Чернівецький національний університет імені Юрія Федьковича
(повне найменування закладу вищої освіти)

Факультет математики та інформатики
(назва факультету/навчально-наукового інституту)

Кафедра математичного моделювання
(назва кафедри, що забезпечує викладання)

“ЗАТВЕРДЖУЮ”
Декан факультету
математики та інформатики

_____ Ольга МАРТИНЮК

“25” 06 2025 року

РОБОЧА ПРОГРАМА
навчальної дисципліни
Основи інформаційної безпеки

(назва навчальної дисципліни)

обов’язкова

(вказати: обов’язкова)

Освітньо-професійна програма «Системний аналіз»
(назва програми)

Спеціальність 124 Системний аналіз
(вказати: код, назва)

Галузь знань 12 Інформаційні технології
(вказати: шифр, назва)

Рівень вищої освіти перший (бакалаврський)
(вказати: перший (бакалаврський) / другий (магістерський) / третій (освітньо-науковий)

Факультет математики та інформатики
(назва факультету/ навчально-наукового інституту, на якому здійснюється підготовка фахівців за вказаною освітньою програмою)

Мова навчання українська
(вказати: на якій мові читається дисципліна)

Чернівці 2025 рік

Робоча програма навчальної дисципліни «*Основи інформаційної безпеки*» складена відповідно до освітньо-професійної програми «Системний аналіз»

Розробник:
Перцов Андрій Сергійович, доцент кафедри математичного моделювання, кандидат фіз.-мат. наук, доцент

Викладач, що забезпечує читання даної навчальної дисципліни:
Перцов Андрій Сергійович, доцент кафедри математичного моделювання, кандидат фіз.-мат. наук, доцент

Погоджено з гарантом ОП _____ **Андрій ПЕРЦОВ**

Затверджено на засіданні кафедри математичного моделювання
Протокол № 15 від «24» червня 2025 року

Завідувач кафедри _____ **Ігор ЧЕРЕВКО**

Схвалено методичною радою факультету математики та інформатики
Протокол № 12 від «25» червня 2025 року

Голова методичної ради _____ **Віра СІКОРА**

Мета навчальної дисципліни: вивчення різних галузей комп'ютерної безпеки, інструментів кібербезпеки, які мають вирішальне значення для вирішення проблем у галузі безпеки, а також вивчення різних сфер безпеки мережі включаючи виявлення вторгнень, збір доказів та захист від кібератак.

У даній дисципліні студенти повинні освоїти основи мережевого та системного адміністрування, основні поняття криптографії, вміти визначати коли відбуваються напади всередині мереж, збирати докази вторгнень в мережу, перевіряти мережі та системи на вразливості.

Пререквізити. Навчальні дисципліни: "Комп'ютерні мережі" та "Операційні системи".

Результати навчання. У результаті вивчення навчальної дисципліни студент повинен

знати: основи мережевого та системного адміністрування, основні поняття криптографії, особливості конфіденційності, цілісності та доступності систем.

вміти: визначати коли відбуваються напади всередині мережі, збирати докази вторгнень в мережу, перевіряти мережі та системи на вразливість, захищатись від мережевих атак.

Дисципліна формує такі **компетенції** у відповідності до стандарту вищої освіти [1] та освітньої програми:

ЗК01. Здатність до абстрактного мислення, аналізу та синтезу

ЗК02. Здатність застосовувати знання у практичних ситуаціях.

ЗК04. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК07. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК14. Здатність оцінювати та забезпечувати якість виконуваних робіт

ФК6. Здатність до комп'ютерної реалізації математичних моделей реальних систем і процесів; проєктувати, застосовувати і супроводжувати програмні засоби моделювання, прийняття рішень, оптимізації, обробки інформації, інтелектуального аналізу даних.

ФК11. Здатність системно аналізувати свою професійну і соціальну діяльність, оцінювати накопичений досвід.

Наведені результати навчання за відповідною дисципліною співвідносяться із такими **програмними результатами навчання:**

ПР10. Знати архітектуру сучасних обчислювальних систем і комп'ютерних мереж.

ПР13. Проектувати, реалізовувати, тестувати, впроваджувати, супроводжувати, експлуатувати програмні засоби роботи з даними і знаннями в комп'ютерних системах і мережах.

