ДЕРЖАВНА СЛУЖБА УКРАЇНИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ (СИЛАБУС)

## ОК 27 «Інструменти кібербезпеки»

(назва навчальної дисципліни)

Рівень вищої освіти: перший (бакалаврський)

Галузь знань: 12 Інформаційні технології

Спеціальність (*спеціалізація*) 125 Кібербезпека та захист інформації

Освітня програма: Управління інформаційною безпекою

Львів 2025

РОЗРОБЛЕНО

Викладач кафедри управління інформаційною безпекою

_____ Артур ТКАЧЕНКО
(підпис) (ім’я, прізвище)

«26» серпня 2025р.

ЗАТВЕРДЖЕНО

Начальник кафедри управління інформаційною безпекою, кандидат технічних наук, доцент

_____ Андрій ІВАНУСА
(підпис) (ім’я, прізвище)

«26» серпня 2025р.

ПОГОДЖЕНО

Гарант освітньої програми «Управління інформаційною безпекою» першого (бакалаврського) рівня вищої освіти, професор кафедри управління інформаційною безпекою, доктор технічних наук, професор

_____ Ростислав ТКАЧУК
(підпис) (ім’я, прізвище)

«26» серпня 2025р.

ПОГОДЖЕНО

Заступник начальника навчально-наукового інституту цивільного захисту, кандидат фізико-математичних наук, доцент

_____ Ольга МЕНЬШИКОВА
(підпис) (ім’я, прізвище)

«26» серпня 2025р.

Розглянуто та затверджено на засіданні кафедри управління інформаційною безпекою, протокол від «26» серпня 2025р. №1

Розглянуто Вченою радою навчально-наукового інституту цивільного захисту, протокол від «15» вересня 2025 № 1

Актуалізовано:

| | | | | | |
|---|---|---|---|---|---|
| Дата перегляду / внесення змін | | | | | |
| Підпис | | | | | |
| Ім’я, прізвище викладача | | | | | |

## 1. Загальна інформація

| | |
|---|---|
| Назва дисципліни | ОК 27. Інструменти кібербезпеки |
| Статус дисципліни | Нормативна |
| Рівень вищої освіти | Перший (бакалаврський) |
| Освітньо-професійна програма | Управління інформаційною безпекою |
| Спеціальність | 125 Кібербезпека та захист інформації |
| Рік навчання, семестр | 3-й рік (5, 6 семестр) |
| Мова викладання | українська |
| Викладачі | ТКАЧЕНКО Артур Мар'янович, викладач кафедри управління інформаційною безпекою |
| Контактний телефон | – |
| Електронна пошта | Ar.Tkachenko@ldubgd.edu.ua |
| Сторінка курсу в ВУ | https://virt.ldubgd.edu.ua/course/view.php?id=4288 |
| Консультації | Згідно розкладу консультацій кафедри управління інформаційною безпекою. Також можливі он-лайн консультації через Skype, Viber, WhatsApp, Microsoft Teams, Element або інші інформаційні ресурси. Для погодження часу он-лайн консультацій слід писати на електронну пошту викладача або телефонувати. |

## 2. Анотація до курсу

Курс являє собою цикл лекційних та лабораторних занять, присвячених вивченню інструментів кібербезпеки. Є нормативною компонентою освітньої програми «Управління інформаційною безпекою». Структуру та зміст курсу побудовано на основі використання моделей, методів та механізмів формування інформаційної безпеки України та інших держав світу, провідних світових підприємств та підприємств із врахування практичних аспектів сьогодення.

## 3. Мета і завдання курсу

**Мета** навчальної дисципліни – ознайомлення здобувачів з основними інструментами кіберзахисту, сучасними інформаційними ресурсами, які надають інформацію про методи та засоби атак на інформаційні ресурси та захисту від них. Оволодіння практичними навиками та методами кіберзахисту від різних типів загроз.

**Завдання:**

— надання здобувачам навичок роботи з існуючими програмними засобами захисту інформації;

— ознайомлення з існуючими методами атак на кінцеві точки, локальні мережі, розподілені мережі організації і захисту від них;

— ознайомлення з основними інформаційними ресурсами, які наводять аналіз і дослідження кібератак і надають рекомендації щодо захисту від них;

— ознайомлення з основними загрозами в роботі протоколів Інтернету;

— вивчення комплексу програмних засобів для тестування та проведення атак на системи захисту інформації;

— вивчення системи, які забезпечують захист і дієздатність інформаційних ресурсів.

