МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

СИЛАБУС ОБОВ'ЯЗКОВОГО ОСВІТНЬОГО КОМПОНЕНТУ

«ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

Мова навчання – ***українська***

Шифр та найменування галузі знань ***12 «Інформаційні технології»***

Код та найменування спеціальності ***122 «Комп'ютерні науки»***

Освітньо-професійна програма ***Інформаційні управляючі системи та технології***

Ступінь вищої освіти ***бакалавр***

Затверджено на засіданні

Методичної Ради зі спеціальностей ***122 «Комп'ютерні науки», 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології»***
« 23 » листопада 2023 р. протокол № 3

Реєстраційний номер в навчальному відділі НЦООП

_____

1. Загальна інформація

Кафедра: Інформаційних технологій та кібезпеки

Викладач: Владімірова Валентина Борисівна, старший викладач кафедри інформаційних технологій та кібербезпеки

Профайл

Контакти:
vladimirova.v.b@gmail.com
048-720-91-18

Викладач: **Бодюл Олена Станіславівна**, доцент кафедри інформаційних технологій та кібербезпеки

Профайл

Контакти:
bodyulolena@ukr.net,
048-720-91-44

Освітній компонент викладається на 3 курсі у 6 семестрі для денної та заочної форми навчання
Кількість: кредитів – 4, годин – 120

Аудиторні заняття, годин:	всього	лекції	лабораторні
денна	42	20	22
заочна	12	6	6
Самостійна робота, годин	Денна –78		Заочна – 108

Розклад занять

2. Анотація освітнього компоненту

Освітній компонент (ОК) «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ» висвітлює основні методи, які використовуються у сучасних автоматизованих системах з метою захисту інформації, питання політики безпеки інформації та комплексу засобів захисту, принципи криптографічного захисту, питання симетричних та асиметричних систем, ідентифікації та перевірки дійсності, електронного цифрового підпису, управління криптографічними ключами та інше.

Освітній компонент «Технології захисту інформації» базується на знаннях, отриманих здобувачем вищої освіти в результаті вивчення освітніх компонент «Алгоритмізація та програмування», «Вища математика», «Дискретна математика», «Об'єктно-орієнтоване програмування», «Теорія алгоритмів», «Чисельні методи», «Процедурне програмування», «Теорія інформації та кодування». Освітній компонент «Технології захисту інформації» забезпечує дисципліни: «Веб-технології та веб-дизайн», «Технології розподілених систем та паралельних обчислень», «Сучасні системи управління базами даних» та дипломне проектування.

3. Мета освітнього компоненту

Мета освітнього компоненту – формування теоретичних знань і практичних навичок у сфері захисту інформації та оволодіння студентами основними методами, які використовуються у сучасних комп’ютерних системах з метою захисту інформації та постановки задачі захисту інформації від несанкціонованого доступу.

Завдання освітнього компоненту «Технології захисту інформації»: ознайомлення студентів з основними принципами політики безпеки та принципами криптографічного

захисту, апаратними, технологіями ідентифікації та автентифікації.

У результаті вивчення навчальної дисципліни «Технології захисту інформації» студент повинен знати:

– основні положення законодавства в галузі захисту інформації;
– основні терміни та визначення політики безпеки;
– предмет та об’єкт захисту;
– принципи криптографічного захисту;
– класичні та сучасні криптографічні методи захисту;
– основні види атак, принципи криптоаналізу;
– основні поняття та аспекти ідентифікації та автентифікації об’єкта;
– алгоритми електронного цифрового підпису;
– механізми та протоколи керування ключами в ІВК інформаційної системи.

У результаті вивчення навчальної дисципліни студент повинен вміти:

– вірно визначити та використати криптографічні та програмні методи захисту інформації для самостійного розв’язання поставленої задачі;
– забезпечити захист інформації, яка оброблюється в персональній ЕОМ і що зберігається в різного роду запам’ятовуючих пристроях;
– забезпечити достовірність та цілісність інформації (зокрема з використанням алгоритмів електронного цифрового підпису) під час обробки інформації, її зберігання і передачі.

4. Компетентності та програмні результати навчання

У результаті вивчення освітнього компоненту «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ» здобувач вищої освіти отримує наступні програмні компетентності та програмні результати навчання, які визначені в Стандарті вищої освіти зі спеціальності № 122 КОМП'ЮТЕРНІ НАУКИ та освітньо-професійній програмі «Інформаційні управляючі системи та технології» підготовки бакалаврів.

