Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

ФТІ
Кафедра інформаційної безпеки

Кореляційний аналіз в кібербезпеці
Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Третій (освітньо-науковий)***
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 К Кібербезпека*
Освітня програма	*Кібербезпека*
Статус дисципліни	*Нормативна*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*2 курс, 1 семестр*
Обсяг дисципліни	*4 кредити ECTS (120 годин)*
Семестровий контроль/ контрольні заходи	*Екзамен*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доктор технічних наук, професор, Ланде Дмитро Володимирович*, Практичні / Семінарські: *доктор технічних наук, професор, Ланде Дмитро Володимирович*, *e-mail: dwlande@gmail.com*
Розміщення курсу	

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Навчальна дисципліна «Кореляційний аналіз в кібербезпеці» присвячена питанням вивчення теоретичних аспектів та практичних питань розробки та застосування сучасних методів прикладної статистики для задач кібербезпеки. Курс містить теоретичні матеріали, після засвоєння яких здобувач буде обізнаний у таких основних напрямках:

- В яких сферах кібербезпеки доцільно використовувати кореляційний аналіз як сучасний метод прикладної статистики;

- Теоретичне підгрунтя, основні принципи і методи реалізації кореляційного аналізу які використовуються в кібербезпеці.

- Використання існуючих та створення власних наборів даних (датасетів) для розв’язання задач кібербезпеки на основі кореляційного аналізу.

. Предметом дисципліни є кореляційний аналіз як сучасна методологія прикладної статистики та його застосунки в задачах кібербезпеки.

Програмні результати[1] навчання згідно ОП:

ПРН 6. Виявляти навички пошуку, збирання та аналізу інформації, розрахунку показників для обґрунтування управлінських рішень.

ПРН 9 Вміння синтезувати науково обгрунтовані рішення по захисту інформації в кіберсистемах та кіберфізичних системах.

ПРН 10 Вміння приймати рішення з питань кібербезпеки в умовах неповної визначеності.

ПРН 11 Вміння знаходити приховані закономірності в даних, одержаних від систем захисту.

ЗК 1 Здатність до абстрактного мислення, аналізу і синтезу.

ЗКЗ Здатність застосовувати знання до розв'язання новітніх науково-практичних задач.

ЗК 5 Здатність до розвитку та вдосконалення існуючих рішень, генерації нових ідей.

ФК 1 Володіння математичним апаратом та технологічним інструментарієм для розв'язання науково-практичних задач за фахом.

ФК 5 Здатність застосовувати сучасні математичні методи до розв'язання задач за фахом.

Після вивчення дисципліни студент володітиме ***знаннями*** щодо принципів роботи, моделей, сучасних методів прикладної статистики та задач кібербезпеки, які розв'язуються цими методами, ***уміннями:*** Досліджувати існуючі рішення, виконувати постановку задачі, формалізувати предметну область та об'єкт дослідження в термінах методів прикладної статистики; володіти принципами виокремлення найбільш суттєвих характеристик об'єкту дослідження; підбирати та застосовувати методи прикладної статистики до розв'язання ряду задач кібербезпеки; розуміти основні теоретичні принципи роботи сучасних методів прикладної статистики; ставити комп'ютерний експеримент по застосуванню методу розв'язання задачі кібербезпеки та інтерпретувати його результати.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Дисципліна використовує результати вивчення дисциплін: "Основи теорії ймовірностей та математичної статистики", "Організація науково-інноваційної діяльності".

Результати вивчення даної дисципліни можуть бути застосовані у професійній діяльності за фахом та для написання бакалаврської дипломної роботи.

3. Зміст навчальної дисципліни

1. Огляд сучасних методів, що будуються на кореляційному аналізі. Методи автокореляційного аналізу, кореляційного аналізу, узагальненого перетворення Фур'є, вейвлет-аналізу, фрактального аналізу, кластеризації. Приклади задач у кібербезпеці: виявлення аномалій, аналіз трафіку, виявлення covert channels. Інтерпретація результатів та обмеження методів.

2. Автокореляційний аналіз. Автокореляційна функція. Визначення та обчислення автокореляційної функції. Властивості автокореляції: симетрія, максимум у нулі, періодичність.

[1] Для нормативних дисциплін зазначається згідно матриці відповідності програмних компетентностей та результатів навчання в освітній програмі.

