилок у формулюванні термінів, категорій, розв’язанні практичних завдань.

39,9-35,0 балів ставиться, якщо студент повністю засвоїв навчальний матеріал, знає основну літературу, вміє виконувати практичні завдання, викладає матеріал у логічній послідовності, але не вміє робити певні узагальнення і висновки, не наводить практичних прикладів у контексті тематичного

теоретичного матеріалу або допускається незначних помилок у формулюванні термінів, категорій, розв’язанні практичних завдань.

34,9-30,0 балів ставиться у випадках, коли студент засвоїв матеріал не у повному обсязі, дає неповні відповіді на поставлені теоретичне запитання, допустився грубих помилок у розв’язанні практичного завдання.

29,9-25,0 балів ставиться у випадках, коли студент засвоїв матеріал не у повному обсязі, дає неповні відповіді на поставлені теоретичне запитання, не вміє чітко узагальнити опрацьований матеріал, допустився грубих помилок у розв’язанні практичного завдання.

24,9-17,5 балів ставиться студенту, який не засвоїв навчальний матеріал, дає неправильні відповіді на більшість поставлених теоретичних запитань, не неправильно виконує розрахунки та розв’язувати практичні завдання.

17,4-0 балів ставиться студенту, який не засвоїв навчальний матеріал, дає неправильні відповіді на поставлені теоретичні запитання, не вміє виконувати розрахунки та розв’язувати практичні завдання.

Критерії оцінювання результатів навчання з навчальної дисципліни
Шкала оцінювання: національна та ЄКТС

<table>
<tr><th rowspan="2">Сума балів за всі види навчальної діяльності</th><th rowspan="2">Оцінка ЄКТС</th><th colspan="2">Оцінка за національною шкалою</th></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90-100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>80-89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>70-79</td><td>C</td></tr>
<tr><td>60-69</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>50-59</td><td>E</td></tr>
<tr><td>35-49</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>незадовільно з обов’язковим самостійним повторним вивченням дисципліни</td><td>не зараховано з обов’язковим самостійним повторним вивченням дисципліни</td></tr>
</table>

9. Перелік питань для підсумкового контролю (залік)

1. Поняття захисту інформації. Основні завдання та принципи.
2. Види інформаційних загроз та канали витоку інформації.
3. Основні напрями та методи захисту інформації.
4. Інформація з обмеженим доступом. Політика безпеки в організації.
5. Концепція конфіденційності, цілісності та доступності (CIA-тріада).
6. Характеристика станів даних.
7. Основні принципи забезпечення цілісності та доступності даних.
8. Механізми розмежування прав доступу.
9. Моделі контролю доступу: дискреційна (DAC), мандатна (MAC), рольова (RBAC), атрибутивна (ABAC).
10. Поняття матриці доступу, списків ACL.
11. Криптографія як основа захисту даних. Основні властивості криптосистем.
12. Види криптографічних алгоритмів.
13. Алгоритми симетричного шифрування (AES, DES, RC4).
14. Алгоритми асиметричного шифрування (RSA, ElGamal, ECC).
15. Хешування даних. Основні властивості хеш-функцій.
16. Основні алгоритми MD і SHA: структура, призначення, відмінності.
17. Протоколи автентифікації користувачів: Kerberos, CHAP, EAP, OAuth 2.0.
18. Принципи побудови систем автентифікації та авторизації.
19. Цифровий підпис: поняття, принцип дії та значення.
20. Основні алгоритми ЕЦП (RSA, DSA, ECDSA).
21. Відмінності між ЕЦП та КЕП. Стандарти електронного підпису.
22. Основні види атак на інформаційні системи.
23. Соціальна інженерія.
24. Принципи криптоаналізу та методи зламу шифрів.
25. Атаки на симетричні та асиметричні алгоритми шифрування.
26. Атаки на мережеві застосунки та бездротові мережі.
27. Атаки типу brute-force, dictionary, side-channel — характеристика та захист.
28. Методи та пристрої забезпечення інформаційної безпеки.
29. Призначення та функції міжмережевих екранів (Firewall).
30. Принципи захисту інформації під час підключення до мережі Інтернет.
31. Системи виявлення і запобігання вторгнень (IDS/IPS).
32. Моделювання загроз та порушників у комп’ютерних системах.
33. Методи захисту пам’яті в сучасних операційних системах.
34. Основні загрози для оперативної пам’яті (buffer overflow, code injection).
35. Підсистема безпеки в ОС Windows: облікові записи, політики, контроль доступу.
36. Засоби захисту ОС Linux: SELinux, AppArmor, права доступу.
37. Порівняльна характеристика систем захисту в ОС Windows та Linux.

38. Використання паролів у системах автентифікації.
39. Вимоги до надійності паролів і політики їхнього управління.
40. Методи зберігання паролів: хешування, сіль, алгоритми bcrypt, Argon2.
41. Багатофакторна автентифікація (MFA) — сутність, принцип роботи, приклади.
42. Механізми контролю доступу у сучасних системах: ACL, RBAC, ABAC.
43. Сучасні тенденції в автентифікації: безпарольні технології, біометрія, токени.
44. Стеганографія як метод приховання інформації.

10. Рекомендована література

Основна (базова)

1. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
2. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с.
3. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
4. Петренко С. І., Руденко О. І. Захист інформації в комп'ютерних системах і мережах. — Київ: Центр учбової літератури, 2018. — 340 с.

Допоміжна

1. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук.-практ. посіб./ За заг. ред. Проф. Я.Ю. Кондратьєва. – К., 2004.
2. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2006.
3. Хорошко В.О. Комп'ютерна стеганографія / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець – Вінниця: ВНТУ, 2014. – 155 с.
4. Кузьмін О. Є., Сидоренко І. М. Кібербезпека та захист інформації. — Київ: НАУ, 2021. — 215 с.
5. Савчук І. М. Правові основи інформаційної безпеки в Україні. — Київ: Алерта, 2019. — 188 с.
6. Stallings W. Cryptography and Network Security: Principles and Practice. — Pearson, 8th ed., 2020. — 760 p.
7. Pfleeger C. P., Pfleeger S. L., Margulies J. Security in Computing. — Pearson, 6th ed., 2021. — 912 p.
8. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. — Wiley, 20th Anniversary Edition, 2015. — 784 p.
9. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. — Wiley, 3rd ed., 2020. — 1232 p.
10. Kizza J. M. Guide to Computer Network Security. — Springer, 5th ed., 2020. — 700 p.

Інформаційні ресурси

1. https://www.netacad.com/ - мережева академія Cisco
2. https://moodle.chnu.edu.ua/course/view.php?id=8204 – Курс «Технології захисту інформації» в Moodle
3. https://zakon.rada.gov.ua/laws/show/2163-19#Text – Закон України про основні засади забезпечення кібербезпеки України
4. https://www.rada.gov.ua – офіційний сайт Верховної Ради України.
5. https://zakon.rada.gov.ua/laws/show/80/94-вр - Про захист інформації в інформаційно-телекомунікаційних системах