ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ПУЛЮЯ

ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ (ФІС)

КАФЕДРА КІБЕРБЕЗПЕКИ

1. Загальна інформація про дисципліну:

Назва дисципліни	ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ
Викладач	Загородна Наталія Володимирівна
Профайл викладача	http://kaf-kb.tntu.edu.ua/wp-content/uploads/2022/01/Zagorodna.pdf
Контактний тел.	Комутатор (0352) 51-97-00, внутрішній 1804 (із зовнішніх телефонів через комутатор, тоді в режимі тонального набору набрати внутрішній номер),
E-mail:	zagorodna_n@tntu.edu.ua
Сторінка дисципліни в A-Tutor	https://dl.tntu.edu.ua, ID 5653
Консультації	Згідно графіку консультацій

2. Коротка анотація до дисципліни

Навчальна дисципліна «**Технології захисту інформації**» належить до вибіркової частини дисциплін циклу професійної підготовки освітньої програми «Комп'ютерні науки» третього (доктора філософії) рівня вищої освіти. Галузь знань 12 «Інформаційні технології», спеціальність 122 «Комп'ютерні науки». Викладається у 3-му (другий курс) семестрі обсягом 4,5 кредитів ECTS. Формою підсумковою контролю є залік.

3. Мета та завдання дисципліни

Мета дисципліни «**Технології захисту інформації**» - підготовка теоретичного фундаменту для подальшого вивчення курсів професійного спрямування; формування знань і навичок з основних понять та визначення захисту інформації, формування політики безпеки, критеріїв оцінки захищеності комп'ютерних систем, основ криптографічного та стеганографічного захисту інформації.

В даній дисципліні розглядаються такі питання: основні поняття безпеки інформації; моделі загроз та порушника; законодавча та нормативно-правова база, стандарти в галузі інформаційної та/або кібербезпеки; управління інформаційною безпекою; криптографічний захист інформації; безпека інформаційно-комунікаційних систем.

Завданням дисципліни є сформувати здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

4. Формат дисципліни:

Дисципліна передбачає проведення лекційних, лабораторних занять та консультацій. Для кращого розуміння та засвоєння викладеного матеріалу дисципліна має супровід у вигляді електронного курсу Тернопільський національний технічний університет ім. І. Пулюя (https://dl.tntu.edu.ua). Електронні навчальні курси мають лекційний матеріал, методичні вказівки до лабораторних робіт та систему тестування.

5. Результати навчання:

В результаті вивчення дисципліни студент повинен **знати:**

- ✓ основні поняття безпеки інформації;
- ✓ моделі загроз та порушника;
- ✓ законодавча та нормативно-правова база, стандарти в галузі інформаційної та/або кібербезпеки;
- ✓ управління інформаційною безпекою;
- ✓ основні терміни та визначення політики безпеки;
- ✓ безпеку інформаційно-комунікаційних систем.

- ✓ криптографічний захист інформації;
- ✓ стеганографічний захист інформації.

В результаті вивчення дисципліни студент повинен **вміти:**

- ✓ визначати вимоги політики безпеки та формувати профіль захисту відповідно до забезпечення послуг безпеки в ІС та Т;
- ✓ ставити завдання, аналізувати, давати порівняльну характеристику різних варіантів застосування механізмів та протоколів захисту інформації в ІКС;
- ✓ здатність забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;
- ✓ здатність аналізувати технічні параметри діючих протоколів та механізмів захисту інформації з точки зору використання в комп'ютерних системах та мережах, впливу їх характеристик на основні показники ІКС ;
- ✓ здійснювати управління безпекою, зокрема знати основні моделі управління ризиками безпеки;
- ✓ здатність проводити аналіз ефективності прийнятих технічних рішень щодо забезпечення захисту інформації в інформаційних системах, користуватися математичним та статистичним апаратом щодо вирішення інженерних завдань, які виникають під час розробки та дослідження механізмів;
- ✓ здатність забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій;
- ✓ застосовувати системи криптографії та стеганографії в професійній діяльності.

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів **загальних компетентностей (ЗК) та фахових компетентностей (ФК)** згідно освітньої програми.

Загальні:

ЗК2. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК3. Здатність працювати в міжнародному контексті.

Спеціальні (фахові):

ФК1. Здатність виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у комп'ютерних науках та дотичних до них міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з комп'ютерних наук та суміжних галузей.

ФК2. Здатність застосовувати сучасні методології, методи та інструменти експериментальних і теоретичних досліджень у сфері комп'ютерних наук, сучасні цифрові технології, бази даних та інші електронні ресурси у науковій та освітній діяльності.

