СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«БЕЗПЕКА ПРОГРАМ ТА ДАНИХ»

Ступінь освіти	бакалавр
Спеціальність	121 Інженерія програмного забезпечення
Освітня програма	Інженерія програмного забезпечення
Загальний обсяг	5 кредитів ЄКТС (150 годин)
Тривалість викладання	8 семестр (15 чверть)
Заняття:	
лекції:	2 години/тиждень
лабораторні заняття:	3 години/тиждень
Мова викладання	українська

Сторінка курсу в СДО НТУ «ДП»: https://do.nmu.org.ua/course/view.php?id=5401

Кафедра, що викладає: Безпеки інформації та телекомунікацій

Інформація про викладача:

Корченко Анна Олександрівна	д.т.н., професор, професор кафедри безпеки інформації та телекомунікацій
Персональна сторінка	https://bit.nmu.org.ua/ua/pro_kaf/prepods/Korchenko.php
E-mail:	Korchenko.A.O@nmu.one

Анотація до курсу

Безпека програм та даних має закласти термінологічний фундамент, навчити здобувачів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам та засобам захисту інформації в програмному забезпеченні комп'ютерних систем з урахуванням сучасного стану та прогнозу розвитку методів та засобів здійснення погроз зі сторони потенційних порушників.

1. Мета та завдання курсу

Мета дисципліни – закласти термінологічний фундамент, навчити здобувачів правильно проводити аналіз погроз інформаційній безпеці, основним методам, принципам, алгоритмам та засобам захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів та засобів здійснення погроз зі сторони потенційних порушників.

Завдання курсу:

У результаті вивчення курсу студенти повинні вивчити: методи забезпечення функціонування спеціального програмного забезпечення щодо захисту даних від

руйнуючих програмних засобів та проводити аналіз ефективності систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів.

2. **Результати навчання:**

Отримання знань та навичок у використанні сучасних методів розроблення програмних засобів захисту інформації та синтезу комплексів засобів захисту інформації.

У результаті навчання студенти будуть:

1. Знати та застосовувати професійні стандарти і інші нормативно-правові документи в галузі безпеки програм та даних.

2. Знати основні принципи побудови систем захисту інформації та методи забезпечення інформаційної безпеки програм та даних в комп'ютерних системах.

3. 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.

Дисциплінарні результати навчання сформовано на основі ПРН освітньо-професійної програми «Інженерія програмного забезпечення» першого (бакалаврського) рівня вищої освіти (ПР4, ПР18, ПР21).

3. Структура курсу

Види та тематика навчальних занять	**Внесок в загальну оцінку, %**
ЛЕКЦІЇ	**40**
Тема 1. Базові поняття інформаційної безпеки Основні поняття. Захист інформації та його основні завдання. Класифікація загроз для інформації та їх джерел. Поняття про інформацію з обмеженим доступом. Структура політики безпеки та її основні частини.	
Тема 2. Механізми і політики розмежування прав доступу TCSEC - перший стандарт у галузі оцінки захищеності комп'ютерних систем. Common Criteria - європейський стандарт у галузі оцінки захищеності комп'ютерних систем. Вимоги довіри. НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу"	
Тема 3. Шифрування даних. Основні поняття роботи К. Шеннона "Теорія зв'язку в секретних системах". Симетричні, асиметричні та комбіновані криптосистеми. Їх переваги та недоліки.	
Тема 4. Системи захисту програмного забезпечення. Мета і доцільність використання систем захисту. Класифікація системи захисту інформації. Пакувальники/шифратори. Системи захисту від несанкціонованого копіювання. Системи захисту від несанкціонованого доступу. Основні алгоритми захисту програмного забезпечення.	
Тема 5. Розповсюджені типи захистів та їх недоліки. Основні вимоги до розробки систем захисту. Розповсюджені типи захистів та їх недоліки	
Тестова контрольна робота №1 (за темами 1-5).	20

Види та тематика навчальних занять	Внесок в загальну оцінку, %
Тема 6. Засоби подолання систем захисту. Проблема існування засобів зламу захистів програмного забезпечення. Класифікація засобів подолання систем захисту програмного забезпечення. Програми розпакування, дешифрування та криптоаналізу.	
Тема 7. Основні поняття ОС, необхідні для створення систем захисту. Склад операційної системи. BIOS. CMOS. Переривання, їх роль і процедура звертання в програмах. Робота з дисками на фізичному рівні.	
Тема 8. Загальні принципи захисту програм від несанкціонованого дослідження. Принципи побудови систем захисту та їх функції. Основні методи та засоби дослідження програм. Способи вбудовування захисних механізмів в програмне забезпечення. Структура програм, захищених від дослідження.	
Тема 9. Захист від дизасемблювання. Необхідність і доцільність захисту від дизасемблювання. Основні методи протидії дизасемблюванню програм. Поняття обфускації та його види.	
Тема 10. Захист від несанкціонованого налагоджування Огляд і класифікація налагоджувачів. Захист від налагоджувачів реального режиму. Боротьба з налагоджувачами захищеного режиму. Додаткові прийоми антиналагоджувального програмування.	
Тестова контрольна робота №2 (за темами 6-10).	20
ЛАБОРАТОРНІ ЗАНЯТТЯ	**60**
Лабораторна робота №1 **Тема: Розмежування повноважень користувачів на основі парольної аутентифікації.** Мета роботи: Розробка програми розмежування повноважень користувачів на основі парольної аутентифікації. Завдання: Розробити програму розмежування повноважень користувачів на основі парольної аутентифікації.	
Звіт з роботи № 1 та захист лабораторної роботи.	20
Лабораторна робота №2 **Тема: Логування дій користувачів у програмних системах.** Мета роботи: Засвоїти методику та отримати практичні навики розробки процедур логування дій користувачів на прикладі підсистем ідентифікації та аутентифікації користувачів із важкооборотними однонапрямленими хеш-функціями. Завдання: Удосконалити розроблену в лабораторній роботі № 1 програмну систему з метою покращення функції ідентифікації та аутентифікації користувачів.	
Звіт з роботи № 2 та захист лабораторної роботи.	20
Лабораторна робота №3	

