МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Фізико-технічний факультет

Кафедра комп'ютерної інженерії та електроніки

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕХАНІЗМИ БОРОТЬБИ ЗІ ШКІДЛИВИМ ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ

Освітня програма	Комп'ютерна інженерія
Галузь знань	12 Інформаційні технології
Спеціальність	123 Комп'ютерна інженерія

Затверджено на засіданні кафедри
Протокол № 12 від "30" 06. 2023 р.

Івано-Франківськ – 2023 рік

ЗМІСТ

1. Загальна інформація
2. Анотація до курсу
3. Мета та цілі курсу
4. Компетентності
5. Результати навчання
6. Організація навчання курсу
7. Система оцінювання курсу
8. Політика курсу
9. Рекомендована література

1. Загальна інформація	
Назва дисципліни	Механізми боротьби зі шкідливим програмним забезпеченням
Рівень вищої освіти	Другий рівень вищої освіти, магістр
Викладач (-і)	доцент, кандидат фізико-математичних наук Павлюк Мирослав Федорович
Контактний телефон викладача	0992637288
E-mail викладача	myroslav.pavlyuk@pnu.edu.ua
Формат дисципліни	Семестровий
Обсяг дисципліни	3 кредити
Посилання на сайт дистанційного навчання	http://www.d-learn.pu.if.ua/
Консультації	відповідно до графіку індивідуальних консультацій, який розміщений на інформаційному стенді кафедри комп'ютерної інженерії та електроніки, через електронну пошту myroslav.pavlyuk@pnu.edu.ua

2. Анотація до курсу

Дисципліна «Механізми боротьби зі шкідливим програмним забезпеченням» належить до переліку вибіркових компонент за освітнім рівнем «магістр», що пропонуються в рамках циклу професійної підготовки студентів за освітньо-професійною програмою «Комп'ютерна інженерія». Вона забезпечує формування у студентів науково-дослідницьких і професійно-орієнтованих компетенцій. Предметом вивчення навчальної дисципліни є вивчення правил виявлення та класифікації зловмисних програм, що стало однією з найважливіших проблем у сфері кібербезпеки. У зв'язку з постійно зростаючим ризиком кібератак, увага лежить на дослідниках безпеки для розробки нових методів виявлення шкідливих програм та розробки нових механізмів захисту проти них.

Силабус навчальної дисципліни" Механізми боротьби зі шкідливим програмним забезпеченням" складений відповідно до освітньо-професійної програми "Комп'ютерна інженерія" підготовки магістрів спеціальності 123 "Комп'ютерна інженерія".

3. Мета та цілі курсу

Мета: Метою викладання дисципліни "Механізми боротьби зі шкідливим програмним забезпеченням" є вивчення правил виявлення та класифікація зловмисних програм, розробка нових механізмів захисту проти них у зв'язку з постійно зростаючим ризиком кібератак, так як в останні роки спостерігається швидке зростання кількості файлів, і аналізувати функціональність кожного файлу вручну стало дуже важко.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- класифікацію зловмисного програмного забезпечення;
- методи виявлення шкідливого програмного забезпечення;
- методи статичного аналізу;
- динамічний аналіз шкідливого програмного забезпечення;
- візуалізований метод аналізу шкідливого програмного забезпечення;

вміти:

- проводити аналіз зловмисного програмного забезпечення;
- використати будь-який доступний антивірус;
- проводити поглиблений аналіз функціональності зловмисного програмного забезпечення;

- застосовувати машинне навчання у класифікації шкідливого програмного забезпечення.

- 4. Компетентності

Здатність розв'язувати складні задачі і проблеми в галузі комп'ютерної інженерії або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.
Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.
Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів;

5. Результати навчання

Застосовувати загальні підходи пізнання, методи математики, природничих та інженерних наук до розв'язання складних задач комп'ютерної інженерії.
Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності
Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.

