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 П.С.Венгерський

Силабус з навчальної дисципліни «Менеджмент інформаційної безпеки» 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	Менеджмент інформаційної безпеки
Адреса викладання дисципліни	Головний корпус ЛНУ ім. І. Франка м. 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 та захист інформації
Викладачі дисципліни	Кропива Михайло Вікторович ст.викладач кафедри кібербезпеки
Контактна інформація викладачів	Mykhailo.Kropyva@lnu.edu.ua Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації в день проведення лекцій/практичних занять (за попередньою домовленістю).
Сторінка курсу	https://ami.lnu.edu.ua
Інформація про дисципліну	Дисципліна “Менеджмент інформаційної безпеки” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у 4-му семестрі в обсязі 4 кредити (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс розроблено таким чином, щоб надати студентам знання і навики побудови системи управління інформаційною безпекою базованої на вимогах міжнародного стандарту ISO27001, ISO27002, NIST CSF, NIST 800-53, OWASP TOP10, MITRE ATT&CK Framework, The 11 Strategies of a World-Class Cybersecurity Operations Center by MITRE.
Мета та цілі дисципліни	Метою вивчення нормативної дисципліни “ Менеджмент інформаційної безпеки” є освоєння студентами теоретичних і практичних знань та навиків побудови системи управління інформаційною безпекою базуючись на вимогах міжнародного стандарту ISO27001, ISO27002, NIST CSF, NIST 800-53, OWASP TOP10, MITRE ATT&CK Framework, The 11 Strategies of a World-Class Cybersecurity Operations Center by MITRE.
Література для вивчення дисципліни	1. Міжнародний стандарт ISO27001та ISO27001 2. https://www.iso27001security.com/html/27001.html 3. https://advisera.com/27001academy/knowledgebase/list-of-mandatory-documents-required-by-iso-27001-2013-revision/ 4. https://cyberblend.net/blog/iso-27001-required-documents-policies-and-procedures/ 5. Information security risks https://www.itgovernanceusa.com/iso27001-risk-assessment 6. Improvement cycle (PDCA) https://bestpractice.biz/pdca-an-implementation-guide-to-iso-270012013/ 7. NIST 800-53. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final 8. NIST CSF. https://www.nist.gov/cyberframework

	9. MITRE ATT&CK Framework https://attack.mitre.org/ 10. OWASP TOP10. https://owasp.org/www-project-top-ten/ 11. The 11 Strategies of a World-Class Cybersecurity Operations Center by MITRE. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf Курс створений на платформі Rangeforce: https://www.rangeforce.com/ Udemy courses: https://www.udemy.com/course/iso-27001-fundamentals/ https://www.udemy.com/course/iso-27001-information-security-management-system-isms/
Обсяг курсу	Загальний обсяг: 120 годин. Аудиторних занять:64 год., з них 32 год. лекцій та 32год. лабораторних робіт. Самостійної роботи: 56 год. К-ть кредитів:4
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: Познайомитись і знати: - З чого складається система управління інформаційною безпеки (ISMS); - Що саме необхідно мати для проходження сертифікації ISO27001; - ISO27002 та його вклад у розробку вимог ISO27001. - Способи оцінки ризиків в інформаційній безпеці; - Принципи побудови політик інформаційної безпеки; - Вимоги стандарту NIST CSF. - Вимоги стандарту NIST 800-53. - Техніки і тактики MITRE ATT&CK Framework. - Деталі найбільш критичних вразливостей веб додатків базуючись на OWASP TOP10 Framework. - Тактики і техніки хакера, базуючись на MITRE ATT&CK Framework. - Кращі практики побудови Cybersecurity Operations Center (SOC) на прикладі методології від компанії MITRE, котрі детально описані в книзі 11 Strategies of a World-Class Cybersecurity Operations Center. Вміти: - Описувати ціль і мету сертифікації; - Будувати підходи оцінки ризиків інформаційної безпеки; - Створювати політики інформаційної безпеки: -Information security policy -Change management policy -Risk management framework -Malware policy -Asset management and inventory policy -Annex A controls - Співставлення вимог NIST 800-53 із відповідними політиками ISO27001. - Розуміння вимог стандарту ISO 27002 та їх співставлення із стандартом ISO27001. - Розуміти вимоги стандарту NIST CSF та вміти скласти модель оцювання зрілості підприємства по цьому стандарту. - Описати проходження шляху хакера (attack kill chain) на прикладі конкретних атак (для прикладу Petya, WannaCry) із привязкою до відповідних технік і тактик MITRE ATT&CK Framework.