Види та тематика навчальних занять	Внесок в загальну оцінку, %
Тема: Методи захисту програмного забезпечення. Мета роботи: Одержати практичні навики реалізації алгоритмів захисту програмного забезпечення для найпоширеніших моделей розповсюдження. Завдання: 1. Розробити програмний продукт (або удосконалити ПЗ розроблене в попередніх лабораторних роботах), що виконує мінімум 10 функцій (для прикладу - відкриття файлу, збереження файлу, довідка, друк, перегляд параметрів файлу, пошук та інші).	
Звіт з роботи № 3 та захист лабораторної роботи.	20
РАЗОМ	**100**

4. Технічне обладнання та/або програмне забезпечення.

Використовується лабораторна база кафедри безпеки інформації та телекомунікацій (комп'ютерне та мультимедійне обладнання).

Дистанційна платформа Moodle. Спеціалізовані середовища розробки (MS Visual Studio).

5. Система оцінювання та вимоги

5.1. Навчальні досягнення здобувачів вищої освіти за результатами вивчення курсу оцінюватимуться за шкалою, що наведена нижче:

Рейтингова шкала	Інституційна шкала
90 – 100	відмінно
74 – 89	добре
60 – 73	задовільно
0 – 59	незадовільно

5.2. Здобувачі вищої освіти можуть отримати підсумкову оцінку з навчальної дисципліни на підставі поточного оцінювання знань за умови, якщо набрана кількість балів захисту лабораторних робіт складатиме не менше 60 балів.

Теоретична частина оцінюється за результатами здачі двох контрольних тестових робіт, кожна з яких містить тестові закриті запитання з однією вірною відповіддю (максимальна кількість – 20 балів за кожною тестовою роботою). Загалом за дві контрольні тестові робіти отримується максимум 40 балів, тобто 40% від оцінки за дисципліну.

Лабораторні роботи (три роботи – у вигляді індивідуального завдання з кожної, розподіл % див. в таблиці розділу 4) виконуються у письмовому вигляді (звіт з кожної роботи оцінюється в межах балів, представлених в таблиці розділу 4, загалом лабораторні враховуються як 60% (максимум 60 балів). Отримані бали за теоретичну частину та лабораторні роботи додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за поточною успішністю здобувач вищої освіти може набрати 100 балів.

5.3. Критерії оцінювання підсумкової роботи. У випадку якщо здобувач

вищої освіти за поточною успішністю отримав менше 60 балів та/або прагне поліпшити оцінку, проводиться підсумкове оцінювання.

Підсумкове оцінювання за дисципліною проводиться у вигляді комплексної контрольної роботи, яка включає запитання з теоретичної та практичної частини курсу. Білет складається з 30 тестових завдань з чотирма варіантами відповідей, одна правильна відповідь оцінюється в 2 бали (разом 60 балів) та 2 завдань з практичної частини, кожне з запитань оцінюється максимум у 20 балів (разом 40 балів).

Отримані бали за тестові завдання та завдання з практичної частини додаються і є підсумковою оцінкою за вивчення навчальної дисципліни. Максимально за підсумковою роботою здобувач вищої освіти може набрати 100 балів.

6. Політика курсу

6.1. Політика щодо академічної доброчесності. Академічна доброчесність студентів є важливою умовою для опанування результатами навчання за дисципліною і отримання задовільної оцінки з поточного та підсумкового контролів. Академічна доброчесність базується на засудженні практик списування (виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання), плагіату (відтворення опублікованих текстів інших авторів без зазначення авторства), фабрикації (вигадування даних чи фактів, що використовуються в освітньому процесі). У НТУ «Дніпровська політехніка» політика щодо академічної доброчесності регламентується положенням "Положення про систему запобігання та виявлення плагіату у Національному технічному університеті "Дніпровська політехніка". У разі порушення студентом академічної доброчесності (списування, плагіат, фабрикація), робота оцінюється незадовільно та має бути виконана повторно. При цьому викладач залишає за собою право змінити тему завдання.

6.2.Комунікаційна політика.

Студенти повинні мати активовану університетську пошту.

Усі письмові запитання до викладачів стосовно курсу мають надсилатися на університетську електронну пошту.

6.3. Відвідування занять.

Поважними причинами для неявки на заняття є хвороба, участь в університетських заходах, відрядження, які необхідно підтверджувати документами у разі тривалої (два тижні) відсутності. Про відсутність на занятті та причини відсутності студент має повідомити викладача або особисто, або через старосту.

7. Рекомендовані джерела інформації

1. Горбенко В. І., Лісняк А. О. Безпека програм та даних : навчальний посібник для здобувачів ступеня вищої освіти бакалавра спеціальності 121 «Інженерія програмного забезпечення» освітньо-професійної програми «Програмна інженерія». Запоріжжя : ЗНУ, 2022. 72 с.3.

2. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. – К.: Видавництво НА СБ України, 2020. – 256 с.

3. Andress J. Foundations of information security: a straightforward introduction. San Francisco : No Starch Press, 2019. 222 p.

4. Stewart J.M., Kinsey D. Network security, firewalls, and VPNs. Burlington : Jones & Bartlett Learning, 2021. 482 p.