ІНСТИТУТ КІБЕРНЕТИКИ
ІМЕНІ В.М. ГЛУШКОВА НАН УКРАЇНИ

«ЗАТВЕРДЖУЮ»
Директор Інституту кібернетики
імені В.М. Глушкова НАН України
академік НАН України

_____ **Іван СЕРГІЄНКО**

«23» 09 2025 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ МЕРЕЖЕВИМ АТАКАМ
(ДВА.1.02)

для здобувачів освітньо-наукового рівня «доктор філософії»

галузь знань	**F «Інформаційні технології»**
спеціальність	**F7 «Комп'ютерна інженерія»**
освітній рівень	**третій (освітньо-науковий)**
освітньо-наукова програма	**«Комп'ютерна інженерія»**
вид дисципліни	**вибіркова**

Форма навчання	**денна / заочна**
Навчальний рік	**2025/2026**
Рік навчання	2
Кількість кредитів ECTS	2
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладач: **Панчук Богдан Олександрович,** доктор філософії

Пролонговано Вченою радою Інституту кібернетики імені В.М. Глушкова НАН України

Навчальні роки пролонгації	Учений секретар вченої ради	Підпис	№ протоколу	Дата протоколу
20____/20____ р.	_____	_____	_____	_____
20____/20____ р.	_____	_____	_____	_____
20____/20____ р.	_____	_____	_____	_____
20____/20____ р.	_____	_____	_____	_____

КИЇВ – 2025

РОЗРОБНИК:
Молодший науковий співробітник відділу теорії цифрових автоматів
доктор філософії,

_____ **Богдан ПАНЧУК**

Робочу програму розглянуто та схвалено на засіданні відділу мікропроцесорної техніки

Протокол від "18" 09 2025 року № 4

Завідувач відділу
професор, д.т.н. _____ **Володимир ОПАНАСЕНКО**
(підпис)

Робочу програму ухвалено науково-методичною радою

Протокол від "22" 09 2025 року № 2

Голова науково-методичної ради
академік НАН України _____ **Іван СЕРГІЄНКО**
(підпис)

Робочу програму затверджено Вченою радою Інституту кібернетики імені В.М. Глушкова НАН України

Протокол від "29" 09 2025 року № 15

Учений секретар
вченої ради _____ **Анатолій КУЛЯС**
(підпис)

Робочу програму погоджено з гарантом освітньої програми F7 «Комп'ютерна інженерія»
"18" 09 2025 року

Гарант освітньої програми
д.т.н., проф. _____ **Володимир РОМАНОВ**
(підпис)

1. МЕТА ДИСЦИПЛІНИ

Полягає у формуванні у аспірантів розуміння сучасних методів виявлення та протидії мережевим атакам, принципів функціонування систем мережевої безпеки та засобів моніторингу інформаційних потоків; опанування теоретичних основ та принципів підвищення захищеності комп'ютерних мереж; оволодіння навичками для проектування систем виявлення мережевих загроз, практичними навичками для їх використання, а також впровадження алгоритмів штучного інтелекту для збільшення діапазону небезпек, які системи безпеки здатні виявляти.

2. ПОПЕРЕДНІ ВИМОГИ ДО ОПАНУВАННЯ АБО ВИБОРУ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

1. *Знати*:
- ✓ основи комп'ютерних мереж, мережеві топології, клієнт-серверну архітектуру, протоколи передачі даних,
- ✓ базові методи аналізу даних,
- ✓ принципи роботи алгоритмів машинного навчання та моделей нейронних мереж.

2. *Вміти*:
- ✓ опрацьовувати наукові джерела,
- ✓ розгортати та налаштовувати мережеві застосунки,
- ✓ шукати та аналізувати документацію програм з відкритим вихідним кодом,
- ✓ працювати з командним рядком та системними утилітами,
- ✓ створювати власні програмні засоби.

3. АНОТАЦІЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

Дисципліна «Методи виявлення та протидії мережевим атакам» є частиною професійної підготовки аспірантів за спеціальністю «Комп'ютерні науки» і має за мету надати знання та навички необхідні для рішення поширених задач кібербезпеки у мережевому середовищі. В її рамках вивчаються різні класи мережевих загроз, засоби їх виявлення та механізми протидії. Особлива увага приділяється принципам проектування інфраструктурних компонент комп'ютерних мереж, пошуку їх вразливостей та моніторингу їх активності з метою виявлення шкідливих дій зловмисників. Розглядаються основі принципи побудови та технічні аспекти застосування систем виявлення загроз, а також впровадження алгоритмів штучного інтелекту для аналізу потоків мережевих даних. Вміння здобуті аспірантами в рамках даної навчальної дисципліни мають за мету сформувати науково-технічну базу для проведення більш глибоких досліджень в галузі інформаційної безпеки.

