Чернівецький національний університет імені Юрія Федьковича
Інститут фізико-технічних та комп'ютерних наук
Кафедра програмного забезпечення комп'ютерних систем

СИЛАБУС
навчальної дисципліни

«Технології захисту інформації»

(обов'язкова)

Освітньо-професійна програма «Інформаційні системи та технології»

Спеціальність 126 – Інформаційні системи та технології

Галузь знань 12 – Інформаційні технології

Рівень вищої освіти перший бакалаврський

Мова навчання українська

Розробник: доктор ф.-м. наук, професор, Остапов С.Е.

Профайл викладача:
https://sites.google.com/chnu.edu.ua/pzks/%D0%BF%D1%80%D0%BE-%D0%BD%D0%B0%D1%81/%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%82%D0%BD%D0%B8%D0%BA%D0%B8/%D0%BE%D1%81%D1%82%D0%B0%D0%BF%D0%BE%D0%B2-%D1%81-%D0%B5

Контактний тел. +38(0372)509 434
E-mail: s.ostapov@chnu.edu.ua

Сторінка курсу в Moodle:
https://moodle.chnu.edu.ua/course/view.php?id=959

Консультації:
Очні та онлайн-консультації – згідно з графіком (за попередньою домовленістю).

1. Анотація дисципліни (призначення навчальної дисципліни).

Навчальна дисципліна «Технології захисту інформації» призначена для формування у студентів знань, вмінь та навичок з основних методів та засобів захисту інформації, які будуть корисними при розгортання та обслуговуванні інформаційних систем.

2. Мета навчальної дисципліни:

Надання студентам систематизованих знань з основ захисту інформації: мети, завдань, принципів організації комплексних систем захисту інформації на основі нормативних документів; забезпечити вмінням боротьби з загрозами інформації в комп'ютерних мережах; теоретичними і практичними знаннями з криптографічних засобів захисту; захисту інформації від витоку технічними каналами; методами боротьби з несанкціонованим доступом до інформації з обмеженим доступом; використанням програмно-апаратних методів для побудови систем захисту.

Завдання дисципліни: випливають з ролі дисципліни у системі підготовки спеціалістів: вивчення студентами основних теоретичних понять з захисту інформації; уміння застосовувати їх для розв'язку завдань, що ставить перед ними суспільство; набуття практичних навичок; вільне володіння основними методами захисту інформації; розуміння основних понять і сучасного стану даного предмету.

3. Пререквізити.

- Дискретна математика.
- Теорія алгоритмів та програмування.
- Об'єктно-орієнтоване програмування.
- Комп'ютерні мережі.

4. Результати навчання. У результаті вивчення навчальної дисципліни студент повинен:

знати:

- найновіші досягнення в галузі захисту інформації;
- характеристики основних підсистем ідентифікації та аутентифікації;
- характеристики основних механізмів доступу;
- характеристики підсистем захисту основних класів операційних систем;
- основні принципи формування політики безпеки підприємства;
- основні принципи та методи криптографічного захисту інформації;
- критерії захищеності автоматизованих систем;
- характеристики основних стандартних профілів захищеності автоматизованих систем;
- основні характеристики захищених протоколів передавання даних.

вміти:

- будувати політику безпеки в комп'ютерних мережах на основі аналізу загроз та оцінки ризиків;
- розробляти прості системи криптографічного захисту інформації;
- використовувати програмні, організаційно-адміністративні та технічні засоби захисту інформації;
- орієнтуватися в законодавчо-нормативній базі в галузі захисту інформації;
- правильно налагоджувати підсистеми захисту сучасних операційних систем;
- правильно визначати та застосовувати критерії захищеності автоматизованих систем.

Під час вивчення даної дисципліни студенти набудуть:

Загальних компетентностей:

КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 2. Здатність застосовувати знання у практичних ситуаціях.

КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальних (фахових, предметних) компетентностей:

КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

КС 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації.

Програмними результатами навчання є:

ПР 3. **Використовувати** базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

ПР 4. **Проводити** системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях.

ПР 5. **Аргументувати** вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій.

ПРН 10. **Розуміти і враховувати** соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень.

