МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ ДЕРЖАВНИЙ АГРОТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ДМИТРА МОТОРНОГО

Кафедра «Комп'ютерні науки»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри КН

доцент_____Юлія ХОЛОДНЯК
"_02_"_вересня_____2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Технології захисту інформації»

для здобувачів ступеня вищої освіти «Бакалавр»
зі спеціальності 122 «Комп'ютерні науки»
за ОПП «Комп'ютерні науки»
(на освітнього ступеня «Молодший спеціаліст»)

факультет енергетики і комп'ютерних технологій

2022–2023 н.р.

Робоча програма навчальної дисципліни «Технології захисту інформації» для здобувачів ступеня вищої освіти «Бакалавр» зі спеціальності 122 «Комп'ютерні науки» за ОПП «Комп'ютерні науки» (на основі освітнього ступеня «Молодший спеціаліст»). – Запоріжжя, ТДАТУ, 2022. – 10 с

Розробник: к.т.н., ст. викл. Мірошниченко М.Ю.

Робочу програму затверджено на засіданні кафедри «Комп'ютерні науки»
Протокол від № 1 від 31 серпня 2022 року
В.о. завідувача кафедри КН
доцент _____ Юлія ХОЛОДНЯК

Схвалено методичною комісією факультету енергетики і комп'ютерних технологій зі спеціальності 122 «Комп'ютерні науки» за ОПП «Комп'ютерні науки» (на основі освітнього ступеня «Молодший спеціаліст»)

Протокол № 1 від 02 вересня 2022 року

Голова, доц. _____ Олександр ВОВК

1 ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, ступінь вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td colspan="2"><u>денна форма навчання</u>
(денна або заочна)</td></tr>
<tr><td>Кількість кредитів 4</td><td>Галузь знань
12 <u>«Інформаційні технології»</u>
(шифр і назва)</td><td colspan="2"><u>обов’язкова</u>
(обов’язкова або за вибором студента)</td></tr>
<tr><td>Загальна кількість годин – 120 годин</td><td rowspan="2">Спеціальність
<u>122 «Компютерні науки»</u>
(шифр та назва)</td><td>Курс</td><td>Семестр</td></tr>
<tr><td>Змістових модулів – 2</td><td>1С-й</td><td>1-й</td></tr>
<tr><td rowspan="7">Тижневе навантаження:
- аудиторних занять 3 год.
- самостійна робота студента 6,4 год.</td><td rowspan="7">Ступінь вищої освіти:
<u>«Бакалавр»</u></td><td>Вид занять</td><td>Кількість годин</td></tr>
<tr><td>Лекції</td><td>10 год.</td></tr>
<tr><td>Лабораторні заняття</td><td>-</td></tr>
<tr><td>Практичні заняття</td><td>20 год.</td></tr>
<tr><td>Семінарські заняття</td><td>-</td></tr>
<tr><td>Самостійна робота</td><td>90 год.</td></tr>
<tr><td colspan="2">Форма контролю:
<u>диференційований залік</u>
(екзамен або диференційований залік)</td></tr>
</table>

2 МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою навчальної дисципліни „Технології захисту інформації” є ознайомлення майбутніх фахівців з комп’ютерних наук з основними принципами побудови комплексної системи захисту інформації з використанням сучасних технологій захисту.

Завданнями дисципліни „Технології захисту інформації” є формування в студентів вміння розробляти інформаційні системи з застосовуючи технології захисту інформації.

Результати навчання (з урахуванням soft skills)

Інтегральна компетентність

Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі комп’ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

Загальні компетентності:

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК5. Здатність спілкуватися іноземною мовою.

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК8. Здатність генерувати нові ідеї (креативність).

ЗК11.Здатність приймати обґрунтовані рішення.

ЗК12.Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК13. Здатність діяти на основі етичних міркувань.

ЗК14.Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Фахові компетентності

ФК3. Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв’язності та нерозв’язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем.

ФК8. Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об’єктно-

орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління.

ФК13. Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп'ютерні системи і мережі передачі даних та аналізує якість роботи комп'ютерних мереж.

ФК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

ФК11. Здатність до інтелектуального аналізу даних на основі методів обчислювального інтелекту включно з великими та погано структурованими даними, їхньої оперативної обробки та візуалізації результатів аналізу в процесі розв'язування прикладних задач.

Soft skills:

- **комунікативні навички:** письмове, вербальне й невербальне спілкування; уміння грамотно спілкуватися по e-mail; вести суперечки і відстоювати свою позицію, спілкування в конфліктній ситуації; навички створення, керування й побудови відносин у команді;
- **уміння виступати привселюдно:** навички, необхідні для виступів на публіці; проводити презентації;
- **керування часом:** уміння справлятися із завданнями вчасно;
- **гнучкість і адаптивність:** гнучкість, адаптивність і здатність мінятися; уміння аналізувати ситуацію, орієнтування на вирішення проблем;
- **лідерські якості:** уміння спокійне працювати в напруженому середовищі; уміння ухвалювати рішення; уміння встановлювати мету, планувати;
- **особисті якості:** креативне й критичне мислення; етичність, чесність, терпіння, повага до колег.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1 Основи захисту інформації

Тема 1. Оцінка ефективності систем захисту інформації[1, с 1-39; 2, с. 18-45; 6, с. 25-44]

Системний підхід. Вимоги до моделі. Опис підходу до формування моделі інформаційної безпеки. Подання елементів матриці. Властивості матриці.