4. ЗАВДАННЯ (НАВЧАЛЬНІ ЦІЛІ):

Набуття здатності застосовувати та розвивати сучасні засоби виявлення й протидії мережевим атакам і критично оцінювати їх ефективність та дієвість, відповідно до кваліфікації «Доктор філософії», зокрема:
- ✓ формування компетентності у розробці та впровадженні багаторівневих систем мережевої безпеки з залученням як класичних методів так і алгоритмів штучного інтелекту,
- ✓ вміння аналізувати існуючі та реалізовувати нові архітектурні рішення з метою підвищення безпеки мережевої інфраструктури та захищеності інтернет-ресурсів.

5. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ДИСЦИПЛІНОЮ:

Результат навчання (РН) (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		**Форми (та/або методи і технології) викладання і навчання**	**Методи оцінювання та пороговий критерій оцінювання (за необхідності)**	**Відсоток у підсумковій оцінці з дисципліни**
Код	**Результат навчання**			
РН 1.1	Знати найбільш розповсюджені методи здійснення мережевих атак.	*Лекція*	*Залік, активна робота на лекції, усні відповіді*	*20%*
РН 1.2	Знати основні засоби моніторингу комп'ютерних мереж та оповіщення про загрози.			
РН 1.3	Знати основні принципи роботи та експлуатації систем виявлення вторгнень.			*20%*
РН 1.4	Знати методи виявлення мережевих загроз алгоритмами штучного інтелекту.			
РН 2.1	Вміти аналізувати мережеву активність веб-застосунків та розпізнавати шкідливу поведінку.	*Лекція, самостійна робота*	*Залік, модульні контролі, виконання завдань, винесених на самостійну роботу*	*20%*
РН 2.2	Вміти здійснювати формалізацію правил виявлення мережевих загроз на основі відомих сигнатур атак.			*20%*
РН 2.3	Вміти використовувати сучасні програмні засоби для забезпечення багаторівневого захисту комп'ютерних ресурсів та мереж.	*самостійна робота*	*Залік, модульні контролі, виконання завдань, винесених на самостійну роботу*	*5%*
РН 3.1	Вміти робити обґрунтовані судження про захищеність мережевих ресурсів, знаходити потенційні вразливості та пропонувати кроки для їх усунення.			*5%*
РН 4.1	Демонструвати авторитетність, інноваційність, високий ступінь самостійності, академічну та професійну доброчесність, послідовну відданість розвитку нових ідей у процесі професійної та наукової діяльності.			*5%*
РН 4.2	Відповідально ставитися до виконуваних робіт, нести відповідальність за їхню якість.			*5%*

6. СПІВВІДНОШЕННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ ДИСЦИПЛІНИ ІЗ ПРОГРАМНИМИ РЕЗУЛЬТАТАМИ НАВЧАННЯ

Результати навчання дисципліни / **Програмні результати навчання**	**РН 1.1**	**РН 1.2**	**РН 1.3**	**РН 1.4**	**РН 2.1**	**РН 2.2**	**РН 2.3**	**РН 3.1**	**РН 4.1**	**РН 4.2**
(з опису освітньої програми)										
ПРН-1. Мати передові концептуальні та методологічні знання з комп'ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх	+	+	+	+						

світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.										
ПРН-3. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні докази, зокрема, результати теоретичного аналізу, експериментальних досліджень (опитувань, спостережень, …) і математичного та/або комп'ютерного моделювання, наявні літературні дані.	+					+		+		
ПРН-4. Розробляти та досліджувати концептуальні, математичні і комп'ютерні моделі процесів і систем, ефективно використовувати їх для отримання нових знань та/або створення інноваційних продуктів у комп'ютерній науці та дотичних міждисциплінарних напрямах.				+		+				
ПРН-6. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.					+					
ПРН-7. Розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми комп'ютерної науки з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.								+		+
ПРН-8. Глибоко розуміти загальні принципи та методи комп'ютерних наук, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері комп'ютерних наук та у викладацькій практиці.			+				+			
ПРН-9. Вивчати, узагальнювати та впроваджувати в навчальний процес інновації комп'ютерних наук.							+		+	+
ПРН-10. Здійснювати пошук та критичний аналіз інформації, концептуалізацію та реалізацію наукових проєктів з комп'ютерних наук.	+							+	+	

7. СХЕМА ФОРМУВАННЯ ОЦІНКИ.