Опис навчальної дисципліни

Загальна інформація

Форма навчання	Рік підготовки	Семестр	Кількість		Кількість годин						Вид підсумкового контролю
			кредитів	годин	лекції	практичні	семінарські	лабораторні	самостійна робота	індивідуальні завдання	
Денна	3	6	4.0	120	15	–	–	30	75	–	екзамен

Структурний зміст 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
Теми лекційних занять	**Змістовий модуль 1**.											
Тема 1. Вступ. Основні поняття, концепції та проблеми безпеки.	21	2	–	4	–	15						
Тема 2. Криптографія.	24	3	–	6	–	15						
Тема 3. Захист систем і мереж.	18	3	–	5	–	10						
Разом за змістовим модулем 1	63	8	–	15	–	40						
Теми лекційних занять	**Змістовий модуль 2.**											
Тема 4. Безпека програмного забезпечення..	23	3	–	5	–	15						
Тема 5. Управління безпекою.	17	2	–	5	–	10						
Тема 6. Хмарна безпека. ШІ та інформаційна безпека	17	2	–	5	–	10						
Разом за ЗМ 2	57	7	–	15	–	35						
Усього годин	120	15	–	30	–	75						

Тематика лекційних занять з переліком питань

№	Назва теми з основними питаннями
1	Вступ. Основні поняття, концепції та проблеми безпеки. Нормативно-правові стандарти
2	Основи криптографії. Асиметричні методи та PKI.
3	Моделі доступу. Безпека ОС.
4	Мережеві атаки. Засоби мережевого захисту.
5	OWASP Top 10. Аутентифікація та керування сесіями.
6	Ризик-менеджмент. Політики безпеки.
7	Хмарна безпека, IoT та ШІ

Матеріали до кожної лекції наведено на сайті електронного навчання на сторінці курсу https://moodle.chnu.edu.ua/course/view.php?id=9086

Тематика лабораторних занять з переліком питань

№	Назва теми (завдання)
1	Аналіз загроз системи.
2	Криптографічні примітиви. Сертифікати та TLS.
3	Налаштування політик ОС.
4	Аналіз мережевого трафіку. Налаштування Firewall.
5	Виявлення вразливостей. Захист веб-додатку.
6	Ризик-менеджмент. Реагування на інциденти.

Матеріали до виконання лабораторних робіт наведено на сайті електронного навчання на сторінці курсу https://moodle.chnu.edu.ua/course/view.php?id=9086

Індивідуальні науково-дослідні завдання (ІНДЗ)

Студент може індивідуально виконувати додаткові завдання навчально-дослідницької спрямованості за завданнями, наданими викладачем.

Студенти можуть отримати до 10 балів в рахунок ІНДЗ, якщо самостійно зареєструються на безкоштовних курсах платформи Prometheus або платформи Coursera з Cybersecurity (за попереднім узгодженням тематики курсів з викладачем), пройдуть навчання, отримають відповідний сертифікат і надішлють його на сайт дистанційного навчання викладачу разом з детальним звітом з практичних завдань пройденого курсу (постановки задач, коди виконаних програм, пояснення коду) та скріншотом успішності на курсі. Кількість балів буде виставлена пропорційно до навчальних результатів студента (згідно зі статистикою сайта Prometheus або Coursera).

Завдання для самостійної роботи студентів

Самостійна робота складається з повторення матеріалу, засвоєного на лекціях, самостійного опанування частини теоретичного матеріалу, роботи з контрольними запитаннями та завданнями.

№	Назва теми	Завдання для самостійної роботи	К-сть год.
1	Теми 1-6	Підготовка до лекційних занять: 1. Вступ. Основні поняття, концепції та проблеми безпеки. Нормативно-правові стандарти 2. Основи криптографії. Асиметричні методи та PKI. 3. Моделі доступу. Безпека ОС. 4. Мережеві атаки. Засоби мережевого захисту. 5. OWASP Top 10. Аутентифікація та керування сесіями. 6. Ризик-менеджмент. Політики безпеки. 7. Хмарна безпека, IoT та ШІ	30
2	Теми 1-6	Підготовка до лабораторних занять: 1. Аналіз загроз системи. Створення моделі STRIDE. 2. Криптографічні примітиви. Сертифікати та TLS. AES, RSA, хеші (OpenSSL/PowerShell). Генерація CA, server/client cert 3. Налаштування політик ОС. Windows Group Policy / Linux sudoers 4. Аналіз мережевого трафіку. Налаштування Firewall. Wireshark, MITM-атак моделювання. Правила iptables / Windows Firewall 5. Виявлення вразливостей. Захист веб-додатку. OWASP ZAP або Burp Suite. Виправлення XSS/SQLi 6. Ризик-менеджмент. Реагування на інциденти. Matrix метод, оцінка ризиків для кейсу. Аналіз логів, форензика файлів	30
3	Теми 1-6	Підготовка до підсумкового модуль-контролю	15