Тема 2. Ідентифікація і аутентифікація[2, с. 49-54; 3, с.85-104; 5, с. 310-346]

Основні поняття і концепції. Ідентифікація і механізми підтвердження достовірності користувача. Взаємна автентифікація користувачів. Протоколи ідентифікації з нульовою передачею знань. Спрощена схема ідентифікації з нульовою передачею знань. Паралельна схема ідентифікації з нульовою передачею знань. Схема ідентифікації Гиллоу-Куискуотера.

Змістовий модуль 2 Технології захисту інформації

Тема 3. Загрози інформації. Основні вірусології[3, с 156-189; 5, с. 178-216; 6, с. 268-302]

Види атак на криптосистеми. Поширення ключів. Алгоритми шифрування. Хеш-функція. Механізми аутентифікації. Введення в вірусологію. Шифри підстановки. Шифри перестановки.

Тема 4. Технологія адаптивного управління інформаційною безпекою. Мережна система виявлення вторгнень – SNORT. [4, с. 139-172; 6, с. 315-348]

Математична криптографія. Теорія чисел в криптографії. Алгоритмічна криптографія. Блокові криптографічні алгоритми. Криптографічні алгоритми гамування. Структура і функціонування системи виявлення вторгнень Snort. Загальний принцип функціонування систем виявлення вторгнень. Архітектура системи виявлення вторгнень Snort. Практичне застосування системи виявлення вторгнень Snort.

Тема 5. Технології захисту приватних мереж. Основи захисту периметру корпоративних мереж. [1, с. 349-416; 4, с. 189-252]

Призначення. Різновиди. Схеми підключення. Адміністрування. Міжмережеві екрани. Віртуальні приватні мережі. Тунелювання. Технічні й економічні переваги впровадження технологій VPN у корпоративні мережі.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Номер тижня	Вид занять	Тема заняття або завдання на самостійну роботу	Кількість				
			годин				балів
			лк	лаб	сем. (пр.)	СРС	
Змістовий модуль 1. Основи захисту інформації							
1	Лекція 1	Оцінка ефективності систем захисту інформації	2	-	-	-	-
	Практичне заняття 1	Математична основа методів криптографії	-	-	2	-	7
	Самостійна робота	Підготовка до практичного заняття 1	-	-	-	7	2
2	Практичне заняття 2	Шифри перестановки	-	-	2	-	7
	Самостійна робота	Підготовка до практичного заняття 2	-	-	-	7	3
3	Лекція 2	Ідентифікація і аутентифікація	2	-	-	-	-
	Практичне заняття 3	Шифри простої заміни	-	-	2	-	8
	Самостійна робота	Підготовка до практичного заняття 3	-	-	-	7	2
4	Практичне заняття 4	Аналіз стійкості криптосистем	-	-	2	-	8
	Самостійна робота	Підготовка до практичного заняття 4	-	-	-	7	3
5	Самостійна робота	Підготовка до ПМК-1	-	-	-	9	-
	ПМК 1	Підсумковий контроль за змістовий модуль 1	-	-	-	-	10
Всього за змістовий модуль 1 - 49 год.			***4***	***-***	***8***	***37***	***50***
Змістовий модуль 2. Технології захисту інформації							
6	Лекція 3	Загрози інформації. Основні вірусології	2	-	-	-	-
	Практичне заняття 5	Аналіз стійкості криптосистем	-	-	2	-	5
	Самостійна робота	Підготовка до практичного заняття 5	-	-	-	7	1
7	Практичне заняття 6	Комбінованні криптографічні алгоритми	-	-	2	-	5

	Самостійна робота	Підготовка до практичного заняття 6	-	-	-	7	1
8	Лекція 4	Технологія адаптивного управління інформаційною безпекою. Мережна система виявлення вторгнень – SNORT	2	-	-	-	-
	Практичне заняття 7	Цифровий підпис RSA	-	-	2	-	5
	Самостійна робота	Підготовка до практичного заняття 7	-	-	-	7	2
9	Практичне заняття 8	Спрошений стандарт шифрування S-DES	-	-	2	-	5
	Самостійна робота	Підготовка до практичного заняття 8	-	-	-	7	2
10	Лекція 5	Технології захисту приватних мереж. Основи захисту периметру корпоративних мереж	2	-	-	-	-
	Практичне заняття 9	Алгоритм шифруваня S-AES	-	-	2	-	5
	Самостійна робота	Підготовка до практичного заняття 9	-	-	-	7	2
11	Практичне заняття 10	Алгоритм шифруваня S-AES	-	-	2	-	5
	Самостійна робота	Підготовка до практичного заняття 10	-	-	-	7	2
12	Самостійна робота	Підготовка до ПМК-2	-	-	-	11	-
	ПМК 2	Підсумковий контроль за змістовий модуль 2	-	-	-	-	10
Всього за змістовий модуль 2 – 71 год.			***6***	***-***	***12***	***53***	***50***
Диференційований залік							***-***
Всього з навчальної дисципліни – 49+71=120 год.							***100***

