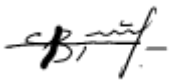
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

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 "Безпека в соціальних мережах", 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	Безпека в соціальних мережах
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	Венгерський Петро Сергійович, доктор фіз.-мат.наук, професор кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	petro.venherskyy@lnu.edu.ua; https://ami.lnu.edu.ua/employee/venherskyi; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua
Інформація про дисципліну	Дисципліна “Безпека в соціальних мережах” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 8-му семестрі першого (бакалаврського) рівня освіти в обсязі 6-ти кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про принципи забезпечення безпеки персональних даних (конфіденційної інформації) в соціальних мережах, використання механізмів послуг безпеки в умовах сучасних загроз.
Мета та цілі дисципліни	Метою курсу є формування у студентів теоретичної та практичної бази знань з безпечної поведінки у мережі, умінь та навичок ефективно та безпечно налаштовувати свої облікові записи та доступи; розуміння принципів передачі через мережу інформації та освоєння основних алгоритмів шифрування та дешифрування даних.
Література для вивчення дисципліни	*Основна* 1. Когут Ю. Кібервійни, кібертероризм, кіберзлочинність. Видавництво: Дакор, Консалтингова компанія Сідкон, 2022. 284 с. 2. Богуш В., Бровко В., Настрадін В. Основи кіберпростору, кіберзахисту та кібербезпеки. Видавництво: Ліра-К., 2021. 554 с. 3. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем: підр. Київ: ДУІКТ, 2019. 316 4. Євсеєв С.П., Мілов О.В., Остапов С.Е. Северінов О.В. Кібербезпека: основи кодування та криптографії: навч. Посібник. – Харків: ХПІ, 2023. – 658 с. 5. Козіна Г. Л. Криптографія від історії до сучасних стандартів: навч. посібник. – Запоріжжя : НУ «Зап. пол.», 2020. – 192 с *Додаткова* 1. Державна служба спеціального зв'язку та захисту інформації України./ www.dsszzi.gov.ua 2. Лабораторний практикум з навчальної дисципліни "Інформаційна

	безпека". Навчально практичний посібник / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2019. – 256 с. (укр. мов.) 3. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2020. 4. Стаття 361-1 Карного Кодексу України. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут / Електронний https://web.archive.org/web/20080228124933 6. 5. ISACA, Advanced Persistent Threats: How to Manage the Risk to Your Business, USA, 2018 6. ISACA, CISA Review Manual, USA, 2018 7. SACA, "Top Business/Security Issues Survey Results," USA, 2021 8. https://www.netacad.com/ - CISCO Networking Academy. 9. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text – Закони про кібербезпеку. 10. https://zakon.rada.gov.ua/laws/show/2297-17#Text 11. https://zakon.rada.gov.ua/laws/show/3855-12#Text 12. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22 https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 70 год., з них 28 години лекцій та 42 годин лабораторних занять. Самостійної роботи: 110 годин.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей. **знати:** - правові аспекти забезпечення інформаційної і кібербезпеки на рівні держави, міжнародному рівні; - принципи побудови соціальних мереж, протоколи обміну даними в кіберпросторі; - типові загрози, атаки та області їх розповсюдження; - проблеми захисту даних; -засоби протидії злочинності; - поняття ідентифікації, методів аутентифікації, авторизації; - основні типи засобів контролю цілісності даних. **вміти:** - ідентифікувати можливі загрози чи атаки; - використовувати сучасні програмні (програмно-апаратні) застосунки забезпечення безпеки персональних даних; - орієнтуватися в сучасних загрозах, їх направленості; - аналізувати ризики використання конфіденційної інформації в соціальних мережах; - відрізняти фейкову інформацію в медіапросторі; - орієнтуватися у послугах і механізмах забезпечення безпеки; - шифрувати конфіденційні дані стандартними алгоритмами шифрування; - налаштовувати безпеку веб-браузера; - користуватися цифровим підписом; - налаштовувати брандмауер; - відрізняти та розуміти який метод шифрування найкраще підійде для використання в певних умовах; - забезпечувати безпеку особистих персональних даних в умовах

	сучасних загроз. Курс забезпечує набуття таких фахових компетентностей: ІК, КФ 5, КФ 8, КФ 10; та програмних результатів навчання: ПРН 9, ПРН 13, ПРН 14, ПРН 17-29, ПРН 31-35, ПРН 41-53.
Ключові слова	Інформація, інформаційна безпека, соціальні мережі, загроза, вразливість, конфіденційність, цілісність, безпека даних, криптографія, криптологічні алгоритми, кодування даних, теорія шифрування даних.
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Залік у кінці 8 семестру. Формат заліку: контрольна робота.
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1) Моделі та методи дискретної математики, 2) Застосування дискретної математики в криптології, 3) Основи криптографії, 4) Прикладна криптологія, 5) Обробка сигналів в кібербезпеці.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Індивідуальні завдання Групові проекти
Необхідне обладнання	Проєкційне мультимедійне обладнання (проєктор, екран, ноутбук/комп'ютер). Доступ до мережі Internet, точка доступу Wi-Fi.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • виконання лабораторних робіт: 10 робіт по 5 балів кожна; максимальна кількість балів 50. • виконання індивідуальних завдань: 3 завдання по 10 балів кожне максимальна кількість балів 30. • підсумкова контрольна робота: максимальна кількість балів 20. 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 незарахуваннння 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.
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу

