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 ПРОГРАМНИХ ПРОДУКТІВ

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:	вибіркова
Мова викладання, навчання та оцінювання:	українська

Івано-Франківськ
2024

2

РОЗРОБНИК:
к.ю.н., доц. кафедри ІТ Тарас СТИСЛО

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

Завідувач кафедри ІТ Сергій ВАЩИШАК

УЗГОДЖЕНО:

Гарант ОП Олександр ІВАНОВ

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

e-mail	taras.styslo@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=3793

ВСТУП

Анотація навчальної дисципліни

Дисципліна забезпечує особистісний і професійний розвиток студента, спрямована на формування теоретичних та практичних знань для вирішення різної складності завдань.

Метою викладання даної навчальної дисципліни є:

- оволодіння студентами комплексом знань у галузі захисту програмних продуктів, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових та набуття на основі цих знань практичних навичок та теоретичних знань, необхідних для творчого підходу в питанні сучасного та майбутнього оперативного захисту комп'ютерної техніки й інформації;
- оволодіння студентами алгоритмами створення сучасних програм захисту; алгоритмами кодування; сучасними методами, технологією; комп'ютерними програмними, технічними засобами у галузі захисту: операційних систем, текстових редакторів, табличних процесорів, систем управління базами даних, конфіденційної інформації тощо. Набуття на основі вказаних знань практичних навичок, необхідних для розробки систем захисту, керування розробкою систем захисту, а на основі вказаного, нормального забезпечення роботи фінансових організацій, регіонів країни зі збереженням характеристик трафіку, швидкості санкціонованого доступу тощо;
- опанування концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденційних документів; стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних та глобальних комп'ютерних мережах із метою використання їх, можливостей для покращення показників безпеки в них.

Для досягнення мети поставлені такі основні **завдання**:

- принципи функціонування вбудованих засобів захисту комп'ютерних систем (BIOS) та шляхи протидії спробам їх злому;
- методи несанкціонованого злому та навмисного пошкодження інформації та засоби протидії цим спробам;
- методи побудови захисту окремих програмних продуктів.

До задач вивчення дисципліни входить формування теоретичних знань та практичних навичок у відповідності з поставленою метою.

Результати навчання. Згідно з вимогами освітньо-професійних та освітньо-кваліфікаційних програм студенти повинні **знати:**

- об'єкти програмного забезпечення, на які можливі атаки з боку комп'ютерних хакерів, та методи здійснення несанкціонованого доступу до інформації;
- принципи функціонування систем захисту, призначення привілей, зберігання паролів та автентифікація користувачів в операційних системах WINDOWS та UNIX, методи хакерів з несанкціонованого проникнення до інформації, привласнення привілей адміністратора тощо;

Вміти:

- виконати аналіз безпеки комп'ютерної системи та усунути можливі шляхи
- несанкціонованого доступу;
- здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- виконувати адміністрування прав доступу до комп’ютерної системи з метою перешкоди призначення невиправданих привілей;
- виконувати постійний моніторинг з пошуку програмних закладок та каналів витоку інформації;
- використовувати основні прийоми та програмні засоби хакерів для перевірки надійності захисту інформації та стійкості його щодо хакерських атак.

Компетентності та результати навчання, **яких набувають здобувачі освіти внаслідок вивчення навчальної дисципліни (шифри та зміст компетентностей та програмних результатів навчання вказано відповідно до ОПП “Розробка та тестування програмного забезпечення”**.

Шифр та назва компетентності	**Шифр та назва програмних результатів навчання**
ФК6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).	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.	
ФК10. Здатність накопичувати, обробляти та систематизувати професійні знання щодо створення і супроводження програмного забезпечення та визнання важливості навчання протягом всього життя.	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**4**		
Семестр	**7**		
Кількість кредитів ECTS	**6**		
Аудиторні навчальні заняття		**денна форма**	**заочна форма**
	лекції	**30 (в годинах)**	**8 (в годинах)**
	практичні	**30 (в годинах)**	**8 (в годинах)**
Самостійна робота		**120 (в годинах)**	**164 (в годинах)**
Форма підсумкового контролю	**екзамен**		

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Перелік тем лекційного матеріалу

Тема 1. Основні поняття безпеки. Конфіденційність, цілісність та доступність даних (2 год.)