6. Організація навчання курсу

Обсяг курсу

Вид заняття	Загальна кількість годин
лекції	14
семінарські заняття/практичні/**лабораторні**	16
самостійна робота	60

Ознаки курсу

Семестр	Спеціальність	Курс (рік навчання)	Нормативний/ **вибірковий**
3	123 "Комп'ютерна інженерія"	2	Професійної підготовки

Тематика курсу

Тема, план	Форма занять-тя	Літера-тура	Кількість годин	Вага оцінки	Термін виконання
Змістовий модуль. Механізми боротьби зі шкідливим програмним забезпеченням.					
Тема 1. Вступ. Мета і задачі дисципліни. Історія виникнення шкідливих програмних забезпечень потреби боротьби із ними.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	1	Згідно розкладу
Тема 2 Шкідливе програмне забезпечення та боротьба з ним. Антишпигунські програми.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	1	Згідно розкладу

Тема 3. Методи захисту від шкідливих програм. Юридичні аспекти.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	1	Згідно розкладу
Тема 4. Методи профілактики зараження комп'ютерними вірусами та методи боротьби із ними.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	1	Згідно розкладу
Тема 5. Автоматична класифікація та виявлення шкідливих програм за допомогою машинного навчання та нейронних мереж.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	1	Згідно розкладу
Тема 6. Кібершпигунство. Програми боротьби з комп'ютерними вірусами	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	1	Згідно розкладу
Тема 7. Статичний та динамічний аналіз шкідливого програмного забезпечення в.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	1	Згідно розкладу
Модульний контроль 1			2	1	Згідно розкладу
Лабораторні роботи					
Тема 1. Дослідження та використання антивіросної програми Norton AntiVirus Internet Security.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **2 год.**	1	Згідно розкладу
Тема 2. Дослідження та використання антивіросної програми Panda Antivirus Internet Security.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **2 год.**	1	Згідно розкладу
Тема 3. Дослідження та використання антивіросної програми Trend Micro Enterprise Protection Strategy.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **4 год.**	1	Згідно розкладу
Тема 4. Дослідження та використання антивіросної програми McAfee Active Virus Defense.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **4 год.**	1	Згідно розкладу
Тема 5. Дослідження та використання антивіросної програми Доктор Касперський.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **4 год.**	1	Згідно розкладу
Модульний контроль.			2 год.	1	Згідно розкладу

Самостійна робота студентів					
Тема 1. Хронологія появи та статистика розвитку шкідливого та руйнуючого програмного забезпечення. (ШПЗ, РПЗ).	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	1	Впродовж семестру
Тема 2. Різні підходи до визначення “комп’ютерного вірусу”, переваги та недоліки. Інші види ШПЗ.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **9 год.**	1	Впродовж семестру
Тема 3 Методи аналізу алгоритму роботи ШПЗ. Класифікації ШПЗ.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	1	Впродовж семестру
Тема 4. Класифікації та види антивірусного програмного забезпечення.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **9 год.**	1	Впродовж семестру
Тема 5. Методи боротьби з ШПЗ засобами операційної системи.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	1	Впродовж семестру
Тема 6. Сучасні засоби боротьби з шкідливим програмним забезпеченням.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	1	Впродовж семестру
Тема 7. Особливості операційних систем щодо стійкості до ШПЗ.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	1	Впродовж семестру
Контроль самостійної роботи			2 год.	1	Згідно розкладу
Підсумковий контроль (екзамен)				1	
7. Система оцінювання курсу					
Загальна система оцінювання курсу	*Поточний контроль* здійснюється під час проведення лабораторних робіт, індивідуальних занять, колоквіумів, контрою за самостійною роботою і має на меті перевірку знань студентів з окремих тем навчальної дисципліни та рівня їх підготовленості до виконання конкретної роботи. Оцінки у 100-бальній шкалі, отримані				

