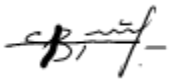
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

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



Завідувач кафедри Венгерський П.С.

Силабус з навчальної дисципліни "Адміністрування систем захисту інформації", що викладається в межах ОПП Кібербезпека та захист інформації першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	Адміністрування систем захисту інформації
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 та захист інформації
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 (а також за розкладом консультацій кафедри).
Сторінка курсу	https://ami.lnu.edu.ua/admission/specializations
Інформація про дисципліну	Дисципліна "Адміністрування систем захисту інформації" є дисципліною за вибором із спеціальності 125 Кібербезпека та захист інформації для освітньої програми першого (бакалаврського) рівня вищої освіти, яка викладається в 6-му семестрі в обсязі 5-и кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про адміністрування систем захисту інформації, розуміння основних принципів протидії кіберзагрозам, розбудови та організації роботи SOC.
Мета та цілі дисципліни	Метою курсу є формування у студентів знань для створення, організації роботи, забезпечення персоналом, повноважень, інструментарію та ресурсів для адміністрування системами захисту інформації.
Література для вивчення дисципліни	Основна література 1. *Kathryn Knerler, Ingrid Parker, Carson Zimmerman.* 11 Strategies of a World-Class Cybersecurity Operations Center. The MITRE Corporation.. 2022. 452 p. 2. C. Crowley, "Common and Best Practices for Security Operations Centers: Resultsof the 2019 SOC Survey," 2019. [Online]. Available: https://www.sans.org/media/ analyst-program/common-practices-security-operations-centers-results-2019-soc- survey-39060.pdf. 3. S. K. White, "IT Asset Management (ITAM): A Centralized Approach to ManagingIT Systems and Assets," CIO, 11 September 2019. [Online]. Available: https://www. cio.com/article/3437476/it-asset-management-itam-a-centralized-approach-to- managing-it-systems-and-assets.html. 4. Google Cloud, Deloitte, "Future of the SOC: SOC People: Skills not Tiers," 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/ about-deloitte/Deloitte_and_Chronicle_Future_of_the_SOC-Skills_Before_Tiers.pdf. Додаткова література 5. National Institute of Standards and Technology (NIST), "Security and Privacy Controls for Information Systems and Organizations," December 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final. 6. European Union - Horizon 2020 Programme Framework, "General Data Protection Regulation (GDPR) Compliance Guidelines," November 2021. [Online]. Available: https://gdpr.eu/. 7. MITRE ATT&CK – https://attack.mitre.org/matrices/enterprise/

	8. FIRST is the global Forum of Incident Response and Security Teams – https://www.first.org/ Cybersecurity and Infrastructure Security Agency (CISA), "CISA Insider Threat Mitigation," November 2021. [Online]. Available: https://www.cisa.gov/insider-threat- mitigation.
Обсяг курсу	Загальний обсяг: 150 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 86 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути такихкомпетентностей: **знати:** функції SOC, сервіси безпеки, адміністрування локальних мереж з використанням систем управління інформаційною безпекою – ISMS. **вміти:** Організувати та враховувати численні функції в оперативних центрах кібербезпеки (SOC) та сучасні стратегії, які можна застосувати в SOC будь-якого розміру, від двох осіб до великих багатонаціональних центрів із сотнями людей. Курс забезпечує набуття таких компетентностей: КІ, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 1-5, КФ 7, КФ 9, КФ-14; та програмних результатів навчання: ПРН 2-31, ПРН 35, ПРН 44-46.
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, локальні мережі, IDS, IPS, DLP, NGFW, EDR\XDR, SIEM, SOAR, SOC.
Формат курсу	Очний
Теми	Тема 1 Системи управління інформаційною безпекою - ISMS (Information Security Management Systems. Тема 2. Безпечне управління пристроями, мобільними пристроями, конфігураціями.. Тема 3. Створення SOC відповідно вимог та потреб організації. Активи, які необхідно захищати, повноваження. Тема 4. Вимоги до персоналу SOC – підбір, навчання. Тема 5. Пріоритети реагування на інциденти. Аналіз кіберзагроз. Тема 6. Вибір необхідних даних для збереження та аналізу. Тема 7. Підбір необхідних інструменти аналітиків SOC. Тема 8. Вимірювання продуктивності роботи SOC. Робота з інформацією галузі кібербезпеки.
Підсумковий контроль, форма	залік
Пререквізити	Для вивчення курсу студенти потребують базових знань з: - Основи кібербезпеки - Організація IT на підприємстві(ITIL) - Безпека комп'ютерних мереж - Менеджмент інформаційної безпеки - Оцінка ризиків в кібербезпеці
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції. лабораторні роботи, індивідуальні завдання, індивідуальні доповіді, самостійна робота
Необхідне обладнання	Комп'ютери, доступ до мережі Internet.

Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються занаступним співвідношенням: • тестування, усне опитування: 50% семестровоїоцінки; максимальна кількість балів 50 • Модульні роботи 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 недобро- чесності 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 виз- начених 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 мо- більними 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.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу " Адміністрування систем захисту інформації "

Тиж.	**Тема, план, короткі тези**	**Форма діяльності (заняття)**	**Література**	**Завдання, год**	**Термін виконання**
1-2	Тема 1 Системи управління інформаційною безпекою - ISMS (Information Security Management Systems.	лекція, лаб, самостійна робота	[7, 8, 9]	4 8 12	2 тижні
3-4	Тема 2. Безпечне управління пристроями, мобільними пристроями, конфігураціями..	лекція, лаб, самостійна робота	[5,6, 9]	4 8 12	2 тижні
5-6	Тема 3. Створення SOC відповідно вимог та потреб організації. Активи, які необхідно захищати, повноваження.	лекція, самостійна робота	[1, 2, 6]	6 8 14	2 тижнів
7-8	Тема 4. Вимоги до персоналу SOC – підбір, навчання.	лекція, самостійна робота	[1, 2, 6]	4 8 10	2 тижні
9-10	Тема 5. Пріоритети реагування на інциденти. Аналіз кіберзагроз.	лекція, самостійна робота	[1, 2, 6, 3, 5]	4 8 10	2 тижні
10-12	Тема 6. Вибір необхідних даних для збереження та аналізу.	лекція, лаб, самостійна робота	[3, 7, 8, 9]	4 8 14	3 тижні
13-16	Тема 7. Підбір необхідних інструменти аналітиків SOC.	лекція, лаб, самостійна робота	[3, 4, 6, 8, 9]	4 8 14	3 тижні