Формат подачі та вимоги

1. Надіслати PDF-звіт (2-4 сторінки).
2. Звіт має містити: постановку задачі, опис даних, підготовку, результати, висновки.
3. Використовуйте посилання на джерела даних, коротко опишіть, чому вибрали саме цей набір.
4. Студенти повинні самостійно виконати аналіз – не просто скопіювати чи «прогнати» чужий код.

Методи навчання

У процесі вивчення навчальної дисципліни використовуються інноваційні освітні технології: інформаційно-комунікаційні, технології студентоцентрованого навчання; традиційні та інтерактивні форми і методи навчання, серед яких: вербальні (словесні), наочні, проблемно-пошукові, індуктивно-дедуктивні, лекція-візуалізація, проблемна лекція, аналіз і розв'язання ситуативних задач та ін, зокрема, електронне навчання з використанням системи Moodle, тестування.

Методи формування професійної компетентності: розповідь, пояснення, бесіда, демонстрація, візуалізація, дискусія тощо. Методи формування практичних умінь та навичок: розв'язування задач лабораторних робіт, виконання завдань, розробка та аналіз алгоритмів і програмного коду, захист звітів з лабораторних робіт.

Система контролю та оцінювання

Засобами оцінювання та демонстрування результатів навчання є: стандартизовані тести; аналітичні звіти з лабораторних робіт; презентації результатів виконаних завдань та досліджень ІНДЗ, усний контроль у вигляді індивідуального та фронтального опитування на лекціях та лабораторних заняттях.

Формами поточного контролю є усна чи письмова (тестування, лабораторна робота, ІНДЗ) відповідь студента.

Формою підсумкового контролю є екзамен.

Критерії оцінювання поточного та підсумкового контролю

Критерієм підсумкового оцінювання є досягнення студентом мінімальних порогових рівнів оцінок (балів) за кожним передбаченим результатом навчання.

Система оцінювання рівня навчальних досягнень ґрунтується на принципах ECTS та є накопичувальною.

Студенти можуть отримувати загалом до 10 балів під час відвідування лекційних занять за правильні відповіді на запитання лектора, активне обговорення багатоваріантних підходів до рішення представленої лектором проблеми (для активізації пошукової та дослідної діяльності студентів).

Протягом семестру студенти виконують 6 лабораторних робіт. Кожна лабораторна робота оцінюється в 10 балів.

Звіт з лабораторної роботи, який студенти завантажують на сайт, повинен мати таку структуру:

1) файл у форматі Word, що містить титульний аркуш (назва університету, факультету, кафедри, навчальної дисципліни, хто виконав, хто перевірив, Чернівці – 202_) , назву лабораторної роботи, умову кожного завдання, код

програми (не скріншот), скріншоти виконання з демонстрацією різних можливих, в т.ч. особливих, випадків роботи програми;

2) усі файли розробленого студентом проєкту, що містять коди програм;

3) всі вищезазначені файли архівуються в один архів, назва архіву має складатися із прізвища студента латиницею, номера лабораторної та номера варіанту, наприклад: Ivanenko_lab_1_var_21.arj.

У разі невиконання студентами вищезазначених правил оформлення кількість отриманих студентом балів при перевірці буде знижуватися. Якщо студент отримав суттєві зауваження до програмного коду і переробив програму та звіт, надіславши його на повторне оцінювання, максимально можлива кількість отриманих ним балів буде щонайменше на 1 (один) бал меншою, ніж максимально можлива кількість балів за цю роботу.

50% балів, відведених на оцінювання ЛР, студент отримує за працюючий програмний продукт, в якому реалізовано всі завдання ЛР та оформлений звіт. Решта 50% балів виставляється після захисту студентом виконаного звіту. На захисті звіту з ЛР студент має відповісти на питання щодо постановки задачі та розробленого ним алгоритму реалізації кожного із завдань ЛР. При відповіді на теоретичні питання та питання щодо програмної реалізації алгоритму у випадку неістотної помилки знімається 10-20% балів, а у випадку істотної 20-40% балів, якщо ж студент не опанував теоретичний матеріал, плутається в означеннях, наводить логічно невірні твердження, то знімається до 50% балів від усієї суми балів за ЛР.

