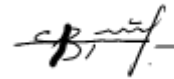


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

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
“Основи кібербезпеки”,
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	Основи кібербезпеки
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.venherskyi@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 “Основи кібербезпеки” є нормативною дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається в 1-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 методи обробки інформації, методів захисту інформації в комп’ютерних системах та мережах і ознайомлення з особливостями їх апаратної та програмної реалізацій та навички про форми і методи захисту інформації.
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	<i>Основна</i> <ol style="list-style-type: none"> 1. Cybersecurity Fundamentals/ ISACA/ www.isaca.org/cyber? Cybersecurity Fundamentals Study Guide/ 2021.- 156 p. 2. Когут Ю. Кібервійни, кібертероризм, кіберзлочинність. Видавництво: Дакор, Консалтингова компанія Сідкон, 2022. 284 с. 3. Богуш В., Бровко В., Настрадін В. Основи кіберпростору, кіберзахисту та кібербезпеки. Видавництво: Ліра-К., 2020. 554 с. <i>Додаткова</i> <ol style="list-style-type: none"> 4. Cyber-Physical Security : Monograph / edit. Clark. – Springer International Publishing, 2017. – ISBN 978-3-319-32822-5 (print) ; 978-3-319-32824-9 (online). 299 p. 7. 5. Enterprise Security : Monograph / edit. Chang. – Springer International Publishing, 2017. – ISBN 978-3-319-54379-6 (print) ;

	<p>978-3-319-54380-2 (online). 277 p. 8.</p> <ol style="list-style-type: none"> 6. Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978-3-319-46528-9 (print) ; 978-3-319-46529-6 (online). 127 p 7. Державна служба спеціального зв'язку та захисту інформації України./ www.dsszzi.gov.ua 8. Огляд різноманітних шкідливих програмних засобів/ Viruslist.com 9. 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.) 10. Ніколаюк С.І., Никифорчук Д.Й., Томма Р.П., Барко В.І. Протидія злочинам у сфері інтелектуальної власності. – К., 2020. 11. Кобозева А.А., Мачалін І.О., Хорошко В.О. Аналіз захищеності інформаційних систем: підр. Київ: ДУІКТ, 2010. 316 12. Стаття 361-1 Кримінального 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/200802281249336. 13. ISACA, Advanced Persistent Threats: How to Manage the Risk to Your Business, USA, 2018 14. ISACA, CISA Review Manual, USA, 2018 15. SACA, "Top Business/Security Issues Survey Results," USA, 2021 16. https://www.netacad.com/ - CISCO Networking Academy. 17. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text – Закони про кібербезпеку. 18. https://zakon.rada.gov.ua/laws/show/2297-17#Text 19. https://zakon.rada.gov.ua/laws/show/3855-12#Text 20. 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
<p>Обсяг курсу</p>	<p>Загальний обсяг: 180 годин. Аудиторних занять: 80 год., з них 32 години лекцій та 48 годин лабораторних занять. Самостійної роботи: 100 години.</p>
<p>Очікувані результати навчання</p>	<p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей.</p> <p>знати:</p> <ul style="list-style-type: none"> - типові загрози, атаки та області їх розповсюдження; - проблеми захисту даних; -засоби протидії злочинності; - основні поняття криптографії, алгоритми шифрування; - поняття ідентифікації, методів аутентифікації, авторизації; - основні типи засобів контролю цілісності даних; - технології реагування на інциденти; - основні кіберзакони, стандарти та відповідальність. <p>вміти:</p> <ul style="list-style-type: none"> - ідентифікувати можливі загрози чи атаки; - налаштовувати локальну та групову політики безпеки системи; - налаштовувати безпеку локальної мережі; - шифрувати конфіденційні дані стандартними алгоритмами

	<p>шифрування; - налаштувати безпеку веб-браузера; - користуватися цифровим підписом; - налаштувати брандмауер; - відрізнити та розуміти який метод шифрування найкраще підійде для використання в певних умовах; - налаштувати базову безпеку на маршрутизаторі; - застосовувати знання з кібербезпеки в практичній діяльності; - здійснювати проектування (розробку) систем, технологій і засобів кіберзахисту при здійсненні професійної діяльності; - розробляти моделі загроз інформації та моделі порушників інформаційної безпеки; - прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави, суспільству організації та дестабілізуючі чинники в роботі систем управління.</p> <p>Курс забезпечує набуття таких фахових компетентностей: ІК, КЗ 1, КЗ 2, КЗ 4, , КФ 2, КФ 3, КФ 5, КФ 10; та програмних результатів навчання: ПРН 10, ПРН 11, ПРН 12, ПРН 5, ПРН 9, ПРН 14.ПРН22, ПРН24, ПРН28, ПРН46,ПРН 47</p>
Ключові слова	Кібербезпека, кібератака, загроза, вразливість, конфіденційність, цілісність, безпека даних, криптографія, криптологічні алгоритми, кодування даних, теорія шифрування даних, формальні граматики і автомати, теорія алгоритмів.
Формат курсу	Очний. Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми подані у Схемі курсу нижче
Підсумковий контроль, форма	Екзамен у кінці першого семестру. Формат екзамену: письмовий тестовий.
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1) Моделі та методи дискретної математики; 2) Застосування дискретної математики в криптології, які читаються впродовж 1–2 семестрів першого (бакалаврського) рівня вищої освіти.
Навчальні методи та техніки, які будуть використовуватися під час викладання курсу	Презентації, лекції Індивідуальні завдання Групові проекти
Необхідне обладнання	Комп'ютер, мережа Internet, проектор. Програмне забезпечення Cisco Packet Tracer, Oracle VM VirtualBox. Образ Linux Ubuntu, KALI Linux.
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> • модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50 • екзамен: 50% семестрової оцінки; максимальна кількість балів 50 <p>Підсумкова максимальна кількість балів 100.</p> <p>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 незарахування викладачем, незалежно від масштабів плагіату чи обману.</p>