Аналіз самоподібних і нерегулярних процесів у мережевому трафіку. Застосування автокореляції для виявлення періодичних патернів у поведінці атакуючих систем.

3. Міжпроцесний кореляційний аналіз: виявлення зв'язків між подіями в розподілених системах. Обчислення крос-кореляції між часовими рядами подій (логів, мережевого трафіку, процесів). Виявлення причинно-наслідкових зв'язків, синхронізації атак, ланцюгів інфікування. Використання кореляції для побудови графів подій та атрибуції загроз.

4. Кореляційний аналіз у часовій та частотній областях: використання перетворення Фур'є та вейвлет-аналізу. Спектральний аналіз сигналів у кібербезпеці. Виявлення прихованих періодичностей за допомогою Фур'є-аналізу. Переваги вейвлет-перетворення для аналізу нестаціонарних процесів. Кореляція в частотній області: виявлення сигнатур атак у зашумлених даних.

5. Фрактальний і кореляційний аналіз самоподібних процесів у мережевому трафіку. Поняття фрактальної розмірності та довгострокової залежності. Методи оцінки Hurst-показника. Кореляційні властивості трафіку на різних масштабах. Застосування для виявлення DDoS-атак, тунелювання даних та стеганографії.

6. Кореляційний аналіз у поєднанні з методами кластеризації для виявлення аномалій. Використання кореляційних матриць як основи для кластеризації поведінки систем і користувачів. Методи: k-means, DBSCAN, ієрархічна кластеризація на основі кореляційної відстані. Виявлення відхилень від норми, визначення підозрілих груп подій або IP-адрес.

7. Інтегровані підходи: використання кореляційного аналізу в системах виявлення та реагування на загрози (SIEM/SOAR). Інтеграція кореляційних методів у SIEM-платформи. Побудова правил кореляції подій (event correlation rules). Приклади: виявлення багатостадійних атак (kill chain), пов'язування подій з різних джерел. Оцінка ефективності, лагів, хибних спрацьовувань. Перспективи використання засобів ШІ для адаптивної кореляції.

задачі, метод ієрархічного агрегування, реалізація методу ієрархічного агрегування.

4. Навчальні матеріали та ресурси

Базова література.

1. *Information Operations Recognition. From Nonlinear Analysis to Decision-Making. A. Dodonov, D. Lande, V. Tsyganok, O. Andriichuk, S. Kadenko, A. Graivoronskaya. - LAP Lambert Academic Publishing, 2019. - 292 p. ISBN-13: 978-620-0-27697-1, ISBN-10: 6200276978, EAN: 9786200276971 (http://arxiv.org/abs/1901.10876)*
2. *А.О. Снарський, Д.В. Ланде, І.Ю. Субач. Основи теорії складних мереж: навч. пос. / Снарський А.О., Ланде Д.В., Субач І.Ю.; ІСЗЗІ КПІ ім. Ігоря Сікорського. - Київ: ТОВ "Інжиніринг", 2023. - 225 с. ISBN 978-966-2344-95-0. (https://ela.kpi.ua/items/2b38e967-5cf8-458e-92b5-83406c419531)*
3. *Ситюк В.Є. Прогнозування. Моделі. Методи. Алгоритми: Навчальний посібник. – К.: «Маклаут», 2008. – 364 с. (https://www.academia.edu/9531484/%D0%A1%D0%BD%D0%B8%D1%82%D1%8E%D0%BA_%D0%92_%D0%95_%D0%9F%D1%80%D0%BE%D0%B3%D0%BD%D0%BE%D0%B7%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D0%B8_%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D1%8B_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC%D1%8B)*
4. *Ланде Д.В., Субач І.Ю., Бояринова Ю.Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник. – К.: ІСЗЗІ КПІ ім. Ігоря Сікрорського, 2018. – 300 с. ISBN 978-966-2577-12-9.*

5. *R companion to elementary applied statistics. Hay-Jahans, Christopher. Chapman & Hall/CRC. 2019. 377 p.*

Додаткова література.

