	Силабус навчальної дисципліни **«СУЧАСНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ»** **Спеціальність: 125 Кібербезпека** **Галузь знань: 12 Інформаційні технології**
Рівень вищої освіти	Доктор філософії
Статус дисципліни	Навчальна дисципліна вибіркового компонента фахового переліку
Курс	2 (другий)
Семестр	4 (четвертий)
Обсяг дисципліни, кредити ЄКТС/загальна кількість годин	5 кредитів/150 годин
Мова викладання	Українська
Що буде вивчатися (предмет навчання)	Дана навчальна дисципліна є теоретичною та практичною основою сукупності знань та вмінь, що формують профіль фахівця в галузі безпеки інформаційних технологій. Місце даної дисципліни є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця в області кібербезпеки. Вивчення сучасних типів та видів кібератак, а також їх класифікацій; базових характеристик систем виявлення вторгнень; Застосовувати на практиці відкриті системи виявлення вторгнень та ознайомлення з сучасними програмно-апаратними засобами виявлення вторгнень.
Чому це цікаво/потрібно вивчати (мета)	Мета та завдання є ознайомлення з сучасними кібератаками та з основними методами, засобами та системами виявлення вторгнень, а також їх використання для ресурсів інформаційних систем.
Чому можна навчитися (результати навчання)	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. 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. ПРН7. Здатність проводити дослідження, розвиток та удосконалення сучасних нейромережевих моделей, методів, засобів та систем виявлення нових загроз, мережевих кібератак, шкідливого програмного забезпечення, аналізу і оцінювання параметрів стану забезпечення активного захисту та кібербезпеки інформаційних (автоматизованих), інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури. 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. ПРН9. Здатність продемонструвати знання та розуміння застосування методів, моделей та засобів ідентифікації аномальних станів для

	побудови систем виявлення вторгнень заснованих на теорії нечітких множин. ПРН10. Вміти аналізувати, обґрунтовувати вибір та застосовувати методи фундаментальної та прикладної математики задля розв'язання задач аналізу, проектування і розробки елементів інтелектуальних систем кібербезпеки. ПРН11. Здатність проводити дослідження, розвиток та удосконалення сучасних моделей, методів, засобів та систем кібербезпеки в умовах неповної визначеності.
Як можна користуватися набутими знаннями і вміннями (компетентності)	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. 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. 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; 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.
Навчальна логістика	**Зміст дисципліни:** Сучасні методи та засоби виявлення вторгнень. Класифікація сучасних атак. Базові характеристики систем виявлення вторгнень. Відкриті системи виявлення вторгнень. Програмні та програмно-апаратні засоби виявлення вторгнень. **Види занять:** лекції, практичні **Методи навчання:** навчальна дискусія, онлайн **Форми навчання:** очна, заочна, дистанційна
Пререквізити	Теоретичною базою вивчення дисципліни є попередні навчальні дисципліни: «Інноваційні методи прийняття рішень в соціотехнічних та соціокультурних системах», «Правове, економічне та інформаційне забезпечення наукових досліджень», «Методологія наукових досліджень у сфері кібербезпеки», «Наукові розробки та дослідження у сфері інформаційної безпеки та кібербезпеки (у т.ч. наукової школи «Кібербезпеки» НАУ)», «Теоретико-множинне моделювання даних для вирішення задач кібербезпеки/захисту інформації», «Англійська мова наукового спрямування».
Пореквізити	Результати навчання даного курсу можуть бути використані під час написання кандидатської дисертації.

Інформаційне забезпечення з фонду та репозитарію НТБ НАУ	**Начальна та наукова література:** 1. Анна Корченко, Методи ідентифікації аномальних станів для систем виявлення вторгнень. Монографія, Київ, ЦП «Компринт», 2019 – 361 с. 2. І. Терейковський, А. Корченко, Т. Паращук, Є. Педченко, «Аналіз відкритих систем виявлення вторгнень», Безпека інформації. Т.24, №3, С. 201-216, 2018. 3. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020. –678 с. 4. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа – Львів: «Магнолія 2006», 2018 – 320 с.
Локація та матеріально-технічне забезпечення	Аудиторія теоретичного навчання, проектор
Семестровий контроль, екзаменаційна методика	Залік, тестування
Кафедра	Безпеки інформаційних технологій
Факультет	Кібербезпеки, комп'ютерної та програмної інженерії
Викладач(і)	 **Корченко Анна Олександрівна** **Посада:** професор **Вчене звання:** доцент **Науковий ступінь:** д.т.н. **Профайл викладача:** http://bit.nau.edu.ua/sklad/124 **Тел.:** +38044 4067642 **E-mail:** anna.korchenko@npp.nau.edu.ua **Робоче місце:** 11.424
Оригінальність навчальної дисципліни	Авторський курс, викладання українською мовою
Лінк на дисципліну	

Завідувач кафедри О. Корченко

Розробник А. Корченко