Процес вивчення дисципліни спрямований на формування елементів таких **компетентностей:**

**Загальні (ЗК):**

ЗК2 Знання та розуміння предметної області та розуміння професії.

ЗК5 Здатність до пошуку, оброблення та аналізу інформації.

**фахових (ФК):**

ФК4 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки.

ФК6 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

ФК9 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

ФК12 Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки.

**Програмні результати навчання (ПРН):**

РН23 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

РН25 Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно- телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

РН26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

РН30 Здійснювати оцінювання можливості несанкціонованого доступу до

елементів інформаційно-телекомунікаційних систем.

РН31 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

РН36 Виявляти небезпечні сигнали технічних засобів.

РН49 Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

РН50 Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).

РН52 Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен: знати: основні протоколи Інтернету, їх призначення, формати та опції повідомлень; знати та вміти користуватися сервісами безпеки, зокрема екрануванням, протоколюванням та аудитом; знати як функціонують основні послуги Інтернету – www, електронна пошта, передача аудіо та відео через мережу, IP-телефонія; ознайомитися з різними типами брандмауерів, які використовуються для захисту ІС; знати які і де (відносно архітектури LAN) мають використовуватися; вміти формувати правила на них; ознайомитися з принципами роботи IDS для захисту ІС. Основні методи та засоби несанкціонованого проникнення в систему і програми для їх виявлення, аналізу вразливостей конфігурації, архітектури та програмного коду, що використовується в ін-формаційних системахі.

вміти: орієнтуватися в забезпеченні функціонування Інтернету – протоколи стеку TCP/IP; орієнтуватися в адресному просторі Інтернету; орієнтуватися в системі доменних імен; використовувати засоби екранування для захисту інформації; встановлювати необхідні правила на Firewall - ах; працювати в мережі з основними сервісами безпеки; використовувати можливості Intrusion Detection Systems (IDS) для захисту і контролю внутрішніх мереж; вміти забезпечувати безпеку web-серверів; користуватися багатофункціональними засобами аудиту і запобігання несанкціонованого вторгнення в систему; використовувати засоби виявлення, дослідження і реагування на інциденти; використовувати засоби збору доказів спроб атак та успішно проведених атак на підзахисну систему; орієнтуватися в програмних засобах для атаки на безпеку інформації та вміти протидіяти їм.

## 4. Передумови для вивчення дисципліни

Передумовами для вивчення курсу є наявність систематичних та ґрунтовних знань з навчальних предметів: ОК14 Комп'ютерна логіка, ОК16 Архітектура комп’ютера та операційні системи, ОК17 Основи WEB розробки, ОК20 Комп'ютерні мережі, ОК21 Проектування та захист WEB додатків, ОК23 Етичний хакінг в комп’ютерних системах та мережах, ОК24 Програмування Python в кібербезпеці.

Ці передумови допоможуть студентам успішно засвоїти матеріал курсу та ефективно застосовувати отримані знання на практиці.

## 5. Формат і обсяг дисципліни

| | |
|---|---|
| **Формат курсу** | Навчальний матеріал дисципліни структурований за тематичним принципом і складається з двох змістових модулів, які є логічно завершеними, відносно самостійними, цілісними частинами, засвоєння яких передбачає проведення чотирнадцятьох лабораторних робіт, тестування 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**: | 8,5 кредитів / 255 академічних годин, з яких:<br>лекції – 48 год.,<br>лабораторні – 64 год.,<br>самостійна робота – 143 год. |
| **Форми навчання** | лекції, лабораторні заняття, консультації, самостійна робота (з подальшою їх перевіркою на лабораторних заняттях) |