<table>
<tr><td></td><td>студентами, виставляються у журналах обліку відвідування та успішності академічної групи.
Модульний контроль (сума балів за окремий змістовий модуль) проводиться (виставляється) на підставі оцінювання результатів знань студентів після вивчення матеріалу з логічно завершеної частини дисципліни – змістового модуля.
Завданням модульного контролю є перевірка розуміння та засвоєння певного матеріалу (теми), вироблення навичок проведення розрахункових робіт, вміння вирішувати конкретні ситуативні задачі, самостійно опрацьовувати тексти, здатності осмислювати зміст даної частини дисципліни, уміння публічно чи письмово подати певний матеріал.
Семестровий (підсумковий) контроль визначається як сума балів за модульні контролі та кількості балів за екзамен.
Екзамен – форма підсумкового контролю, яка передбачає перевірку розуміння студентом теоретичного та практичного матеріалу з усієї дисципліни, здатності творчо використовувати здобуті знання та вміння, формувати власне ставлення до певної проблеми тощо.
<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Оцінка ECTS</td><td colspan="2">Оцінка за національною шкалою</td></tr>
<tr><td>для екзамену, курсового проекту (роботи), практики</td><td>для заліку</td></tr>
<tr><td>90 – 100</td><td>A</td><td>відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>80 – 89</td><td>B</td><td rowspan="2">добре</td></tr>
<tr><td>70 – 79</td><td>C</td></tr>
<tr><td>60 – 69</td><td>D</td><td rowspan="2">задовільно</td></tr>
<tr><td>50 – 59</td><td>E</td></tr>
<tr><td>26 – 49</td><td>FX</td><td>незадовільно з можливістю повторного складання</td><td>не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-25</td><td>F</td><td>незадовільно з обов’язковим повторним вивченням дисципліни</td><td>не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>
</td></tr>
<tr><td>Вимоги до письмової роботи</td><td>Підсумкова письмова робота виконується у формі тестових завдань з вибором правильної відповіді. Кількість тестових завдань – 25.</td></tr>
<tr><td>Лабораторні заняття</td><td>Після узагальнення (вступного слова) викладач дає відповіді на окремі теоретичні запитання, які виникли в студентів у процесі підготовки до заняття. Зазвичай з кожної теми лекційного курсу на лабораторні заняття виносять індивідуалізовані теми комплексного характеру, які дають змогу студенту ширше застосувати здобуті знання та підготуватися до самостійного виконання домашнього завдання.
На лабораторній роботі кожен студент отримує інструкцію до виконання. Після завершення роботи студент здає звіт у вигляді</td></tr>
</table>

	результатів експерименту, розрахунків та висновків та виконує підсумкове тестування.
Умови допуску до підсумкового контролю	Студент допускається до складання екзамену, якщо впродовж семестру він за змістові модулі набрав сумарно 25 балів і вище. Студент не допускається до складання екзамену, якщо впродовж семестру він за змістові модулі набрав менше 25 балів. У цьому випадку студенту у відомості робиться запис *"не допущений"* і виставляється набрана кількість балів. Допускається, як виняток, з дозволу декана факультету за заявою, погодженою з відповідною кафедрою, одноразове виконання студентом додаткових видів робіт з навчальної дисципліни (відпрацювання пропущених занять, перескладання змістових модулів, виконання індивідуальних завдань тощо) для підвищення оцінок за змістові модулі. Напередодні екзамену викладач подає доповідну декану про недопуск студентів академічної групи (груп). Відмітка про недопуск у відомості робиться при наявності розпорядження декана.

8. Політика курсу

Студент зобов'язаний відвідувати заняття відповідно до встановленого розкладу, не запізнюватися, мати відповідний зовнішній вигляд. У разі відсутності через хворобу надається відповідна довідка.

Пропущена лекція відпрацьовується студентом самостійно, у вигляді тесту за темою заняття.

