**Львівський державний університет безпеки життєдіяльності**
**Навчально-науковий інститут цивільного захисту**

**Кафедра управління інформаційною безпекою**

## 1. Загальна інформація

| | |
|---|---|
| **Назва дисципліни** | Комп'ютерна криміналістика |
| **Статус дисципліни** | Нормативна |
| **Рівень вищої освіти, форма навчання** | перший(бакалаврський), денна форма |
| **Освітньо-професійна програма** | Управління інформаційною безпекою |
| **Спеціальність** | 125 Кібербезпека |
| **Рік навчання, семестр** | 4-й рік (7 семестр) |
| **Мова викладання** | українська |
| **Викладач** | Полотай Орест Іванович, к. т. наук, доцент кафедри управління інформаційною безпекою |
| **E-mail** | o.polotaj@ldubgd.edu.ua |
| **Сторінка курсу в ВУ** | http://virt.ldubgd.edu.ua/course/view.php?id=2698 |
| **Консультації** | Згідно розкладу консультацій кафедри управління інформаційною безпекою |

## 2. Анотація до курсу

Курс являє собою цикл лекційних та лабораторних занять, присвячених вивченню основних понять та методів цифрової криміналістики, навиків збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем.

Основні знання, що їх повинні набути здобувачі освіти, стосуються таких розділів: аналіз шкідливого програмного забезпечення, технічні канали витоку інформації, поняття та кримінологічна характеристика кіберзлочинності. розслідування кіберзлочинів, електронні (цифрові) докази, криміналістичне дослідження ОС Windows, мережне дослідження, аналіз журналів аудиту і дослідження трафіку мережі, криміналістичні дослідження безпровідних атак, атак на web застосування і сервера.

## 3. Мета і завдання курсу

**3.1. Метою** навчальної дисципліни є сформувати у студентів теоретичних знань основних принципів побудови сучасних мереж, до яких відносяться локальні, глобальні та регіональні мережі, за допомогою яких реалізовуються нові підходи управління сучасним інформаційним

суспільством, а також формування практичних навичок із побудови та управління корпоративними системами та мережами.

**3.2. Завдання:**

− діяти на основі законодавчої, нормативно-правової баз України та вимог відповідних стандартів, тому числі міжнародних;
− готувати пропозиції до нормативних актів щодо забезпечення інформаційної безпеки;
− обирати відповідну технологію програмування, виконати аналіз специфікації задач;
− виконувати аналіз програмного забезпечення з метою пошуку, ідентифікації, виявлення та усунення помилок програмування.

**3.3. Компетентності:**

*Загальні компетентності:*

– ЗК02 Знання та розуміння предметної області та розуміння професії.

*Спеціальні (фахові) компетентності:*

– ФК01 Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
– ФК02 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
– ФК08 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

**3.4. Програмні результати навчання:**

– РН04 Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
– РН07 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
– РН09 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
– РН19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
– РН42 Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
– РН43 Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

## 4. Формат і обсяг курсу

**Формат курсу** Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох змістових модулів, які є логічно завершеними, відносно самостійними, цілісними частинами, засвоєння яких передбачає проведення шести лабораторних робіт та аналіз результатів їх виконання. В процесі вивчення курсу здобувачі вищої освіти також повинні брати активну участь в обговорені дискусійних питань, вирішувати індивідуально та у групі ситуативні завдання.

**Обсяг дисципліни**: 4,5 кредити / 105 академічних годин, з яких: лекцій 32 години,

| | |
|---|---|
| **Форми навчання** | лабораторних 32 години, самостійної роботи 71 година.<br>лекції, лабораторні заняття, консультації, самостійна робота (в тому числі виконання здобувачами освіти індивідуальних завдань у поза аудиторний час з подальшою їх перевіркою на лабораторних заняттях). |