## 6. Тематика та зміст курсу

| Назви змістових модулів і тем | Кількість годин | | | | | |
|---|---|---|---|---|---|---|
| | Усього | у тому числі | | | | |
| | | Лекції | Практичні/ семінарські | Лабораторні | Практичні двома | Самостійна робота |
| **5-ий семестр** | | | | | | |
| Змістовний модуль 1. Сервіси безпеки, екранування та засоби тестування вразливостей інформаційних систем. | | | | | | |
| Тема 1. Віртуальна лабораторія. Засоби перегляду файлів та редактори загального призначення | 15 | 3 | - | 4 | - | 8 |
| Тема 2. Класифікація firewall-ів. | 12 | 2 | - | 3 | - | 7 |
| Тема 3. Політики firewall-у. | 12 | 2 | - | 3 | - | 7 |
| Тема 4. Різні типи середовища навколо firewall-у. | 13 | 2 | - | 4 | - | 7 |
| Тема 5. DMZ. VPN-мережі. | 13 | 3 | - | 3 | - | 7 |
| Тема 6. Intrusion Detection/Prevention Systems (IDS/IPDS). | 12 | 2 | - | 3 | - | 7 |
| Тема 7. Сканери портів. | 12 | 2 | - | 3 | - | 7 |
| Тема 8. Сканери вразливостей. | 12 | 2 | - | 3 | - | 7 |

| Назви змістових модулів і тем | Кількість годин | | | | | |
|---|---|---|---|---|---|---|
| | Усього | у тому числі | | | | |
| | | Лекції | Практичні/ семінарські | Лабораторні | Практичні двома | Самостійна робота |
| Тема 9. Системні утиліти різних ОС | 13 | 3 | - | 3 | - | 7 |
| Тема 10. Засоби зламу паролів. | 13 | 3 | - | 3 | - | 7 |
| **Усього годин за семестр** | **127** | **24** | **-** | **32** | **-** | **71** |
| **6-ий семестр** | | | | | | |
| Змістовий модуль 2. Засоби аудиту, виявлення інцидентів і збору доказів в інфраструктурі інформаційних систем | | | | | | |
| Тема 11. Засоби зламу Web-прикладень. | 14 | 3 | - | 4 | - | 7 |
| Тема 12. Програми віддаленого доступу «чорний хід». | 12 | 2 | - | 3 | - | 7 |
| Тема 13. Засоби аудиту вихідних кодів. | 12 | 2 | - | 3 | - | 7 |
| Тема 14. Засоби системного аудиту. | 14 | 2 | - | 3 | - | 7 |
| Тема 15. Аналізатори мережних потоків. | 13 | 3 | - | 3 | - | 7 |
| Тема 16. Засоби виявлення бездротових мереж. | 13 | 2 | - | 3 | - | 8 |
| Тема 17. Інструменти цифрового криміналістичного аналізу. | 12 | 2 | - | 3 | - | 7 |
| Тема 18. Інфраструктура мережевої безпеки | 12 | 2 | - | 3 | - | 7 |
| Тема 19. Оцінка вразливості кінцевої точки та її захист | 13 | 3 | - | 3 | - | 7 |
| Тема 20. Робота з даними мережевої безпеки. Оцінювання попереджень | 13 | 3 | - | 3 | - | 7 |
| Усього годин за семестр | **128** | **24** | | **32** | | **72** |
| **Усього годин** | **255** | **48** | | **64** | | **143** |

## 7. Інформаційний обсяг навчальної дисципліни

*7.1.Теми лекційних занять*

| № | Назва теми | Кількість годин |
|---|---|---|
| 1. | Віртуальна лабораторія. Засоби перегляду файлів та редактори загального призначення | 3 |
| 2. | Класифікація firewall-ів. | 2 |
| 3. | Політики firewall-у. | 2 |
| 4. | Різні типи середовища навколо firewall-у. | 2 |
| 5. | DMZ. VPN-мережі. | 3 |
| 6. | Intrusion Detection/Prevention Systems (IDS/IPDS). | 2 |
| 7. | Сканери портів. | 2 |
| 8. | Сканери вразливостей. | 2 |
| 9. | Системні утиліти різних ОС | 3 |

| № | Назва теми | Кількість годин |
|---|---|---|
| 10. | Засоби зламу паролів. | 3 |
| 11. | Засоби зламу Web-прикладень. | 3 |
| 12. | Програми віддаленого доступу «чорний хід». | 2 |
| 13. | Засоби аудиту вихідних кодів. | 2 |
| 14. | Засоби системного аудиту. | 2 |
| 15. | Аналізатори мережних потоків. | 3 |
| 16. | Засоби виявлення бездротових мереж. | 2 |
| 17. | Інструменти цифрового криміналістичного аналізу. | 2 |
| 18. | Інфраструктура мережевої безпеки | 2 |
| 19. | Оцінка вразливості кінцевої точки та її захист | 3 |
| 20. | Робота з даними мережевої безпеки. Оцінювання попереджень | 3 |
| **Разом** | | **48** |

Короткий зміст лекційних занять охоплює кілька важливих тем, які стосуються побудови віртуальнаної лабораторії для дослідження інструментів кібербезпеки та шкідливого програмного забезпечення. Засоби перегляду файлів та редактори загального призначення.