Тиж.	Тема, план, короткі тези	Форма діяльності (заняття)	Література	Завдання, год.	Термін виконання
1	**Тема 1. Огляд безпеки системи.** Основні поняття та визначення безпеки. Роль захисту інформації в кіберпросторі, умови функціонування підсистеми безпеки в соціальних (комп'ютерних) мережах та системах. Вимоги щодо безпеки системи, ризики безпеки. Складові та послуги безпеки: конфіденційність, цілісність, доступність, причетність, спостережність. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Критерії захищеності комп'ютерних систем. Національні нормативні акти і міжнародні регулятори системи безпеки	лекція, самостійна робота, лаб.	[1-5]	2 7 2	1 тиждень
2	**Тема 2. Сучасні загрози в соціальних (комп'ютерних) мережах.** Формальне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, ризиків та вразливих на елементи інформаційних систем в кіберпросторі. Синергія та гібридність сучасних загроз, основні тенденції спрямованості.	лекція, самостійна робота лаб.	[1-5] [1-5]	2 8 4	1 тиждень
3-4	**Тема 3. Механізми забезпечення конфіденційності та цілісності.** Принципи побудови симетричного та несиметричного шифрування. Основні критерії їх використання. Блочні симетричні шифри, алгоритми блокового симетричного шифрування DES, ГОСТ-28147, Rijndael, Калина-256. Несиметричні криптосистеми RSA, Ель Гамаля та Діффі – Геллмана. Принципи їх використання с соціальних мережах.	лекція, самостійна робота, лаб.	[1-5]	4 16 6	2 тижні
5-6	**Тема 4. Механізми забезпечення автентичності.** Класифікація механізмів автентифікації: MDC-коди, MAC-коди, цифровий підпис. Основні стандарти цифрового підпису.	лекція, самостійна робота	[1-5]	4 16	2 тижні

	Класифікація механізмів автентифікації на основі методів двофакторній автентифікації. Класифікація загроз на процедури двофакторній автентифікації. Основні вимоги до протоколів двофакторній автентифікації. Основні процедури, які забезпечують безпеку в протоколах двофакторній автентифікації.				
	Індивідуальні завдання	лаб.	[1-5]	6	під час заняття
7	**Тема 5. Основи цифровій стеганографії.** Класифікація методів цифровій стеганографії з відкритим ключем. Основні методи приховування конфіденційної інформації.	лекція, самостійна робота	[1-5]	2 7	1 тиждень
		лаб.	[1-5]	2	
8-9	**Тема 6. Протоколи захисту інформації на мережевому рівні.** Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність. Системи захисту PGP та CS MIME. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта	лекція, самостійна робота, лаб.	[1-5]	4 16 6	2 тижні
10-11	**Тема 7. Механізми та протоколи керування ключами в ІВК в соціальних мережах.** Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Основні вимоги стандарту відкритих ключів, управління сертифікатами. Системи PKI. Основні вимоги до політиці PKI.	лекція, самостійна робота	[1-5]	4 16	2 тижні
	Індивідуальні завдання	лаб.	[1-5]	6	під час заняття
12	**Тема 8. Програмно-апаратні засоби захисту інформації в мережі Internet.** Основні принципи захисту інформації при підключенні до мережі Інтернет. Використання паролів і механізмів контролю.	лекція, самостійна робота, лаб.	[1-5]	2 8 4	1 тиждень
13	**Тема 9. Програмно-апаратні (програмні) засоби захисту інформації в мережі Wi-Fi.** Основні принципи захисту інформації при підключенні до мережі Wi-Fi. Використання паролів і механізмів контролю. Основні вимоги стандарту безпеки технології DTE (4G).	лекція, самостійна робота	[1-5]	2 8	1 тиждень
		лаб.	[1-5]	2	1 тиждень
14	**Тема 10. Програмно-апаратні (програмні) засоби захисту інформації в хмарних технологіях.** Основні принципи захисту інформації при використанні хмарних мереж (технологій).	лекція, самостійна робота	[1-5]	2 8	1 тиждень
	Індивідуальні завдання	лаб.	[1-5]	4	під час заняття