7.1. Форми оцінювання здобувачів освітньо-наукового ступеня:

- оцінювання впродовж навчального періоду (бали максимальні/мінімальні):

№	Метод оцінювання	Результати навчання, які оцінюються	Кількість балів	
			Максимум	Мінімум
1	Активна робота на лекції, усні відповіді	РН1.1, РН1.2, РН1.3, РН1.4	10	6
2	Виконання завдань, винесених на самостійну роботу	РН2.1, РН2.2	30	18
3	*Виконання модульних контрольних робіт* у формі тестів	РН2.2, РН2.3, РН3.1, РН4.1, РН4.2	20	12
	Всього		60	36

- підсумкове оцінювання: Залік.

- *максимальна/мінімальна кількість балів які можуть бути отримані:* 40/24 балів;
- *результати навчання які будуть оцінюватись:* РН1, РН2, РН3, РН4;
- *форма проведення і види завдань:* письмова контрольна робота (тести 20 запитань).

Здобувачі освітньо-наукового ступеня, які за результатами поточного оцінювання набрали сумарно меншу кількість балів ніж критично-розрахунковий мінімум – 20 балів, до Заліку не допускаються.

Рекомендований мінімум поточного оцінювання – 36 балів, що при мінімумі підсумкового оцінювання 24 бали забезпечує сумарно 60 балів, тобто мінімуму для отримання позитивної оцінки (зарахування) з дисципліни.

7.2. Організація оцінювання:

Обов'язковим є виконання завдань, винесених на самостійну роботу за графіком робочої програми. Обов'язковим для допуску до Заліку є виконання модульних контрольних робіт №1 та №2 до вказаної викладачем дати, перед початком екзаменаційної сесії, згідно навчального плану.

Терміни проведення форм оцінювання:

1. Активна робота на лекції, усні відповіді: протягом навчального періоду;

2. Виконання завдань, винесених на самостійну роботу: протягом навчального періоду;

3. Модульні контрольні роботи*:* після закінчення кожного змістового модуля до початку екзаменаційної сесії.

У випадку відсутності з поважних причин відпрацювання та перескладання завдань здійснюються у відповідності до „Положення про організацію освітнього процесу у Інституті кібернетики ім. В.М. Глушкова НАН України".

7.3. Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.
ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ

№	Назва лекції	Кількість годин		
		Лекції	Семінари	Самостійна робота
Модуль 1. Основи безпеки комп'ютерних мереж та їх моніторинг				
1	**Комп'ютерні мережі та базові засоби мережевої безпеки.** Модель OSI та її рівні. Локальні та глобальні мережі. Адресація та маршрутизація. Шифрування (симетричне, асиметричне). DNS та резолюція доменних імен. Перетворення мережевих адрес (NAT). Брандмауери. Концепція Zero Trust. Сегментація мереж. Тунелювання. VPN. IPsec. *Самостійна робота:* Аналіз мережевих даних за допомогою інструменту Wireshark. Налаштування правил брандмауера.	2		5
2	**Методи здійснення мережевих атак та моделі загроз інформаційних систем.** Відмова в обслуговування (DoS, DDoS). Витік даних. Сканування на вразливості. Спуфінг. Фрагментація. Виконання довільного коду (RCE). Ін'єкція коду. Поняття CVE. Ескалація повноважень. Ботнети (класи, архітектура, життєвий цикл). Моделі загроз STRIDE, DREAD та PASTA. *Самостійна робота:* Моделювання вразливості системи. Робота з базою CVE.	2		5
3	**DoS/DDoS атаки та засоби протидії.** Класи DDoS атак (екстенсивні, розтягнені в часу, експлуатація мережевих протоколів). Атаки на основі відображення та підсилення. Підсилюючий фактор. Атака Smurf. Ping of Death. Slowloris. TCP/UDP/HTTP-flood. SSL/TLS-виснаження. Мінімізація площі атаки. ACL-правила. Багатошарова фільтрація. BCP38. Проксі та зворотні проксі. Доставка статичного контенту. CDN. Proof of Work. Anycast мережі. Гео-фільтрація. *Самостійна робота:* Моделювання багатошарової схеми захисту від DDoS. Налаштування Nginx як reverse-proxy сервера.	3		5
4	**Ботнети, засоби їх виявлення та протидії.** Мережі ботів та алгоритми їх координації. Канали зв'язку ботнетів (HTTP, P2P, DNS-тунелювання, Chat-based). Алгоритм генерації доменних імен (DGA). Алгоритм Fast-flux. Приклади ботнетів та принципи їх роботи (Mirai та Zeus). Виявлення часових кореляцій. Аналіз мережевих графів. DNS-аномалії. Honeypot. Sinkhole/Blackhole. *Самостійна робота:* Аналіз відкритих наборів прикладів активності ботнетів.	3		5
Модуль 2. Проектування та використання засобів виявлення мережевих атак				
5	**Моніторинг веб-застосунків та реагування на загрози.** Збір телеметрії. Журнали подій. Спостереження та оповіщення про загрози. Стек ELK. Систем и збереження, обробки та візуалізації часових рядів. Аналіз мережевих даних. Точки контролю та реплікації трафіку. Дзеркальне відображення пакетів за допомогою Hub, TAP та SPAN. Мережеві потоки (NetFlow, IPFIX, Argus). *Самостійна робота:* Використання HIDS Fail2ban та AIDE.	2		5
6	**Системи виявлення вторгнень.**	2		5