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.
ЗК6 Здатність вчитися й оволодівати сучасними знаннями.
ЗК7 Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК10 Здатність бути критичним і самокритичним.
ЗК11 Здатність приймати обґрунтовані рішення.
ЗК12 Здатність оцінювати та забезпечувати якість виконуваних робіт.
ЗК13 Здатність діяти на основі етичних міркувань.
ЗК15 Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя

Спеціальні (фахові, предметні) компетентності:

СК1 Здатність до математичного формулювання та досліджування неперервних та дискретних математичних моделей, обґрунтовування вибору методів і підходів для розв’язування теоретичних і прикладних задач у галузі комп’ютерних наук, аналізу та інтерпретування.

СК2 Здатність до виявлення статистичних закономірностей недетермінованих явищ, застосування методів обчислювального інтелекту, зокрема статистичної, нейромережевої та нечіткої обробки даних, методів машинного навчання та генетичного програмування тощо.

СК3 Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проєктування, 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.

СК8 Здатність проєктувати 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.

СК9 Здатність реалізувати багаторівневу обчислювальну модель на основі архітектури клієнт-сервер, включаючи бази даних, знань і сховища даних, виконувати розподілену обробку великих наборів даних на кластерах стандартних серверів для забезпечення обчислювальних потреб користувачів, у тому числі на хмарних сервісах.

СК11 Здатність до інтелектуального аналізу даних на основі методів обчислювального інтелекту включно з великими та погано структурованими даними, їхньої оперативної обробки та візуалізації результатів аналізу впроцесі розв'язування прикладних задач.

СК12 Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення.

СК13 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.

СК14 Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

СК16 Здатність реалізовувати високопродуктивні обчислення на основі хмарних сервісів і технологій, паралельних і розподілених обчислень при розробці й експлуатації розподілених систем паралельної обробки інформації.

Програмні результати навчання:

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.

ПРН2 Використовувати сучасний математичний апарат неперервного та дискретного аналізу, лінійної алгебри, аналітичної геометрії, в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі проєктування та реалізації об'єктів інформатизації.

ПРН3 Використовувати знання закономірностей випадкових явищ, їх властивостей та операцій над ними, моделей випадкових процесів та сучасних програмних середовищ для розв'язування задач статистичної обробки даних і побудови прогнозних моделей.

ПРН4 Використовувати методи обчислювального інтелекту, машинного навчання, нейромережевої та нечіткої обробки даних, генетичного та еволюційного програмування для розв'язання задач розпізнавання, прогнозування, класифікації, ідентифікації об'єктів керування тощо.

ПРН5 Проєктувати, розробляти та аналізувати алгоритми розв'язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислюваних функцій.

ПРН6 Використовувати методи чисельного диференціювання та інтегрування функцій, розв'язання звичайних диференціальних та інтегральних рівнянь, особливостей чисельних

методів та можливостей їх адаптації до інженерних задач, мати навички програмної реалізації чисельних методів.

ПРН7 Розуміти принципи моделювання організаційно□технічних систем і операцій; використовувати методи дослідження операцій, розв'язання одно- та багатокритеріальних оптимізаційних задач лінійного, цілочисельного, нелінійного, стохастичного програмування.

ПРН12 Застосовувати методи та алгоритми обчислювального інтелекту та інтелектуального аналізу даних в задачах класифікації, прогнозування, кластерного аналізу, пошуку асоціативних правил з використанням програмних інструментів підтримки багатовимірного аналізу даних на основі технологій DataMining, TextMining, WebMining.

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.

ПРН15 Розуміти концепцію інформаційної безпеки, принципи безпечного проєктування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

5. Інформаційний обсяг освітнього компоненту

5.1 Перелік лекційних завдань

Тема	Зміст теми	Кількість годин	
		денна	заочна
Змістовний модуль 1. ОГЛЯД БЕЗПЕКИ СИСТЕМИ. ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ (КЛАСИЧНІ СИМЕТРИЧНІ КРИПТОСИСТЕМИ)			
1	Актуальність проблеми забезпечення безпеки інформаційних технологій. Термінологія, основні положення та законодавча база в галузі захисту інформації. Загрози безпеки інформації	2	1
2	Політика безпеки та моделі безпеки	2	
3	Основні поняття криптографічних методів захисту інформації та математичні основи криптографії.	2	1
4	Шифрування. Класичні симетричні криптосистеми.	3	2
Змістовний модуль 2. ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ. ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ			
5	Шифрування. Складна заміна.	2	
6	Сучасні симетричні криптосистеми.	1	
7	Асиметричні криптосистеми	2	1
8	Ідентифікація та перевірка дійсності.	1	
9	Електронний цифровий підпис.	3	1
10	Управління криптографічними ключами.	1	
11	Основні види атак, принципи криптоаналізу.	1	
Разом за ОК:		20	6

