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 комп'ютерних мереж”,
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 комп'ютерних мереж
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	Кирик Мар'ян Іванович, доктор технічних наук, професор кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	marian.kyryk@lnu.edu.ua; https://ami.lnu.edu.ua/employee/kyryk-m-i
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/department/kiberbezpeky
Інформація про дисципліну	Дисципліна "Безпека комп'ютерних мереж" є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 5-му семестрі першого (бакалаврського) рівня освіти в обсязі 6-ох кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Курс спрямований на формування у студентів професійних компетентностей в області безпеки комп'ютерних мереж, знань про основні типи та види загроз, протоколи безпеки, основні програмні та апаратні засоби захисту інформації в комп'ютерних мережах, реалізації захисту конфіденційності інформації, здійснення захисту цілісності інформації, організації доступності інформації.
Мета та цілі дисципліни	Метою навчальної дисципліни "Безпека комп'ютерних мереж" є формування знань з мережевої безпеки, використання методів та інструментів захисту мережі та підключених до неї пристроїв від несанкціонованого доступу, методів захисту конфіденційності даних у мережах, підготовка фахівців, здатних аналізувати, обирати, застосовувати методи та засоби забезпечення безпеки мереж.
Література для вивчення дисципліни	*Основна* 1. Технології захисту локальних мереж на основі обладнання CISCO: навч.посіб. /Т.І. Коробейнікова, С.М. Захарченко. – Львів: Видавництво Львівська політехніка, 2021. – 232 с. 2. Комп'ютерні мережі. Частина 1: / Б. Ю. Жураковський, І.О. Зенів. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 336 с. 3. Ходаківський І.В. Безпека інформаційних систем та мереж. Навчальний посібник. Київ: Видавництво ЦНЛ, 2020. – 280 с. 4. Tanenbaum A., Wetherall D. Computer Networks, 6th Edition. – 2021. 5. Cisco systems. Навчальні матеріали мережних академій Cisco за курсом Network Security https://www.netacad.com/courses/cybersecurity/network-security/

	6. Cisco systems. Навчальні матеріали мережних академій Cisco за курсом CCNA Cybersecurity Operations https://www.netacad.com/courses/cybersecurity/cyberops-associate/ *Додаткова* 7. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с. 8. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с. ISBN 978–617–7092–78–9. 9. Kaufman, C., Perlman, R., and Speciner, M.: Network Security, 2nd ed., Upper Saddle River, NJ: Prentice Hall, 2002. 10. Gilman, Evan and Barth, Doug. Zero trust networks. O'Reilly Media, Incorporated, 2017. 11. Kurose J., Ross K. Computer Networking: A Top-Down Approach, 7th Edition. – 2017.
Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 64 год., з них 32 години лекцій та 32 годин лабораторних занять. Самостійної роботи: 116 годин.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей. **знати:** - теоретичні та практичні підходи до організації безпеки комп'ютерних мереж; - протоколи безпеки та особливості організації мережевої безпеки; - методи розробки і впровадження систем мережевої безпеки; - види загроз інформації в інформаційно-комунікаційних системах та мережах; - основні протоколи безпеки та принципи функціонування систем безпеки мереж; - основні програмні та апаратні засоби захисту інформації в комп'ютерних мереж. **вміти:** - здійснювати аналіз безпеки комп'ютерних мереж та усувати можливі шляхи несанкціонованого доступу; - ідентифікувати можливі загрози чи атаки; - планувати та реалізувати відповідні заходи, щодо безпеки інформаційно-комунікаційних систем та мереж; - проектувати системи захисту і безпеки комп'ютерних мереж з урахуванням усіх аспектів поставленої задачі, включаючи створення, налагодження, експлуатацію та технічне обслуговування; - обґрунтовувати вибір окремих технічних та програмних рішень безпеки комп'ютерних мереж з урахуванням їх взаємодії та потенційного впливу на вирішення організаційних проблем, організовувати їх впровадження та використання. Курс забезпечує набуття таких компетентностей: ІК, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 2, КФ 3, КФ 4, КФ 5, КФ 6, КФ 11, КФ 12; та програмних результатів навчання: ПРН 2-6, ПРН 10-32, ПРН 39, ПРН 49-53.
Ключові слова	Мережева безпека, мережеві атаки, міжмережеві екрани, технологія VPN, протокол IPSec, протокол SSH, IPS, IDS, сигнатури, списки