Далі обговорюються firewall-и. Їх класифікація , застосування, функціонал, політики та архітектуру мереж, які з їх допомогою можна розбудовувати. Типи та функціонал систем захисту локальних мереж , та кінцевих точок – Intrusion Detection/Prevention Systems (IDS/IPDS).

У рамках курсу обговорюються утиліти та прогрмні комплекси для роботи blue та red teams: сканери портів, сканери вразливостей, засоби відновлення паролів.

Наступні лекції присвячені засобам зламу/тестування Web-прикладень. Програмам віддаленого доступу - «чорний хід». Розглядаються засоби аудиту вихідних кодів та системного аудиту. Аналізатори мережних потоків. Засоби виявлення бездротових мереж.

Окрема тема присвячена ознайомленню з інструментами цифрового криміналістичного аналізу.

Далі розглядаються теми, присвячені інфраструктурі мережевої безпеки. Служби та сервіси безпеки. Оцінка вразливості кінцевої точки та її захист. Профілювання мережі та серверів Загальна система оцінки вразливості – CVSS. Безпечне управління пристроями. Системи управління інформаційною безпекою – ISMS. Захист від шкідливих програм. Запобігання проникненню на основі хоста. Безпека додатків.

У рамках курсу також обговорюються системи адміністрування локальних

мереж такі, як Identity Manager-и, системи Mobile Device Management-у (MDM), систем управління конфігураціями Configuration management tools, управління оновленнями – Patch Management tools та управління інформаційною безпекою – Information Security Management Systems (ISMS).

На завершення розглядаються питання роботи з даними мережевої безпеки. Оцінювання попереджень. SIEM. SOAR. A Common Data Platform. ELK. Security Onion. Logstash, Beats, Elasticsearch та Kibana, Sguil. SPLUNK. Джерела отримання попереджень (alerts) та їх оцінювання.

## 8. Теми практичних, семінарських та лабораторних занять

*8.1.Практичні заняття не передбачені*

*8.2.Семінарські заняття не передбачені.*

*8.3.Теми лабораторних занять*

| № | Назва теми | Кількість годин |
|---|---|---|
| 1. | Аналіз та порівняння характеристик Firewall-ів апаратних і програмних від різних виробників. | 6 |
| 2. | Аналіз можливостей IDS, IPS , DLP різних виробників. | 4 |
| 3. | Аналіз та порівняння можливостей сканерів портів та сканерів вразливостей. | 4 |
| 4. | Аналіз роботи програм відновлення паролів | 4 |
| 5. | Аналіз роботи програм моніторингу та адміністрування мережі, віддаленого доступу та створення “чорного ходу” | 4 |
| 6. | Аналіз і можливості застосування аналізаторів мережних потоків (сніффери) | 4 |
| 7. | Ознайомлення та аналіз функціоналу інструментів цифрового криміналістичного дослідження. | 6 |
| 8. | Аналіз функціоналу та порівняння Identity Manager-ів | 6 |
| 9 | Аналіз функціоналу та порівняння систем Mobile Device Management-у (MDM) | 6 |
| 10 | Аналіз функціоналу та порівняння систем управління конфігураціями Configuration management tools | 6 |
| 11 | Аналіз функціоналу та порівняння систем управління оновленнями – Patch Management tools | 6 |
| 12 | Аналіз функціоналу та порівняння систем управління інформаційною безпекою – Information Security Management Systems (ISMS) | 6 |
| 13 | Аналіз засобів конфіденційності в Інтернеті. | 4 |

| | | |
|---|---|---|
| 14 | Аналіз засобів віртуалізації для дослідження загроз безпеці інформації та спеціалізованих (для спеціалістів кібербезпеки) ОС. | 6 |
| **Разом** | | **64** |