	Принципи роботи IDS. Особливості NIDS. Сигнатури атак. Системи виявлення на основі правил та скриптів. Розробка правил виявлення атак системами Snort/Suricata. Аналіз мережевих даних системою Zeek. Виявлення спроб авторизації пошуком грубою силою. Виявлення HTTP SQL-ін'єкцій та спроб завантаження виконуваних файлів. Виявлення підозрілих User-Agent. *Самостійна робота:* Створення правил виявлення DNS-тунелювання та атак XSS. Створення скриптів Zeek для виявлення Port Scan та витоку даних через DNS.			
7	**Виявлення мережевих загроз методами штучного інтелекту (частина 1).** Аналіз мережевих даних програмними засобами. Алгоритм виділення мережевих потоків. Відкриті набори мережевих даних. Алгоритми логістичної регресії та випадкового лісу. *Самостійна робота:* Кластерний аналіз мережевих даних.	2		5
8	**Виявлення мережевих загроз методами штучного інтелекту. (частина 2).** Нейронні мережі. Критерії якості класифікаторів. Змагальні атаки. Формальна верифікація стійкості класифікаторів мережевих потоків. *Самостійна робота:* Дисперсійний аналіз мережевих даних.	2		5
ВСЬОГО:		18		40

Загальний обсяг 60 *годин*, в тому числі:
Лекцій – **18** *годин*,
Консультація – **2** *годин,*
Самостійна робота – **40** *годин***.**

9. СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

9.1.Основна:

1. Панчук Б. О. Виявлення мережевих атак алгоритмами штучного інтелекту : Доктор філософії : спец.. 122 - Комп'ютерні науки : дата захисту 2025-06-26; . Інститут кібернетики імені В. М. Глушкова Національної академії наук України. – Київ, 167 с. URL: https://nrat.ukrintei.ua/searchdoc/0825U002589/
2. Trost, Ryan. *Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century*. Boston: Addison-Wesley Professional, 2010. URL: https://www.oreilly.com/library/view/practical-intrusion-analysis/9780321591890/
3. Tanenbaum, A. S., Wetherall, D. J., & Feamster, N. (2021). Computer Networks (6th ed.). Pearson Education. URL: https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188/9780137523214
4. Stallings, W. (2010). Network Security Essentials: Applications and Standards (4th ed.). Pearson. URL: https://www.abebooks.com/9780136108054/Network-Security-Essentials-Applications-Standards-0136108059/plp
5. C. Sanders, Practical Packet Analysis, 3rd Edition: Using Wireshark to Solve Real-World Network Problems. No Starch Press, 2017. URL: https://nostarch.com/packetanalysis3

9.2.Додаткова:

1. Sanjeev Kumar. 2007. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. In Proceedings of the Second International Conference on Internet Monitoring and Protection (ICIMP '07). IEEE Computer Society, USA, 25. https://doi.org/10.1109/ICIMP.2007.42

2. C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in *Computer*, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.
3. Arnaldo I. Learning Representations for Log Data in Cybersecurity / I. Arnaldo, A. Cuesta-Infante, A. Arun, M. Lam, C. Bassias, K. Veeramachaneni // Lecture Notes in Computer Science. – 2017. – Vol. 10423. – P. 250–268. – DOI: 10.1007/978-3-319-60080-2_19.
4. Livadas C. Using Machine Learning Techniques to Identify Botnet Traffic / C. Livadas, R. Walsh, D. Lapsley, W. T. Strayer // Proceedings of the 31st IEEE Conference on Local Computer Networks. – Tampa, FL: IEEE, 2006. – P. 967–974. – DOI: 10.1109/LCN.2006.322210.
5. Чичкарьов Є. Метод вибору ознак для системи виявлення вторгнень з використанням ансамблевого підходу та нечіткої логіки / Є. Чичкарьов, О. Зінченко, А. Бондарчук, Л. Асєєва // Кібербезпека: освіта, наука, техніка. – 2023. – № 1(21). – С. 234–251. – DOI: 10.28925/2663-4023.2023.21.234251.
6. Olivier Bonaventure. Computer Networking: Principles, Protocols and Practice (2011). Open Textbooks. 296. URL: https://mds.marshall.edu/oa-textbooks/296