5. Опис навчальної дисципліни

5.1. Загальна інформація

Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**		**Кількість годин**						**Вид підсумкового контролю**
			кредитів	**годин**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	4	6,7	8	240	69			56	115		іспит

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. Класичні криптосистеми												
Тема 1.1. Вступ	8	2				6						
Тема 1.2. Класичні	24	6		6		12						

техніки шифрування. Елементи теорії зв'язку.												
Тема 1.3. Потокові та блокові шифри.	16	2		4		10						
Разом за змістовим модулем 1	**48**	**10**		**10**		**28**						
Змістовий модуль 2. Моделі і методи забезпечення безпеки БД.												
Тема 2.1. Стандарт шифрування DES	8	2		2		4						
Тема 2.2. Сучасні симетричні криптоалгоритми.	6	2				4						
Тема 2.3. Український стандарт шифрування ДСТУ 76242014.	6	2				4						
Тема 2.4. Елементи теорії чисел	3	1				2						
Тема 2.5. Асиметрична криптосистема RSA	5	1		2		2						
Тема 2.6. Інші асиметричні криптосистеми	7	1		2		4						
Тема 2.7. Функції хешування	5	1				4						
Тема 2.8. Алгоритми електронного цифрового підпису	9	1		4		4						
Тема 2.9. Класифікація атак на криптографічні системи	6	2				4						
Тема 2.10. Розподіл криптографічних ключів	8	2		2		4						
Тема 2.11. Генерування випадкових та псевдовипадкових послідовностей	9	1		4		4						
Разом за змістовим модулем 2	**72**	**16**		**16**		**40**						
Змістовий модуль 3. Політика безпеки та криптографічний захист інформації												
Тема 1.1Основні поняття та визначення захисту інформації	2	1		-		1						
Тема 1.2. Політика інформаційної безпеки та її основні поняття	4	1		-		3						
Тема 1.3. Основні поняття криптології. Класифікація сучасних криптосистем.	4	2		-		2						
Тема 1.4. Симетричні криптосистеми.	12	4		2		6						

Тема 1.5. Криптографічні функції хешування.	12	2		4		6						
Тема 1.6. Асиметричні криптоалгоритми.	12	2		4		6						
Тема 1.7. Електронний цифровий підпис.	12	2		4		6						
Тема 1.8. Елементи криптоаналізу.	6	2		2		2						
Разом за змістовим модулем 3	**64**	**16**		**16**		**32**						
Змістовий модуль 4. Безпека сучасних операційних систем												
Тема 2.1. Формальні моделі доступу.	8	2		2		4						
Тема 2.2. Критерії захищеності комп'ютерних систем від несанкціонованого доступу	16	4		6		6						
Тема 2.3. Протоколи аутентифікації	10	2		2		6						
Тема 2.4. Безпека сучасних операційних систем.	22	6		4		12						
Разом за змістовим модулем 4	**56**	**14**		**14**		**28**						
Усього годин	**240**	**69**		**56**		**115**						

5.2.1. Теми лабораторних занять

№ з/п	Назва теми
1	Шифрувальна система на основі шифру Цезаря
2	Дослідження афінної системи шифрування Цезаря
3	Шифрувальна система на основі шифру гаммування
4	Система блокового шифрування S-DES
5	Дослідження розсіювальних властивостей S-DES
6	Використання асиметричної системи RSA для цифрового підпису
7	Відкритий розподіл криптографічних ключів
8	Потоковий шифр на основі генератора BBS
9	Шифрувальна система на основі шифру простої заміни
10	Використання CryptoAPI Windows XP для розробки криптографічного ПЗ
11	Дослідження розповсюдження помилки в симетричних шифрах
12	Вивчення можливостей статистичного пакету NIST STS
13	Порівняльні дослідження потокових шифрів власної розробки
14	Розробка та дослідження генератора випадкових чисел за допомогою пристроїв комп“ютера
15	Коди аутентифікації повідомлень на основі хеш-функцій
16	Електронний цифровий підпис на основі симетричної криптосистеми
1	Механізми захисту ОС Windows XP
2	Захист реєстру ОС Windows XP

3	Налаштування політики безпеки ОС Windows XP SP2
4	Вивчення можливостей шифрованої файлової системи ОС Windows
5	Дослідження можливостей центру забезпечення безпеки ОС Windows
6	Засоби аналізу захищеності
7	Аутентифікація користувачів на основі токенів безпеки
8	Підсистема керування доступом
9	Підсистема реєстрації
10	Дослідження стійкості парольного захисту
11	SQL-ін'єкції та методи боротьби з ними
12	Дослідження стійкості точок доступу бездротової мережі
13	Дослідження ефективних методів захисту від експлойтів

Лабораторний практикум складається з 16 робіт і має кілька рівнів складності.

Студент може обирати будь-яку кількість робіт, виконувати їх в будь-якому порядку (за винятком випадків, коли для виконання певної роботи необхідно виконати попередню/попередні).

Задача студента — набрати максимально можливу кількість балів. У навчальному плані на лабораторний практикум відводиться 50 балів (20 в першому модулі + 30 — в другому). Звісно, можна набрати й більше/менше балів, виконавши більшу/меншу кількість лабораторних робіт.

Лабораторні роботи будуть оцінюватися так, як подано в таблиці. Звісно, якщо робота виконана не повністю, або якщо виконано полегшений варіант — повна кількість балів не нараховується.

