Дисципліна	Вибіркова дисципліна 1.1 «Розвідка OSINT»
Рівень ВО	Бакалавр
Назва спеціальності/освітньо-професійної програми	256 Національна безпека / ОПП Забезпечення національної безпеки силами національного спротиву
Форма навчання	Денна
Курс, семестр, протяжність	Курс 2, семестр 1, протягом семестру
Семестровий контроль	Залік
Обсяг годин (усього: з них лекції/практичні)	150 годин (5 кредитів ECTS): з них лекції – 10 годин / практичні – 20 годин
Мова викладання	Українська
Кафедра, яка забезпечує викладання	Кафедра державної безпеки
Автор дисципліни	Стрелков Владислав Володимирович Ph.D., асистент кафедри державної безпеки.
Короткий опис	
Вимоги до початку вивчення	Повна загальна середня освіта. Базові знання інформаційних технологій та володіння персональним комп'ютером на рівні користувача.
Що буде вивчатися	Методики Open source intelligence (OSINT) – шляхи добування розвідувальної інформації з відкритих джерел даних.
Чому це цікаво/треба вивчати	Курс надасть вам інструменти для підвищення рівня ситуаційної обізнаності. Ви дізнаєтеся де шукати необхідну вам інформацію та яким чином її шукати. Отримаєте базові навички безпечної роботи в кіберпросторі.
Чому можна навчитися (результати навчання)	ПРЗ 1. Застосовувати отримані знання про поняття, зміст, складові та суб'єкти забезпечення основних сфер національної безпеки (воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки та кібербезпеки) під час організації професійної діяльності. ПРЗ 2. Використовувати законодавство, вітчизняний та зарубіжний досвід у сферах забезпечення національної безпеки і оборони, здійснювати науковий аналіз їх сучасного стану. ПРУ 3. Здатність відповідально ставитись до виконання службової діяльності, самостійно приймати рішення, досягати поставленої мети з дотриманням вимог професійної етики. ПРУ 4. Демонструвати уміння вирішувати проблеми та приймати інноваційні рішення, мислити та застосовувати здібності до формування принципово нових ідей. ПРК 4. Ефективно працювати із засобами масової

	інформації. ПРАіВ 3. Виявляти внутрішні та зовнішні загрози, умови, джерела походження та граничні показники, моніторити розвиток та оцінювати їх можливі наслідки, давати експертизу рішень, що приймаються з точки зору безпеки. ПРАіВ 5. Розробляти та проводити загальні і спеціальні заходи з безпеки, які реалізуються в усіх напрямах і видах діяльності суб'єктів господарювання.
Як можна користуватися набутими знаннями й уміннями (компетентності)	ЗК 2. Здатність до абстрактного мислення, аналізу та синтезу. ЗК 3. Здатність застосовувати знання у практичних ситуаціях. ЗК 4. Знання та розуміння предметної області та розуміння професійної діяльності. ЗК 6. Навички використання інформаційних і комунікаційних технологій. ЗК 7. Здатність вчитися і оволодівати сучасними знаннями. ЗК 8. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК 9. Вміння виявляти, ставити та вирішувати проблеми. ФК 1. Здатність здійснювати професійну діяльність з урахуванням потреб забезпечення сфер національної безпеки і оборони держави. ФК 2. Здатність аналізувати та розуміти сучасний стан і тенденції розвитку міжнародних відносин, їх вплив на національну безпеку і оборону держави, об'єктивний характер європейських та євроатлантичних інтеграційних процесів, шляхи досягнення сумісності із збройними силами країн Організації Північноатлантичного договору (НАТО). ФК 3. Здатність формувати та вдосконалювати організаційні структури та створювати відповідні умови для забезпечення безпеки. ФК 4. Здатність розробляти та проводити загальні і спеціальні заходи з безпеки, які реалізуються в усіх напрямах і видах діяльності суб'єктів господарювання. ФК 5. Здатність кваліфіковано давати рекомендації керівникам підрозділів відділів, установ та органів з питань, пов'язаних з проблемами забезпечення безпеки. ФК 7. Здатність збирати, обробляти, оцінювати й аналізувати інформацію з різних джерел, використовувати методи обробки інформації, профілювання ризиків, використовувати програмне забезпечення для оцінки обстановки,

	прийняття рішень та оцінки ефективності застосування підрозділів.
Інформаційне забезпечення та/або web-покликання	1. NATO OSINT Handbook v1.2 URL: https://github.com/lawsecnet/OPSEC/blob/master/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf 2. Soesanto S. The IT Army of Ukraine: Structure, Tasking, and Ecosystem. Zürich : Center for Security Studies (CSS), 2022. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf 3. Bielska A. Open source intelligence Tools and resources handbook. URL: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf 4. Курбан О. Сучасні інформаційні війни в мережевому онлайн просторі: навчальний посібник. Київ : ВІКНУ, 2016. 286 с. URL:http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf 5. Кожушко О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. Науковий вісник Національного авіаційного університету. № 4. 2011. URL:https://jrnl.nau.edu.ua/index.php/IMV/article/view/3264