**(Ф 21.01 - 03)**

|  |  |
| --- | --- |
|  | **Силабус навчальної дисципліни****«ЦИФРОВА КРИМІНАЛІСТИКА»****Освітньо-професійної програми «Управління інформаційною безпекою»****Галузь знань: 12  «Інформаційні технології»****Спеціальність: 125 «Кібербезпека»** |
| **Рівень вищої освіти**(перший (бакалаврський), другий (магістерський) | Перший (бакалаврський) |
| **Статус дисципліни** | Навчальна дисципліна вибіркового компонента з фахового переліку |
| **Курс** | 4 (четвертий) |
| **Семестр** | 8 (восьмий) |
| **Обсяг дисципліни,****кредити ЄКТС/години** | 4 кредити /120 годин |
| **Мова викладання** | Українська |
| **Що буде вивчатися (предмет вивчення)** | Концепції, методи та інструменти цифрової криміналістики, зосереджені на зборі, аналізі та використанні інформації з відкритих джерел (Open Source Intelligence, OSINT) для розслідувань у сфері кіберзлочинів, економічних правопорушень, воєнних злочинів і забезпечення інформаційної безпеки. |
| **Чому це цікаво/треба вивчати (мета)** | Курс спрямований на формування теоретичних знань та практичних навичок із використання методів і інструментів OSINT для проведення розслідувань цифрових злочинів, аналізу відкритих даних, збору доказів і забезпечення інформаційної безпеки у різних сферах. |
| **Чому можна навчитися (результати навчання)** | * Розуміння принципів цифрової криміналістики та OSINT.
* Здатність збирати та аналізувати дані з відкритих джерел для розслідувань.
* Вміння використовувати спеціалізовані OSINT-інструменти.
* Розуміння правових і етичних аспектів застосування OSINT у криміналістиці.
* Здатність інтегрувати OSINT-дані в загальний процес цифрового розслідування.
 |
| **Як можна користуватися набутими знаннями і уміннями (компетентності)** | Набуті знання та вміння дозволять:* Проводити розслідування цифрових злочинів із використанням відкритих джерел інформації (OSINT).
* Здійснювати пошук, аналіз та перевірку даних із відкритих цифрових джерел.
* Виявляти та документувати цифрові сліди злочинної діяльності для їх використання в судових процесах.
* Застосовувати OSINT-інструменти для дослідження економічних злочинів, шахрайства, корупції та легалізації доходів.
* Використовувати дані OSINT для розслідування воєнних злочинів і документування доказів.
* Забезпечувати інформаційну безпеку через моніторинг та оцінку відкритих даних.
* Дотримуватись етичних стандартів та захищати конфіденційну інформацію у процесі OSINT-розслідувань.
 |
| **Навчальна логістика** | **Зміст дисципліни:** Поняття OSINT. OSINT та суміжні дисципліни розвідки. Етапи OSINT розслідування. Захист персональних даних та OSINT. Пошукові системи та онлайн-ресурси для OSINT. Інструменти для збору даних із соціальних мереж. Методи збору та аналізу метаданих. Використання картографічних даних і геолокаційних інструментів. Аналіз зображень та відео за допомогою OSINT-інструментів. Поняття електронних доказів у кримінальному процесі. Достовірність електронних доказів. Особливості збирання електронних доказів у кримінальному провадженні. Розслідування в сфері кіберзлочинів. Використання OSINT у розслідуванні економічних злочинів. Протидія тероризму та міжнародним злочинам за допомогою OSINT. Розслідування воєнних злочинів за допомогою відкритих даних.**Види занять:** лекції, лабораторні заняття**Методи навчання:** мультимедійні презентації, кейс-стаді, використання онлайн-ресурсів**Форми навчання:** очна, заочна |
| **Пререквізити** | Загальні та фахові знання з галузі інформаційних технологій, отримані на першому (бакалаврському) рівні вищої освіти. |
| **Пореквізити** | Знання та вміння, можуть бути використані під час написання курсових робіт та є базовими для вивчення суміжних дисциплін, пов'язаних з правом, безпекою та інформаційними технологіями. |
| **Інформаційне забезпечення****з репозитарію та фонду НТБ ДУ «КАІ»** | **Навчальна та наукова література:**1. Ланде Д. В.OSINT у кібербезпеці : навч. пос.Київ : ТОВ "Інжиніринг", 2024. 522 с. ISBN 978-966-2344-97-4.
2. Торбас О. О.OSINT при розслідуванні кримінальних правопорушень : підручник.Одеса : Видавництво «Юридика», 2024. 180 с. ISBN 978-617-8182-13-7.
3. Самойленко О. А.Протидія кіберзлочинам: криміналістичний аспект: навчально-методичний посібник.Одеса, 2020. 133 с.
4. Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. та ін**.** Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком.за заг. ред. О. В. Корнейка. 2-ге вид., доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.
5. Скрипник А. В.Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія.Харків : Право, 2022. 408 с.
 |
| **Локація та матеріально-технічне забезпечення** | Навчальні та мультимедійні аудиторії, проектор |
| **Семестровий контроль, екзаменаційна методика** | Диф. залік, модульний контроль |
| **Кафедра** | Кібербезпеки |
| **Факультет** | Комп’ютерних наук та технологій |
| **Викладач(і)** | **https://lh7-rt.googleusercontent.com/docsz/AD_4nXf_pmeyJAiGibnybhJPWoMh4bCp10s8Hbuf233gMygNydGM5ulWxNkkQsul5tIxjhJnNqTgtZpKoLavM5FX4fsifjY7-a8LQfjdzanxOqM17t8C7Ho5D840_PSr4GNDkp8wd0w6YypTJmHKGEUgZ1U?key=alRG6QO9GB7NeaOk_jYV5xY-** | **Різак Михайло Васильович****Посада:** доцент**Профайл викладача:** http://kszi.nau.edu.ua/pro-kafedru-menu/kadrovij-sklad/39-vukladachi/256-rizak-mikhajlo-vasilovich**Тел.:** 0444067642**E-mail**:  mykhailo.rizak@npp.nau.edu.ua**Робоче місце:** 11.424 |
|  | **https://lh7-rt.googleusercontent.com/docsz/AD_4nXcCTmmZqNyKjMY89UJiZillt7BsVdenVAgJj5q0LDvwIPkLNrx1V9X0hW3gvj9lI-uN5XKj7qINK7QmDwBx7m8uGdpBneh6nAVNBR5D2X8hkRvbPdnTHfYm6vaZCXz7OCLc8rHUzrQuJlT9Od3IyA?key=alRG6QO9GB7NeaOk_jYV5xY-** | **Лозова Ірина Леонідівна****Посада:** старший викладач**Профайл викладача:** http://kszi.nau.edu.ua/pro-kafedru-menu/kadrovij-sklad/39-vukladachi/250-lozova-irina-leonidivna**Тел.:** 0444067642**E-mail**:  iryna.lozova@npp.nau.edu.ua**Робоче місце:** 11.424 |
| **Оригінальність навчальної дисципліни** | Авторський курс |
| **Лінк на дисципліну** | https://classroom.google.com/c/NzQ2ODczOTU0NzUz |