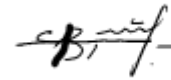


**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**Львівський національний університет імені Івана Франка**  
**Факультет прикладної математики та інформатики**  
**Кафедра кібербезпеки**

**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**  
**“Основи протидії кіберзлочинності”,**  
**що викладається в межах ОПП Кібербезпека**  
**першого (бакалаврського) рівня вищої освіти для здобувачів з**  
**спеціальності 125 – Кібербезпека та захист інформації**

Львів 2023 р.

<b>Назва дисципліни</b>	Основи протидії кіберзлочинності
<b>Адреса викладання дисципліни</b>	Головний корпус ЛНУ ім. І. Франка м. Львів, вул. Університетська 1
<b>Факультет та кафедра, за якою закріплена дисципліна</b>	Факультет прикладної математики та інформатики Кафедра кібербезпеки
<b>Галузь знань, шифр та назва спеціальності</b>	12 – інформаційні технології 125 – кібербезпека та захист інформації
<b>Викладачі дисципліни</b>	В'ячало Михайло Михайлович, асистент кафедри кібербезпеки (лекції та лабораторні заняття)
<b>Контактна інформація викладачів</b>	<a href="mailto:Mykhaylo.Vyachalo@lnu.edu.ua">Mykhaylo.Vyachalo@lnu.edu.ua</a> ; Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
<b>Консультації з питань навчання по дисципліні відбуваються</b>	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.
<b>Сторінка курсу</b>	<a href="https://ami.lnu.edu.ua/course/osnovy-protydii-kiberzlochynnosti">https://ami.lnu.edu.ua/course/osnovy-protydii-kiberzlochynnosti</a>
<b>Інформація про дисципліну</b>	Курс спрямований на формування у студентів професійних компетентностей, розвиток системи знань про методи аналізу, моніторингу та захисту інформації в суспільній сфері від атак.
<b>Коротка анотація дисципліни</b>	Дисципліна “Основи протидії кіберзлочинності ” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека , яка викладається у 8-му семестрі в обсязі 6 кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
<b>Мета та цілі дисципліни</b>	Метою є формування умінь та компетенцій для забезпечення ефективного захисту інформації, необхідних для подальшої роботи та застосуванню методів та засобів захисту інформації в умовах широкого використання сучасних інформаційних технологій
<b>Література для вивчення дисципліни</b>	<p>Основна</p> <ol style="list-style-type: none"> <li>1. Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення. Навч. посіб. – К.: Видавництво Ліра-К, 2023. – 484 с.</li> <li>2. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.</li> <li>3. Cybercrime: An Encyclopedia of Digital Crime, Nancy E. Marian, Jason Twede, Bloomsbury, 2020. – 520 p.</li> <li>4. Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології, Когут Ю. – К.: Видавництво Сідкон, 2022. – 284 с.</li> <li>5. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення, актуальна судова практика, Петков С.В., Журавльов Д.В., Дрозд О.Ю., Дрозд В.Г. -К: Видавництво ЦУЛ, 2022. – 460 с.</li> </ol> <p>Допоміжна</p> <ol style="list-style-type: none"> <li>6. Голубев В.О., Гавловський В.Д., Цимбалюк В.С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання</li> </ol>

	<p>комп'ютерних технологій. /За загальною редакцією доктора юридичних наук, професора Р.А. Калюжного. - Запо-ріжжя: "Просвіта", 2001. – 208 с.</p> <p>7. Організація розслідування окремих видів злочинів : навч. посіб. / [А.Ф. Во-лобуєв, О.Є. Користін, Р.Л. Степанюк] ; за заг. ред. А.Ф. Волобуєва ; МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2011. – 568 с.</p> <p>8. Петрович Л. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України / Л. Петрович, Н. В'ятов. – К. : Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Укра-їні»), 2014. – 60 с.</p> <p>9. Довгань О. Д., Доронін І. М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія. Київ, 2017. 107 с</p>
<b>Обсяг курсу</b>	Загальний обсяг: 180 годин. Аудиторних занять: 70 год., з них 28 год. лекцій та 42 год. лабораторних робіт. Самостійної роботи: 110 год.
<b>Очікувані результати навчання</b>	<p>У результаті вивчення навчальної дисципліни студент має набути таких компетентностей:</p> <p><b>знати:</b></p> <ul style="list-style-type: none"> <li>– теоретичне визначення основ інформаційної та кібернетичної безпеки;</li> <li>– властивості інформації та її впливу на свідомість та поведінку людини, суспільства, сучасних механізмів та інструментарію маніпулювання свідомістю</li> <li>– інформаційне законодавства як правової бази забезпечення інформаційної безпеки в умовах розбудови інформаційного суспільства та змін, які відбуваються у європейської та світової системах забезпечення безпеки;</li> <li>– формування у студентів навичок щодо застосування норм інформаційного права у практичній діяльності забезпечення інформаційної та кібернетичної безпеки.</li> </ul> <p><b>вміти:</b></p> <ul style="list-style-type: none"> <li>– орієнтуватися у законодавстві та спеціальній літературі;</li> <li>– порівнювати національне законодавство з міжнародними стандартами;</li> <li>– керуватися принципами права при виконанні своїх професійних обов'язків.</li> </ul> <p>Курс забезпечує набуття таких компетентностей: КІ, КЗ 1, КЗ 2, КЗ 4, КЗ 5, КФ 1-5, КФ 7, КФ 9-13; та програмних результатів навчання: ПРН 2-31, ПРН 33-40, ПРН 44-53.</p>
<b>Ключові слова</b>	Кібербезпека, кібератака, злочин, загроза, безпека.
<b>Формат курсу</b>	Очний Проведення лекцій, лабораторних робіт і консультацій.
<b>Теми</b>	Теми подані у Схемі курсу нижче
<b>Підсумковий контроль, форма</b>	Залік
<b>Пререквізити</b>	Для вивчення курсу студенти потребують базові знання щодо кібербезпеки та кіберзлочинності

