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

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та
інформатики
Львівського національного університету
імені Івана Франка
(протокол № _/__ від __ _____ 2023 р.)

Завідувач кафедри .

Венгерський П.С.

Силабус з навчальної дисципліни "Мережева безпека та виявлення вторгнень", що викладається в межах ОПП Кібербезпека другого (магістерського) рівня вищої освіти для здобувачів з спеціальності 125 – Кібербезпека

Львів 2023 р.

Назва дисципліни	Мережева безпека та виявлення вторгнень
Адреса викладання дисципліни	Львів, вул. Університетська 1
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	Брич Тарас Богданович, доцент кафедри кібербезпеки
Контактна інформація викладачів	taras.brych@lnu.edu.ua
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньоюдомовленістю).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна “Мережева безпека та виявлення вторгнень” є дисципліною за вибором зі спеціальності 125 – кібербезпека для освітньої програми Кібербезпека, яка викладається в 1-му семестрі в обсязі 4-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про безпеку інформаційних мереж та засоби виявлення вторгнень, розуміння основних принципів протидії кіберзагрозам.
Мета та цілі дисципліни	Метою курсу є формування у студентів знань про джерела інформації про кібератаки та інструменти, які можуть бути застосовані для збору, обробки даних про вторгнення та захисту інформаційних мереж від атак.
Література для вивчення дисципліни	1. Перелік загальних недоліків – https://cwe.mitre.org/ 2. MITRE ATT&CK – https://attack.mitre.org/matrices/enterprise/ 3. BLEEPING COMPUER – https://www.bleepingcomputer.com/ 4. SANS – https://www.sans.org/ 5. FIRST is the global Forum of Incident Response and Security Teams – https://www.first.org/ 6. *Chris Sanders.* PRACTICAL PACKET ANALYSIS. 3-RD EDITION. Usng Wireshark to Solve Real-World Problems.San Francisco. 2017. 450 p. 7. *James D. Miller* Implementing Splunk 7. Third Edition. Effective operational intelligence to transform machine-generated data into valuable business insightr. Packt Publishing. 2018. 490 p 8. J. Muniz, A. Lakhani. Web Penetration Testing with Kali Linux – http://marcel.marcelandkim.com/ruby/Web_Penetration_Testing_with_Kali_Linux.pdf 9. K. Knerler, I. Parker, Carson Zimmerman. 11 Strategies of a World-class Cybersecurity Operations Center. MITRE. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 56 год.

Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** сервіси безпеки, зокрема екранування, протоколювання та аудит; основні методи, засоби, апаратне та програмне забезпечення виявлення атак; аналізу вразливостей конфігурації, архітектури та програмного коду, що використовується в інформаційних системах. **вміти:** вирішувати завдання захисту інформації, яка обробляється в локальних мережах; проводити профілювання мережі, загальну оцінку вразливості CVSS; проводити безпечне управління пристроями, які використовуються в мережі підприємства; використовувати системи управління інформаційною безпекою ISMS Курс забезпечує набуття таких компетентностей: КЗ 2, КЗ 5, КФ 2, КФ 4, КФ 9, КФ 12 ; та програмних результатів навчання: ПРН 23, ПРН 25, ПРН 26, ПРН 30, ПРН 31, ПРН 49, ПРН 50, ПРН 52.
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, локальні мережі, IDS, IPS, DLP, NGFW, EDR\XDR, SIEM, SOAR, SOC.
Формат курсу	змішаний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Тема 1. Інфраструктура мережевої безпеки. Мережеві топології. Пристрої безпеки. Служби безпеки. Тема 2. Зловмисники та їх інструменти. Мережевий моніторинг. Тема 3.Загрози . Моделі контролю доступом. Джерела контролю загроз. Тема 4. Точка доступу, як елемент мережі. Оцінка вразливості та захист. Тема 5. Дані мережної безпеки. Технології та протоколи. Alert, Session and Transaction Data, Full Packet Captures, Статистичні дані. Тема 6. Робота з даними мережевої безпеки. Оцінка попереджень. Тема 7. Аналіз та реагування на інциденти. Цифрова криміналістика.
Підсумковий контроль, форма	залік у кінці семестру

Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції. Модульний контроль
Необхідне обладнання	Комп'ютери, комп'ютерні системи та мережі. Віртуальні машини. Інтернет ресурси. Додаткове програмне забезпечення у вигляді trial-версійдля 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, усне опитування: 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. **Політика 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 екзамену.	1. Віртуальні машини, контейнери, хмарні сервіси, пісочниці. Приклади. 2. Security Onion. 3. Kali linux. 4. Tails. 5. Parrot. 6. CSI Linux. 7. Tsurugi Linux. 8. IDS, IPS, DLP. Класифікація, функціонал, призначення, приклади. 9. Мережні топології. Типи, класифікація, фізична та логічна діаграми топологій. 10. DMZ – характеристика , принципи використання. 11. ZPF - Zone-based policy firewalls. 12. Пристрої безпеки. AMP – Advanced Malware Protection. WSA – Web Security Appliance. ESA – Email Security Appliance. Функціонал, призначення. 13. Служби безпеки. ACL – Access Control List, SNMP – Simple Network Management Protocol. 14. Служби безпеки. NetFlow, Port Mirroring. Функціонал, призначення. 15. Сервери Syslog. Функціонал, призначення. 16. NTP – Network Time Protocol. Функціонал, призначення. 17. AAA – Authentication-Authorization-Accounting. Функціонал, призначення. 18. VPN – Virtua Private Network. Функціонал, призначення, приклади. 19. Профілювання мережі. Елементи мережного профілю. 20. Профілювання сервера. Елементи профілю сервера. 21. Аналіз поведінки мережі (network behavior analysis – NBA). 22. CVSS (Common Vulnerability Scoring System. 23. Метричні групи CVSS. 24. Джерела інформації про вразливості (Common Vulnerabilities and Exposures – CVE, National Vulnerability Database – NVD, Forum of Incident Response and Security Teams – FIRST). 25. Безпечне управління пристроями. Управління ризиками, вразливостями, активами. 26. Безпечне управління пристроями. Mobile device management MDM. Управління конфігураціями та оновленнями (Patch Management). 27. NIST Cybersecurity Framework. 28. Information Security Management System ISMS. 29. Моніторинг мереженої безпеки (NSM) – джерела попереджень. 30. Оцінювання попереджень NSM. 31. ELK. Функціонал, склад, призначення. 32. Logstash. Функціонал, склад, призначення. 33. Beats. Функціонал, склад, призначення. 34. Elasticsearch. Функціонал, склад, призначення. 35. Kibana. Функціонал, склад, призначення. 36. Network security management. Data Reduction, Normalization, Archiving. 37. Процес цифрової криміналістики. 38. Порядок збору доказів у цифровій криміналістиці. Послідовність зберігання та забезпечення цілісності доказів у цифровій криміналістиці. 39. Атрибути атаки. TTP - Tactics, Techniques, and Procedures. MITRE ATT & CK. Функціонал, призначення.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.