## 5. Тематика та зміст курсу

| Назви змістових модулів і тем | Кількість годин (денна форма) | | | | |
|---|---|---|---|---|---|
| | усього | у тому числі | | | |
| | | л | п | лаб | с.р. |
| 1 | 2 | 3 | 4 | 5 | 6 |
| **Змістовний модуль 1.** Термінологія та зміст основних понять. | | | | | |
| **Тема 1.** Вступ в комп'ютерну криміналістику. | 8 | 2 | | 2 | 4 |
| **Тема 2.** Комп'ютерні злочини: поняття, класифікація, захист | 8 | 2 | | 2 | 4 |
| **Тема 3.** Класифікація шкідливого програмного забезпечення | 8 | 2 | | 2 | 4 |
| **Тема 4.** Особливості розслідування комп'ютерних злочинів | 8 | 2 | | 2 | 4 |
| **Тема 5.** Поняття, завдання і структура криміналістичної техніки. Спеціальні технічні засоби в комп'ютерній криміналістиці | 8 | 2 | | 2 | 4 |
| **Тема 6.** Криміналістична трасологія. використання спеціальних знань при розслідуванні комп'ютерних злочинів. Цифрові сліди в комп'ютерній криміналістиці. | 8 | 2 | | 2 | 4 |
| **Тема 7.** Електронні (цифрові) докази. Криміналістичне дослідження ОС Windows | 8 | 2 | | 2 | 4 |
| **Тема 8.** Методи та засоби блокування технічних каналів витоку інформації. | 8 | 2 | | 2 | 4 |
| **Змістовний модуль 2.** Прогнозування. Методи прогнозування. | | | | | |
| **Тема 9.** Засоби копіювання даних. Збір даних та створення дублікатів носіїв даних. | 10 | 2 | | 2 | 6 |
| **Тема 10.** Відновлення видалених файлів і логічних розділів носіїв даних. Аналіз зібраної інформації | 10 | 2 | | 2 | 4 |
| **Тема 11.** Засоби блокування запису. | 8 | 2 | | 2 | 4 |
| **Тема 12.** Технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події. | 9 | 2 | | 2 | 5 |
| **Тема 13.**. Криміналістичні дослідження безпровідних атак, атак на web застосування і сервера. Мережне | 10 | 2 | | 2 | 6 |

| Назви змістових модулів і тем | Кількість годин (денна форма) | | | | |
|---|---|---|---|---|---|
| | усього | у тому числі | | | |
| | | л | п | лаб | с.р. |
| 1 | 2 | 3 | 4 | 5 | 6 |
| дослідження, аналіз журналів аудиту і дослідження трафіку мережі. | | | | | |
| **Тема 14.** Продукти аналізу і обробки ризиків інформаційної безпеки. | 8 | 2 | | 2 | 4 |
| **Тема 15.** Програмне забезпечення для розслідування комп'ютерних злочинів. | 10 | 2 | | 2 | 6 |
| **Тема 16.** Апаратно-програмні засоби шифрування мобільного зв'язку. | 8 | 2 | | 2 | 4 |
| **Усього годин за семестр** | 105 | 32 | | 32 | 71 |
| **Усього годин** | **105** | **32** | | **32** | **71** |

## 6. Інформаційний обсяг навчальної дисципліни

**Змістовний модуль 1. Термінологія та зміст основних понять.**

**Тема 1. Вступ в цифрову криміналістику.**

Комп’ютерна злочинність. Загрози інформаційної безпеки. Забезпечення інформаційної безпеки. Роль експертно криміналістичних підрозділів. Спеціальні технічні засоби.

**Тема 2. Комп’ютерні злочини: поняття, класифікація, захист печення.**

Класифікація комп’юиерних злочинів. Способи захисту від комп’юиерних злочинів.

**Тема 3. Класифікація шкідливого програмного забезпечення.**

Зловмисне програмне забезпечення. Поширені методи аналізу шкідливого програмного забезпечення. Огляд еврістичних методів виявлення шкідливого коду. Аналіз шкідливих програм методом візуалізації двійкових файлів.

**Тема 4. Особливості розслідування комп’ютерних злочинів.**

Криміналістична характеристика комп’ютерних злочинів. Початковий етап розслідування комп’ютерних злочинів. Проведення окремих слідчих (розшукових) дій.

**Тема 5. Поняття, завдання і структура криміналістичної техніки. Спеціальні технічні засоби в комп’ютерній криміналістиці.**

Завдання і структура криміналістичної техніки.Т засоби в комп’ютерній криміналістиці.

**Тема 6. Криміналістична трасологія. використання спеціальних знань при розслідуванні комп’ютерних злочинів. Цифрові сліди в комп’ютерній криміналістиці**

Поняття, предмет і завдання судової трасології.

**Тема 7. Електронні (цифрові) докази. Криміналістичне дослідження ОС Windows.**

Електронні докази. Криміналістичне дослідження ОС Windows.

