ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра інформаційних технологій

ЗАТВЕРДЖУЮ
Проректор з методичної роботи
_____ Ярослав ШТАНЬКО
"30" 08 2024 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
2024

2

РОЗРОБНИК

к.т.н., доцент Мар'ян СЛАБІНОГА

ЗАТВЕРДЖЕНО:

на засіданні кафедри інформаційних технологій,
протокол № 1 від 28.08.2024 р.

Завідувач кафедри Сергій ВАЩИШАК

УЗГОДЖЕНО:

Гарант ОПП Олександр ІВАНОВ

на засіданні кафедри інформаційних технологій,
протокол № 1 від 28.08.2024 р.

Завідувач кафедри Сергій ВАЩИШАК

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 1 від 30.08.2024 р.

e-mail	marian.slabinoha@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра інформаційних технологій, ауд 206
Посилання на сайт	https://ukd.edu.ua
Сторінка курсу в СДО	https://online.ukd.edu.ua/course/view.php?id=3791

ВСТУП

Анотація навчальної дисципліни

Навчальна дисципліна "Захист інформації в комп’ютерних системах" є обов’язковою складовою освітньо-професійної програми підготовки фахівців за освітнім ступенем "бакалавр" галузі знань 12 "Інформаційні технології" спеціальності 121 "Інженерія програмного забезпечення" освітньої програми "Розробка та тестування програмного забезпечення". Дисципліна вивчає основні концепції і поняття теорії захисту інформації та принципи розробки програмного забезпечення з урахуванням вимог до захищеності та стійкості програмних продуктів.

Завдання дисципліни:

- 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.

Цілі: 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.

Результати навчання. Згідно з вимогами освітньо-професійної програми, в результаті вивчення дисципліни студенти повинні

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.

Мета навчальної дисципліни

Мета дисципліни - 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.

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
ЗК3. Здатність спілкуватися державною мовою як усно, так і письмово.	ПРН11. Вибирати вихідні дані для проектування, керуючись формальними методами опису вимог та моделювання.
ЗК7. Здатність працювати в команді.	ПРН18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних.
ФК2. Здатність брати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування.	ПРН21. 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.
ФК7. Володіння знаннями про інформаційні моделі даних, здатність створювати програмне забезпечення для зберігання, видобування та опрацювання даних.	
ФК13. Здатність обґрунтовано обирати та освоювати інструментарій з розробки та супроводження програмного забезпечення.	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**3**		
Семестр	**5**		
Кількість кредитів ECTS	**3**		
Аудиторні навчальні заняття		**денна форма**	**заочна форма**
	лекції	**14 (в годинах)**	**4 (в годинах)**
	практичні	**28 (в годинах)**	**8 (в годинах)**
Самостійна робота		**48 (в годинах)**	**78 (в годинах)**
Форма підсумкового контролю	**Залік**		

Структурно-логічна схема вивчення навчальної дисципліни:

Попередні дисципліни	**Наступні дисципліни**
Основи програмування	Якість програмного забезпечення та тестування

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основи кібербезпеки (2 год.)

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

Тема 2. Способи приховати хакерські атаки. Використання вразливостей системи (2 год.)

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

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

Завдання для самостійної роботи. Методи захисту від DDoS атак (2 години).

Тема 3. Види шкідливого коду. (2 год.)

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

Тема 4. Техніки захисту та аналізу. Основні проблеми захисту програмного забезпечення. (2 год.)

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

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

Завдання для самостійної роботи. Інструменти реверс-інжинірингу (4 години).

Тема 5. 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.

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

Завдання для самостійної роботи. Алгоритми хешування (2 години)

Тема 6. Code Review (2 год.)

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

Тема 7. Аналіз архітектурних ризиків. Комплексний підхід та тестування інформації в контексті кібербезпеки (2 год.)

Термінологія аналізу ризиків. Обрахунок ризику. Підходи до аналізу ризиків при розробці архітектури.