	контролю доступу (ACL), політика безпеки.
Формат курсу	Очний
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Екзамен у кінці семестру. Формат екзамену: письмовий тестовий.
Пререквізити	Для вивчення курсу студенти потребують базові знання з дисциплін "Операційні системи", "Фізичні основи електроніки", "Основи кібербезпеки" та "Менеджмент інформаційної безпеки".
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Лекції з мультимедійними презентаціями; лабораторні заняття у вигляді виконання практичних завдань (у тому числі командних); самостійне опрацювання навчальних матеріалів, розміщених у хмарних сховищах; обговорення тем та консультації в середовищі Microsoft Teams, індивідуальні завдання. Лекції та лабораторні: інформаційно-рецептивний метод, репродуктивний метод, евристичний метод, метод проблемного викладу. Самостійна робота: репродуктивний метод, дослідницький метод.
Необхідне обладнання	Комп'ютер, мережа Internet, проектор. Програмне забезпечення Cisco Packet Tracer, Oracle VM VirtualBox, мережеве обладнання.
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 • екзамен: 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 лабораторні заняття 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	1. Який вид розсилки необхідно використати для передавання

екзаменів.	повідомлення всім пристроям локальної мережі? 2. Для чого необхідні протоколи при передаванні даних? 3. Яка адреса використовується для доставки даних у віддалену мережу? 4. Яку адресу використовує маршрутизатор при прийомі пакету? 5. Який варіант доставки повідомлень використовується, щоб усі пристрої одночасно отримували однакове повідомлення? 6. Що використовує TCP протокол для встановлення з'єднання? 7. Що є характерним для ієрархії DNS? 8. Який тип атаки може відключити комп'ютер, змушуючи його надлишково використовувати пам'ять або перевантажувати процесор? 9. Який метод намагається отримати пароль шляхом перебору усіх можливих комбінацій? 10. Який нетехнічний метод кіберзлочинець використовуватиме для збору конфіденційної інформації з організації? 11. Який принцип не дозволяє розкривати інформацію неавторизованим особам, ресурсам та процесам? 12. Яка служба визначає, до яких ресурсів користувач може отримати доступ та які операції може виконувати користувач? 13. Назвіть важливу характеристику черв'яків (worms) 14. Який тип мережевої загрози призначений для перешкоджання доступу до ресурсів авторизованих користувачів? 15. Яке рішення потрібно запропонувати, щоб забезпечити безпечний канал зв'язку між віддалено розташуваними користувачами і компанією 16. Яка мета атаки мережевої розвідки? 17. У чому перевага SSH у порівнянні з Telnet при віддаленому керуванні маршрутизатором? 18. Назвіть найбільш ефективні способи захисту від шкідливих програм 19. Які існують методи забезпечення конфіденційності? 20. Які рішення мережевої безпеки можна використовувати для зниження ризику DoS-атак 21. Яка служба дозволить поставити у відповідність веб-адресі конкретну IP-адресу веб-сервера призначення 22. Які рішення мережевої безпеки можна використовувати для зниження ризику DoS-атак? 23. Які заходи безпеки маршрутизатора потрібно підтримувати для захисту граничного маршрутизатора на периметрі мережі? 24. Назвіть перевагу використання фаєрвола зі збереженням стану в порівнянні з проксі-сервером 25. Назвіть недоліки використання IDS. 26. Назвіть спільні характеристики систем IDS та IPS. 27. У чому недолік механізму виявлення загроз на основі шаблонів (signatures)? 28. Які протоколи IPsec використовуються для забезпечення цілісності даних? 29. Які твердження справедливі щодо стандартних списків ACL? 30. Як сканування мережі допомагає оцінити операційну безпеку?
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. Сучасні безпечні мережі.** (Вплив мереж на наше життя. Компоненти мережі. Основні типи мереж. Технології інтернет-доступу. Надійні мережі та основні характеристики мережевої архітектури. Тенденції розвитку мереж. Мережева безпека.)	лекція, самостійна робота	[1-8]	27	1 тиждень
	Тема 1. Створення та налаштування ізольованої віртуальної мережі VirtualBox.	лаб.	[1-8]	2	
2	**Тема 2. Архітектура безпечних мереж. Мережеве обладнання.** (Ієрархічні мережі. Масштабовані мережі. Комутаційне обладнання. Обладнання для маршрутизації.)	лекція, самостійна робота	[1-8]	27	1 тиждень
	Тема 2. Налаштування автентифікації, авторизації та обліку.	лаб.	[1-8]	2	
3	**Тема 4. Загрози для безпеки мережі.** (Забезпечення мережевої безпеки. Мережеві загрози. Інструментарій хакерів. Шкідливі програмні засоби. Поширені мережеві атаки.)	лекція, самостійна робота	[1-8]	27	1 тиждень
	Тема 3. Перевірка цілісності даних.	лаб.	[1-8]	2	
4	**Тема 4. Загрози для безпеки мережі.** (Забезпечення мережевої безпеки. Мережеві загрози. Інструментарій хакерів. Шкідливі програмні засоби. Поширені мережеві атаки.)	лекція, самостійна робота	[1-8]	27	1 тиждень
	Тема 4. Виявлення загроз і вразливостей в ОС Ubuntu.	лаб.	[1-8]	2	
5	**Тема 5. Захист мережі та нейтралізація загроз.** (Захист мережі. Фахівці з мережевої безпеки. Домени мережевої безпеки. Архітектура Cisco SecureX. Протидія поширеним мережевим атакам. Структура захисту мережевої платформи Cisco.)	лекція, самостійна робота	[1-8]	27	1 тиждень
	Тема 5. Режими віддаленого доступу.	лаб.	[1-8]	2	
6	**Тема 6. Інфраструктура забезпечення безпеки мережі.** (Пристрої забезпечення безпеки. Пристрої виявлення та запобігання вторгненням. Сервіси безпеки.)	лекція, самостійна робота	[1-8]	27	1 тиждень
	Тема 6. Відновлення паролів на комутаторах та маршрутизаторах Cisco.	лаб.	[1-8]	2	
7	**Тема 7. Безпека мережевих пристроїв.**	лекція,	[1-8]	2	1