Пропущена лабораторна робота виконується студентом самостійно вдома або в комп'ютерному класі, результати оцінюються викладачем.

У випадку, коли студент приймав участь у програмі мобільності, можливе врахування отриманих оцінок в іншому навчальному закладі за умови відповідності навчальних планів.

Можливе зарахування результатів неформальної освіти згідно з Положенням про порядок зарахування результатів неформальної освіти у ДВНЗ «Прикарпатський національний університет імені Василя Стефаника».

Політика академічної поведінки і етики

Студент повинен бути толерантним і поважати думку інших.

Заперечення повинні формулюватися тільки в коректній формі.

Плагіат та академічна недоброчесність несумісні з принципами діяльності ЗВО.

Не допускається підказування та списування під час здачі будь-яких робіт поточного, рубіжного чи підсумкового контролю.

Не допускається користування телефонами та будь-якими іншими електронними засобами під час здачі будь-яких робіт поточного, рубіжного, чи підсумкового контролю.

9. Рекомендована література

Базова

1. В.О. Казіміров, С.В. Мостовий, В.С. Орленко // «Інтелектуальний потенціал – 2020» - збірник наукових праць молодих науковців і студентів / Колектив авторів – Хмельницький: ПВНЗ УЕП, 2020. – Частина 2. С. 45-49 2.

2. Захист інформаційних ресурсів: навчально-методичний посібник до курсу – Захист інформаційних ресурсів‖ / укл. С. О. Троян. – Умань : [б.в.], 2012. –120 с.

3. DIGITAL 2020: APRIL GLOBAL STATSHOT. [Electronic resource] – Access: https://datareportal.com/reports/digital-2020-april-global-statshot

4. Malware. [Electronic resource] – Access: https://www.avtest.org/en/statistics/ malware/

5. Microsoft Word - Into the Web of Profit FINAL. [Electronic resource] – Access: https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Brom ium.pdf

6. Sikorski M., H. A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software.

7. Mirai (ботнет). [Електронний ресурс] – Режим доступу https://uk.wikipedia.org/wiki/Mirai_(ботнет)
8. WannaCry. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/WannaCr
9. Szor, P. (2005). The Art of Computer Virus Research and Defense.
10. S. Staniford, V. P. and Weaver, N. (2002). How to own the internet in your spare time. In Proceedings of the 11th USENIX Security Symposium.
11. Spafford, E. H. (1989). The Internet worm incident. In Proceedings of the 2nd European Software Engineering Conference.
12. Ransomware. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Ransomware
13. Nasi, E. (2014). Bypass Antivirus Dynamic Analysis. [Electronic resource] – Access: https://wikileaks.org/ciav7p1/cms/files/BypassAVDynamics.pdf
14. VirusTotal (2020). Daily Statistics. [Electronic resource] – Access: https://www.virustotal.com/en/statistics/
15. Cohen, F. (1987). Computer Viruses: Theory and Experiments. [Electronic resource] – Access: http://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohenviruses.html 66
16. Honkela, A. (2001). Nonlinear switching state-space models. [Electronic resource] – Access: https://www.cs.helsinki.fi/u/ahonkela/dippa/

Допоміжна

1. Singh, A. (2017). Malware Classification using Image Representation. [Electronic resource] – Access: https://security.cse.iitk.ac.in/node/254
2. Garnier, S. (2018). Implementation of the Matplolib 'viridis' color map in R. [Electronic resource] – Access: https://github.com/sjmgarnier/viridis
3. ResNet and ResNetV2. Keras. [Electronic Resource] – Access: https://keras.io/api/applications/resnet/
4. ImageNet. [Electronic Resource] – Access: http://www.image-net.org/
5. Pandalabs (2017). Quaterly Report. [Electronic resource] – Access: http://www.pandasecurity.com/mediacenter/src/uploads/2017/05/Pandalabs-2017-T1- EN.pdf

Викладач  **Павлюк М.Ф.**