5.2 Перелік лабораторних робіт

№ з/п	Назва практичної/лабораторної роботи	Кількість годин	
		денна	заочна
1	Модулярна арифметика. Основні властивості	4	1
2	Модулярна арифметика. Розв'язок порівнянь першого ступеня	2	1
3	Шифри перестановки	2	
4	Шифри простої заміни	4	2
5	Шифрі складної заміни. Біграмні шифри	2	
6	Асиметричні криптосистеми (RSA)	4	1
7	Електронний цифровий підпис (RSA)	2	1
8	Метод Диффи-Хелмана	2	
Всього за ОК:		**22**	**6**

5.3 Перелік завдань до самостійної роботи

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1	Опрацювання лекційного матеріалу з відповідями на тестові питання за темами лекцій	20	6
2	Підготовка до лабораторних занять	16	10
3	Опрацювання теоретичних відомостей, які не виносяться на лекції, а саме: 1. Актуальність проблеми забезпечення безпеки інформаційних технологій. 2. Термінологія, основні положення в галузі захисту інформації. 3. Законодавча база в галузі захисту інформації. 4. Загрози безпеки інформації 5. Політика безпеки та моделі безпеки 6. Основні поняття криптографічних методів захисту інформації та математичні основи криптографії. 7. Шифрування. Класичні симетричні криптосистеми. 8. Шифрування. Складна заміна. 9. Сучасні симетричні криптосистеми. 10. Асиметричні криптосистеми 11. Ідентифікація та перевірка дійсності. 12. Електронний цифровий підпис. 13. Управління криптографічними ключами. 14. Основні види атак, принципи криптоаналізу.	 1 1 2 2 2 4 3 3 2 1 3 3 1 2	 5 5 6 4 6 6 6 6 6 6 6 6 6 6
4	Виконання індивідуальних навчально-дослідних завдань: 1. Комплекс засобів захисту, який реалізує політику безпеки інформації. Підсистема керування доступом 2. Комплекс засобів захисту, який реалізує політику безпеки інформації. Підсистема автентифікації та ідентифікації	 6 6	 6 6
Всього за ОК:		**78**	**108**

6. Система оцінювання та вимоги

Контроль успішності навчання здобувача проводиться у формах вхідного, поточного і підсумкового контролів.

Вхідний контроль якості навчання здійснюється на початку курсу проведенням перевірки залишкових знань здобувачів за ОК, що забезпечують вивчення даного освітнього компоненту (діагностика первинних знань здобувачів).

Формами поточного контролю є:

– тестування знань здобувачів за певних тем або з певних окремих питань ОК;

– виконання і захист лабораторних робіт;

– виконання і захист індивідуальних завдань.

Підсумковий контроль – ***екзамен.***

Нарахування балів:

Вид роботи, що підлягає контролю	Максимальна кількість оціночних балів	
	Денна	Заочна
Змістовний модуль 1. ОГЛЯД БЕЗПЕКИ СИСТЕМИ. ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ (КЛАСИЧНІ СИМЕТРИЧНІ КРИПТОСИСТЕМИ)		
Лабораторні роботи*	24	32
Опрацювання лекційного матеріалу*	5	5
Виконання індивідуальних завдань*	6	6
Всього за змістовний модуль 1	**35**	**43**

Змістовний модуль 2. ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ. ТЕХНОЛОГІЙ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ		
Лабораторні роботи*	24	16
Опрацювання лекційного матеріалу*	5	5
Виконання індивідуальних завдань*	6	6
Всього за змістовний модуль 2	**35**	**27**
Екзамен	**30,0**	**30,0**
Всього за ОК	**100,0**	**100,0**

**Є можливість визнання результатів неформальної освіти відповідно до п.2*
Положення про порядок перезарахування результатів навчання (навчальних дисциплін) в Одеському національному технологічному університеті

