Назва курсу	**«Методи та засоби захисту програмного забезпечення»**
Викладач (-і)	Шевчук Руслан Петрович
Профайл викладача (-ів)	http://www.wunu.edu.ua/fkit/department-kn-fkit/
Контактний тел.	+38(0352)475050*16129
E-mail:	**rsh(@)wunu.edu.ua**
Сторінка курсу в moodle	https://moodle.tneu.edu.ua
Консультації	Очні консультації: середа 19:00, ауд.6402 У групі viber кожного дня.

1. Коротка анотація до курсу.

Навчальна дисципліна спрямована на формування теоретичних знань і практичних навичок, необхідних майбутнім фахівцям для захисту програмного забезпечення. Під час вивчення дисципліни опрацьовуються сучасні методи та засоби захисту програмних систем.

Матеріали дисципліни спрямовані на формування достатнього рівня теоретичних знань, необхідних для написання захищених програм та використання сучасних засобів та методів захисту програмного забезпечення. Розглядаються способи написання захищених програм, засоби захисту програм від зловмисного програмного забезпечення, методи та алгоритми захисту програм від несанкціонованого копіювання.

2. Пререквізити. Раніше вивчені дисципліни необхідні для освоєння курсу: «Безпека програм та даних», «Алгоритми та структури даних», «Аналіз вимог до програмного забезпечення», «Архітектура та проектування програмного забезпечення», «Засоби програмування баз даних», «Архітектура комп'ютера», «Основи програмної інженерії».

Постреквізити. Дисципліни, які будуть використовувати результати навчання даного курсу: міждисциплінарна курсова робота, переддипломна практика, кваліфікаційна робота.

3. Опис курсу

Метою вивчення курсу «Методи та засоби захисту програмного забезпечення» є формування системи теоретичних знань і практичних вмінь застосування методів та засобів побудови ефективних систем захисту програмного забезпечення відповідно до моделі SSDLC. Особливу увагу приділено сучасним методам та інструментам зламу / захисту, які зазвичай використовуються для компрометації / захисту програмних систем.

Найменування та опис програмних компетентностей, формування котрих забезпечує вивчення дисципліни **«Методи та засоби захисту програмного забезпечення»:**

СК05. Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення;

СК08. Здатність розробляти і координувати процеси, етапи та ітерації життєвого циклу програмного забезпечення на основі застосування сучасних моделей, методів та технологій розроблення програмного забезпечення;

СК09. Здатність забезпечувати якість програмного забезпечення;

СК10. Здатність розробляти програмне забезпечення, використовуючи концепції інформаційної безпеки, безпеки баз даних, мережевої безпеки та криптографії.

Результати навчання:

РН01. Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення;

РН07. Аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для розв'язання складних задач інженерії програмного забезпечення;

РН08. Розробляти і модифікувати архітектуру програмного забезпечення для реалізації вимог замовника;
РН13. Конфігурувати програмне забезпечення, керувати його змінами та розробленням програмної документації на всіх етапах життєвого циклу;
РН18. Планувати, організовувати, впроваджувати та контролювати розробку програмного забезпечення систем захисту інформації, використовуючи концепції інформаційної безпеки, безпеки баз даних, мережевої безпеки та криптографії.

4. Загальна інформація про дисципліну

Ступінь вищої освіти	**Магістр**
Спеціальність	**121 – «Інженерія програмного забезпечення»**
Курс (рік навчання)	**1**
Семестр	**1**
Рік викладання	**2021-2022**
Формат курсу	Очний (offline)
Нормативна \ вибіркова	**нормативна**
Загальна кількість год/ кредитів	**150/5**
Лекції, год.	**30**
Лабораторні, год	**15**
Самостійна робота, год.	**96**

5. Перелік тем

Години (лек./прак.)	**Тема**
4/4	Тема 1. Загальний огляд методів та засобів захисту ПЗ
6/4	Тема 2. Модель SSDLC
4/2	Тема 3. Нефункціональні вимоги безпеки для розробки ПЗ
4/2	Тема 4. Захист програмного забезпечення від несанкціонованого дослідження
6/1	Тема 5. Класифікація вразливостей програмного забезпечення
6/2	Тема 6. Засоби аудиту безпеки та аналізу захищеності програмного забезпечення

6. Рекомендовані джерела інформації

1. Microsoft Security Development Lifecycle (SDL) – Process Guidance https://msdn.microsoft.com/en-us/library/windows/desktop/84aed186-1d75-4366-8e61-8d258746bopq.aspx
2. OWASP Foundation. OWASP Testing Guide v4.0. URL: https://www.owasp.org/index.php/Web_Application_Penetration_Testing.
3. J. Koo, Y. Kim and S. Lee, "Security Requirements for Cloud-based C4I Security

Architecture", 2019 International Conference on Platform Technology and Service (PlatCon), pp. 1-4, 2019.