1. *Бондаренко, Я. С. Посібник до вивчення дисципліни "Статистичний аналіз даних" [Текст] / Я.С. Бондаренко, С.В. Кравченко. – Д: Ліра, 2018. – 40 с. — Режим доступу до ресурсу: https://www.researchgate.net/publication/335340316_Posibnik_do_vivcenna_disciplini_Statisticnij_analiz_danih*
2. *Статистика (модульний варіант з програмованою формою контролю знань). Навч. посіб. – К.: Центр учбової літератури, 2012. – 448 с. — Режим доступу до ресурсу: https://nubip.edu.ua/sites/default/files/u104/Навчальний%20посібник.pdf*
3. *Про пріоритетні напрями інноваційної діяльності в Україні Верховна Рада України; Закон від 08.09.2011 № 3715-VI // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3715-17*
4. *Про Загальнодержавну комплексну програму розвитку високих наукоємних технологій. Верховна Рада України; Закон, Програма від 09.04.2004 № 1676-IV// [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1676-15*
5. *Про пріоритетні напрями розвитку науки і техніки.Верховна Рада України; Закон від 11.07.2001 № 2623-III // [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2623-14*

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

В рамках дисципліни заплановано наступні види навчальних занять:

- лекції;
- практичні заняття;
- самостійна робота.

На лекціях розкриваються найбільш суттєві теоретичні питання, які дозволяють забезпечити аспірантам можливість глибокого самостійного вивчення всього програмного матеріалу. Теми та порядок самостійної роботи сформовано в логічній послідовності і повністю узгоджуються з метою дисципліни та здійснюються з використанням рекомендованої літератури та глобальної мережі Internet. На заняттях використовуються звичайна дошка, а також презентації лекцій з використанням мультимедіа-проектора. В дистанційному режимі використовуються засоби Google Meet або Zoom та відповідні слайди лекцій, а також матеріали дистанційного курсу, викладені на платформі Сікорський.

Теми та порядок освоєння дисципліни «Сучасні методи прикладної статистики» наведений нижче.

№ з/п	Назви тем і питань, що виноситься на заняття	Кількість годин		
		Лекції	Практичні заняття	Самостійна робота
1	**Тема 1. Огляд сучасних методів кореляційного аналізу.** Мета, предмет та об'єкт курсу. Методи автокореляційного аналізу, кореляційного аналізу, узагальненого перетворення Фур'є, вейвлет-аналізу, фрактального аналізу, кластеризації. Приклади задач у кібербезпеці: виявлення аномалій, аналіз трафіку,	2	2	14

	виявлення covert channels. Інтерпретація результатів та обмеження методів. Основна література: [1-3]. Додаткова література: [2, 3, 5].			
2	**Тема 2. Автокореляційний аналіз.** Автокореляційна функція. Визначення та обчислення автокореляційної функції. Властивості автокореляції: симетрія, максимум у нулі, періодичність. Аналіз самоподібних і нерегулярних процесів у мережевому трафіку. Застосування автокореляції для виявлення періодичних патернів у поведінці атакуючих систем. Основна література: [1,2]. Додаткова література: [1, 3]	2	2	13
3	**Тема 3. Міжпроцесний кореляційний аналіз: виявлення зв'язків між подіями в розподілених системах.** Обчислення крос-кореляції між часовими рядами подій (логів, мережевого трафіку, процесів). Виявлення причинно-наслідкових зв'язків, синхронізації атак, ланцюгів інфікування. Використання кореляції для побудови графів подій та атрибуції загроз. Основна література: [1,3,4]. Додаткова література: [1, 3]	2	2	13
4	**Тема 4. Кореляційний аналіз у часовій та частотній областях: використання перетворення Фур'є та вейвлет-аналізу.** Спектральний аналіз сигналів у кібербезпеці. Виявлення прихованих періодичностей за допомогою Фур'є-аналізу. Переваги вейвлет-перетворення для аналізу нестаціонарних процесів. Кореляція в частотній області: виявлення сигнатур атак у зашумлених даних. Основна література: [3, 4]. Додаткова література: [1, 2]	2	2	13
5	**Тема 5. Фрактальний і кореляційний аналіз самоподібних процесів у мережевому трафіку.** Поняття фрактальної розмірності та довгострокової залежності. Методи оцінки Hurst-показника. Кореляційні властивості трафіку на різних масштабах. Застосування для виявлення DDoS-атак, тунелювання даних та стеганографії. Основна література: [1,3,4]. Додаткова література: [1, 2]	2	2	13
6	**Тема 6. Кореляційний аналіз у поєднанні з методами кластеризації для виявлення аномалій.** Використання кореляційних матриць як основи для кластеризації поведінки систем і користувачів. Методи: k-means, DBSCAN, ієрархічна кластеризація на основі кореляційної відстані. Виявлення відхилень від норми, визначення підозрілих груп подій або IP-адрес. Основна література: [1,3]. Додаткова література: [1, 2]	2	2	13
7	**Тема 7. Інтегровані підходи: використання кореляційного аналізу в системах виявлення та реагування на загрози (SIEM/SOAR).** Інтеграція кореляційних методів у SIEM-платформи. Побудова правил кореляції подій (event correlation rules). Приклади: виявлення багатостадійних атак (kill chain), пов'язування подій з різних джерел. Оцінка ефективності, лагів,	2	2	13

