




**Силабус навчальної дисципліни  
«МЕТОДИ ІДЕНТИФІКАЦІЇ  
АНОМАЛЬНИХ СТАНІВ ДЛЯ СИСТЕМИ  
ВИЯВЛЕННЯ ВТОРГНЕНЬ»**

**Спеціальність: 125 Кібербезпека  
Галузь знань: 12 Інформаційні технології**

<b>Рівень вищої освіти</b>	Доктор філософії
<b>Статус дисципліни</b>	Навчальна дисципліна вибіркового компонента фахового переліку
<b>Курс</b>	2 (другий)
<b>Семестр</b>	4 (четвертий)
<b>Обсяг дисципліни, кредити ЄКТС/загальна кількість годин</b>	5 кредитів/150 годин
<b>Мова викладання</b>	Українська
<b>Що буде вивчатися (предмет навчання)</b>	<p>Дана навчальна дисципліна є теоретичною та практичною основою сукупності знань та вмінь, що формують профіль фахівця в галузі безпеки інформаційних технологій.</p> <p>Місце даної дисципліни є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки.</p> <p>Використання методів фундаментальних наук для розв'язання загально інженерних, професійних та наукових задач; Генерація нових ідей і варіантів розв'язання задач в галузі кібербезпеки; Застосування сучасних методів та моделей ідентифікації аномальних станів для побудови систем виявлення вторгнень заснованих на теорії нечітких множин; Розробка та використання засобів, що розширюють функціональні можливості сучасних систем виявлення вторгнень.</p>
<b>Чому це цікаво/потрібно вивчати (мета)</b>	<p>Мета та завдання є застосування сучасних методів та засобів ідентифікації аномальних станів для ефективного виявлення існуючих і нових видів кібератак.</p>
<b>Чому можна навчитися (результати навчання)</b>	<p>ПРН4. Здатність та уміння використовувати математичний апарат (теорії нечітких множин, математичної статистики, теорії імовірності тощо) для освоєння теоретичних основ, моделювання даних, практичного використання (обробки експериментальних даних), розробки нових та удосконалення існуючих методів, засобів та систем у сфері інформаційної та кібербезпеки.</p> <p>ПРН5. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання ризиків інформаційної та/або кібербезпеки при побудові комплексних систем захисту інформації, систем управління інформаційною безпекою, аудит стану кібербезпеки.</p> <p>ПРН6. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем аналізу і оцінювання негативних наслідків (шкоди) державі, суспільству, приватній чи юридичній особі у разі витоку державних інформаційних ресурсів, інформації з обмеженим доступом.</p> <p>ПРН7. Здатність проводити дослідження, розвиток та удосконалення сучасних нейромережових моделей, методів, засобів та систем виявлення нових загроз, мережових кібератак, шкідливого</p>

	<p>програмного забезпечення, аналізу і оцінювання параметрів стану забезпечення активного захисту та кібербезпеки інформаційних (автоматизованих), інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури.</p> <p>ПРН8. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем виявлення вторгнень, визначати їх базові характеристики, а також обґрунтовано обирати та застосовувати в практичній роботі при побудові систем кібербезпеки.</p> <p>ПРН9. Здатність продемонструвати знання та розуміння застосування методів, моделей та засобів ідентифікації аномальних станів для побудови систем виявлення вторгнень заснованих на теорії нечітких множин.</p> <p>ПРН10. Вміти аналізувати, обґрунтовувати вибір та застосовувати методи фундаментальної та прикладної математики задля розв'язання задач аналізу, проектування і розробки елементів інтелектуальних систем кібербезпеки.</p> <p>ПРН11. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем кібербезпеки в умовах неповної визначеності.</p>
<p><b>Як можна користуватися набутими знаннями і вміннями (компетентності)</b></p>	<p>ФК3. Здатність та уміння проводити дослідження теоретичних, науково-технічних і технологічних проблем, пов'язаних із організацією, створенням методів та засобів забезпечення захисту інформації та/або кібербезпеки при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів.</p> <p>ФК4. Здатність та уміння проводити дослідження проблеми забезпечення інформаційної безпеки національних інтересів України, вивчати і обґрунтовувати форми та методи захисту людини, суспільства й держави від зовнішніх і внутрішніх загроз в інформаційній сфері, а також шляхи підвищення ефективності функціонування інформаційних систем держави в сучасних умовах.</p> <p>ФК5. Уміння застосовувати та розробляти сучасні технології, системи, технічні засоби, методи та моделі, бази даних та інші електронні ресурси, спеціалізоване програмне забезпечення у науковій, освітній та професійній діяльності;</p> <p>ФК7. Здатність та уміння проводити дослідження проблеми забезпечення функціонування інформаційних систем і технологій, інших бізнес-операційних процесів, інформаційні ресурси різних класів на об'єктах інформаційної діяльності та критичної інфраструктури, системи управління, на основі технології, методів, моделей та засобів у сфері інформаційної безпеки та/або кібербезпеки (пропозиція на основі стандарту магістра 125 «Кібербезпека»).</p>
<p><b>Навчальна логістика</b></p>	<p><b>Зміст дисципліни:</b> Кортежна модель формування атакуючих середовищ. Методи формування еталонного середовища для ідентифікації аномальних станів. Методи виявлення аномальних станів породжених кібератаками. Засоби розширення функціональних можливостей систем виявлення вторгнень.</p> <p><b>Види занять:</b> лекції, практичні</p> <p><b>Методи навчання:</b> навчальна дискусія, онлайн</p> <p><b>Форми навчання:</b> очна, заочна, дистанційна</p>
<p><b>Пререквізити</b></p>	<p>Теоретичною базою вивчення дисципліни є попередні навчальні дисципліни: «Правове, економічне та інформаційне забезпечення наукових досліджень», «Методологія наукових досліджень у сфері кібербезпеки», «Наукові розробки та дослідження у сфері інформаційної безпеки та кібербезпеки»</p>

	(у т.ч. наукової школи «Кібербезпеки» НАУ)», «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації», «Англійська мова наукового спрямування».
<b>Пореквізити</b>	Результати навчання даного курсу можуть бути використані під час написання кандидатської дисертації.
<b>Інформаційне забезпечення з фонду та репозитарію НТБ НАУ</b>	<b>Начальна та наукова література:</b> 1. С. Казмірчук, А. Корченко, Т. Паращук, «Аналіз систем виявлення вторгнень», Захист інформації, Т.20, №4, С. 259-276, 2018. 2. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с. 3. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. – 320 с.
<b>Локація та матеріально-технічне забезпечення</b>	Аудиторія теоретичного навчання, проектор
<b>Семестровий контроль, екзаменаційна методика</b>	Залік, тестування
<b>Кафедра</b>	Безпеки інформаційних технологій
<b>Факультет</b>	Кібербезпеки, комп'ютерної та програмної інженерії
<b>Викладач(и)</b>	 <p><b>Корченко Анна Олександрівна</b>  <b>Посада:</b> професор  <b>Вчене звання:</b> доцент  <b>Науковий ступінь:</b> д.т.н.  <b>Профайл викладача:</b> <a href="http://bit.nau.edu.ua/sklad/124">http://bit.nau.edu.ua/sklad/124</a>  <b>Тел.:</b> +38044 4067642  <b>E-mail:</b> <a href="mailto:anna.korchenko@npp.nau.edu.ua">anna.korchenko@npp.nau.edu.ua</a>  <b>Робоче місце:</b> 11.424</p>
<b>Оригінальність навчальної дисципліни</b>	Авторський курс, викладання українською мовою
<b>Лінк на дисципліну</b>	