<b>Навчальні методи та техніки, які будуть використовуватися під час викладання курсу</b>	Презентації, лекції Вирішення кейсів. Робота в групах Індивідуальні домашні завдання Модульний контроль
<b>Необхідне обладнання</b>	Проектор, дошка, комп'ютер, Moodle LMS
<b>Критерії оцінювання (окремо для кожного виду навчальної діяльності)</b>	<p>Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням:</p> <ul style="list-style-type: none"> <li>• лабораторні –60% семестрової оцінки; максимальна кількість балів 60</li> <li>• написання двох контрольних робіт (модулів): по 20% семестрової оцінки кожен; максимальна кількість балів –40</li> </ul> <p>Підсумкова максимальна кількість балів 100.</p> <p><b>Академічна доброчесність:</b> 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><b>Відвідання занять</b> 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><b>Література.</b> 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><b>Політика виставлення балів.</b> 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 запізнь 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.</p>
<b>Опитування</b>	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. Концептуальні засади забезпечення інформаційної безпеки України	лекція, самостійна робота	[1-2, 5-6, 9]	2 6	1 тиждень
	Тема 1. Концептуальні засади забезпечення інформаційної безпеки України	лаб.	[1-2, 5-6, 9]	2	1 тиждень

2	Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації	лекція, самостійна робота	[1-3]	2 6	1 тиждень
	Тема 2. Технічні канали витоку інформації. Способи несанкціонованого зняття інформації	лаб.	[1-3]	2	1 тиждень
3	Тема 3. Поняття та кримінологічна характеристика кіберзлочинності	лекція, самостійна робота	[2-6]	2 6	1 тиждень
	Тема 3. Поняття та кримінологічна характеристика кіберзлочинності	лаб.	[2-6]	2	1 тиждень
4	Тема 4. Розслідування кіберзлочинів.	лекція, самостійна робота	[2-8]	2 8	1 тиждень
	Тема 4. Розслідування кіберзлочинів	лаб.	[2-8]	2	1 тиждень
5	Тема 5. Засоби стирання, видалення даних та інформації.	лекція, самостійна робота	[2-4]	2 8	1 тиждень
	Тема 5. Засоби стирання, видалення даних та інформації.	лаб.	[2-4]	2	1 тиждень
6	Тема 6. Засоби копіювання даних	лекція, самостійна робота	[2-4]	2 8	1 тиждень
	Тема 6. Засоби копіювання даних	лаб.	[2-4]	4	1 тиждень
7	Тема 7. Обладнання для блокування запису	лекція, самостійна робота	[2-4]	2 8	1 тиждень
	Тема 7. Обладнання для блокування запису	лаб.	[2-4]	2	1 тиждень
8	Тема 8. Аналіз зібраної інформації.	лекція, самостійна робота	[2-4]	2 8	1 тиждень
	Тема 8. Аналіз зібраної інформації.	лаб.	[2-4]	4	1 тиждень
9	Тема 9. Відновлення даних	лекція, самостійна робота	[2-4]	2 8	1 тиждень
	Тема 9. Відновлення даних	лаб.	[2-4]	2	1 тиждень
10	Тема 10. Продукти аналізу і обробки ризиків інформаційної безпеки.	лекція, самостійна робота	[2-4]	2 8	1 тиждень
	Тема 10. Продукти аналізу і обробки ризиків інформаційної безпеки.	лаб.	[2-4]	4	1 тиждень
11	Тема 11. Оцінка захищеності інформаційних систем від несанкціонованого доступу та інших загроз інформаційній безпеці.	лекція, самостійна робота	[2-4]	2 10	2 тижні
	Тема 11. Оцінка захищеності інформаційних систем від несанкціонованого доступу та інших загроз інформаційній безпеці.	лаб.	[2-4]	4	2 тижні
12	Тема 12. ПЗ для розслідування комп'ютерних злочинів	лекція, самостійна робота	[2-4, 8]	2 8	1 тиждень

	Тема 12. ПЗ для розслідування комп'ютерних злочинів	лаб.	[2-4, 8]	2	1 тиждень
13	Тема 13. Апаратно-програмні засоби шифрування мобільного зв'язку.	лекція, самостійна робота	[2-4]	2 8	1 тиждень
	Тема 13. Апаратно-програмні засоби шифрування мобільного зв'язку.	лаб.	[2-4]	2	1 тиждень
14	Тема 14. Захищені модульні системи зберігання даних	лекція, самостійна робота	[2-4]	2 10	1 тиждень
	Тема 14. Захищені модульні системи зберігання даних	лаб.	[2-4]	4	1 тиждень