МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА

Фізико-технічний факультет

Кафедра комп'ютерної інженерії та електроніки

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ

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

Затверджено на засіданні кафедри
Протокол № 1 від "26" серпня 2020 р.

Івано-Франківськ – 2020 рік

ЗМІСТ

1. Загальна інформація	
Назва дисципліни	Захист інформації в комп'ютерних системах
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

2. Анотація до курсу

Дисципліна «Захист інформації в комп'ютерних системах» 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 захисту інформації.

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 " Захист інформації в комп'ютерних системах " є вивчення методів та механізмів захисту інформації, розробка нових механізмів захисту та боротьби з постійно зростаючим ризиком кібератак.

У результаті вивчення навчальної дисципліни студент повинен

знати:

Концепції інформаційної безпеки, принципи безпечного проектування ІС а ІТ, методології безпечного програмування, загроз і атак, безпеки комп'ютерних мереж, методи криптографії.

вміти:

Зберігати конфіденційність, цілісність та доступність інформації, забезпечувати автентичність, відстежуваність та надійність інформації в умовах неповноти та невизначеність вихідних даних, багатокритеріальності професійних задач.

4. Компетентності

- здатність виконувати лабораторні дослідження в групі під керівництвом лідера, подібні навички, що демонструють здатність до врахування строгих вимог дисципліни, планування та управління часом.
- здатність і готовність спрямувати дії на розв'язання складних непередбачуваних задач і проблем у сфері комп'ютерної інженерії
- Здатність проектувати інформаційні та спеціалізовані комп'ютерні системи, захищати інформацію.

5. Результати навчання (компетентності)

Здатність демонструвати, аналізувати і використовувати знання сучасних друкованих та електронних ресурсів (в тому числі іншомовних) науково-технічної, довідникової та наукової інформації щодо стану, тенденцій і розвитку спеціалізованих комп'ютерних систем.

Здатність застосовувати знання методів обробки та відображення інформації в сучасних спеціалізованих комп'ютерних системах та демонструвати уміння проектування, розрахунку та програмування мікропроцесорних електронних засобів та систем.

Застосовувати методи та засоби опрацювання аналогових і цифрових сигналів, проектувати системи швидкісної обробки сигналів, захищати інформацію.

6. Організація навчання курсу

Обсяг курсу

Вид заняття	Загальна кількість годин
лекції	14
семінарські заняття/практичні/**лабораторні**	20
самостійна робота	56

Ознаки курсу

Семестр	Спеціальність	Курс (рік навчання)	Нормативний/ **вибірковий**
3	123 “Комп’ютерна інженерія”	2	Професійної підготовки

Тематика курсу

Тема, план	Форма занять	Література	Кількість годин	Вага оцінки	Термін виконання
Змістовий модуль. Технології захисту інформації в комп’ютерних системах та мережах.					
Тема 1. Види комп’ютерних злочинів. Поняття і класифікація комп’ютерних вірусів. Методи захисту текстових документів. Біометричний захист інформації.	лекція	Згідно списку літератури	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	0	Згідно розкладу
Тема 2 Класифікація програмних загроз. Природа вірусів. Структура вірусу. Антивірусний захист	лекція	Згідно списку літератури	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	0	Згідно розкладу
Тема 3. Безпека інформації	лекція	Згідно	Пояснити, узагальнити,	0	Згідно

в мережі ІНТЕРНЕТ. Захист електронної пошти. Захист інформації в електронних платіжних системах. Сучасні технології захисту комп'ютерних мереж.		списку літерату-ри	порівняти, проаналізувати, структурувати, визначити причини. **2 год.**		розкладу
Тема 4. Захист баз даних, електронних архівів. Захист програмного забезпечення, методи та рекомендації щодо підвищення рівня захисту програмного забезпечення.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	0	Згідно розкладу
Тема 5. Конфіденційність передачі мовної інформації. Перспективні напрямки підвищення безпеки акустичної інформації в мережах стандарту GSM.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	0	Згідно розкладу
Тема 6. Захищені операційні та мережеві середовища. Їх позитивні та негативні характеристики щодо загроз.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	0	Згідно розкладу
Тема 7. Сертифікація засобів захисту інформації від несанкціонованого доступу. Експертиза захищеності інформації в комп'ютерних системах.	лекція	Згідно списку літерату-ри	Пояснити, узагальнити, порівняти, проаналізувати, структурувати, визначити причини. **2 год.**	0	Згідно розкладу
Модульний контроль 1			2	1	Згідно розкладу
Лабораторні роботи					
Тема 1. Використання засобів захисту текстових документів.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **2 год.**	1	Згідно розкладу
Тема 2. Використання засобів захисту електронних таблиць.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **2 год.**	1	Згідно розкладу
Тема 3. Апаратні засоби захисту інформації в комп'ютерних системах.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **2 год.**	1	Згідно розкладу
Тема 4. Аналіз ефективності парольного захисту PDF-документів, архівів у різних форматах, текстових документів та електронних	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **4 год.**	1	Згідно розкладу