**Тема 8. Методи та засоби блокування технічних каналів витоку інформації.**

Пасивні засоби захисту. Активні засоби захисту.

**Змістовний модуль 2. Прогнозування. Методи прогнозування.**

**Тема 9. Засоби копіювання даних. Збір даних та створення дублікатів носіїв даних.**

Концепції збору даних та створення дублікатів носіїв даних. Типи збору даних. Вимоги до засобів створення дублікату диска. Методи валідації. Рекомендації найкращих практик збору даних. Програмні та апаратні засоби збору даних. Правила безпечного зберігання даних. Програмне забезпечення для зберігання даних.

**Тема 10. Відновлення видалених файлів і логічних розділів носіїв даних. Аналіз зібраної**

**інформації.**
Відновлення видалених файлів. Засоби відновлення файлів для Windows. Засоби відновлення файлів для MAC. Засоби відновлення файлів для Linux. Відновлення видалених логічних розділів. Засоби відновлення логічних розділів. Аналіз зібраної інформації.

**Тема 11. Засоби блокування запису.**
Апаратні блокатори запису. Програмні блокіратори запису.

**Тема 12. Технічні особливості огляду засобів комп'ютерної техніки, виявлених на місці події.**
Огляд стандартних засобів комп'ютерної техніки. Огляд мобільних засобів комп'ютерної техніки із функцією телефону. Огляд автомобільних засобів комп'ютерної техніки.

**Тема 13.. Криміналістичні дослідження безпровідних атак, атак на web застосування і сервера. Мережне дослідження, аналіз журналів аудиту і дослідження трафіку мережі.**
Безпровідні технології. Атаки на безпровідні технології. Дослідження атак на безпровідні технології. Можливості кращих засобів криміналістичного дослідження безпровідних атак. Засоби криміналістичного дослідження безпровідних атак. Засоби захоплення трафіку і аналізу. Криміналістичне дослідження веб атак. Засоби виявлення веб атак. Криміналістичне дослідження мережі. Атаки ін'єкцій у журнали аудиту. Розслідування та аналіз журналів аудиту. Дослідження трафіку мережі. Захват трафіку і засоби його аналізу. Документування зібраних у мережі доказів.

**Тема 14. Продукти аналізу і обробки ризиків інформаційної безпеки.**
CRAMM. Risk. Watch. ГРИФ 2006. NIST. COBRA. OCTAVE.

**Тема 15. Програмне забезпечення для розслідування комп'ютерних злочинів.**
ACELab, ICS, Decision Group, Guidance Software, Cellebrite, Tableau, eDEC, iStorage, Barracuda Networks, X-Ways, NRTeam, Rapid7.

**Тема 16. Апаратно-програмні засоби шифрування мобільного зв'язку.**
Апаратно-програмні засоби захисту комп'ютерної інформації.

## 7. Завдання для самостійного опрацювання

З метою закріплення отриманих практичних навиків, здобувачі освіти виконують індивідуальні завдання, які отримують в кінці лабораторних занять. Лабораторні завдання відображені у електронному освітньому середовищі «Віртуальний університет». Перевірка правильності виконання лабораторних завдань проводиться на наступному практичному занятті.

## 8. Методи навчання

Основні форми організації навчання: лекції, лабораторні заняття із поточним контролем виконання індивідуальних завдань та проведенням тематичних лабораторних робіт, консультації.
Методи організації та здійснення навчально-пізнавальної діяльності:

- лекції – словесні та наочні методи навчання із елементами мозкового штурму;
- лабораторні завдання – частково-пошуковий метод навчання (певні елементи матеріалу відомі, решта студенти здобувають самостійно виконуючи завдання, тощо);
- консультації – словесний та дискусійний методи.

## 9. Технічне й програмне забезпечення /обладнання

Комп'ютери на базі процесорів Intel Pentium Gold G5400, компоненти програмного забезпечення MS Office 365 (Teams, PowerPoint, Word), електронне освітнє середовище "Віртуальний університет"(на базі платформи Moodle).

## 10. Критерії оцінювання

Оцінювання результатів навчання здобувачів вищої освіти здійснюється відповідно до «Положення про організацію освітнього процесу у ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/polozhennya_pro_organizaciyu_osvitnogo_procesu_ldu_bzhd_nova_redakciya_10.2020.pdf та «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/nakazy/polozh_ldubzhd_poryadok_ocinyuvannya_.pdf.