5. ПЕРЕЛІК ПИТАНЬ, ЩО ВИНОСЯТЬСЯ НА ПІДСУМКОВІ МОДУЛЬНІ КОНТРОЛІ

Підсумковий модульний контроль 1

1. Системний підхід оцінки ефективності систем захисту інформації.
2. Опис підходу до формування моделі інформаційної безпеки.
3. Особливості подання елементів матриці в системах захисту інформації.
4. Охарактеризуйте базову схему ідентифікації та аутентифікації.
5. Наведіть та охарактеризуйте методи аутентифікації.
6. Протоколи ідентифікації з нульовою передачею знань.
7. Особливості парольних систем, їх переваги та недоліки.
8. Спрощена схема ідентифікації з нульовою передачею знань.
9. Паралельна схема ідентифікації з нульовою передачею знань.
10. Схема ідентифікації Гиллоу-Куискуотера.
11. Основні рекомендації при практичній реалізації парольних систем.
12. Оцінкастійкості парольних систем.
13. Методи зберігання паролів. Передача паролів по мережі.

Підсумковий модульний контроль 2

1. Охарактеризуйте види атак на криптосистеми.
2. Наведіть основні алгоритми шифрування.
3. Особливості застосування хеш-функцій в системах захисту інформації.
4. Введення в вірусологію. Шифри підстановки.
5. Введення в вірусологію. Шифри перестановки.
6. Поясніть сутність теорії чисел в криптографії.
7. Характеристика алгоритмічної криптографії. Переваги та недоліки.
8. Блокові криптографічні алгоритми.
9. Криптографічні алгоритми гамування.
10. Опишіть структуру й механізм функціонування системи виявлення вторгнень Snort.
11. Загальний принцип функціонування систем виявлення вторгнень.
12. Архітектура системи виявлення вторгнень Snort.
13. Практичне застосування системи виявлення вторгнень Snort.
14. Призначення приватних і корпоративних мереж.
15. Опишіть схему підключення приватної мережі.
16. Опишіть схему підключення корпоративної мережі.
17. Наведіть класифікацію корпоративних мереж.
18. Технології захисту мереж. Адміністрування.
19. Технології захисту мереж. Міжмережеві екрани.
20. Віртуальні приватні мережі.
21. Технології захисту мереж. Тунелювання.
22. Переваги впровадження технологій VPN у корпоративні мережі.

6. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

БАЗОВА

1. Грайворонський М.В. Безпека інформаційно-комунікаційних систем. Навч. посібник. – К.: Видавнича група BHV, 2009. 608 с.
2. Остапов С.Е., Євсеєв С.П., Король О.Г. Технології захисту інформації: навчальний посібник. Х. : Вид. ХНЕУ, 2013. 476 с.
3. Антонюк А.О. Основи захисту інформації в автоматизованих системах. Навч. посібник. - К: Видавничий дім «КМ Академія», 2003. 244 с.
4. Ємець В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. Львів: Бак, 2003. 144 с.
5. Кузнецов О.О., Євсеєв С.П., Кузнецов О.О., Король О.Г. Захист інформації в інформаційних системах. Методи традиційної криптографії: навч. посібн. Х.: Вид. ХНЕУ, 2010. 316 с.
6. Смірнов О.А., Віхрова Л.Г., Осадчий С.І. Основи захисту інформації: навч. посібн. Кіровоград, 2010. 322 с.
7. Кавун С.В., Смірнов О.А., Столбов В.Ф. Основи інформаційної безпеки. Кіровоград: Вид. КНТУ, 2012. 414 с.

ДОПОМІЖНА

8. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. К.: Держстандарт України, 2002. 40 с.
9. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Введ. 01.01.98. К.: Держстандарт України, 1997. 11 с.
10. Галузевий стандарт Вищої освіти України з напряму спеціальності 122 "Комп'ютерні науки" - К.: Видавнича група BHV, 2019. 86 с.

7. ІНФОРМАЦІЙНІ РЕСУРСИ

1. Освітній портал ТДАТУ http://op.tsatu.edu.ua/course/view.php?id=778
2. Наукова бібліотека ТДАТУ http://www.tsatu.edu.ua/biblioteka/
3. Сайт кафедри комп’ютерних наук http://www.tsatu.edu.ua/kn/course/tehnolohiji-zahystu-informaciji/