	(Безпечний доступ до пристроїв. Налаштування SSH. Присвоєння адміністративних ролей. Моніторинг та керування пристроями. Захист конфігураційних файлів та образа Cisco IOS. Використання системного журналу Syslog для безпеки мережі. Використання SNMP для безпеки мережі.**)**	самостійна робота		7	тиждень
	Тема 7. Резервування маршрутизаторів та комутаторів, посилення їхньої стійкості до атак.	лаб.	[1-8]	2	
8	**Тема 8. Безпека бездротових мереж.** **(**Переваги бездротового зв'язку. Бездротові технології. Принципи роботи WLAN. Загрози WLAN. Безпека WLAN.**)**	лекція, самостійна робота	[1-8]	2 7	1 тиждень
	Тема 8. Захист Wi-Fi мереж.	лаб.	[1-8]	2	
9	**Тема 9. Захист інфраструктури мережі за допомогою списків контролю доступу ACL.** **(**Призначення ACL. Шаблонні маски в ACL. Рекомендації щодо створення ACL. Типи ACL для IPv4. ACL-списки IPv6.)	лекція, самостійна робота	[1-8]	2 7	1 тиждень
	Тема 9. Використання списків контролю доступу ACL для управління мережевим трафіком.	лаб.	[1-8]	2	
10	**Тема 10. Впровадження технологій брандмауера.** (Технології міжмережевого екрану. Захист мереж за допомогою міжмережевих екранів. Типи міжмережевих екранів. Зональні міжмережеві екрани.)	лекція, самостійна робота	[1-8]	2 7	1 тиждень
	Тема 10. Брандмауери на сервері та ACL на маршрутизаторі.	лаб.	[1-8]	2	
11	**Тема 11. Технології системи запобігання вторгненням. IPS сигнатури.** (Характеристики IDS та IPS. Впровадження мережевих IPS. IPS на основі хоста. Мережеві IPS. Аналізатори портів. Характеристики IPS сигнатури. Сигналізація IPS сигнатур. Дії сигнатур IPS. Управління та моніторинг IPS. Глобальна кореляція IPS)	лекція, самостійна робота	[1-8]	2 7	1 тиждень
	Тема 11. Режими віддаленого доступу.	лаб.	[1-8]	2	
12	**Тема 12. Захист локальної мережі.** (Загрози безпеці на канальному рівні. Атаки на таблиці CAM. VLAN атаки).	лекція, самостійна робота	[1-8]	2 8	1 тиждень
	Тема 5. Налаштування механізмів безпеки комутаторів Ethernet.	лаб.	[1-8]	2	
13	**Тема 13. Поглиблений аналіз мережевих атак.** (DHCP атаки. ARP атаки. Протидія атакам	лекція, самостійна робота	[1-8]	2 8	1 тиждень

	підміни адреси.)				
	Тема 13. Забезпечення безпеки на 2-му рівні.	лаб.	[1-8]	2	
14-15	**Тема 14. Віртуальні приватні мережі VPN.** (Віртуальні приватні мережі VPN. Топології VPN. Компоненти та робота IPsec VPN. Протоколи IPsec. Протокол Internet Key Exchange (IKE). Реалізація мереж Site-to-Site IPsec VPN.)	лекція, самостійна робота	[1-8]	28	2 тижні
	Тема 14. Конфігурація і перевірка IPsec VPN між двома пунктами (site-to-site).	лаб.	[1-8]	2	
16	**Тема 15. Безпека нульової довіри (Zero Trust Security).** (Модель Zero Trust. Переваги та недоліки ZTA. Області захисту моделі Zero Trust. Мережеві екрани в умовах Zero Trust)	лекція, самостійна робота	[1-8]	28	1 тиждень
	Тема 15. Налаштування режиму VPN Transport та створення тунелю VPN.	лаб.	[1-8]	2	
ВСЬОГО				**180**	