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

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

Зміст практичних занять

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

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

3. Використання сервісу nmap. (2 години)

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

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

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

7. Використання інструментів стрес-тестування (2 години)

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

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

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

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

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

Зміст самостійної роботи здобувачів

Розподіл годин, виділених на вивчення дисципліни:

Найменування видів робіт	Розподіл годин за формами навчання	
	денна	**заочна**
Самостійна робота, год, у т.ч.:	48	78
Опрацювання матеріалу, викладеного на лекціях	14	14
Підготовка до практичних занять та контрольних заходів	14	14
Підготовка звітів з практичних робіт	12	12
Підготовка до поточного тестування	-	
Опрацювання матеріалу, винесеного на самостійне вивчення	8	38

ПОЛІТИКА КУРСУ

Коротко, з покликанням на відповідну нормативну базу УКД, висвітлити питання:[1]

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) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та

[1] зміст пунктів може редагуватись з огляду на особливості курсу

врегулювання конфліктних ситуацій». Ознайомитись з документом можна за покликанням.

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/робочою програмою 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.[2] *"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, окрім виробничої необхідності. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його

[2] визначається політика використання ШІ в навчальній дисципліні - дозволене/заборонене, правила використання

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.[3]

Під час вивчення навчальної дисципліни "Радіовиробництво і подкасти" студентам надається можливість перерахування неформальної освіти. До прикладу, із запропонованого переліку можна пройти сертифіковані (безкоштовні) курси на освітніх платформах, відтак сертифікат, який отримали під час навчання, – є підтвердженням засвоєння студентом окремих тем, що включені у зміст дисципліни.

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 інформаційних технологій.

Програмний результат навчання	Метод навчання	Метод оцінювання
ПРН11. Вибирати вихідні дані для проектування, керуючись формальними методами опису вимог та моделювання. ПРН18. Знати та вміти застосовувати інформаційні технології обробки, зберігання та передачі даних. ПРН21. Знати, аналізувати, вибирати,	Лекція, розповідь-пояснення, мультимедійні методи, практичні роботи, індуктивний метод, дедуктивний метод, синтетичний метод, виокремлення основного, творчий, проблемно пошуковий, кейс-метод	Екзамен, усний контроль,поточний контроль, тестовий контроль.

[3] визначається перелік електронних та інших ресурсів та умови перезарахування

кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.		

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».

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.

Критерії оцінювання:

«незадовільно»	володіє навчальним матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об’єктів, що позначаються окремими словами чи реченнями; володіє матеріалом на елементарному рівні засвоєння, викладає його уривчастими реченнями, виявляє здатність висловити думку на елементарному рівні; володіє матеріалом на рівні окремих

	фрагментів, що становлять незначну частину навчального матеріалу;
«задовільно»	володіє матеріалом на початковому рівні, значну частину матеріалу відтворює на репродуктивному рівні; володіє матеріалом на рівні, вищому за початковий, здатний за допомогою викладача логічно відтворити значну його частину; може відтворити значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, за допомогою викладача може аналізувати навчальний матеріал, порівнювати та робити висновки, виправляти допущені помилки;
«добре»	здатний застосовувати вивчений матеріал на рівні стандартних ситуацій, частково контролювати власні навчальні дії, наводити окремі власні приклади на підтвердження певних тверджень: вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати її на практиці, контролювати власну діяльність, виправляти помилки і добирати аргументи на підтвердження певних думок під керівництвом викладача; вільно володіє вивченим обсягом матеріалу, та вміє застосовувати його на практиці; вільно розв’язує задачі в стандартних ситуаціях, самостійно виправляє допущені помилки, добирає переконливі аргументи на підтвердження вивченого матеріалу;
«відмінно»	виявляє початкові творчі здібності, самостійно визначає окремі цілі власної навчальної діяльності, оцінює окремі нові факти, явища, ідеї; знаходить джерела інформації та самостійно використовує їх відповідно до цілей, поставлених викладачем; вільно висловлює власні думки і відчуття, визначає програму особистої пізнавальної діяльності, самостійно оцінює різноманітні життєві явища і факти, виявляючи особисту позицію щодо них; без допомоги викладача знаходить джерела інформації і використовує одержані відомості відповідно до мети та завдань власної пізнавальної діяльності; використовує набуті знання і вміння в нестандартних ситуаціях; виявляє особливі творчі здібності, самостійно розвиває власні обдарування і нахили, вміє самостійно здобувати знання.

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. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».[4]

[4] можна вказати теми чи завдання, які є обов’язковими до виконання, а також особисті підходи до оцінювання рівня знань здобувачів під час аудиторної роботи

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 підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. 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 з **Шкалою 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.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

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": Тернопіль, 2019. 268 с.
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.