МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА»

Фізико-технічний факультет

Кафедра комп’ютерної інженерії та електроніки

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ В КОМП’ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

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

Затверджено на засіданні кафедри
Протокол № __ від “_” ___ 2023 р.

Івано-Франківськ – 2023 рік

ЗМІСТ

1. Загальна інформація	
Назва дисципліни	Захист інформації в комп’ютерних системах і мережах
Рівень вищої освіти	Перший рівень вищої освіти
Викладач (-і)	доцент, кандидат фізико-математичних наук Запухляк Руслан Ігорович
Контактний телефон викладача	0342596007
E-mail викладача	ruslan.zapukhlyak@pnu.edu.ua
Формат дисципліни	Семестровий
Обсяг дисципліни	6 кредитів
Посилання на сайт дистанційного навчання	https://d-learn.pnu.edu.ua/
Консультації	відповідно до графіку індивідуальних консультацій, який розміщений на інформаційному стенді кафедри комп’ютерної інженерії та електроніки

2. Анотація до курсу

Дисципліна «Захист інформації в комп’ютерних системах і мережах» належить до переліку обов’язкових компонент за освітнім рівнем «бакалавр», що пропонуються в рамках циклу професійної підготовки студентів за освітньо-професійною програмою «Комп’ютерна інженерія». Вона забезпечує формування у студентів загальних та професійно-орієнтованих компетенцій. Предметом вивчення навчальної дисципліни є принципи побудови систем захисту інформації, вивчення видів та каналів витоку інформації та методи їх усунення, засвоєння основних принципів та вивчення алгоритмів криптографічного захисту інформації в комп’ютерних системах і мережах.

Силабус навчальної дисципліни “Захист інформації в комп’ютерних системах і мережах” складений відповідно до освітньо-професійної програми “Комп’ютерна інженерія ” підготовки бакалаврів спеціальності 123 «Комп’ютерна інженерія».

3. Мета та цілі курсу

Мета: формування у студентів основних вимог до створення систем захисту інформації, підсистем парольного захисту інформації, апаратно-програмних підсистем криптографічного захисту інформації, вивчення особливостей формування та керування ключовою інформацією для підсистем аутентифікації.

У результаті вивчення навчальної дисципліни студент повинен

знати:

- основні способи вразливості комп’ютерних систем та базові схеми атак ;
- організацію витоку інформації та систем захисту інформації;
- моделі систем захисту та характеристики парольного захисту;
- основні компоненти та загрози безпеки парольних систем;
- методи управління доступом;
- симетричні та асиметричні алгоритми та схеми шифрування інформації.

вміти:

- застосовувати алгоритми простих шифрів: підстановки, перестановки, Цезаря, Вернама та інших;
- використовувати криптографічні методи захисту інформації;
- використовувати симетричні та асиметричні алгоритми захисту інформації;
- застосовувати стандарти Україна НД 2.5-004-99 та США TCSEC, ISO 15408-99;
- розраховувати відкриті та таємні ключі при застосуванні алгоритму RSA;
- використовувати парольний захист в комп’ютерних системах і мережах.

4. Результати навчання (компетентності)

Інтегральна компетентність

- І. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності в комп’ютерній галузі або навчання, що передбачає застосування теорій та методів комп’ютерної інженерії і характеризується комплексністю та невизначеністю умов.

Загальні компетентності

- ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
- ЗК2. Здатність вчитися і оволодівати сучасними знаннями.
- ЗК3. Здатність застосовувати знання у практичних ситуаціях.

Спеціальні (фахові) компетентності

- Р12. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп’ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання.
- В10. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення захищеності комп’ютерних систем і мереж.

5. Організація навчання курсу

Обсяг курсу

Вид заняття	Загальна кількість годин
лекції	30
семінарські заняття / практичні / **лабораторні**	44
самостійна робота	106

Ознаки курсу

Семестр	Спеціальність	Курс (рік навчання)	Нормативний / вибірковий
VII	123 Комп’ютерна інженерія	4	загальної підготовки

Тематика курсу

Тема, план	Форма заняття	Літера-тура	Кіль-кість годин	Вага оцінки	Термін виконання
Змістовий модуль 1. Основні поняття та концептуальні моделі організації систем захисту інформації в ком’ютерних системах і мережах.					
Тема 1. Зміст базових понять: вразливість КС, канал витоку інформації, загрози безпеці, атака та вторгнення в КС.	лекція	1-4,7	2	0	Згідно розкладу
Тема 2. Організація каналів витоку інформації та систем захисту інформації.	лекція	1-4,8	2	0	Згідно розкладу
Тема 3. Моделі систем захисту Adept-50, Бела і Лападули.	лекція	1-3,9	2	0	Згідно розкладу
Тема 4. Модель моніторингу безпеки. Лічильники небезпечних подій. Вектор індикації аномалій в діях користувачів.	лекція	1-8	2	0	Згідно розкладу