	- Виявляти, вміти експлуатувати та виправляти найбільш критичні вразливості веб додатків базуючись на OWASP TOP10 Framework. - Співставляти вразливості та конкретний спосіб експлуатації базуючись на MITRE ATT&CK Framework. - Оприділяти розміри SOC в залежності від розміру компанії. - Вміти описати здатності (capabilities) малого, середнього та великого SOC базуючись на підходах компанії MITRE, описаних у книзі 11 Strategies of a World-Class Cybersecurity Operations Center **Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 3, КЗ 4, КЗ 5, КЗ 6, КЗ 7, КФ 1, КФ 2, КФ 4, КФ 5, КФ 8, КФ 9, КФ 12,** **та програмних результатів навчання: ПРН 1, ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 7, ПРН 8, ПРН 9, ПРН 19, ПРН 22, ПРН 23, ПРН 24, ПРН 30, ПРН 31, ПРН 34, ПРН 42, ПРН 43, ПРН 54.**
Ключові слова	ISO27001, NIST CSF, ISO27002, NIST 800-53, MITRE, OWASP, Risk management, Information security policy,
Формат курсу	Очний
Теми	1. Знайомство із стандартом ISO27001 2. Система управління інформаційною безпекою (ISMS) - що це і для чого сворюється 3. PDCA (або цикл постійного покращення чи цикл Демінга). що це, для чого і як накладається на ISMS 4. Знайомство із SMART підхідом. (підхід описаний для прикладу: https://www.mindtools.com/pages/article/smart-goals.htm) 5. Структура політик інформаційної: - Policy ### - Document Owner and Approval - Scope - Responsibilities - Policy - Enforcement 6. Знайомство із матрицею відповідальностей (RACI matrix) 7. Підходи до визначення ризиків інформаційної безпеки (ISO27001 risk management) 8. Знайомство із додатком з контролями AnnexA ISO27001 9. Написання політики управління змінами (Change management) 10. Написання Mobile device policy 11. Написання Teleworking policy 12. Написання Information security training and awareness policy 13. Знайомство із ISO 27002 14. Співставлення вимог ISO 27001 із рекомендаціями ISO27002 15. Знайомство із NIST CSF 16. Розробка методології оцінки зрілості підприємства згідно з NIST CSF 17. Знайомство із NIST 800-53