	хибних спрацьовувань. Перспективи використання засобів ШІ для адаптивної кореляції. Основна література: [1,4]. Додаткова література: [1, 3]			
	Разом годин	14	14	92

Теми практичних занять

№ КП	Теми практичних занять	Кількість ауд. годин
1.	Обчислення автокореляційної функції для часових рядів мережевого трафіку. Аналіз періодичних патернів. Практичне обчислення ACF у Python/MATLAB. Виявлення регулярних запитів, beaconing-поведінки C2-серверів. Інтерпретація графіків автокореляції в контексті кібератак.	2
2.	Крос-кореляційний аналіз подій у розподілених системах: встановлення причинно-наслідкових зв'язків. Синхронізація логів із різних джерел (мережа, хост, автентифікація). Пошук часових зв'язків між подіями (наприклад, SSH-логін після сканування портів). Візуалізація кореляційних піків.	2
3.	Спектральний аналіз та вейвлет-перетворення часових рядів кіберподій. Застосування FFT та вейвлетів для виявлення прихованих частот у трафіку. Практика: аналіз трафіку при DDoS, covert timing channels. Порівняння ефективності методів у часовій та частотній областях.	2
4.	Оцінка Hurst-показника та фрактальних властивостей трафіку. Дослідження самоподібності. Розрахунок Hurst-показника (R/S-аналіз, DFA). Аналіз довгострокової залежності в нормального та аномального трафіку. Виявлення стеганографічних або тунельованих потоків даних.	2
5	Побудова кореляційних матриць для подій безпеки та їх візуалізація. Формування матриць кореляції між типами подій (наприклад, IDS-алерти, помилки входу, DNS-запити). Використання теплових мап (heatmaps) для виявлення аномальних зв'язок. Аналіз щільності кореляцій у різні періоди.	2
6	Кластеризація об'єктів за кореляційною відстанню: виявлення груп підозрілих IP-адрес чи користувачів. Реалізація кластеризації (k-means, DBSCAN). Аналіз кластерів на предмет колективної підозрілої поведінки. Оцінка якості кластеризації (silhouette score).	2
7	Розробка правила кореляції подій у модельній SIEM-системі. Інтеграція з LLM для інтерпретації результатів. Налаштування правила кореляції (наприклад, "сканування + помилки входу + внутрішній трафік") у ELK/Splunk. Генерація природно-мовного звіту за допомогою LLM. Оцінка точності, чутливості та можливих хибних спрацьовувань.	2

6. Самостійна робота здобувача

Назва розділу, теми, що виноситься на самостійне опрацювання	Кількість годин СРС
Тема 1. Огляд сучасних методів кореляційного аналізу. Виконання завдань практики №1. Опанування основної та додаткової літератури.	14
Тема 2. Автокореляційний аналіз. Виконання завдань практики №2. Опанування основної та додаткової літератури.	13
Тема 3. Міжпроцесний кореляційний аналіз: виявлення зв'язків між подіями в розподілених системах. Виконання завдань практики №3. Опанування основної	13
Тема 4. Кореляційний аналіз у часовій та частотній областях: використання перетворення Фур'є та вейвлет-аналізу. Виконання завдань практики №4.	13
Тема 5. Фрактальний і кореляційний аналіз самоподібних процесів у мережевому трафіку. Виконання завдань практики №5. Опанування основної та додаткової літератури.	13
Тема 6. Кореляційний аналіз у поєднанні з методами кластеризації для виявлення аномалій.Виконання завдань практики №6. Опанування основної та додаткової літератури.	13
Тема 7. Інтегровані підходи: використання кореляційного аналізу в системах виявлення та реагування на загрози (SIEM/SOAR). Виконання завдань практики №7. Опанування основної та додаткової літератури.	13
Всього	92

Політика та контроль

1. Політика навчальної дисципліни (освітнього компонента)

Програмні результати навчання, політика навчальної дисципліни, методика її опанування, контрольні заходи та терміни виконання оголошуються аспірантам на першому занятті.