Тема 5. Зміст етапів ідентифікації, авторизації та автентифікації користувачів. Прості паролі. Характеристики парольного захисту.	лекція	1,6,11	2	0	Згідно розкладу
Тема 6 Модифікації системи паролів. Паролі одноразові, ідентифікатори, секретні функції, процедури «рукостискання».	лекція	1,4,7,10	2	0	Згідно розкладу
Тема 7. Списки доступу, мандатні списки. Механізми розширення прав доступу.	лекція	1,5,7,9	2	0	Згідно розкладу
Модульний контроль 1			2	0,05	Згідно розкладу
Змістовий модуль 2. Симетричні та асиметричні алгоритми та системи шифрування.					
Тема 8. Перестановки та підстановки. Шифри «скітала», Полібія, Цезаря, Плейфера, Уітстона та Вермана. Шифрувальні таблиці та роторні машини.	лекція	1,4,11	2	0	Згідно розкладу
Тема 9. Симетричне шифрування по Шеннону. Стандарт DES. Функція шифрування та управління ключами. Режими ECB, CBC, OFB, CFB.	лекція	1,4,12	2	0	Згідно розкладу
Тема 10. Стандарт ГОСТ 28147-89. Мережа Фейстеля. Підвищення довжини ключів. Шифри зі змінною довжиною ключів.	лекція	1-3,9	2	0	Згідно розкладу
Тема 11. Хеш-згортка повідомлень. Алгоритми MD-5, SHA, ГОСТ 34.11-94.	лекція	1,9,12	2	0	Згідно розкладу
Тема 12. Схема Диффі-Хелмана розділення ключів на відкриту та таємну складові.	лекція	1,4,13	2	0	Згідно розкладу
Тема 13. Асиметрична схема Ель-Гамаля. Шифрування на основі множення за mod p.	лекція	1,2,6,12	2	0	Згідно розкладу
Тема 14. Асиметрична схема RSA. Шифрування на основі швидкого дискретного потенціювання. Генерування великих простих чисел. Тест Рабіна.	лекція	1,7,8-11	2	0	Згідно розкладу
Тема 15. Розрахунок	лекція	1,4,7-11	2	0	Згідно розкладу

відкритого та таємного ключів RSA. Розширений алгоритм Евкліда. Крипостійкість схем шифрування.					
Модульний контроль 2			2	0,05	Згідно розкладу
Лабораторні роботи					
Тема 1. Шифрування даних методами підстановки, перестановки і поліабетними шифрами.	Лаб. робота	1,4,10	4	1	Згідно розкладу
Тема 2. Шифрування даних за допомогою генератора псевдовипадкових чисел.	Лаб. робота	1,4,9	4	1	Згідно розкладу
Тема 3. Мережі Фейстеля.	Лаб. робота	1,4,8	4	1	Згідно розкладу
Тема 4. Дослідження криптоалгоритму шифрування RSA.	Лаб. робота	1,4,7	4	1	Згідно розкладу
Тема 5. Дослідження електронного цифрового підпису RSA.	Лаб. робота	1,2,10	4	1	Згідно розкладу
Тема 6. Дослідження криптоалгоритму шифрування Рабіна.	Лаб. робота	1,2,10	4	1	Згідно розкладу
Тема 6. Дослідження криптоалгоритму шифрування Ель-Гамаля.	Лаб. робота	3,4,7,10	4	1	Згідно розкладу
Тема 7. Дослідження електронного цифрового підпису Ель-Гамаля.	Лаб. робота	2-10	4	1	Згідно розкладу
Тема 8. Реалізація парольного захисту в комп’ютерних системах.	Лаб. робота	1-4	6	1	Згідно розкладу
Тема 9. Дослідження крипто алгоритму шифрування даних DES	Лаб. робота	1,2,10	6	1	Згідно розкладу
Модульний контроль				0,3	
Самостійна робота студентів					
Тема 1. Інформаційна безпека комп’ютерних систем. Класифікація загроз безпеки інформації та інформаційних систем.	Само-стійна робота	1-4	6	0	Впродовж семестру
Тема 2. Базові схеми атак: перехват, переривання. Модифікація та фальсифікація.	Само-стійна робота	1-7	8	0	Впродовж семестру
Тема 3. Законодавча база захисту інформації в Україні. Політика безпеки.	Само-стійна робота	2-8	6	0	Впродовж семестру