ФК3. Здатність виявляти, ставити та вирішувати дослідницькі науково-прикладні задачі та/або проблеми в сфері комп'ютерних наук, оцінювати та забезпечувати якість виконуваних досліджень.

ФК4. Здатність ініціювати, розробляти і реалізовувати комплексні інноваційні проєкти у галузі комп'ютерних наук та дотичні до неї міждисциплінарних проєктах, демонструвати лідерство під час їх реалізації.

ФК6. Здатність аналізувати та оцінювати сучасний стан і тенденції розвитку комп'ютерних наук та інформаційних технологій.

Вивчення навчальної дисципліни передбачає формування у студента таких прикладних **результатів навчання (ПР)** згідно освітньої програми:

РН1. Мати передові концептуальні та методологічні знання з комп'ютерних наук і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень на рівні останніх світових досягнень з відповідного напряму, отримання нових знань та/або здійснення інновацій.

РН2. Вільно презентувати та обговорювати з фахівцями і нефахівцями результати досліджень, наукові та прикладні проблеми комп'ютерних наук державною та іноземною мовами, оприлюднювати результати досліджень у наукових публікаціях у провідних міжнародних наукових виданнях.

РН6. Застосовувати сучасні інструменти і технології пошуку, оброблення та аналізу інформації, зокрема, статистичні методи аналізу даних великого обсягу та/або складної структури, спеціалізовані бази даних та інформаційні системи.

РН7. Розробляти та реалізовувати наукові та/або інноваційні інженерні проєкти, які дають можливість переосмислити наявне та створити нове цілісне знання та/або професійну практику і розв'язувати значущі наукові та технологічні проблеми комп'ютерної науки з дотриманням норм академічної етики і врахуванням соціальних, економічних, екологічних та правових аспектів.

РН10. Відшуковувати, оцінювати та критично аналізувати інформацію щодо поточного стану та трендів

розвитку, інструментів та методів досліджень, наукових та інноваційних проєктів з комп'ютерних наук.

6. Обсяг дисципліни

Вид заняття	Загальна кількість годин
лекції	**24**
лабораторні заняття	**24**
самостійна робота	**87**
Всього за дисципліну	**135**

7. Ознаки дисципліни:

Рік викладання	Семестр	Курс	Спеціальність	Нормативна/ вибіркова
2023	3	2	122 «Комп'ютерні науки»	Вибіркова

8. Пререквізити

Студенти повинні володіти знаннями з дискретної математики, теорія ймовірностей та математичної статистики, теорії інформації та кодування, основ програмування.

9. Технічне й програмне забезпечення /обладнання:

Обладнання: персональні комп'ютери з доступом до інтернет,

Програмне забезпечення: операційна система Microsoft Windows,.Linux, Microsoft Office, FoxitReader, WinZip, Total Commander, Dev C++, Python 3.5.8

10. Політика дисципліни

Усі процедури навчального процесу під час викладання дисципліни відповідають положенню про академічну доброчесність учасників освітнього процесу та недопущення академічного плагіату в Тернопільському національному технічному університеті імені Івана Пулюя.

11. Схема дисципліни

Теми лабораторних занять:

1. Побудова моделі загроз та порушника.
2. Управління ризиками.
3. Симетричні криптосистеми.
4. Асиметричні криптосистеми.
5. Дослідження хеш-функцій.
6. Дослідження електронного цифрового підпису.
7. Стеганографічні методи захисту інформації.

Види самостійної роботи

1. Опрацювання матеріалу лекцій.
2. Опрацювання теоретичного матеріалу, що не виноситься на лекції.
3. Підготовка до захисту лабораторних робіт.
4. Підготовка до тесту.
7. Підготовка до іспиту.

12. Система оцінювання та вимоги

Форма підсумкового семестрового контролю – **екзамен.**

Підсумкова семестрова оцінка заліку складається з суми балів, отриманих студентом при проведенні проміжних (модульних) контролів рівня засвоєння теоретичних знань (за перший та другий модулі) та отриманих балів за практичні роботи.

МОДУЛЬ 1			МОДУЛЬ 2			ПІДСУМКОВА СЕМЕСТРОВА ОЦІНКА ЗА ЗАЛІК	РАЗОМ З ДИСЦИПЛІНИ
АУДИТОРНА ТА САМОСТІЙНА РОБОТА			АУДИТОРНА ТА САМОСТІЙНА РОБОТА				
ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)	ЛАБОРАТОРНА РОБОТА		ТЕОРЕТИЧНИЙ КУРС (ТЕСТУВАННЯ)	ЛАБОРАТОРНА РОБОТА			
СЕМЕСТРОВА ОЦІНКА						25	100
25	15		20	15			
№ ЛЕКЦІЙ	ВИД РОБІТ	БАЛ	№ ЛЕКЦІЙ	ВИД РОБІТ	БАЛ		
Лекція 1			Лекція 5			Залік*	
Лекція 2	Лаб. роб. №1	5	Лекція 6	Лаб. роб. №4	5		
Лекція 3	Лаб. роб. №2	5	Лекція 7	Лаб. роб. №5	5		
Лекція 4	Лаб. роб. №3	5	Лекція 8	Лаб. роб. №6	5		

*за кожних три бали семестрової оцінки студент отримує один бал підсумкової семестрової оцінки автоматично

Підсумкова оцінка записується за 100-бальною шкалою із подальшим переведенням її у шкалу Європейської кредитно-трансферної системи (ECTS) відповідно A, B, C, D, E, F, FX при цьому чотирибальна шкала оцінок (з записом семестрової оцінки «відмінно» - A, «добре» - B,C, «задовільно» - D, E відповідають підсумковому результату «зараховано», «незадовільно» - F, FX відповідає підсумковому результату «незараховано»).

13. Навчально-методичне забезпечення

1. Електронний навчальний курс «Технології захисту інформації» на платформі dl.tntu.edu.ua для студентів спеціальності 122 «Комп'ютерні науки».
2. Актуальний календарний план проходження дисципліни.
3. Систему оцінювання.
4. Конспекти і презентації до лекцій.
5. Методичні вказівки до виконання лабораторних робіт.
6. Усі актуальні оголошення, опитування, рекомендації, тощо.

.

14. Рекомендована література

Базова

1. Shuangbao Paul Wang, Robert S. Ledley. Computer Architecture and Security: Fundamentals of Designing Secure Computer Systems, 2013.
2. Баранов О. А. Інформаційне право України: стан, проблеми, перспективи / О. А. Баранов. – К. : Видавничий дім "СофтПрес", 2005. – 316 с.
3. Антоненко О. Криптографічні методи перетворення інформації: навч. посіб. – Бердянськ: БДПУ, 2015. – 180 с
4. Гаврилова Л.В. Практична методологія IT-аудиту. – К.: Наукова думка, 2015. – 304 с.
5. Горбенко Ю.І., Горбенко І.Д. Інфраструктури відкритих ключів . Системи ЕЦП. Теорія та практика. Харків. Форт. 2010 , 593с.
6. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія. Практика. Застосування. Монографія Харків, Видавництво Форт, 2012 р.
7. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації - Харків: ХНУРЕ, 2004 - 368 с.
8. Аудит та управління інцидентами інформаційної безпеки: навч.посіб. / Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін. – К.: Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.
9. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2010. – 316 с.
10. Кузнецов О. О. Захист інформації в інформаційних системах / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 510 с

Допоміжна

1. . Neil Rerup, Milad Aslaner. Hands-On Cybersecurity for Architects: Plan and design robust security architectures, 2018.
2. Eduardo Fernandez-Buglioni. Security Patterns in Practice: Designing Secure Architectures Using Software Patterns, 2013.
3. Ризик-орієнтоване планування діяльності з внутрішнього аудиту. Методичний посібник. Київ, 2020. – 104 с.

4. Karapetrovic, S. and Willborn, W. (2000), "Quality assurance and effectiveness of audit systems", International Journal of Quality & Reliability Management, Vol. 17 No. 6, pp. 679-703. https://doi.org/10.1108/02656710010315256
5. Лагун А.Е. Криптографічні системи та протоколи, Львівська політехніка, 2013, 96с.
6. Bruce Schneier. Applied Cryptography Protocols, Algorithms, and Source Code in C, New York :Wiley, 658 p.

15. Інформаційні ресурси

1. http://dl.tntu.edu.ua Електронні навчальні курси ТНТУ імені І. Пулюя.
2. Конспект лекцій http://kist.ntu.edu.ua/textPhD/tzi.pdf
3. www.nist.gov
4. www.cryptography.org
5. www.iso.org
6. https://cip.gov.ua/ua
7. Історія розвитку інформаційних технологій в Україні [Електронний ресурс]. – Режим доступу : http://www.icfcst.kiev.ua/MUSEUM/IT_u.html
8. Information Technology Security Evaluation Criteria, v. 1.2. – Office for Official publications of the European Communities, 1991 [Electronic resource]. – Access mode : www.fbi.gov.
9. www.pgpi.org
10. www.securityfocus.com
11. www.sysinternals.com
12. Стандарти систем управління ІБ серії ISO/IEC 27000. [Електронний ресурс]. Режим доступу: https://www.iso27001security.com/
13. OWASP Top Ten: https://owasp.org/www-project-top-ten/