Відвідування лекцій, а також відсутність на них, не оцінюється. Однак, здобувачам рекомендується відвідувати заняття, оскільки викладений на них теоретичний матеріал та надані інструкції дозволять ефективніше зорієнтуватися у темі, вибраній для самостійної роботи, спланувати її виконання та спосіб дослідження.

Заохочувальні бали наведені в таблиці.

Заохочувальні бали	
Критерій	Ваговий бал
Звіт з участі у міжнародних, всеукраїнських та/або інших заходах та/або конкурсах за тематикою близькою до тематики курсу	До 15 балів, залежно від рівня представництва і якості звіту
Виступ із лекцією перед студентами молодших курсів на обрану тему за тематикою близькою до тематики курсу	До 15 балів за кожну із доповідей

Самостійне опанування сертифікованого курсу за тематикою дисципліни або дотичною до неї.	Від 15 балів і до повного зарахування дисципліни

Академічна доброчесність
Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» (https://kpi.ua/code).
Норми етичної поведінки

Норми етичної поведінки здобувачів вищої освіти і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». (https://kpi.ua/code).

Процедура оскарження результатів контрольних заходів

Здобувачі вищої освіти мають можливість підняти будь-яке питання, яке стосується процедури контрольних заходів та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами (згідно «Положення про систему забезпечення якості вищої освіти у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського», «Положення про організацію навчального процесу»).

2. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

№ з/п	Контрольний захід	%	Ваговий бал	Кіл-ть	Всього
1.	Бліц-опитування на лекційних заняттях	10	2	5	10
2.	Робота на практичних заняттях	20	5	4	20
3.	Самостійна робота (огляд, презентація, результат моделювання тощо)	30	15	2	30
4.	Екзамен	40	40	1	40
	Всього				100

Активність на лекційних заняттях дозволяє отримати бали до рейтингу. За кожну вірну відповідь під час бліц-опитування отримується до 2 балів.

За кожний окремий звіт у вигляді презентації, огляду літератури, програмного коду, інших можливих видів самостійної роботи за обраними здобувачем отримується до 15 балів за кожний вид роботи.

Обов’язкова умова допуску до іспиту		Критерій
1	Поточний рейтинг	RD ≥ 36

Екзамен

Білет на екзамені складається з 2-х теоретичних питань, правильна і повна відповідь на кожне з яких оцінюється в 20 балів.

Кожне запитання оцінюється в 20 балів за такими критеріями:

- «відмінно» – повна відповідь (не менше 90% потрібної інформації), надані відповідні обґрунтування та особистий погляд – 20 - 19 балів;
- «добре» – достатньо повна відповідь (не менше 75% потрібної інформації), що виконана згідно з вимогами до рівня «умінь», або незначні неточності) – 18…15 балів;
- «задовільно» – неповна відповідь (не менше 60% потрібної інформації. що виконана згідно з вимогами до «стереотипного» рівня та деякі помилки) – 14…12 балів;
- «незадовільно» – незадовільна відповідь – 0 балів.

Таблиця переведення рейтингових балів до оцінок за університетською шкалою

Рейтингові бали, RD	Оцінка за університетською шкалою
95 ≤ RD ≤ 100	Відмінно
85 ≤ RD ≤ 94	Дуже добре
75 ≤ RD ≤ 84	Добре
65 ≤ RD ≤ 74	Задовільно
60 ≤ RD ≤ 64	Достатньо
RD < 60	Незадовільно
Невиконання умов допуску	Не допущено

Робочу програму навчальної дисципліни (силабус):

Складено: доктор технічних наук, професор, професор кафедри ІБ Ланде Дмитро Володимирович

Ухвалено кафедрою інформаційної безпеки (протокол No5/2025 від 25.06.2025)

Погоджено Методичною комісією НН ФТІ (протокол No6/2025 від 30.06.2025)