Можливий варіант дистанційного захисту лабораторної роботи, коли студент, зробивши роботу, знімає скрин-каст протоколу дій, робить архів зі звітом та кодом, і відправляє це викладачу (попередньо домовившись про такий спосіб захисту!).

Таблиця: Оцінювання лабораторних робіт з курсу “Технології захисту інформації”

ЛР№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
К-сть балів	4	4	4	6	6	4	4	4	4	8	10/6	8	10	10	10	10

	- лабораторні роботи I рівня;
	- лабораторні роботи II рівня;
	- лабораторні роботи III рівня.

Лабораторні роботи I рівня — прості роботи, в яких необхідно розробити програмне забезпечення, що використовує класичні криптоалгоритми (шифр Цезаря, спрощені потокові шифри, спрощений RSA).

Лабораторні роботи II рівня вимагають більш ретельної роботи та написання більших об’ємів коду.

Лабораторні роботи III рівня — досить серйозні криптографічні застосування, які продемонструють студенту, що їх виконав, можливості сучасного криптографічного програмного забезпечення та принципів його розробки.

ЗАУВАЖЕННЯ: В усіх лабораторних роботах висуваються вимоги до правил написання коду, наприклад, *C++ Programming Style Guideline* або аналогічного для обраної Вами мови програмування. Змінні типу Form1, Procedure1, a1,b2,c3 не допускаються, і код буде відхилений. Крім цього, код повинен супроводжуватися коментарями, які давали би

повне розуміння про функції тієї чи іншої процедури/функції/класу/об’єкту тощо. Код без коментарів також буде відхилятися.

5.2.2. Самостійна робота

№ з/п	Назва теми
1	Порівняльний аналіз сучасних антивірусних програм
2	Сучасні міжмережеві екрани та їх властивості
3	Сучасні системи аналізу втручань
4	Порівняльний аналіз сучасних систем підсилення парольного захисту
5	Порівняльний аналіз сучасних механізмів доступу
6	Використання електронних засобів доступу
7	Засоби криптографічного захисту інформації в ОС Windows 10.
8	Засоби захисту ОС Windows 10.
9	Підтримка електронних засобів ідентифікації в ОС Windows 10.

5.2.3. Індивідуальні завдання

Індивідуальні завдання включають:

- Формування політики безпеки. Приклади та їх аналіз.
- Захист аудіоінформації від витоку технічними каналами.
- Захист ліній зв’язку та телефонних апаратів.
- Класична система безпеки. Основні особливості.
- Методи захисту периметру.
- Адміністративні методи захисту.
- Електронні системи ідентифікації та аутентифікації.
- Адміністративні засоби контролю доступу.
- Основні методи біометричної ідентифікації особи. Їх переваги та недоліки.
- Сучасні методи багатофакторної аутентифікації.

6. Система контролю та оцінювання

Види та форми контролю

Формами поточного контролю при вивченні курсу є:

- Усна відповідь студентів під час опитування на лекціях;
- Захист лабораторних робіт;
- Тестування з використанням платформи Moodle;
- Написання та захист рефератів.

Формами підсумкового контролю служать:

- Іспит;
- Залік, якщо він передбачений освітньою програмою.

Засобами оцінювання є:

- Модульні та поточні контрольні роботи;
- Тестувальна система на платформі Moodle;
- Реферати з тематики курсу;
- Виконання та захист лабораторних робіт.

6.1. Критерії оцінювання результатів навчання з навчальної дисципліни

Оцінювання знань студентів з навчальної дисципліни “Технології захисту інформації” здійснюється на основі результатів поточного та підсумкового контролю.

Оцінювання знань студентів здійснюється за 100-бальною шкалою. Результати роботи студентів впродовж навчального семестру оцінюються в ході поточного контролю в

діапазоні від 1 до 70 балів (включно), а результати підсумкового контролю (6 семестр – залік, 7 семестр - екзамен) оцінюються від 1 до 30 балів (включно).

Поточний контроль роботи студентів з навчальної дисципліни "Технології захисту інформації" здійснюється за наступними критеріями: оцінювання рефератів (20 балів) та лабораторних робіт (50 балів).

Іспит (30 балів) здійснюється у вигляді тестування в системі електронного навчання Moodle. У сумі з модульними контролями (70 балів) це загалом складатиме максимально 100 балів.