Критерії оцінювання програмних результатів навчання здобувачів

Підсумковий контроль – екзамен

27-30 балів	якщо здобувач демонструє повні й глибокі знання навчального матеріалу, достовірний рівень розвитку умінь і навичок, правильне й обґрунтоване формулювання практичних висновків, уміння приймати необхідні рішення в різних нестандартних ситуаціях, вільне володіння науковими термінами, високу комунікативну культуру	відмінно
23-26 балів	якщо здобувач виявляє дещо обмежені знання навчального матеріалу, допускає окремі несуттєві помилки й неточності	дуже добре
18-22 бали	якщо здобувач засвоїв основний навчальний матеріал, володіє необхідними уміннями та навичками для вирішення стандартних завдань, проте при цьому допускає неточності, не виявляє самостійності суджень, демонструє недоліки комунікативної культури	задовільно
0-17 балів	якщо здобувач не володіє необхідними знаннями, уміннями й навичками, науковими термінами, демонструє низький рівень комунікативної культури	незадовільно

Лабораторні роботи (денна форма навчання)

5,2 - 6 балів	Лабораторна відпрацьована та вчасно захищена, надані повні обґрунтовані відповіді	відмінно
4,6 - 5,1 балів	Лабораторна відпрацьована та вчасно захищена, при відповіді допущені неточності	дуже добре
3,9 – 4,5 балів	Лабораторна відпрацьована, відповіді неповні, допущені помилки	добре
2,1 – 3,8 балів	Лабораторна відпрацьована, відповіді незадовільні, допущені грубі помилки	достатньо
0-2 балів	Лабораторна не відпрацьована або дані незадовільні відповіді	незадовільно

Лабораторні роботи (заочна форма навчання)

13,6 – 16,0 балів	Лабораторна відпрацьована та вчасно захищена, надані повні обґрунтовані відповіді	відмінно
12,0 - 13,5 балів	Лабораторна відпрацьована та вчасно захищена, при відповіді допущені неточності	дуже добре
10,0 – 11,9 балів	Лабораторна відпрацьована, відповіді неповні, допущені помилки	добре
5,0 – 9,9 балів	Лабораторна відпрацьована, відповіді незадовільні, допущені грубі помилки	достатньо
0-4,9 балів	Лабораторна не відпрацьована або дані незадовільні відповіді	незадовільно

Самостійна робота (тестування: опрацювання лекційного матеріалу)

4,5 - 5 балів	90 - 100 % правильних відповідей	відмінно
4,0 - 4,4 балів	74 – 89% правильних відповідей	дуже добре
3,5 – 3,9 балів	60 – 73% правильних відповідей	добре
2,1 – 3,4 балів	35 – 59 % правильних відповідей	достатньо
0-2 балів	0-35 % правильних відповідей	незадовільно

Самостійна робота (індивідуальне завдання)

5,2 - 6 балів	Самостійна робота відпрацьована та вчасно захищена, надані повні обґрунтовані відповіді	відмінно
4,6 - 5,1 балів	Самостійна робота відпрацьована та вчасно захищена, при відповіді допущені неточності	дуже добре
3,9 – 4,5 балів	Самостійна робота відпрацьована, відповіді неповні, допущені помилки	добре
2,1 – 3,8 балів	Самостійна робота відпрацьована, відповіді незадовільні, допущені грубі помилки	достатньо
0-2 балів	Самостійна робота не відпрацьована або дані незадовільні відповіді	незадовільно

7. Засоби діагностики успішності навчання

Методи навчання, які використовуються у процесі проведення занять, а також самостійних робіт за ОК:

***Лекційні заняття**: Словесні методи: розповідь, пояснення, бесіда, дискусія; Наочні: ілюстрація (мультимедійна презентація), спостереження, демонстрація; пояснювально-демонстративний метод, проблемний виклад.*

***Лабораторні заняття:** виконання лабораторних дослідів з наступних захистом результатів досліджень.*

***Самостійна робота**: робота з навчально-методичними матеріалами, тестування за результати опрацювання теоретичного матеріалу, оцінка виконання індивідуальних завдань; складання планової та звітної документації, науково-дослідна робота студентів (методи пізнання, аналогій, оцінка, ілюстрація тощо*

8. Інформаційні ресурси

Базові (основні):

1. Владімірова, В. Б. Технології захисту інформації : метод. вказівки до самост. роботи [Електронний ресурс] : для здобувачів освіти галузі знань 12 "Інформаційні технології" спец. 122 "Комп’ютерні науки" освітньої програми "Інформаційні управляючі системи та

технології" / В. Б. Владімірова ; зав. каф. В. Плотніков ; Каф. інформаційних технологій та кібербезпеки. – Одеса : ОНАХТ, 2022. – 35 с. https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.1835285
2. Проєктування комплексних систем захисту інформації [Текст] : підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало та ін. ; Нац. ун-т "Львівська політехніка". — Львів : Вид-во Львів. політехніки, 2020. — 320 с : іл. — Бібліогр.: с. 683-694. https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.1620169
3. