МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри інформаційних систем
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(протокол №15/23 від 29 серпня 2023 р.)

Завідувач кафедри Венгерський П.С.

Силабус з навчальної дисципліни

“Розширені інструменти SecOps”,

що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	Розширені інструменти SecOps
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека
Викладачі дисципліни	Карпюк Роман Валентинович, асистент\аспірант кафедри кібербезпеки
Контактна інформація викладачів	roman.karpiuk@lnu.edu.ua
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна “Розширені інструменти SecOps” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека яка викладається в 8-му семестрах в обсязі 6 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про використання актуальних методів та засобів щодо забезпечення кібебезпеки в організації. Також розуміння основних принципів побудови та функціонування центрів з протидії кіберзагрозам (CSOC).
Мета та цілі дисципліни	Метою курсу є формування у студентів уявлення про сучасні рішення в сфері кібербезпеки. Поглибити їхні знання в межах специфічного інструментарію, до прикладу як: honeypots, BAS, DRP etc.
Література для вивчення дисципліни	**Основна** 1. Cybersecurity for Information Professionals: Concepts and Applications, Hsia-Ching Chang, Suliman Hawamdeh, 2020 2. Red Team Development and Operations: A practical guide, Joe Vest, James Tubberville, 2020 3. Operator Handbook: Red Team + OSINT + Blue Team Reference, Joshua Picolet, 2020 4. Cybersecurity A Complete Guide, Gerardus Blokdyk , 2021 5. Cyber Attack Survival Manual: From Identity Theft to The Digital Apocalypse: and Everything in Between, Heather Vescent, Nick Selby, 2020
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 70год., з них 28 год. лекцій та 42 год. лабораторних робіт. Самостійної роботи: 100 год.

Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** - мету використання додаткового інструментарію - вузькі домени застосування - актуальність тих чи інших рішень **вміти:** - обґрунтувати необхідність впровадження інструменту - базово використовувати інструментарій - будувати комплексний підхід до роботи з багатьма вузькоспеціалізованими інструментами Курс забезпечує набуття таких компетентностей: КЗ 1, КЗ 2, КЗ 5, КФ 2, КФ 3, КФ 5, КФ 8, КФ 9, КФ 11, КФ 12 ; та програмних результатів навчання: ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 9, ПРН 10, ПРН 11, ПРН 12, ПРН 13, ПРН 14, ПРН 15, ПРН 16, ПРН 17, ПРН 18, ПРН 19, ПРН 20, ПРН 22, ПРН 27, ПРН 28, ПРН 29, ПРН 30, ПРН 31, ПРН 33, ПРН 34, ПРН 39, ПРН 41
Ключові слова	Кібербезпека, кібератака, blueteam, redteam, виявлення, DLP, BAS, DRP, CASB, SOAR, TI, XDR, Threat Hunting
Формат курсу	Очний.
Теми	Теми подані у Схемі курсу нижче
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1. Основи кібербезпеки 2. Операційні системи 3. Мережеві технології 4. Математичні основи криптографії 5. Організація ІТ на підприємстві 6. Менеджмент інформаційної безпеки
Підсумковий контроль, форма	Залік у кінці семестру
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції, практичні завдання у вигляді імітації атаки на систему, комплексної аналітики щодо розслідування атаки, формування звіту щодо інциденту та захисту звіту перед умовним CISO, RangeForce платформа.
Необхідне обладнання	Комп’ютери, комп’ютерні системи та мережі. Віртуальні машини. Інтернет ресурси. Додаткове програмне забезпечення у вигляді trial-версій для типових інструментів з кібербезпеки.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування: 50% семестрової оцінки; максимальна кількість балів 50 • залік: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в

	роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахуванння викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. П**олітика виставлення балів.** Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до контролю.	1. Як використовуються платформи SOAR (Security Orchestration, Automation, and Response) для автоматизації реагування на кіберзагрози в SecOps? 2. Які конкретні переваги використання інтегрованих рішень SOAR у контексті розширених інструментів SecOps? 3. Які бази безпеки (BAS) застосовуються для створення об'єднаних інформаційних баз даних для аналізу потоків даних в SecOps? 4. Як платформи Digital Risk Protection (DRP) допомагають забезпечити проактивне виявлення потенційних атак? 5. Як Honeypots використовуються для приваблення та виявлення потенційних злочинців в мережі в рамках розширених інструментів SecOps? 6. Як використовуються інструменти Threat Intelligence для інтеграції з Honeypots та аналізу стеження за загрозами в реальному часі? 7. Які механізми автоматизованого реагування вбудовані в системи SOAR для ефективного контролю за інцидентами в SecOps? 8. Які технології Threat Hunting використовуються для активного пошуку потенційних загроз в мережі в контексті розширених інструментів SecOps? 9. Які конкретні інструменти для аналізу поведінки загроз використовуються в системах SecOps? 10. Які технології виявлення та захисту від зловмисного програмного забезпечення (Malware) використовуються в рамках розширених інструментів SecOps? 11. Які інструменти для аналізу вмісту пакетів даних використовуються для виявлення потенційно шкідливих дій в мережі в реальному часі? 12. Які конкретні методи використовуються для розгортання та управління Honeynets в контексті SecOps? 13. Як системи BAS допомагають у формуванні звітів та аналізі безпеки для вдосконалення стратегій SecOps? 14. Як DRP і SOAR взаємодіють для максимізації ефективності відновлення після кібератаки в SecOps?

	15. Як використовуються інтелектуальні системи SOAR для розпізнавання та класифікації різних типів кіберзагроз? 16. Які методи інтеграції Threat Intelligence з Honeypots сприяють збільшенню ефективності виявлення загроз в мережі? 17. Які основні характеристики інструментів для Threat Hunting допомагають аналізувати великі обсяги даних та виявляти потенційні загрози? 18. Як системи SOAR автоматизують процеси взаємодії між різними рішеннями в рамках SecOps для швидкого реагування на інциденти? 19. UEBA – наступний крок після SIEM чи доповнення?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

тиж	Тема, план, короткі тези	Форма діяльності/ заняття	Література. Інтернет-ресурси	Термін виконання
1	**Introduction to the course**	лекція – 2 год лабораторна – 2 год самостійна робота – 6год	[1-5]	тиждень
2	**Threat Intelligence**	лекція – 2 год лабораторна – 4 год самостійна робота – 8 год		тиждень
3-4	**Bridge Attack Simulation (BAS)**	лекція – 2 год лабораторна – 6 год самостійна робота – 16 год		2 тижні
5	**Digital Risk Protection (DRP)**	лекція – 2 год лабораторна – 4год самостійна робота – 6 год		тиждень
6	**Security Orchestration, Automation and Response (SOAR)**	лекція – 2 год лабораторна – 2 год самостійна робота – 6год		тиждень
7-8	**User and entity behavior analytics (UEBA)**	лекція – 4 год лабораторна – 4 год самостійна робота – 16 год		2 тижні
9	**Extended Detection and Response (XDR)**	лекція – 2 год лабораторна – 2 год		тиждень

		самостійна робота – 6 год		
10	**Cloud Access Security Broker (CASB)**	лекція – 2 год лабораторна – 6год самостійна робота – 16 год		тиждень
11	**Conditional Access**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
12	**Identity Protection**	лекція – 2 год лабораторна – 4 год самостійна робота – 6 год		тиждень
13	**Honeypots**	лекція – 2 год лабораторна – 2 год самостійна робота – 6 год		тиждень
14	**Threat Hunting**	лекція – 4год лабораторна – 4 год самостійна робота – 12год		2 тижні