

**СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ  
«КОНКУРЕНТНА РОЗВІДКА ТА ОСНОВИ КІБЕРБЕЗПЕКИ»**

**1. Профіль дисципліни**

<i>Кафедра економіки</i>	<p>Ступінь вищої освіти – бакалавр, магістр Дні занять – відповідно до розкладу. Форма навчання – денна, заочна Компонент освітньої програми – вибіркова Консультації – відповідно до графіка навчального процесу. Мова викладання – українська.</p>
--------------------------	--

**2. Інформація про викладача**

<b>Викладач</b>	Д.е.н., в.о. професора Черевко Ірина Василівна
<b>Профайл викладача</b>	<a href="http://lnau.edu.ua/lnau/index.php/uk/component/content/article/7302.html">http://lnau.edu.ua/lnau/index.php/uk/component/content/article/7302.html</a>
<b>Контактна інформація</b>	irener@ukr.net

## **АНОТАЦІЯ**

Стрімке зростання інформаційних процесів у суспільстві, цифровізація економіки, нові технології, відкритість Інтернету і використання інформаційно-комунікаційних технологій призвело до появи кібератак і як ніколи раніше попит на фахівців з кібербезпеки. Крім того в Україні формується ринок розвідувальних послуг для комерційного успіху бізнес-структур та прийняття управлінських рішень, де необхідна чітка та проаналізована інформація, що дозволить вести конкурентну боротьбу в сучасному бізнес середовищі.

На сьогодні значення цієї специфічної сфери діяльності людини важко переоцінити. Особливо важливим є вивчення цього курсу здобувачами вищої освіти, оскільки у процесі господарської діяльності конкурентна розвідка виступає інструментом забезпечення безпеки і управління підприємств

### **МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Метою навчальної дисципліни є формування у студентів розуміння необхідності і методів та способів здійснення конкурентної розвідки для оцінки і підвищення бізнес-можливостей підприємства у конкурентному середовищі а також усвідомлення потреби та методів і способів забезпечення адекватного рівня кібербезпеки.

Завданням навчальної дисципліни є 1) ознайомити здобувачів освіти із сучасними пріоритетними технологіями та інструментами здійснення конкурентної розвідки в умовах зростаючих потоків інформації та підвищення темпів науково-технічного прогресу; 2) представити механізм зниження та нейтралізації бізнес-ризиків та загроз у сучасному конкурентному середовищі; 3) навчити ідентифкувати та аналізувати загрози безпеці у кіберпросторі в епоху глобальної цифровізації, в т.ч. кіберзлочини як окремий вид кіберзагроз; 4) сформувати вміння відбору та використання технологій протидії та боротьби з кіберзлочинами та попередження виникнення і елімінації кіберзагроз.

### **ОРГАНІЗАЦІЯ НАВЧАННЯ**

Основними видами навчальних аудиторних занять, під час яких здобувачі вищої освіти отримують необхідні знання, є лекції та практичні заняття. В межах робочого часу викладач може проводити консультації для здобувачів вищої освіти. Аналогічні форми навчання можуть бути при необхідності проводитись з використанням навчальних інтернет-платформ у режимі он-лайн.

При викладанні лекційного матеріалу передбачено поєднання таких форм і методів навчання, як лекції у формі бесіди, розповіді, пояснення, дискусії та лекції з відповідним ілюструванням і демонстрування за допомогою мультимедійних пристроїв.

Лекція у формі бесіди, розповіді, пояснення, дискусії дозволяє привернути увагу здобувачів вищої освіти до найбільш важливих питань теми лекції, винести на обговорення дискусійні питання та визначити у процесі інтерактивного комунікування особливостей сприйняття навчального матеріалу здобувачами освіти.

Лекція у формі ілюстрування і демонстрування за допомогою

мультимедійних пристроїв – це візуальна форма подачі лекційного матеріалу з розгорнутим або коротким коментуванням візуальних матеріалів, що переглядаються за допомогою мультимедійних технічних засобів. Ці дві форми лекцій можуть бути поєднані.

При проведенні практичних занять передбачене виконання практичних завдань у формі вирішення здобувачами вищої освіти ситуативних завдань (кейсів) і тестів, проведення ділових ігор, заслуховування усних відповідей, доповідей, а також рефератів та демонстрація презентацій, підготованих як індивідуальні завдання за темами, що виносяться на самостійне вивчення.