**Поточний контроль**

Поточний контроль проводитися у формі тестування та виконання лабораторних завдань. Оцінювання результатів поточного контролю здійснюється за національною (чотирибальною) шкалою. Результати поточного контролю (поточна успішність) враховуються викладачем при виставленні підсумкової оцінки за екзамен.

| Вид робіт | Формат проведення та критерії оцінювання |
|---|---|
| Тестові завдання | Курсом передбачено проходження 5 тестових завдань. Критерії оцінювання тестів наведені у електронному курсі «Віртуального університету». За успішне виконання тестових завдань сумарно можна отримати до 25 балів. Наприкінці семестру питання тестових завдань винесені у екзаменаційний тест. |
| Лабораторна робота | Курсом передбачено виконання та захист 6-ти лабораторних робіт. Типові завдання та критерії оцінювання наведені у електронному курсі «Віртуального університету». За виконання кожної лабораторної роботи можна отримати до 5 балів. |
| Робота на практичному занятті; самостійна робота | Оцінювання здійснюється за національною (чотирибальною) шкалою, відповідно до Додатку Б «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД». За роботу на лабораторних заняттях протягом семестру можна отримати до 30 балів. |

**Підсумковий контроль**

Семестровий контроль проводиться у формі екзамену. Допуск до семестрового контролю здійснюється за умови виконання здобувачем лабораторних робіт та успішно пройденими підсумковими тестами в середовищі «Віртуальний університет».

Екзамен **(максимально 45 балів)** складається із двох компонентів: тестування у електронному освітньому середовищі "Віртуальний університет" (максимум 15 балів) та розв'язуванні двох типових завдань по 15 балів кожна, які оцінюються:

- 15 балів – студент правильно виконав завдання.
- 10 - студент правильно виконав половину завдання.
- 5 - студент правильно виконав окремі завдання завдання.

Підсумкова семестрова оцінка обчислюється як сума балів поточного та підсумкового контролю за 100-бальною шкалою і переводяться в національну (чотирибальну) шкалу ("відмінно", "добре", "задовільно", "незадовільно", для заліків – "зараховано", "не зараховано").

Підсумкові оцінки виставляються та вносяться до екзаменаційної відомості, залікової книжки (позитивні результати) здобувача в національній, 100-бальній шкалі та шкалі ЄКТС відповідно до співвідношень, поданих у наступній таблиці.

**Шкала оцінювання результатів навчання здобувачів вищої освіти**

| Сума балів за всі види навчальної діяльності | Оцінка ECTS | Оцінка за національною шкалою | |
|---|---|---|---|
| | | для екзамену, диференційованого заліку, курсового проекту (роботи), практики | для заліку |

| | | | |
|---|---|---|---|
| 91 – 100 | **A** | відмінно | зараховано |
| 81-90 | **B** | добре | |
| 71-80 | **C** | | |
| 61-70 | **D** | задовільно | |
| 51-60 | **E** | | |
| 36-50 | **FX** | незадовільно | не зараховано |
| 0-35 | **F** | | |

## 11. Політика курсу

Виконання навчальних завдань і робота в курсі має відповідати вимогам «Кодекс академічної доброчесності та корпоративної культури ЛДУ БЖД» https://ldubgd.edu.ua/sites/default/files/1_nmz/nakazy/kodeks_akademichnoyi_dobrochesnosti_ta_korpo.pdf

*Академічні очікування від здобувачів* – своєчасне виконання завдань, передбачених силабусом дисципліни; обов'язкове відвідування і виконання практичних занять та завдань самостійної роботи.

*Політика щодо термінів виконання завдань та ліквідації академічної заборгованості:* терміни виконання завдань вказуються у електронному курсі «Віртуального університету». Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Відпрацювання академічної заборгованості з дисципліни можливо до дня проведення підсумкового контролю (відповідно до розкладу).

Недопущені до підсумкового контролю здобувачі освіти здійснюють перездачу в терміни, відведені для усунення академічної заборгованості у два етапи:

заборгованість із поточного контролю;

заборгованість із підсумкового контролю.

Ліквідація заборгованості поточного контролю відбувається шляхом проходження тестових завдань та виконання лабораторних робіт згідно із тематичним планом курсу. Ліквідація заборгованості з підсумкового контролю організовується в форматі перездачі екзамену.