## 9. Завдання для самостійного опрацювання

| № | Назва теми/види завдань | Кількість годин |
|---|---|---|
| 1. | Віртуальна лабораторія. | 12 |
| 2. | firewall-и – функціонал, класифікація, політики. DMZ. VPN-мережі | 12 |
| 3. | Intrusion Detection/Prevention Systems (IDS/IPDS). | 12 |
| 4. | Сканери портів. | 11 |
| 5. | Сканери вразливостей. | 12 |
| 6 | Засоби зламу паролів. | 12 |
| 7 | Засоби зламу Web-прикладень. | 12 |
| 8 | Програми віддаленого доступу «чорний хід». | 12 |
| 9 | Засоби аудиту вихідних кодів. | 12 |
| 10 | Аналізатори мережних потоків. | 12 |
| 11 | Інструменти цифрового криміналістичного аналізу. | 12 |
| 12 | Інфраструктура мережевої безпеки | 12 |
| **Разом** | | **143** |

## 10. Методи навчання

Основні форми організації навчання: лекції, лабораторні заняття із поточним контролем виконання індивідуальних завдань та проведенням тематичних лабораторних робіт, курсовий проект, консультації.

Методи організації та здійснення навчально-пізнавальної діяльності:

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

## 11. Технічне й програмне забезпечення /обладнання

Апаратне забезпечення: ноутбуки на базі процесорів Intel U7-255U – 20 шт., Uninterruptible Power Supply Eaton 9E 3000VA/2400W LCD USB RS232 6xC13 1xC19/Джерело безперебійного живлення Eaton 9E, 3000VA/2400W, LCD,

USB, RS232, 6xC13, 1xC19 - кількість 1 шт., PowerEdge R260 Server [PowerEdge R260 - Full Configuration - [EMEA_R260]]/ Сервер Dell PowerEdge R260 - кількість 1 шт., мультимедійний проєктор – EPSON EB-536WI,

Програмне забезпечення: операційна система Windows 11, компоненти програмного забезпечення MS Office 365 (Teams, PowerPoint, Word, Excel), Zoom Workplace, електронне освітнє середовище “Віртуальний університет”(на базі платформи Moodle).

Nessus Professional — призначений для сканування мереж і систем з метою виявлення вразливостей та проблем безпеки.

Windows Server 2019 Datacenter — серверна операційна система для розгортання, тестування та адміністрування IT-інфраструктури.

Hydra — інструмент для підбору паролів до різних сервісів методом brute force.

FTK Imager — призначений для створення образів дисків і збору цифрових доказів без зміни оригінальних даних.

Wireshark — застосовується для перехоплення та аналізу мережевого трафіку в реальному часі.

The Sleuth Kit — набір інструментів командного рядка для аналізу файлових систем і розслідування інцидентів.

Trend Micro Worry-Free XDR — призначений для виявлення, аналізу та реагування на кіберзагрози на рівні кінцевих пристроїв, серверів і електронної пошти.

ОС: Security Onion, Black Arch, Kali Linux, Parrot Security OS, Tails, Whonix.

## 12. 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/nakazy/polozhennya_pro_organizaciyu_osvitnogo_procesu_2024.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 проводится за виконання лабораторних робіт та звітування у вигляді доповіді, які виносяться на лабораторні заняття. Оцінювання результатів поточного контролю здійснюється за п'ятибальною шкалою, відповідно до Додатку Б «Положення про порядок та критерії оцінювання результатів навчання здобувачів вищої освіти у ЛДУ БЖД». Результати поточного контролю (поточна успішність) враховуються викладачем при виставленні підсумкової оцінки за екзамен.

| Вид робіт | Формат проведення та критерії оцінювання |
|---|---|
| **Лабораторна робота** | Курсом передбачено виконання 14 лабораторних робіт. За роботу на лабораторних заняттях протягом семестру можна отримати до 3 балів за роботу, в сумі **42 бали**. |
| **Індивідуальні завдання (доповіді)** | Звітування у вигляді доповіді, які виносяться на лабораторні заняття загалом за семестр оцінюється до **7 балів**. |

**Підсумковий контроль**

Семестровий контроль проводиться у формі екзамену. Допуск до семестрового контролю здійснюється за умови виконання здобувачем усіх лабораторних робіт. (максимально 42 бали).

Екзамен (максимально **51 бал**) складається з результатів відповідей на екзаменаційний білет. Білет формується з трьох запитань.

Критерії оцінювання відповідей: за кожну правильну відповідь здобувач отримує до 17 балів

14-17 балів – здобувач правильно вирішив завдання.