	18. Співставлення вимог NIST 800-53 із відповідними політиками ISO27001. 19. Ознайомлення із техніками і тактиками MITRE ATT&CK Framework. 20. Проходження шляху хакера (attack kill chain) на прикладі конкретних атак (Petya, WannaCry) із відповідним мапінгом до відповідних технік і тактик. 21. Знайомство із OWASP TOP10 22. Детальний розбір двох вразливостей. Способи експлуатації, виявлення та виправлення. 23. Мапінг вразливостей та конкретного способу експлуатації на MITRE ATT&CK Framework. 24. Знайомство з кращими практики побудови Cybersecurity Operations Center (SOC) на прикладі методології від компанії MITRE, котрі детально описані в книзі 11 Strategies of a World-Class Cybersecurity Operations Center. 25. Розміри SOC в залежності від розміру компанії. Детальний розбір здатності (capabilities) малого, середнього та великого SOC.
Підсумковий контроль, форма	екзамен у кінці семестру
Пререквізити	Для вивчення курсу студенти потребують базових знань з - Основ кібербезпеки; - Захист сервісів та підтримка IT процесів; - Англійської мови; - Критичного мислення для можливості створення моделі оцінки ризиків інформаційної безпеки
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Індивідуальні завдання Групові проекти, менторство
Необхідне обладнання	Комп'ютер (Windows, Mac, Linux)
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • індивідуальні завдання : 30% семестрової оцінки; максимальна кількість балів 30 • Проходження курсів у платформі RangeForce: 20% семестрової оцінки; максимальна кількість балів 20. • екзамен: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100. **Письмові роботи:** Очікується, що студенти виконають одну письмову роботу (тест з теоретичних завдань) і звіт про виконання проекту. **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 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 екзамену.	- Вимоги до «The scope of the management system» - Що ISO/IEC 27000 визначає як актив (an 'asset') - Що саме визначає ISO 27001 в додатку Annex A - Про що говорить цикл постійного покращення (PDCA cycle) - Які кібер загрози (Threats) в організації - Які саме цілі інформаційної безпеки - Про що говорить вимога "shall" в стандарті і чим відрізняється від "should" - Як Інформаційна безпека визначена в ISMS (CIA Triade) - Опис методології оцінки ризиків інформаційної безпеки - Опис політики управління змінами - Співставлення вимог ISO 27001 із технічною реалізацією NIST 800-53 - Описати дві вразливості із OWASP TOP10 Framework - Описати шлях, який проходить хакер для компроментації системи використовуючи MITRE ATT&CK Framework
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдан-ня, год.	Термін виконання
1	**Тема 1.** - Знайомство із стандартом ISO27001 - Система управління інформаційною безпекою (ISMS) - що це і для чого сворюється	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень
2	**Тема 2.** - PDCA (або цикл постійного покращення чи цикл Демінга). що це, для чого і як накладається на ISMS - Знайомство із SMART підходом.	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень
3	**Тема 3.** - Структура політик інформаційної: • Policy ### • Document Owner and Approval • Scope • Responsibilities • Policy • Enforcement - Знайомство із матрицею відповідальностей (RACI matrix)	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень
4	**Тема 4.** - Підходи до визначення ризиків інформаційної безпеки (ISO27001 risk management)	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень
5	**Тема 5.** - Знайомство із додатком з контролями AnnexA ISO27001	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень
6	**Тема 6.** - Написання політики управління змінами (Change management)	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень
7	**Тема 7.** - Написання Mobile device policy - Написання Teleworking policy - Написання Information security training and awareness	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень

	policy				
8	**Тема 8.** - Знайомство із ISO 27002. - Рекомендації щодо впровадження ISO 27001. - Співставлення вимог ISO 27001 із рекомендаціями ISO27002	лекція, лабораторна, самостійна робота	[1-6]	2 2 3.5	1тиждень
9	**Тема 9.** - Знайомство із NIST CSF - Розробка методології оцінки зрілості підприємства згідно з NIST CSF	лекція, лабораторна, самостійна робота	[7-8]	2 2 3.5	1тиждень
10	**Тема 10.** - Знайомство із NIST 800-53 - Співставлення вимог NIST 800-53 із відповідними політиками ISO27001.	лекція, лабораторна, самостійна робота	[7-8]	2 2 3.5	1тиждень
11	**Тема 11.** - Ознайомлення із техніками і тактиками MITRE ATT&CK Framework	лекція, лабораторна, самостійна робота	[9]	2 2 3.5	1тиждень
12	**Тема 12.** - Проходження шляху хакера (attack kill chain) на прикладі конкретних атак (Petya, WannaCry) із відповідним мапінгом до відповідних технік і тактик.	лекція, лабораторна, самостійна робота	[9]	2 2 3.5	1тиждень
13	**Тема 13.** - Знайомство із OWASP TOP10	лекція, лабораторна, самостійна робота	[10]	2 2 3.5	1тиждень
14	**Тема 14.** - Детальний розбір вразливостей. - Способи експлуатації, виявлення та виправлення.	лекція, лабораторна, самостійна робота	[10]	2 2 3.5	1тиждень
15	**Тема 15.** - Мапінг вразливостей та конкретного способу експлуатації на MITRE ATT&CK Framework.	лекція, лабораторна, самостійна робота	[9]	2 2 3.5	1тиждень
16	**Тема 16.** - Знайомство з кращими практики побудови Cybersecurity Operations Center (SOC) на прикладі методології від компанії	лекція, лабораторна, самостійна робота	[11]	2 2 3.5	1тиждень

	MITRE, котрі детально описані в книзі 11 Strategies of a World-Class Cybersecurity Operations Center. - Розміри SOC в залежності від розміру компанії. Детальний розбір здатності (capabilities) малого, середнього та великого SOC.				