Чернівецький національний університет імені Юрія Федьковича
(повне найменування закладу вищої освіти)
факультет математики та інформатики
(назва інституту/факультету)
Кафедра математичного моделювання
(назва кафедри)

СИЛАБУС
навчальної дисципліни
Захист інформації
(вкажіть назву навчальної дисципліни (іноземною, якщо дисципліна викладається іноземною мовою))
обов'язкова
(вказати: обов'язкова)

Освітньо-професійна програма *«Інформаційні технології та управління проектами»*
(назва програми)
Спеціальність *122 - Комп`ютерні науки*
(вказати: код, назва)
Галузь знань *12 - Інформаційні технології*
(вказати: шифр, назва)
Рівень вищої освіти *перший (бакалаврський)*
(вказати: перший (бакалаврський)/другий (магістерський)/третій (освітньо-науковий)
факультет математики та інформатики
(назва факультету/інституту, на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання *українська*
(вказати: на яких мовах читається дисципліна)

Розробники: *Перцов А.С., доцент, кандидат фізико-математичних наук*
(вказати авторів (викладач (ів)), їхні посади, наукові ступені, вчені звання)

Профайл викладача (-ів) http://matmod.fmi.org.ua/pro-kafedru/spivrobitnyky/pertsov-andriy-sergiyovych/

Контактний тел. (0372)584825

E-mail: a.pertsov@chnu.edu.ua

Сторінка курсу в Moodle https://moodle.chnu.edu.ua/enrol/index.php?id=4860

Консультації Онлайн-консультації за домовленістю

1. Анотація дисципліни.

Комп'ютерні інформаційні технології швидко розвиваються та вносять помітні зміни в наше життя. Інформація стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто в сотні разів перевершує вартість комп'ютерної системи, в якій вона зберігається.

Інформаційна безпека комп'ютерних систем досягається забезпеченням конфіденційності, цілісності та достовірності даних, що обробляються, а також доступності та цілісності інформаційних компонентів і ресурсів системи.

При розробці комп'ютерних систем, вихід з ладу або помилки в роботі можуть призвести до тяжких наслідків, питання комп'ютерної безпеки стають першочерговими. Відомо багато заходів, спрямованих на забезпечення комп'ютерної безпеки, основними серед них є технічні, організаційні та правові.

Захищеність інформаційної системи від випадкового або навмисного втручання, що завдає шкоди власникам або користувачам інформації, залежить, в основному, від доступності (можливість за розумний час одержати необхідну інформаційну послугу); цілісності (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованого зміни); конфіденційності (захист від несанкціонованого прочитання)

2. Мета навчальної дисципліни

Метою навчальної дисципліни є вивчення різних галузей комп’ютерної безпеки, інструментів кібербезпеки, які мають вирішальне значення для вирішення проблем у галузі безпеки, а також вивчення різних сфер безпеки мережі включаючи виявлення вторгнень, збір доказів та захист від кібератак.

У даній дисципліні студенти повинні освоїти основи мережевого та системного адміністрування, основні поняття криптографії, вміти визначати коли відбуваються напади всередині мереж, збирати докази вторгнень в мережу, перевіряти мережі та системи на вразливості.

3. Пререквізити. Комп’ютерні мережі, Операційні системи

4. Результати навчання

знати:

- основи мережевого та системного адміністрування,
- основні поняття криптографії
- особливості конфіденційності, цілісності та доступності систем.

вміти:

- визначати коли відбуваються напади всередині мережі,
- збирати докази вторгнень в мережу,
- перевіряти мережі та системи на вразливість,
- захищатись від мережевих атак.

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.
ЗК6. Здатність вчитися й оволодівати сучасними знаннями.
ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК8. Здатність генерувати нові ідеї (креативність).
ФК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

ПРН1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.
ПРН9. Розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв'язання задач в галузі комп'ютерних наук.
ПРН13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп'ютерних систем, знати мережні технології, архітектури комп'ютерних мереж, мати практичні навички технології адміністрування комп'ютерних мереж та їх програмного забезпечення.
ПРН16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

5. Опис навчальної дисципліни

5.1. Загальна інформація

Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**			**Кількість годин**						**Вид підсумкового контролю**
			кредитів	**годин**	**Змістових модулів**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	3	6	4	120	2	15			30	75		екзамен

5.2. Дидактична карта навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. ***Основи інформаційної безпеки.***												
Тема 1. **Вступ. Основні поняття, концепції та проблеми безпеки**	10	3		2		5						
Тема 2. **Криптографія. Мережі.**	24	4		6		14						

Тема 3. **Системне адміністрування. Виявлення та запобігання атак. Зловмисне програмне забезпечення.**	24	2		6		16						
Разом за ЗМ 1	58	9		14		35						
Змістовий модуль 2. ***Мережева безпека***												
Тема 1. **Перехоплення пакетів. Злом паролів.**	26	2		6		18						
Тема 2. **Сканування портів. Експлойти. Списки контролю доступу.**	22	2		6		14						
Тема 3. **Снортінг. DHCP, DNS та атаки комутації. Атаки MTM.**	14	2		4		8						
Разом за ЗМ 2	62	6		16		40						
Усього годин	120	15		30		75						

5.3. Зміст завдань для самостійної роботи

№	Назва теми
1.	DNS, DHCP
2.	Хешування паролів
3.	Кешування даних
4.	Різновиди мереж VPN та коли їх використовувати

6. Система контролю та оцінювання

Види та форми контролю

Формами поточного контролю є захист лабораторних робіт.

