ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ
Проректор з методичної роботи
_____ Ярослав ШТАНЬКО
"29" 08 2025 р.

Захист інформації в комп'ютерних системах

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань:	12 Інформаційні технології
Спеціальність:	121 Інженерія програмного забезпечення
Освітньо-професійна (освітньо-наукова) програма:	Розробка та тестування програмного забезпечення
Освітній рівень:	перший (бакалаврський)
Статус дисципліни:	обов'язкова
Мова викладання, навчання та оцінювання:	українська

Івано-Франківськ
2025

РОЗРОБНИК:

викладач кафедри інформаційних технологій Владислав Василенко

ЗАТВЕРДЖЕНО:

на засіданні кафедри інформаційних технологій, протокол № 1 від 28.08.2025 р.

Завідувач кафедри Олександр ІВАНОВ

УЗГОДЖЕНО:

Гарант ОПП/ОНП Володимир МАКОВИШИН

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 1 від 29.08. 2025 р.

e-mail	vladyslav.v.vasylenko@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра інформаційних технологій
Сторінка курсу в СДО	https://online.ukd.edu.ua/course/view.php?id=6442

ВСТУП

Мета вивчення дисципліни "Захист інформації в комп'ютерних системах" – отримання студентами теоретичних знань та практичних навиків щодо основ кібербезпеки, методів та засобів атак на комп'ютерні системи, методів захисту інформації, а також методик проектування програмного забезпечення з метою мінімізації ризиків його зламу.
Для досягнення мети поставлені такі основні **завдання:**

- ознайомити студентів з концепцією тріади CIA та заходів, що забезпечують реалізацію її складових;
- навчити студентів виконувати аналіз комп'ютерних систем на предмет вразливостей з метою їх усунення;
- ознайомити студентів з методами та засобами збору інформації про комп'ютерну систему з відкритих джерел та інструментами, що знаходяться у відкритому доступі;
- ознайомити студентів з типовими вразливостями, які може містити програмне забезпечення та методиками їх усунення або мінімізації на етапі проектування та реалізації;
- ознайомити студентів з засобами захисту комп'ютерних систем, аналізу наслідків атаки та їх усунення.

У результаті вивчення навчальної дисципліни студент повинен:

знати:

- складові тріади CIA
- методи атак на комп'ютерні системи
- засоби атак на комп'ютерні системи
- наслідки атак на комп'ютерні системи
- методи захисту комп'ютерних систем
- методики проектування програмного забезпечення з метою мінімізації його вразливості до атак

вміти:

- застосовувати інструменти збору та аналізу інформації про роботу комп'ютерних систем;
- використовувати зібрану інформацію з метою виявлення можливих вразливостей та їх усунення;
- застосовувати методи захисту комп'ютерних систем;
- застосовувати рекомендації щодо розробки стійкого до зламу програмного забезпечення.

Професійні компетентності та результати навчання, яких набувають здобувачі внаслідок вивчення навчальної дисципліни «Захист інформації в комп'ютерних системах» (шифри та зміст компетентностей та програмних результатів вказані відповідно до освітньої програми "Розробка та тестування програмного забезпечення")

Шифр та назва компетентності	Шифр та назва результату навчання
К01. Здатність до абстрактного мислення, аналізу та синтезу	ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.
К02. Здатність застосовувати знання у практичних ситуаціях.	
К18. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).	
К19. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.	
К22. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**3**		
Семестр	**5**		
Кількість кредитів ECTS	**3**		
Аудиторні навчальні заняття	лекції	**14 (в годинах)**	**2**
	практичні	**28 (в годинах)**	**6**
Самостійна робота		**48 (в годинах)**	**82**
Форма підсумкового контролю	**Залік**		

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль I. Основи кібербезпеки та методи захисту програмного забезпечення.

Тема 1. Основи кібербезпеки (4 год.)

Тріада CIA. Основи криптографії. Симетричні та несиметричні алгоритми. Віртуалізація. Фаєрволи.

Тема 2. Способи приховати хакерські атаки. Ботнети. Техніки обману. (2год.)

Проксі-сервери. Тунелювання. Фішінг. Інфраструктура бот-нетів.

Тема 3. Використання вразливостей системи (2 год.)

Шелкоди. Вразливості, пов'язані з переповненням. SQL-ін'єкції. Конкуретні потоки. Експлойти. Методи перебору паролів. DoS-атаки.

Тема 4. Види шкідливого коду. (4 год.)