Тема 4. Радіотехнічне, організаційне, комунікаційне та програмно-технічне забезпечення.	Самостійна робота	2,4,9	6	0	Впродовж семестру
Тема 5. Способи формування та реєстрації паролів. ”Слабкі” паролі.	Самостійна робота	2,6,11	6	0	Впродовж семестру
Тема 6. Модель простору безпеки Хартсона. Домени повноважень користувачів.	Самостійна робота	6-11	8	0	Впродовж семестру
Тема 7. Принцип мінімальних привілей.	Самостійна робота	4-9	6	0	Впродовж семестру
Контроль самостійної роботи			2	0,05	Згідно розкладу
Тема 9. Автентифікація суб’єктів на основі симетричних схем. Сеансові та майстер ключі. Протоколи Нідхема-Шредера та Деннінга.	Самостійна робота	1-5	8	0	Впродовж семестру
Тема 10. Автентифікація суб’єктів на основі асиметричних схем. Сертифікати відкритих ключів. Цифрові паспорти. Схеми «рукостискання».	Самостійна робота	1-4,7	8	0	Впродовж семестру
Тема 11. Схема аутентифікації Гіллоу-Куіскуотера. Цикли акредитації. Схема Шейге, Фіата, Шаміра.	Самостійна робота	1-5,10	8	0	Впродовж семестру
Тема 12. Аутентифікація повідомлень. Цифрові підписи. Алгоритми EGSA, DSA. Поняття відкритого ключа та відбитку хеш-образу повідомлення.	Самостійна робота	4-6	8	0	Впродовж семестру
Тема 13. Електронні платіжні системи. Пластикові картки. Банки-емітенти, банки-еквайєри.	Самостійна робота	4-8	6	0	Впродовж семестру
Тема 14. Організаційно-технічні задачі забезпечення захисту інформації: цілісності, конфіденційності, доступності та спостереженості.	Самостійна робота	1,3,4,7	8	0	Впродовж семестру
Тема 15. Стандарти: США TCSEC, ISO 15408-99, Україна НД 2.5-004-99.	Самостійна робота	1-6	6	0	Впродовж семестру
Контроль самостійної			2	0,05	Згідно розкладу

роботи					
Підсумковий контроль (екзамен)				0,5	

6. Система оцінювання курсу

Загальна система оцінювання курсу

Поточний контроль здійснюється під час проведення лабораторних робіт, індивідуальних занять при контролі за самостійною роботою та колоквіумів при оцінюванні лекційного матеріалу 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 (добуток балів за окремий змістовий модуль на ваговий коефіцієнт) 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 програмного матеріалу з усієї дисципліни, здатності творчо використовувати здобуті знання та вміння, формувати власне ставлення до певної проблеми тощо.

		Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	
80 – 89	**B**		
70 – 79	**C**		
60 – 69	**D**		
50 – 59	**E**		
26 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-25	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

Вимоги до письмової роботи	Всі письмові роботи виконуються у формі тестових завдань з вибором правильної відповіді. Кількість тестових завдань – від 10 до 25.
Лабораторні роботи	Після узагальнення (вступного слова) викладач дає відповіді на окремі теоретичні запитання, які виникли в студентів у процесі підготовки до лабораторної роботи. На лабораторні роботи виносять задачі криптографічного змісту, які є індивідуалізованими темами комплексного характеру, які дають змогу студенту ширше застосувати здобуті знання та підготуватися до самостійного виконання домашнього завдання. Для перевірки рівня засвоєння навчального матеріалу студенти виконують тестові завдання. На лабораторній роботі кожен студент отримує інструкцію до виконання. Після завершення роботи студент оформляє і захищає звіт з результатами роботи та складає підсумковий тест.
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"* івиставляється 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.

7. 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, як короткий конспект 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.

8. Рекомендована література

Базова

1. Закон України «Про інформацію».
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах».
3. Закон України «Про науково-технічну інформОстапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. – Новий світ -2000, 2020. – 678 с.
4. Bruce Schneier. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons, 2017, 784 p.
5. Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарєв та інші Інформаційна безпека. – видавництво ”Львівської політехніки”, 2019. – 580 с.
6. В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та інші Захист систем електронних комунікацій. – навчальний посібник, КНТЕУ, 2019. – 164 с.
7. А.Е. Лагун Криптографічні системи та протоколи. - видавництво ”Львівської політехніки”, 2013. – 96 с.
8. Р.А. Бурачок, М.М. Климаш, Б.В. Король Телекомунікаційні системи передавання інформації. Методи кодування. видавництво ”Львівської політехніки”, 2015. – 476 с.
9. Кузнецов О.О. Захист інформації в інформаційних системах. / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2011.– 510 с.
10. Кузнецов О.О. Захист інформації в інформаційних системах. методи традиційної криптографії / О.О. Кузнецов, С.П. Євсеєв, О.Г. Король. - Харків: Вид. ХНЕУ, 2010.– 316 с.
11. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Л – Луцьк: Вежа-Друк, 2014. – 164 с.

Допоміжна

12. Богуч В.М.. Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. –К.: ДУІКТ, 2006. –126 с.
13. J.-P. Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption. No Starch Press, 2017, 312 p.
14. William J. Buchanan. Cryptography. River Publishers, 2017, 350 p.
15. Douglas Robert Stinson, Maura Paterson. Cryptography: Theory and Practice. CRC Press, 2018, 598 p.
16. Denis Trcek. Managing Information Systems Security and Privacy. Springer Berlin Heidelberg, 2005, 234 p.
17. Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. Cryptography Engineering: Design Principles and Practical Applications. John Wiley & Sons, 2011, 384 p.

Викладач **Запухляк Р.І.**