	<p>Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні 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.</p> <p>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.</p> <p>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.</p> <p>Жодні форми порушення академічної доброчесності не толеруються.</p>
<p>Питання до екзаменів.</p>	<p>РОЗДІЛ 1. ВСТУП ДО КІБЕРБЕЗПЕКИ . Різниця між інформаційною безпекою та кібербезпекою. Цілі, ролі кібербезпеки. Зміст та розділи курсу.</p> <p>РОЗДІЛ 2. КОНЦЕПЦІЇ КІБЕРБЕЗПЕКИ Ризики. Загальні типи та вектори атак. Політика та процедури. Керування кібербезпекою.</p> <p>РОЗДІЛ 3. ПРИНЦИПИ АРХІТЕКТУРИ БЕЗПЕКИ Огляд архітектури безпеки. Модель OSI (Open Systems Interconnect) Захист у глибину. Фаєрволи(Firewalls). Ізоляція та сегментація Моніторинг, виявлення та ведення журналу Основи шифрування</p> <p>РОЗДІЛ 4. БЕЗПЕКА МЕРЕЖ, СИСТЕМ, ПРОГРАМ ТА ДАНИХ Оцінка ризиків Управління вразливостями Тестування проникнення Безпека мережі Безпека операційної системи Безпека програми Безпека даних</p> <p>РОЗДІЛ 5. ВІДПОВІДАЛЬНІСТЬ ТА ВІДНОШЕННЯ ДО ІНЦИДЕНТІВ Подія проти інциденту Відповідь на інцидент безпеки Розслідування, правові заходи та збереження Криміналістика Плани аварійного відновлення та неперервності бізнесу</p> <p>РОЗДІЛ 6. ВПЛИВ НА БЕЗПЕКУ ТА РОЗВИТОК НОВИХ</p>

	ТЕХНОЛОГІЙ І ПРИСТРОЇВ Типові загрози та їх розширення Мобільні технології. Уразливості, загрози та ризик Споживачі ІТ та мобільних пристроїв Хмарні технології та цифрова співпраця ..
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. ВСТУП ДО КІБЕРБЕЗПЕКИ (Різниця між інформаційною безпекою та кібербезпекою. Цілі, ролі кібербезпеки. Зміст та розділи курсу.)	лекція, самостійна робота	[1-3]	2 6	1 тиждень
		Лаб.		2	
2	Тема 2. КОНЦЕПЦІЇ БЕЗПЕКИ (Ризики. Загальні типи та вектори атак. Політика та процедури. Керування кібербезпекою.)	лекція, самостійна робота	[1-3]	2 6	1 тиждень
		лаб.	[1-3]	4	
3-5	Тема 3. Принципи архітектури безпеки (Огляд архітектури безпеки. Модель OSI (Open Systems Interconnect). Захист у глибину. Фаєрволи (Firewalls). Ізоляція та сегментація. Моніторинг, виявлення та ведення журналу	лекція, самостійна робота	[1-3]	6 18	3 тижні
		лаб.	[1-3]	8	
		лаб.	[1-3]	8	
6	Тема 4. Основи шифрування Системи шифрування з відкритим ключем Основні відомості. Алгоритм RSA. Алгоритм Діффі Хеллмана. Алгоритм Ель-Гамала	лекція, самостійна робота	[1-3]	2 6	1 тиждень
		лаб.	[1-3]	4	
7	Тема 5. Цифровий підпис Електронний підпис. Хеш-функції та вимоги до них. Керування ключами.	лекція, самостійна робота	[1-3]	2 6	1 тиждень
		лаб.	[1-3]	2	

8-9	Тема 6. Безпека мереж, систем, програм та даних Оцінка ризиків. Управління вразливостями. Тестування проникнення. Безпека мережі. Безпека операційної системи. Безпека програми. Безпека даних.	лекція, самостійна робота	[1-3]	4 14	2 тижні
		лаб.	[1-3]	6	
10	Тема 7. Політика безпеки Приклади кібератак та методи протидії. Поняття політики безпеки. Види політик безпеки. Організація секретного діловодства.	лекція, самостійна робота	[1-3]	2 7	1 тиждень
		лаб.	[1-3]	4	
11-13	Тема 8. Відповідальність та відношення до інцидентів Подія проти інциденту. Відповідь на інцидент безпеки. Розслідування, правові заходи та збереження. Криміналістика. Плани аварійного відновлення та неперервності бізнесу.	лекція, самостійна робота	[1-3]	6 18	3 тижні
		лаб.	[1-3]	8	
14-16	Тема 10. Вплив на безпеку та розвиток нових технологій і пристроїв Типові загрози та їх розширення. Мобільні технології. Уразливості, загрози та ризик. Споживачі ІТ та мобільних пристроїв Хмарні технології та цифрова співпраця.	лекція, самостійна робота	[1-3]	6 18	3 тижні
		лаб.	[1-3]	10	