Червяки та віруси. Обфускація коду. Проникнення в код. Руткіти. Шпигунське програмне забезпечення. Ескалація прав. Крадіжка токенів. Кейлогінг.

Тема 5. Техніки захисту та аналізу. (2 год.)

Експертиза пам'яті комп'ютера. Аналіз шкідливого коду. Системи виявлення проникнення.

Тема 6. Основні проблеми захисту програмного забезпечення. (2 год.)

Три проблеми захисту ПЗ - з'єднання з інтернетом, розширення сторонніми модулями та складність. Проблеми безпеки ПЗ.

Тема 7. Менеджмент ризиків пов'язаних із кібербезпекою. (2 год.)

Розуміння контексту програми. Ідентифікація бізнес та технічних ризиків. Синтез та ранжування ризиків. Визначення стратегії зниження ймовірності ризиків. Врахування зворотнього зв'язку практичного застосування стратегії.

Тема 8. Точки дотику кібербезпеки в процесі інженерії ПЗ. (2 год.)

Точки дотику кібербезпеки в процесі інженерії ПЗ. Належність точок дотику до конкретних етапів розробки ПЗ. Обов'язки команди розробників в контексті кібербезпеки.

Тема 9. Code Review (2 год.)

Виявлення багів в коді з допомогою автоматизованих інструментів. Підходи до статичного аналізу ПЗ. Опис багів. Ключові характеристики аналізаторів коду.

Тема 10. Аналіз архітектурних ризиків(2 год.)

Термінологія аналізу ризиків. Обрахунок ризику. Підходи до аналізу

ризиків при розробці архітектури.

Тема 11. Тестування інформації в контексті кібербезпеки.Методи недокументованого використання ПЗ. (2 год.)

Тестування на проникнення. Тестування на основі ризиків. Зворотній зв’язок за результатами тестування. Створення антивимог. Моделювання атак.

Тема 12. Комплексний підхід до розробки в контексті кібербезпеки (2 год.)

Стратегія кібербезпеки в команді розробників. Навчання учасників процесу інженерії програмного забезпечення в контексті кібербезпеки. Таксономія помилок.

ТЕМАТИКА ПРАКТИЧНИХ РОБІТ

Змістовий модуль I. Основи кібербезпеки

Тема 1. Робота з VirtualBox. Встановлення операційної системи Kali Linux. (4 год.)

Тема 2. Робота з консольним інтерфейсом Linux. (4 год.)

Тема 3. Використання сервісу nmap. (2 години)

Тема 4. Використання сервісу Wireshark для аналізу трафіку в мережі. (2 години)

Тема 5. Бази експлойтів. Використання nmap в режимі скриптів для виявлення вразливостей. (2 години)

Тема 6. Інструменти аналізу вразливостей сайтів, що використовують системи керування контентом. WPScan та JoomScan (2 години)

Тема 7. Використання інструментів стрес-тестування (2 години)

Тема 8. Злам паролів методом bruteforce та перебору за словником (2 години)

Тема 9. Проведення SQL ін'єкцій засобами інструменту SQLmap (2 години)

Тема 10. Проведення сканування вразливостей веб-сайтів засобами пакету Nikto2 (2 год.)

Тема 11. Аналіз метаданих зображень інструментами Exif та exiftool (2 години).

Тема 12. Аналіз даних з допомогою автоматизованого інструменту збору даних з відкритих джерел Spiderfoot (2 години).

ПЕРЕЛІК ТЕМ ДЛЯ САМОСТІЙНОГО ОПРАЦЮВАННЯ

Найменування показників Розподіл годин	
Самостійна робота, год, у т.ч.: 48	
Опрацювання матеріалу, викладеного на лекціях	14
Підготовка до практичних занять та контрольних заходів	14
Підготовка звітів з практичних робіт 12	
Опрацювання матеріалу, винесеного на самостійне вивчення: 1. Методи захисту від DDoS атак (2 години) 2. Інструменти реверс-інжинірингу (4 години) 3. Алгоритми хешування (2 години)	8

ПОЛІТИКА КУРСУ

1) щодо системи поточного і підсумкового контролю

Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюється згідно з "Положенням про систему

поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти". Ознайомитись з документом можна за покликанням.