таблиць. Створення стійких паролів.					
Тема 5. Використання облікових записів користувачів та груп для реалізації політик безпеки з обмеженими правами доступу.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **2 год.**	1	Згідно розкладу
Тема 6. Налаштування рівнів безпеки сучасних браузерів.	Лаб. робота	Згідно списку літерату-ри	Виконати завдання. Проаналізувати, структурувати, визначити причини, узагальнити, аргументувати. **4 год.**	1	Згідно розкладу
Тема 7. Застосування криптографічних засобів захисту інформації. Формування пар відкритих та закритих ключів для реалізації асиметричного шифрування.	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. Основні відомості про захист інформації в комп'ютерних системах. Програмно-апаратні засоби захисту.	Само-стійна робота	Згідно списку літерату-ри	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	0	Впродовж семестру
Тема 2. Спам. Методи боротьби зі спамом. Методи боротьби із спамом. Сучасні технології спамерів.	Само-стійна робота	Згідно списку літерату-ри	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	0	Впродовж семестру
Тема 3. Система S/MIME. Електронні пластикові картки. Забезпечення безпеки електронних платежів через мережу Інтернет	Само-стійна робота	Згідно списку літерату-ри	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	0	Впродовж семестру
Тема 4. Криптографічні засоби захисту інформації в комп'ютерних системах. Криптографія в сучасних комп'ютерних технологіях.	Само-стійна робота	Згідно списку літерату-ри	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	0	Впродовж семестру
Тема 5. Особливості захисту інформації в системах мобільного зв'язку стандарту IS-95. Особливості захисту інформації в прямому та	Само-стійна робота	Згідно списку літерату-ри	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати,	0	Впродовж семестру

зворотньому каналах зв'язку.			узагальнити. **9 год.**		
Тема 6. Захист компонентів операційних систем. Порядок експлуатації, управління та супроводження систем захисту інформації в захищених комп'ютерних системах.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	0	Впродовж семестру
Тема 7. Методика проведення спецдосліджень захищеності засобів електронно-обчислювальної техніки (ЕОТ). Захист серверних приміщень.	Самостійна робота	Згідно списку літератури	Опрацювати питання самостійної роботи. Встановити залежність, проаналізувати, структурувати, узагальнити. **8 год.**	0	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 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.

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	

<table>
<tr><td></td><td>
<table>
<tr><td>80 – 89</td><td>B</td><td rowspan="2">добре</td><td rowspan="4">зараховано</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 результатів експерименту, розрахунків та висновків та виконує підсумкове тестування.</td></tr>
<tr><td>Умови допуску до підсумкового контролю</td><td>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.</td></tr>
<tr><td colspan="2">8. Політика курсу</td></tr>
<tr><td colspan="2">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</td></tr>
</table>

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. Захист інформаційних ресурсів: навчально-методичний посібник до курсу – Захист інформаційних ресурсів‖ / укл. С. О. Троян. – Умань : [б.в.], 2012. –120 с.
2. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. / В. Ф. Шаньгин. - М.: ДМК Пресс, 2012. – 576 с.
3. Проскурин В. Г. Защита программ и данных: учебное пособие / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. – М.: Академия, 2011. – 198 с.
4. DIGITAL 2020: APRIL GLOBAL STATSHOT. [Electronic resource] – Access: https://datareportal.com/reports/digital-2020-april-global-statshot
5. Malware. [Electronic resource] – Access: https://www.avtest.org/en/statistics/ malware/
6. 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
7. Sikorski M., H. A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software.
8. Mirai (ботнет). [Електронний ресурс] – Режим доступу https://uk.wikipedia.org/wiki/Mirai_(ботнет)
9. WannaCry. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/WannaCr
10. Szor, P. (2005). The Art of Computer Virus Research and Defense.
11. 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.
12. Spafford, E. H. (1989). The Internet worm incident. In Proceedings of the 2nd European Software Engineering Conference.
13. Ransomware. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Ransomware
14. Nasi, E. (2014). Bypass Antivirus Dynamic Analysis. [Electronic resource] – Access: https://wikileaks.org/ciav7p1/cms/files/BypassAVDynamics.pdf
15. VirusTotal (2020). Daily Statistics. [Electronic resource] – Access: https://www.virustotal.com/en/statistics/
16. Cohen, F. (1987). Computer Viruses: Theory and Experiments. [Electronic resource] – Access: http://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohenviruses.html 66
17. 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.**