Підсумкова оцінка. Підсумкова оцінка виставляється за загальною сумою балів, набраних студентом під час модульних контролів та на іспиті, згідно із наступною таблицею:

Шкала оцінювання: національна та ЄКТС

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	зараховано
80 – 89	**B**	добре	
70 – 79	**C**		
60 – 69	**D**	задовільно	
50 – 59	**E**		
35 – 49	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0 – 34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

6 семестр

Поточне тестування та самостійна робота														Підсумковий тест (залік)	Сума
Змістовий модуль 1				Змістовий модуль 2											
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	Т13	Т14	30	100
4	10	6	10	5	5	5	5	2	4	4	2	4	4		

7 семестр

Поточне тестування та самостійна робота												Кількість балів (іспит)	Сума
Змістовий модуль 1								Змістовий модуль 2					
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	Т12	30	100
2	2	3	7	7	6	7	6	7	7	8	8		

6.2 Умови зарахування результатів неформальної освіти

Результати неформальної освіти можуть бути зараховані студенту згідно з Положенням ЧНУ "Про взаємодію формальної та неформальної освіти, визнання результатів навчання (здобутих шляхом неформальної та/або інформальної освіти, в системі формальної освіти)".

Також, як виконані види роботи з відповідних тем, студенту можуть бути зараховані бали за наукові публікації у матеріалах науково-практичних конференцій та фахових чи апробаційних виданнях або подання роботи на конкурс студентських наукових робіт.

6.3. Політика курсу

Політика щодо відвідування: відвідування занять є обов'язковим (виключення складають студенти, які навчаються за індивідуальним графіком та ті, кому зараховано результати неформальної освіти). Для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей. Засвоєння теми лекції, пропущеної з поважної причини, перевіряється під час складання підсумкового контролю. Пропуск лекції з неповажної причини відпрацьовується студентом (співбесіда, реферат тощо). Пропущені лабораторні заняття, незалежно від причини пропуску, студент відпрацьовує згідно з графіком консультацій. За об'єктивних причин (наприклад, хвороба, участь у програмі міжнародного обміну, індивідуальний графік навчання) навчання може відбуватись у змішаній формі (очнодистанційній) за погодженням із керівником курсу.

Політика академічної доброчесності: обов'язковими є посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації; списування під час контрольних заходів заборонені (в т. ч. із використанням мобільних пристроїв).

Політика щодо дедлайнів та перескладання: роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (від 10% до -50% від максимальної кількості балів – залежно від терміну затримки здачі роботи). Порушення терміну здачі роботи з поважної причини не призводить до втрати балів. Складання (перескладання) іспиту відбувається за встановленим деканатом розкладом.

Політика щодо оскарження оцінювання: забезпечення об'єктивності та прозорості оцінювання регламентується п.3.8-3.9 Положення ЧНУ "Про контроль і систему оцінювання результатів навчання здобувачів вищої освіти"; оскарження результатів підсумкового оцінювання здійснюється у відповідності до Положення ЧНУ "Про апеляцію на результати підсумкового семестрового контролю знань студентів".

7. Рекомендована література

Базова

1. Остапов С.Е., Жихаревич В.В., Добровольський Ю.Г. Сучасні методи та засоби захисту інформації. Монографія. Чернівці : ЧНУ, 2021. 71 С.
2. Остапов С.Е., Євсеєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник. - Львів: Новий світ-2000, 2019. - 678 с.
3. Остапов С.Е., Валь Л.О. Основи криптографії. Чернівці: Книги-ХХІ, 2008. – 188 с.
4. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації. Чернівці: Родовід, 2015. - 438 С.
5. Ємець А.В., Мельник В.В., Попович П.А. Сучасна криптографія. Основні поняття. Львів, 2003 р. – 156 С.
6. Б.Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные коды на языке С. - М.: Триумф, 2002. - 816 с.

Допоміжна

1. . Tanasyuk, S. Ostapov. Development and Research of Cryptographic Hash Functions Based on Two-Dimentional Cellular Automata//Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 2018. – 8 (1), PP.24-27.

2. S. Ostapov, O. Val, S. Yanushevsky, D. Chyzhevsky. Cryptography on the Base of Cellular Automata // Internet in the Information Society. Monograph / Publisher: Scientific Publishing University of Dabrowa Gornicza, Editors: Maciej Rostanski, Piotr Pikiewicz, Pawel Buchwald, 2015. – pp.71-86.
3. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко. Х. : НТУ "ХПІ", 2014. 251с.
4. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування : монографія. Х. : Видавництво "Форт", 2012. 870 с.
5. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. – К.: Видавничий дім «Кондор», 2019. – 272 с.
6. Кормич Б.А. Кібербезпека: організаційно-правові основи : Навч. посібн. / Б.А. Кормич. – К. : Кондор, 2008. – 382 с
7. Закон України "Про захист інформації в автоматизованих системах"
8. Закон України "Про інформацію"
9. Закон України "Про державну таємницю"

8. Інформаційні ресурси

1. Український центр інформаційної безпеки . – Електронний ресурс. – http://www.bezpeka.com/.
2. Криптографічний захист інформації. - Електронний ресурс. Режим доступу: https://web.archive.org/web/20100301080922/http://bezpeka.com/ru/lib/spec/cript.html