Здобувачі вищої освіти працюють з друкованими чи надісланими їм в електронній формі інформативним матеріалом та завданнями, або з інформацією в мережі Інтернет.

Процес вивчення здобувачами вищої освіти супроводжується вивченням позитивного досвіду провідних зарубіжних компаній із застосування конкурентної розвідки.

### **ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ») В АУДИТОРНИЙ ЧАС**

Лекції і практичні заняття можуть проводитися з використанням сервісу платформ ZOOM.US., Google Classroom, Microsoft Teams. Також викладач і здобувачі вищої освіти можуть спілкуватись через електронну пошту, навчальну платформу Moodle, Viber, Google Classroom, Microsoft Teams, Telegram інші доступні засоби комунікації. Усі завдання, передбачені програмою, мають бути виконані у встановлений термін. Якщо здобувач вищої освіти відсутній на занятті з поважної причини, він/вона презентує виконані самостійно завдання на консультації у викладача. Під час роботи над виконанням завдань не допускається порушення засад академічної доброчесності.

### **ПОРЯДОК ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ**

Підсумковий (семестровий) контроль з навчальної дисципліни «Конкурентна розвідка та основи кібербезпеки» здійснюється при закінченні семестру і проводиться відповідно до навчального плану у формі заліку (іспиту) в терміни, встановлені графіком навчального процесу та в обсязі навчального матеріалу, визначеному робочою програмою дисципліни.

**Політика оцінювання** – передбачає дотримання принципів академічної доброчесності та студентоцентрованого підходу.

**Академічна доброчесність** - дотримання вимог Положення про академічну доброчесність у ЛНУП». Доступне за посиланням: <https://www.lnup.edu.ua/attachments/article/2009/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%BF%D1%80%D0%BE%20%D0%B0%D0%BA%D0%B0%D0%B4%D0%B5%D0%BC%D1%96%D1%87%D0%BD%D1%83%20%D0%B4%D0%BE%D0%B1%D1%80%D0%BE%D1%87%D0%B5%D1%81%D0%BD%D1%96%D1%81%D1%82%D1%8C%20%D1%83%20%D0%9B%D0%9D%D0%90%D0%A3.pdf>

# **ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

## **ТЕМА 1. ПОНЯТТЯ КОНКУРЕНТНОЇ РОЗВІДКИ**

*Тенденції розвитку конкурентної розвідки. Проблеми та особливості розвитку конкурентної розвідки в Україні. Сфери застосування конкурентної розвідки, її значення та завдання у системі бізнесу. Правові засади конкурентної розвідки в Україні.*

*Конкурентна розвідка і захист комерційної таємниці, авторського права, персональних даних. Приклад провідних зарубіжних компаній із застосуванням конкурентної розвідки.*

## **ТЕМА 2. ВИДИ КОНКУРЕНТНОЇ РОЗВІДКИ**

*Види конкурентної розвідки. Особливості проведення мережевої (Інтернет-розвідки), економічної, технологічної, технічної, комп'ютерної, стратегічної, тактичної конкурентної розвідки. Конкурентна розвідка та OSINT (Open Sources INtelligence).*

*Бенчмаркінг (конкурентний моніторинг) як спосіб одержання конкурентних переваг. Характерні особливості та відмінності конкурентної розвідки та промислового шпигунства.*

*Кіберрозвідка (Threat Intelligence): характерні особливості, переваги, тенденції. Світовий ринок платформ та сервісів кіберрозвідки.*

## **ТЕМА 3. ОРГАНІЗАЦІЯ КОНКУРЕНТНОЇ РОЗВІДКИ СУБ'ЄКТА ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ.**

*Конкурентна розвідка як інструмент інформаційно-аналітичного супроводу забезпечення бізнесу та управління бізнес-діяльністю.*

*Місце конкурентної розвідки в діяльності компанії. Організація служби конкурентної розвідки. Алгоритм процесу конкурентної розвідки. Розвідувальна інформація у конкурентній розвідці. Обробка результатів конкурентної розвідки. Оцінка результативності конкурентної розвідки на корпоративному рівні.*

## **ТЕМА 4. КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ**

*Генезис проблеми кібербезпеки в контексті формування інформаційного суспільства. Суспільство як об'єкт інформаційного управління. Державна стратегія з протидії кібертероризму в Україні. Забезпечення захисту персональних даних в умовах розвитку цифрового суспільства та економіки. Технології глобального управління соціополітичними процесами в умовах реалізації кіберзагроз та ведення кібервійн. Засоби протистояння кібервпливу на особистість в умовах цифровізації суспільства.*