4. C. Bryce, "Security governance as a service on the cloud", J Cloud Comp, vol. 8, 2019.

5. G. Levitin, L. Xing and H.Z. Huang, "Security of separated data in cloud systems with competing attack detection and data theft processes", Risk Analysis, vol. 39, no. 4, pp. 846-858, 2019.

6. K. O'Loughlin, M. Neary, E.C. Adkins and S.M. Schueller, "Reviewing the data security and privacy policies of mobile apps for depression", Internet interventions, vol. 15, pp. 110-115, 2019.

7. B Ouyang and Y. Cui, "Research on Computer Network Security Prevention in the Era of Big Data[J]", Journal of Physics: Conference Series, vol. 1648, no. 2, pp. 022011, 2020.

8. C. Wang, S. Chen, Z. Feng, Y. Jiang and X. Xue, "Block Chain-Based Data Audit and Access Control Mechanism in Service Collaboration", 2019 IEEE International Conference on Web Services, pp. 214-218, 2019.

9. Shevchuk R. Software for Automatic Estimating Security Settings of Social Media Accounts / R. Shevchuk, A. Melnyk, O. Opalko, H. Shevchuk // Proceedings of the 2020 10th International Conference "Advanced Computer Information Technologies" – Deggendorf, Germany. – September 16–18, 2020 – P. 769 – 773.

10. Cheshun V. Safe Decentralized Applications Development Using Blockchain Technologies / V. Cheshun, I. Muliar, V. Yatskiv, R. Shevchuk, S. Kulyna // Proceedings of the 2020 10th International Conference "Advanced Computer Information Technologies" – Deggendorf, Germany. – September 16–18, 2020 – P.800 – 805.

11. Wojtowicz M. Monte Carlo Type Method of Attack on the RSA Cryptosystem / M. Wojtowicz, D. Bodnar, R. Shevchuk, O. Bodnar, I. Bilanyk // // Proceedings of the 2020 10th International Conference "Advanced Computer Information Technologies" – Deggendorf, Germany. – September 16–18, 2020 – P.755 - 758.

12. Shevchuk R. Improve the Security of Social Media Accounts / R. Shevchuk, Y. Pastukh // Proceedings of the 2019 9th International Conference "Advanced Computer Information Technologies" – Ceske Budejovice, Czech Republic. – June 5–7, 2019 –P.439-442.

7. Система оцінювання та вимоги.

Підсумковий бал (за 100-бальною шкалою) з дисципліни **"Методи та засоби захисту програмного забезпечення"** визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ, враховуючи поточне опитування)	Заліковий модуль 4 (письмовий екзамен)	Разом
20%	20 %	20 %	40%	100%
Модуль 1 (теми 1-3) 1. Усне опитування під час заняття (3 тем по 15 балів = 45 балів) Письмова робота = 50 балів	Модуль 2 (теми 4-6) 1. Усне опитування під час заняття (3 теми по 10 балів = 30 балів) Письмова робота = 70 балів	1. Написання та захист КПІЗ = 80 балів. 2. Виконання завдань під час тренінгу = 20 балів	1. Тестові завдання (25 тестів по 2 бали за тест) – макс. 50 балів 2. Завдання. 1 – макс. 25 балів 3. Завдання. 2 – макс. 25 балів	100

Будь-яке завдання, за яке студент отримав оцінку, яка його не задовільняє може бути повторно перездано протягом наступних двох тижнів.

Незадовільну оцінку за заліковий модуль студент може перездати до здачі наступного модуля.

Шкала оцінювання:

За шкалою ТНЕУ	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85– 89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

8. Навчальні ресурси

№	Найменування
1.	**Обладнання:** проектор, комп'ютери з доступом до мережі Інтернету.
2.	**Програмне забезпечення:** bWAPP, OpenVAS, XAMPP, MS Visual Studio

9. Політики курсу.

Академічна доброчесність. **Дотримання академічної доброчесності студентами передбачає**:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.