2) *Здобувачі вищої освіти мають право на оскарже оцінки з дисципліни отриманої під час контроли заходів. Апеляція здійснюється відповідно до «Положе про політику та врегулювання конфліктних ситуаі Ознайомитись з документом можна за покликанням.*

щодо оскарження результатів контрольних заходів

3) щодо відпрацювання пропущених занять

Згідно "Положення про організацію освітнього процесу" здобувач допускається до семестрового контролю з ***конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку), якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав ≥35 бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній.*** *Ознайомитись з документом можна за покликанням.*

4) щодо дотримання академічної доброчесності

"Положення про академічну доброчесність" закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за покликанням.

5) щодо використання штучного інтелекту

"Положення про академічну доброчесність" визначає політику щодо використання технічних засобів на основі штучного інтелекту в освітньому процесі. Ознайомитись з документом можна за покликанням. "Положення про

систему запобігання та виявлення академічного плагіату, самоплагіату, фабрикації та фальсифікації академічних творів" містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за покликанням.

6) щодо використання технічних засобів в аудиторії та правила комунікації

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анульовується без права перескладання.
Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.

7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти». Ознайомитись з документом можна за покликанням.

МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання студентів з метою розвитку їх логічного та абстрактного мислення, творчих здібностей, підвищення мотивації до навчання та формування особистості майбутнього фахівця в галузі права.

Програмний результат навчання	Метод навчання	Метод оцінювання
ПР21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.	МН 1.1 - лекція, МН 1.2 – розповідь -пояснення, МН 2.2 - демонстрування, МН 2.4 - комп'ютерні і мультимедійні методи, МН 9 - порівняння, МН 14 - творчий метод, МН 3.1 - вправи, МН 19 - робота під керівництвом викладача, МН 20 - інтерактивні методи, МН 3.4 - практичні роботи.	МФО 4 - поточний контроль, МФО 8 -тестовий контроль, МФО 1 - залік

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Вид	Зміст	% від загальної оцінки	Бал	
			min	max
Поточні контрольні заходи	всього	60	35	60
Підсумкові контрольні заходи	екзамен	40	24	40
Всього:	-	100	60	100

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється «Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів», яке розміщено на сайті університету в розділі «Публічна інформація»: https://ukd.edu.ua/node/1149

Фіксація **поточного** контролю здійснюється в "Електронному журналі обліку успішності академічної групи" на підставі чотирибальної шкали - "2"; "3"; "4"; "5". У разі відсутності студента на занятті виставляється "н". За результатами поточного контролю у Журналі, автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

Усі пропущені заняття, а також негативні оцінки студенти зобов'язані відпрацювати впродовж трьох наступних тижнів. У випадку недотримання цієї норми, замість "н" в журналі буде виставлено "0" (нуль балів), без права перездачі.

До підсумкового контролю допускаються студенти які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 балів і

менше, не допускаються до складання підсумкового контролю і на [1]підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру.

Підсумковий контроль знань у формі екзамену (І семестр) проводиться у вигляді комп'ютерного тестування. За результатами підсумкового контролю (диференційований залік/екзамен) студент може отримати 40 балів.

Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен/диференційований залік і повинні йти на перездачу.

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях оцінюється в балах (згідно Шкали оцінювання знань за ЄКТС) і є сумою балів отриманих під час поточного та підсумкового контролю.

Шкала оцінювання знань за ЄКТС:

Оцінка за національною шкалою	Рівень досягнень, %	Шкала ECTS
Національна диференційована шкала		
Відмінно	90 – 100	A
Добре	83 – 89	B
	75 – 82	C
Задовільно	67 – 74	D
	60 – 66	E
Незадовільно	35 – 59	FX
	0 – 34	F
Національна недиференційована шкала		
Зараховано	60 – 100	-
Не зараховано	0 – 59	-

Студенти, які не з'явилися на екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

Об’єктивність процедур проведення контрольних заходів забезпечується відмежуванням результатів поточного контролю від результатів підсумкового контролю.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Жаровський Р. О. Конспект лекцій з дисципліни Захист інформації у комп’ютерних системах для студентів денної та заочної форми навчання спеціальності 123 "Комп'ютерна інженерія" / Руслан Олегович Жаровський. Тернопіль, 2019. 268 с.

[1]

2. Charles J. Brooks, Christopher Grow, Philip A. Craig, Jr., Donald Short (2018). Cybersecurity Essentials Somerset : John Wiley & Sons 768 p.
3. Todd Barnum (2021). The Cybersecurity Manager's Guide: The Art of Building Your Security Program - O'Reilly Media; 1st edition 396 p.