## **ТЕМА 5. КІБЕРТЕРОРИЗМ В АСПЕКТІ ГЛОБАЛІЗАЦІЇ: АКТУАЛЬНІ ПРОБЛЕМИ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ КІБЕРБЕЗПЕКИ**

*Кібертероризм: історія розвитку та сучасні тенденції. Загрози кібертероризму та найбільш відомі кібератаки в сучасному цифровому суспільстві як інформаційні виклики національній безпеці. Правові засади*

формування та розвитку державної системи протидії кібертероризму в Україні як загрози інформаційній безпеці. Зарубіжний досвід щодо розвитку систем протидії загрозам кібертероризму на державному рівні: національні структури, які забезпечують кібербезпеку у зарубіжних країнах, а також кібервійська провідних держав світу, їх можливості та перспективи. Національні команди реагування на надзвичайні комп'ютерні інциденти CERT/CSIRT. Міжнародні структури, які забезпечують кібербезпеку на глобальному рівні. Суб'єкти національної системи кібербезпеки України.

## РЕКОМЕНДОВАНІ ДЖЕРЕЛА

### Нормативно-правові акти

1. Конституція України: Закон України від 28. 06. 1996 р. / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
2. Цивільний кодекс України: Документ 435-IV, чинний, поточна редакція — Редакція від 01.08.2022, підстава - [1591-IX](https://zakon.rada.gov.ua/laws/main/435-15#Text). / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/main/435-15#Text>
3. Господарський процесуальний кодекс України Документ 1798-XII, чинний, поточна редакція — Редакція від 07.05.2022, підстава - [2079-IX](https://zakon.rada.gov.ua/laws/main/1798-12#Text) / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/main/1798-12#Text>
4. Про адміністративні послуги: <https://zakon.rada.gov.ua/laws/show/5203-17#Text>
5. Про інформацію: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
6. Про науково-технічну інформацію: Закон України від 25.06.1993 р. / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/main/3322-12#Text>
7. Про наукову і науко-технічну експертизу: Закон України від 10 лютого 1995 року. Документ 51/95-ВР, чинний, поточна редакція — Редакція від 16.10.2020, підстава - [124-IX](https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80#Text). <https://zakon.rada.gov.ua/laws/show/51/95-%D0%B2%D1%80#Text>
8. Про основні засади забезпечення кібербезпеки України: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
9. Про доступ до публічної інформації: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
10. Про електронні документи та електронний документообіг: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>
11. Про електронну комерцію: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/675-19#Text>
12. Про захист інформації в інформаційно-комунікаційних системах: Закон України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
13. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

## Основна література

1. Когут Ю. Кібервійни, кібертероризм, кіберзлочинність. Видавництво: Дакор, Консалтингова компанія Сідкон, 2022. 284 с.
2. Когут Ю. Корпоративна безпека: практичний посібник. Видавництво: Дакор, Консалтингова компанія Сідкон, 2021. 460 с.
3. Лісовська Ю. Кібербезпека. Ризики та заходи. Видавництво: Кондор, 2019. 272 с.
4. Мистецтво залишатися непоміченим. Хто ще читає ваші мейли/ пер. з англ. О. Асташова. К.: Наш Формат, 2019. 280 с.
5. Конкурентна розвідка підприємств : курс лекцій / І. С. Керницький, З. Б. Живко, М. І. Копитко. – Львів: Ліга-Прес, 2015. – 388 с.