Максимальна кількість, яку можна набрати на підсумковому модулі (тестування) – 40 балів. Тестування проводиться з використанням системи електронного навчання.

Підсумкова оцінка виставляється за результатами суми балів, набраних на змістових модулях під час семестру та підсумковому модулі згідно з нижче наведеною таблицею.

Розподіл балів, які отримують студенти

Поточне оцінювання						Кількість балів (модуль-контроль)	Сумарна к-ть балів
Змістовий модуль №1			Змістовий модуль №2				
Т1	Т2	Т3	Т4	Т5	Т6	40	100
10	10	10	10	10	10		

Шкала оцінювання: національна та ЄКТС

Оцінка за національною шкалою	Оцінка за шкалою ECTS	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Відмінно	A (90-100)	відмінно
Добре	B (80-89)	дуже добре
	C (70-79)	добре
Задовільно	D (60-69)	задовільно
	E (50-59)	достатньо
Незадовільно	FX (35-49)	(незадовільно) з можливістю повторного складання
	F (1-34)	(незадовільно) з обов'язковим самостійним опрацюванням освітнього компоненту до перескладання

На оцінку "відмінно" заслуговує студент, який виявив всебічні, систематичні та глибокі знання, здатність самостійно виконувати завдання, передбачені програмою, ознайомлений з основною і додатковою літературою, рекомендованою програмою. Така оцінка передбачає також засвоєння студентом взаємозв'язку основних понять дисципліни та їх значення для набутої професії.

Оцінку "добре" ставлять студентові, який засвоїв навчально-програмовий матеріал у повному обсязі, успішно виконує передбачені програмою завдання, опрацював основну літературу, рекомендовану програмою, тобто студентові, який засвідчив систематичний характер знань із дисципліни і здатний до їх самостійного поповнення й оновлення у процесі подальшої навчальної роботи і професійної діяльності.

На оцінку "задовільно" заслуговує студент, який виявив знання основного навчального матеріалу в обсязі, необхідному для подальшого навчання і майбутньої роботи за професією, здатний виконувати завдання, передбачені програмою, ознайомлений з основною літературою, рекомендованою програмою. Як правило, цю оцінку виставляють студентам, які припустилися огріхів у відповіді на іспиті та при виконанні екзаменаційних завдань, але продемонстрували спроможність усунути їх.

Оцінку "незадовільно" ставлять студентові, у знаннях якого є прогалини, який припустився принципових помилок у виконанні передбачених програмою завдань, тобто студентові, який неспроможний продовжити навчання чи приступити до професійної діяльності після закінчення вищого навчального закладу без додаткових занять з відповідної дисципліни.

Перелік питань для самоконтролю та підсумкового контролю навчальних досягнень студентів

1. Дайте визначення поняття *інформаційна безпека* та охарактеризуйте її основні цілі.
2. Поясніть сутність тріади CIA (конфіденційність, цілісність, доступність).
3. Які основні загрози інформаційній безпеці сучасних комп'ютерних систем?
4. Охарактеризуйте основні нормативно-правові документи та стандарти у сфері інформаційної безпеки (ISO/IEC 27001, законодавство України).
5. Що таке модель загроз і для чого вона використовується в інформаційній безпеці?
6. Опишіть модель STRIDE та наведіть приклади загроз для кожної її категорії.
7. Дайте визначення криптографії та поясніть її роль у забезпеченні інформаційної безпеки.
8. Порівняйте симетричні та асиметричні криптографічні алгоритми.
9. Поясніть принцип роботи алгоритмів AES та RSA.
10. Що таке криптографічна хеш-функція та які її основні властивості?
11. Призначення та структура інфраструктури відкритих ключів (PKI).
12. Як працюють цифрові сертифікати та протокол TLS?
13. Поясніть поняття *модель доступу* та наведіть приклади моделей контролю доступу.
14. Основні механізми безпеки операційних систем (Windows, Linux).
15. Що таке політики безпеки ОС та як вони застосовуються на практиці?
16. Охарактеризуйте основні типи мережевих атак (DoS/DDoS, MITM, spoofing).
17. Які засоби мережевого захисту використовуються для протидії атакам?
18. Призначення та принципи роботи міжмережевих екранів (firewall).
19. Роль аналізу мережевого трафіку в забезпеченні інформаційної безпеки.
20. Що таке OWASP Top 10 і яке його значення для безпеки вебдодатків?
21. Поясніть загрози, пов'язані з автентифікацією та керуванням сесіями.
22. Наведіть приклади вразливостей XSS та SQL Injection і способи їх усунення.
23. Дайте визначення ризику в інформаційній безпеці.
24. Опишіть основні етапи процесу ризик-менеджменту.
25. Що таке політика інформаційної безпеки організації та її складові?
26. Поясніть процедуру реагування на інциденти інформаційної безпеки.
27. Особливості забезпечення безпеки в хмарних обчисленнях.
28. Основні загрози інформаційній безпеці в IoT-системах.
29. Вплив технологій штучного інтелекту на сучасні загрози та засоби захисту інформації.
30. Роль системного аналізу у виявленні, оцінюванні та мінімізації ризиків інформаційної безпеки.