9-13 балів – здобувач правильно вирішив основну частину завдання (представив повний алгоритм рішеня), але не отримав остаточного результату.

5-8 – здобувач вирішив основну частину завдання, допустивши помилки.

0-4 – здобувач вирішив правильно окремі завдання (менше половини).

Здобувач допускається до підсумкового контролю, якщо він набрав не менше 50% від загальної кількості відведених балів на поточний контроль.

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”).

Підсумкові оцінки виставляються та вносяться до екзаменаційної відомості 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** | | |

## 13. 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 виконання контрольних та індивідуальних 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 оформленому цитуванні.

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

## 14. Рекомендована література

**Основна література:**

1. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
2. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).
3. ДСТУ ISO/IEC 27000:2015. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT).

4. Про інформацію : Закон України від 2 жовт. 1992 р. № 2657-XII. URL: http://www.rada.gov.ua.

5. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу : НД ТЗІ 1.1-002-99. Київ : ДСТСЗІ СБ України, 1999. 16 с.

6. ДСТУ 7564:2014. Інформаційні технології. Криптографічний захист інформації. Функція хешування. Київ : ПАТ «Інститут інформаційних технологій» Мінекономрозвитку України, 2016. 228 с.

7. Грайворонський М. В., Новіков О. М. *Безпека інформаційно-комунікаційних систем*. Київ : BHV, 2009. 607 с.

8. Muniz J., Lakhani A. *Web Penetration Testing with Kali Linux*. Birmingham : Packt Publishing, 2013. 342 p.

9. MITRE ATT&CK : вебсайт. URL: https://attack.mitre.org/matrices/enterprise/.

10. Ivanusa A., Tkachuk R., Brych T., Balatska V., Tkachenko A. Методи та моделі проєктування системи автоматизованого пошуку вразливостей у WEB-додатках // *Вісник Львівського державного університету безпеки життєдіяльності*. 2024. № 30. С. 110–122. DOI: https://doi.org/10.32447/20784643.30.2024.11.

11. Ткачук Р. Л., Івануса А. І., Ящук В. І., Маслова Н. О., Ткаченко А. М. Управління інформаційною безпекою та кіберзахистом у закладах вищої освіти // *Вісник ЛДУБЖД : зб. наук. праць*. Львів : ЛДУБЖД, 2025. № 31. С. 101–116. DOI: https://doi.org/10.32447/20784643.31.2025.11.

**Додаткова література:**

1. Sanders Ch. *Practical Packet Analysis: Using Wireshark to Solve Real-World Problems*. 3rd ed. San Francisco, 2017. 450 p.

2. Miller J. D. *Implementing Splunk 7*. 3rd ed. Birmingham : Packt Publishing, 2018. 490 p.

3. Knerler K., Parker I., Zimmerman C. *11 Strategies of a World-Class Cybersecurity Operations Center*. The MITRE Corporation, 2022. 452 p.

4. Ткаченко А. М., Ткачук Р. Л., Андріїв Р. Р. Розроблення та застосування експлойтів з подальшою інтеграцією в ботнет. *Безпека інформаційних технологій* : матеріали XIII Міжнародної науково-технічної конференції ITSec-2024 (Львів, 9–11 травня 2024 р.). Львів : ЛНУ ім. І. Франка, 2024. С. 200–202.

5. Ткаченко А., Ткачук Р. Кібербезпека: комплекс заходів щодо захисту критичної інфраструктури в умовах сучасних загроз. *Цивільний захист в умовах війни* : зб. тез доповідей І Міжнародної науково-практичної конференції (Львів, 17-18 квітня 2025 р.). Львів: ЛДУ БЖД, 2025. С. 128–291.

**Інформаційні ресурси:**

1. Віртуальний університет ЛДУ БЖД : вебсайт. URL: http://virt.ldubgd.edu.ua/.

2. Безпека програмного забезпечення / Брич Тарас Богданович : електронний курс. URL: http://virt.ldubgd.edu.ua/course/view.php?id=2458.
3. Kali Linux – Website Penetration Testing : вебсайт. URL: https://www.tutorialspoint.com/kali_linux/kali_linux_website_penetration_testing.htm.
4. MITRE ATT&CK : вебсайт. URL: https://attack.mitre.org/.
5. FIRST – Forum of Incident Response and Security Teams : вебсайт. URL: https://www.first.org/