*Дотримання принципів академічної доброчесності:* роботи (завдання) виконуються здобувачами самостійно, ідеї та ініціативи інших авторів використовуються лише при належно оформленному цитуванні.

*Поведінка в аудиторії* – неприпустимо запізнення та користування телефоном на заняттях, за винятком виконання громіздких обчисленнях та використанні додаткових програм в освітніх цілях; повага до думки інших колег; дотримання норм культури мовлення та ін.

## 12. Рекомендована література

### 12.1. Основна:

1. Полотай О.І. Роль комп'ютерної криміналістики у забезпеченні інформаційної безпеки. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення": матеріали Міжнародної наукової інтернет-конференції. – Тернопіль. вип. 67. 2022. – С. 41-43

2. Полотай О.І. Комп'ютерна криміналістика: основні завдання та проблеми. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення": матеріали Міжнародної наукової інтернет-конференції. – Тернопіль. вип. 68. 2022. – С. 29-30

3. *Шепітько В.Ю.* Криміналістика: Підручник / Кол. авт.: В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. / За ред. проф. В. Ю. Шепітька. — 4-е вид., перероб. і доп. — Х.: Право, 2008. — 464 с.

4. *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 Україні»), 2014. – 60 с.

5. *Федотов Н.Н.* Форензика – компьютерная криминалистика. М.: Юридический Мир, 2007. – 432 с.

6. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень: наказ Міністерства юстиції України № 53/5 від 08.10.1998 р. [із змінами і доповненнями на 22.01.2013] // Офіційний вісник України. – 1998. – № 46 (03.12.1998). – ст. 1715.

**12.2. Додаткова:**

2. Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet. Third Edition. Edited by Eoghan Casey. www.elsevierdirect.com/companions/9780123742681.

3. Handbook of Digital Forensics and Investigation Edited by Eoghan Casey. http://www.elsevierdirect.com/product.jsp?isbn=9780123742674.

4. Digital Forensics and Preservation. Digital Preservation Coalition and Jeremy Leighton John. [Електронний ресурс] / Published in association with Charles Beagrie Ltd. 2012. Режим доступу: http://dx.doi.org/10.7207/twr12-03.

5. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, Second Edition (Information Security) Auerbach Publications; 2 edition (December 19, 2007).

6. Good Practice Guide for Computer-Based Electronic Evidence. Official release version 4.0. Published by 7Safe. www.7safe.com

7. Dan Farmer, Wietse Venema. Forensic Discovery. Pearson Education, Inc., December 2004.

8. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.

9. Davidoff, Sherri. Network forensics : tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. Pearson Education, Inc. 2012.

**12.3. Інформаційні ресурси:**

1. Віртуальний університет ЛДУ БЖД [Електронний ресурс]. — Режим доступу: http://virt.ldubgd.edu.ua/
2. Елкетронний ресурси з основ комп'ютерної криміналістики. [Електронний ресурс] — Режим доступу: https://www.securitylab.ru/blog/personal/Informacionnaya_bezopasnost_v_detalyah/344671.php

Розглянуто на засіданні кафедри управління інформаційною безпекою
протокол від «___» _____ №___

РОЗРОБНИК
Доцент кафедри управління інформаційною безпекою
кандидат технічних наук

ЗАТВЕРДЖЕНО
Завідувач кафедри управління інформаційною безпекою
доктор технічних наук, доцент

**Львівський державний університет безпеки життєдіяльності**
**Навчально-науковий інститут цивільного захисту**

_____ Орест ПОЛОТАЙ
«___» _____ 20__ р.

_____ Ростислав ТКАЧУК
«___» _____ 20__ р.

ПОГОДЖЕНО
Гарант освітньої програми «Управління інформаційною безпекою»
першого (бакалаврського) рівня вищої освіти

_____ Орест ПОЛОТАЙ
«___» _____ 20__ р.

ПОГОДЖЕНО
Заступник начальника навчально-наукового інституту цивільного захисту

_____ Ольга МЕНЬШИКОВА
«___» _____ 20__ р.

| | | | | | |
|---|---|---|---|---|---|
| Дата актуалізації* | | | | | |
| Підпис | | | | | |
| Ім’я, прізвище завідувача кафедри | | | | | |