Зарахування результатів неформальної/інформальної освіти

Здобувачі вищої освіти має право на участь у неформальній/інформальній освіті.

У межах поточного контролю можуть визнаватися результати неформальної/інформальної освіти за умови наявності сертифікату або освітньої декларації про результати неформальної/інформальної освіти з питань, що відповідає тематиці курсу («Порядок визнання у Чернівецькому національному університеті імені Юрія Федьковича результатів навчання, здобутих шляхом неформальної та/або інформальної освіти», https://www.chnu.edu.ua/media/4g5fzssb/poriadok-vyznannia-rezultativ-navchannia-zdobutykh-shliakhom-neformalnoi-ta-abo-informalnoi-osvity.pdf).

Студентам можуть бути зараховані додаткові бали, отримані через неформальну освіту, до загальної суми балів, набраної з освітньої компоненти, за умови, що результати з проблеми, за якою відбувалося навчання, відповідають тематиці курсу.

Рекомендована література

Основна

1. Стандарт вищої освіти України перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 124 – Системний аналіз // Затверджено і введено в дію наказом Міністерства освіти і науки України від 13.11.2018 р. № 1245.– 23 с. URL: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/124-sistemn.analiz-bakalavr-1.pdf
2. Кириленко, О. Криптографічні засоби захисту інформації: навч. посіб. - Київ: Вид-во НПУ ім. М. П. Драгоманова, 2018.
3. Алексєєнко, В. Основи кібербезпеки: навч. посіб. - Київ: КНЕУ, 2019.
4. Державні стандарти зі зберігання і передачі інформації з обмеженим доступом: ДСТУ 7564:2014, ДСТУ 7565:2014, ДСТУ 7566:2014.
5. Інструкції з захисту інформації від несанкціонованого доступу, витоку, порушення цілісності та конфіденційності: ICO/MEK 27001 (міжнародний стандарт ISO/IEC 27001)
6. "Information Security Principles and Practice" by Mark Stamp, 2nd Edition, Wiley, 2011.
7. "Network Security Essentials" by William Stallings, 6th Edition, Pearson, 2017.
8. "Cryptography and Network Security: Principles and Practice" by William Stallings, 7th Edition, Pearson, 2017.
9. Закон України "Про захист персональних даних" від 01.06.2010 року;
10. OWASP Application Security Verification Standard.

Допоміжна

1. Курс "Cryptography I" на платформі Coursera, який викладає професор Ден Боне з Університету Стенфорда;
2. Bruce Schneier. Applied Cryptography 784 p., Wiley, 2015

Інформаційні ресурси

https://moodle.chnu.edu.ua/course/view.php?id=9086
https://crackstation.net/hashing-security.htm
https://www.webopedia.com/TERM/V/VPN.html
https://www.tutorialspoint.com/difference-between-dns-and-dhcp

Політика академічної доброчесності

Дотримання політики щодо академічної доброчесності учасниками освітнього процесу при вивченні навчальної дисципліни регламентовано такими документами:

1. «Етичний кодекс Чернівецького національного університету імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/etychnyi-kodeks-chernivetskoho-natsionalnoho-universytetu-imeni-yuriia-fedkovycha/
2. «Положенням про виявлення та запобігання академічного плагіату у Чернівецькому національному університету імені Юрія Федьковича» https://www.chnu.edu.ua/universytet/normatyvni-dokumenty/polozhennia-pro-vyiavlennia-ta-zapobihannia-akademichnomu-plahiatu/