Формою підсумкового контролю є екзамен.

Засоби оцінювання

Засобами оцінювання та демонстрування результатів навчання є:

- виконанні лабораторні роботи;
- аналітичні звіти.

Критерії оцінювання результатів навчання з навчальної дисципліни

Лабораторні роботи виконуються студентами індивідуально. Структура лабораторних робіт для усіх студентів однакова.

Кожна лабораторна робота оцінюється з точки зору вчасності та якості виконання. Викладач слідкує за виконанням та оцінює студента під час захисту лабораторної роботи. Мінімальна позитивна оцінка формується на основі оцінок виконаних робіт протягом семестру та результату екзамену.

Шкала оцінювання: національна та ЄКТС

Оцінка за національною шкалою	**Оцінка за шкалою ECTS**	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Відмінно	A (90-100)	відмінно
Добре	B (80-89)	дуже добре
	C (70-79)	добре
Задовільно	D (60-69)	задовільно
	E (50-59)	достатньо
Незадовільно	FX (35-49)	(незадовільно) з можливістю повторного складання
	F (1-34)	(незадовільно) з обов'язковим повторним курсом

Розподіл балів, які отримують студенти

Поточне оцінювання (*аудиторна та самостійна робота*)						Кількість балів (залік)	Сумарна к-ть балів
Змістовий модуль №1			Змістовий модуль № 2				
Т1	Т2	Т3	Т4	Т5	Т6	30	100
10	10	10	10	10	10		

7. Рекомендована література

7.1. Базова (основна)

1. Кириленко, О. Криптографічні засоби захисту інформації: навч. посіб. - Київ: Вид-во НПУ ім. М. П. Драгоманова, 2018.
2. Алексєєнко, В. Основи кібербезпеки: навч. посіб. - Київ: КНЕУ, 2019.
3. Левицький, Г. Захист інформації в інформаційних системах та мережах: навч. посіб. - Київ: Вид-во НУБіП України, 2017.
4. Методичні вказівки до виконання курсової роботи з курсу "Захист інформації" для студентів спеціальності 125 "Кібербезпека" усіх форм

навчання / укладачі: Васильєва Н. В., Левицький Г. А. - Київ: Вид-во НУБіП України, 2020.
5. Державні стандарти зі зберігання і передачі інформації з обмеженим доступом: ДСТУ 7564:2014, ДСТУ 7565:2014, ДСТУ 7566:2014.
6. Інструкції з захисту інформації від несанкціонованого доступу, витоку, порушення цілісності та конфіденційності: ІСО/МЕК 27001, НСЗУ-Б-1, Інструкція з захисту від дії іонізуючих випромінювань (ІЗВ-97), Інструкції з обмеження доступу до державної таємниці.
7. Карпенко В.А., Хітрук І.В. Захист інформації: навч. посібник. – К.: Центр учбової літератури, 2014. – 528 с.
8. Захист інформації в комп'ютерних системах: навчальний посібник / С.І. Шевчук, В.Г. Костів, В.О. Мамчур та ін. – Львів: Видавництво Львівської політехніки, 2015. – 496 с.
9. Андрущак О.М. Захист інформації в комп'ютерних системах і мережах: навчальний посібник. – К.: МАУП, 2011. – 376 с.
10. Соломко Ю.М., Яглін М.А., Катушин В.О. та ін. Захист інформації: підручник. – К.: Вид-во НПУ імені М.П. Драгоманова, 2016. – 400 с.
11. Національний стандарт України ДСТУ 8302:2015 Захист інформації. Терміни та визначення.
12. Національний стандарт України ДСТУ 4152:2003 Захист інформації. Методи захисту від несанкціонованого доступу.
13. Національний стандарт України ДСТУ 4274:2004 Інформаційні технології. Захист інформації на персональних комп'ютерах. Вимоги та методи захисту.
14. Національний стандарт України ДСТУ 4363:2005 Захист інформації. Криптографічний захист інформації.
15. "Information Security Principles and Practice" by Mark Stamp, 2nd Edition, Wiley, 2011.
16. "Network Security Essentials" by William Stallings, 6th Edition, Pearson, 2017.
17. "Cryptography and Network Security: Principles and Practice" by William Stallings, 7th Edition, Pearson, 2017.
18. "Security Engineering: A Guide to Building Dependable Distributed Systems" by Ross Anderson, 2nd Edition, Wiley, 2008.
19. "Security in Computing" by Charles P. Pfleeger, Shari Lawrence Pfleeger, and Jonathan Margulies, 5th Edition, Prentice Hall, 2015.