Тема 2. Традиційне шифрування та його модель (2 год.)

Тема 3. Криптографія та криптоаналіз (2 год.)

Тема 4. Потокові та блокові шифри. Шифр Файстеля (2 год.)

Тема 5. DES-стандарт шифрування даних (2 год.)

Тема 6. Блокові шифри та режими їх роботи (2 год.)

Тема 7. Випадкові числа та їх генерування. Генератори псевдовипадкових чисел (2 год.)

Тема 8. Криптографія. Криптографія з відкритим ключем (2 год.)

Тема 9. Алгоритм RSA. Шифрування та дешифрування (2 год.)

Тема 10. Симетричні та асиметричні алгоритми. Порівняння основних характеристик (2 год.)

Тема 11. Аутентифікація повідомлень та функції хешування (2 год.)

Тема 12. Коди автентичності повідомлень та функції хешування (2 год.)

Тема 13. Алгоритм HMAC (2 год.)

Тема 14. Цифрові підписи та протоколи аутентифікації. Вимоги до цифрового підпису. Стандарт цифрового підпису DSS (2 год.)

Тема 15. Методи та засоби створення захищеного програмного забезпечення (2 год.)

Зміст практичних занять

Тема 1. Альтернативні потоки даних (2 год.)

Тема 2. Створення програми генерації випадкових паролей (2 год.)

Тема 3. Створення журналу (2 год.)

Тема 4. Захист від копіювання. Прив'язка до апаратного забезпечення. Використання реєстру (2 год.)

Тема 5. Стенографія з *.JPEG (2 год.)

Тема 6. Криптографічні хеш-функції (4 год.)

Тема 7. Генерація криптографічно-безпечної псевдовипадкової послідовності (4 год.)

Тема 8. Криптографічні бібліотеки (4 год.)

Тема 9. Рольове управління доступом. Розробка захищених додатків (8 год.)

Зміст самостійної роботи здобувачів
Розподіл годин, виділених на вивчення дисципліни:

Найменування видів робіт	**Розподіл годин**	
	денна форма	**заочна форма**
Самостійна робота, год, у т.ч.:	120	164
Опрацювання матеріалу, викладеного на лекціях	30	8
Підготовка до практичних занять та контрольних заходів	15	10
Підготовка звітів з практичних робіт	15	-
Підготовка до поточного контролю	8	-
Опрацювання матеріалу, винесеного на самостійне вивчення	52	146

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) 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 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. "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 інформаційних технологій.

Результат навчання	Метод навчання	Метод оцінювання
ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення	Лекція, розповідь-пояснення, мультимедійні методи, практичні роботи,	Екзамен, поточний контроль, тестовий контроль.

інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.	індуктивний метод, дедуктивний метод, синтетичний метод, виокремлення основного, творчий, проблемно пошуковий метод	

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.

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».

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 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 заліки/екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Юрчишин В.М., Пасєка М.С., Стисло Т.Р., Безпека програм та даних: методичні вказівки до виконання лабораторних.Івано-Франківськ: ІФНТУНГ, 2017. 45с.

2. Сенів М. М., Яковина В.С. Безпека програм та даних: навчальний посібник. Львів : Видавництво Львівської політехніки, 2015. 256 с.

3. С. Е. Остапов, С. П. Євсеєв, О. Г. Король. Технології захисту інформації: навч. посібник. Харків : Вид. ХНЕУ, 2013. 476 с.

4. Жураковский Ю.П., Полторак В.П. Теорія інформації кодування: Підручник. Київ : Вища школа, 2001. 255 с.

5. В.Л. Кожевников, А.В. Кожевников.Теорія інформації та кодування : навч. посібник. Дніпродзержинськ : Національний гірничий університет, 2012. 108 с.

6. Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. Захист інформації в автоматизованих системах управління : навч. посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

7. Мнушка, О.В. Безпека програм і даних : конспект лекцій для студентів за спеціальністю 121 «Інженерія програмного забезпечення». Харків, ХНАДУ, 2020.

8. Мнушка О.В. Методичні вказівки для самостійної роботи з дисципліни «Безпека програм і даних» для студентів за спеціальністю 121 «Інженерія програмного забезпечення». Харків, ХНАДУ, 2020.