## Додаткова література.

1. Андрощук Г. Глобальні стандарти етики штучного інтелекту. *Інтелектуальна власність*. 2021. № 11. С. 34-41.
2. Баконіна О. Для чого потрібна конкурентна розвідка Liga Zakon. [https://jurliga.ligazakon.net/intervyu/196164\\_dlya-chogo-potrnbna-konkurentna-rozvdka](https://jurliga.ligazakon.net/intervyu/196164_dlya-chogo-potrnbna-konkurentna-rozvdka)
3. Богуш В., Бровко В., Настрадін В. Основи кіберпростору, кіберзахисту та кібербезпеки. Видавництво: Ліра-К., 2021. 554 с.
4. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека»суспільства знань»: монографія. Київ-Одеса : Фенікс, 2021. 176 с.
5. Зянько В.В. Раціоналізація бізнесової поведінки підприємств України шляхом аналізу переваг та небезпек конкурентної розвідки та промислового шпигунства / В.В. Зянько, В.С. Ревенко // Причорноморські економічні студії. 2016. Вип. 6. С. 187-191
6. Інтеграція цифрових технологій в освітній процес: виклики та перспективи: монографія / Саєнко Н.С., Голуб Т.П., Лавриш Ю.Е., Лук'яненко В.В., Литовченко І.М. Видавництво: Центр навчальної літератури, 2022. 220 с.
7. Ковтуненко К.В., Парєва О.О. Конкурентна розвідка: сутність, підходи до визначення, задачі. *Економічний журнал Одеського політехнічного університету*. 2020. № 1 (11). С. 120-128. <https://economics.opu.ua/ejopu/2020/No1/120.pdf>. DOI: 10.15276/EJ.01.2020.15. DOI: 10.5281/zenodo.4664295.
8. Копотун І. М., Падалка А. М., Кузьмічова-Кисленко Є. В. Конкурентна розвідка: навчальний посібник. Ірпінь: Університет ДФС України, 2020. 188 с.
9. Кулініч О.О. Охорона та захист прав інтелектуальної власності: економіко-правові підходи. Видавництво «Ліра-К», 2019. 276 с.
10. Ланде Д.В., Правові питання конкурентної розвідки. *Інформація і право*. 2020. 2(33). С. 51-68. DOI: [https://doi.org/10.37750/2616-6798.2020.2\(33\).208089](https://doi.org/10.37750/2616-6798.2020.2(33).208089)
11. Скакун Т.О. Економічні злочини: сутнісні ознаки та криміналістичний аналіз їх вчинення [Електронний ресурс]/ – Режим Т.О. Скакун// Ефективна економіка. – 2018. – №3. – Режим доступу:<http://www.economy.nayka.com.ua/?op=1&z=6195>

12. Хвальчик І.Л. Конкурентна розвідка як засіб інформаційного забезпечення підприємства / І. Л. Хвальчик, С. В Філіппова // Економічний журнал Одеського політехнічного університету. – 2020. – № 1 (11). – С. 77-86. – Режим доступу до журн.: <https://economics.opu.ua/ejoru/2020/No1/77.pdf>. DOI: 10.15276/EJ.01.2020.9. DOI: 10.5281/zenodo.4529478.

### 13. Інформаційні ресурси

1. *Бібліотечно-інформаційні ресурси* - книжковий фонд читального залу Львівського НУП (м. Дубляни, вул. В. Великого, 1, Львівської наукової бібліотеки ім. Стефаника НАН України (вул. Стефаника, 2).

2. *Електронні інформаційні ресурси:*

Всесвітня організація інтелектуальної власності (ВОІВ). Режим доступу: <https://www.wipo.int/portal/en/index.html>

Міністерство захисту довкілля та природних ресурсів. Режим доступу: <https://mepr.gov.ua/>

Міністерство фінансів України. <https://www.mof.gov.ua/uk>

Міністерство юстиції України. Режим доступу: <https://minjust.gov.ua/>

Міністерство аграрної політики та продовольства України. <https://minagro.gov.ua/>

Офіційний портал Верховної Ради України. Режим доступу <https://www.rada.gov.ua/>

Національна бібліотека України ім. В. І. Вернадського. Режим доступу: <http://www.nbuv.gov.ua/>

Львівська національна наукова бібліотека ім. В. Стефаника. Режим <https://www.lsl.lviv.ua/index.php/uk/golovna2/>

Державне підприємство "Український інститут інтелектуальної власності" (Укрпатент). Режим доступу <https://ukrpatent.org/uk>

IP Center of Ukraine - Розвиток відносин у сфері інтелектуальної власності <https://www.facebook.com/uanipo>

Біржа промислової власності. Режим доступу: <http://exchange.iii.ua/uk>

Український інститут науково-технічної експертизи та інформації. Режим доступу: <http://www.uintai.kiev.ua/>

Журнал «Інтелектуальна власність в Україні». Режим доступу: <https://intelvlas.com.ua/>

Журнал «Інформація і право» Режим доступу: <http://ippi.org.ua/jpage/76>