7.2. Нормативні документи

1. Закон України "Про захист персональних даних" від 01.06.2010 року;
2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.2018 року;
3. Наказ НБУ "Про затвердження Правил захисту інформації в банківській сфері" від 22.03.2017 року;

4. Наказ Міністерства цифрової трансформації України "Про затвердження Положення про захист державної таємниці в інформаційно-телекомунікаційних системах органів державної влади та управління" від 01.12.2020 року.

7.3. Матеріали для теми "Криптографія"

1. "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell, 2nd Edition, CRC Press, 2014.
2. "Cryptography: Theory and Practice" by Douglas R. Stinson, 3rd Edition, CRC Press, 2005.
3. "Cryptographic Engineering" by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Wiley, 2010.
4. "Serious Cryptography: A Practical Introduction to Modern Encryption" by Jean-Philippe Aumasson, No Starch Press, 2017.

7.3. Матеріали для теми "Мережева безпека"

1. "Network Security Private Communication in a Public World" by Charlie Kaufman, Radia Perlman, and Mike Speciner, 2nd Edition, Prentice Hall, 2002.
2. "Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems" by Chris Sanders, 3rd Edition, No Starch Press, 2017.
3. "TCP/IP Illustrated, Volume 1: The Protocols" by W. Richard Stevens, 2nd Edition, Addison-Wesley Professional, 2011.
4. "The Practice of Network Security Monitoring: Understanding Incident Detection and Response" by Richard Bejtlich, No Starch Press, 2013.

7.4. Матеріали для теми "Web-безпека"

1. "Web Application Security: A Beginner's Guide" by Bryan Sullivan and Vincent Liu, McGraw-Hill, 2011.
2. "The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto, 2nd Edition, Wiley, 2011.
3. "The Tangled Web: A Guide to Securing Modern Web Applications" by Michal Zalewski, No Starch Press, 2012.
4. "Web Security for Developers: Real Threats, Practical Defense" by Malcolm McDonald, Packt Publishing, 2015.

7.5. Додаткові матеріали для курсу "Захист інформації"

1. Книга "Security Engineering: A Guide to Building Dependable Distributed Systems" авторів Ross J. Anderson.

2. Книга "Applied Cryptography: Protocols, Algorithms, and Source Code in C" автора Bruce Schneier.

3. Курс "Cybersecurity Fundamentals" від SANS Institute.

4. Курс "Network Security" від Cybrary.

5. Курс "Cybersecurity Essentials" від Cisco Networking Academy.

6. Курс "Penetration Testing and Ethical Hacking" від Offensive Security.

7. Журнал "Information Security Magazine".

8. Журнал "Network Security".

9.. Науковий журнал "Journal of Cybersecurity".

10. Науковий журнал "IEEE Transactions on Information Forensics and Security".

11. Ресурс "OWASP" (Open Web Application Security Project) з матеріалами про безпеку веб-додатків.

12. Ресурс "National Institute of Standards and Technology (NIST)" з матеріалами про стандарти та рекомендації з кібербезпеки.

7.6. Навчальні посібники та книги

1. Дейтел, Х. М. Безпека інформаційних технологій / Х. М. Дейтел, Д. Р. Чаффін. - К.: Видавництво "Діалог-МІФ", 2017;
2. Калінін, О. І. Захист інформації: підручник / О. І. Калінін, А. А. Кільченко. - К.: Кондор, 2018;
3. Костенко, В. І. Захист інформації в комп'ютерних системах і мережах: навч. посібник / В. І. Костенко, Є. І. Лазаренко. - Харків: Видавництво НТУ "ХПІ", 2017.

7.7. Журнали

1. "Кібербезпека та захист інформації" (журнал);
2. "Інформаційна безпека" (журнал);
3. "Захист інформації" (журнал);
4. "Проблеми захисту інформації" (журнал).

7.8. Додаткові матеріали

1. Книга "Cryptography Engineering: Design Principles and Practical Applications" авторів Нігеля Смарта, Джона Фергюсона та Брюса Шнайера
2. Курс "Cryptography I" на платформі Coursera, який викладає професор Ден Боне з Університету Стенфорда
3. Курс "Network Security" на платформі edX, який викладає професор Венджі Ху з Університету Цинциннаті
4. Курс "Security and Privacy in Your Pocket: Mobile Security and Privacy" на платформі Coursera, який викладає професор Ніколь Біббі з Університету Алабами
5. Курс "Applied Cryptography" на платформі Coursera, який викладає професор Дан Боне з Університету Стенфорда
6. Книга "Security Engineering: A Guide to Building Dependable Distributed Systems" авторів Росса Андерсона та Тайлера Мурі
7. Курс "Foundations of Cybersecurity" на платформі edX, який викладає професор Дейвід Бранд з Університету Гарварда

8. Інформаційні ресурси

1. https://www.edx.org/course/cybersecurity-fundamentals
2. https://www.edx.org/course/network-security-2
3. https://crackstation.net/hashing-security.htm
4. https://www.webopedia.com/TERM/V/VPN.html
5. https://www.tutorialspoint.com/difference-between-dns-and-dhcp
6. https://aws.amazon.com/caching/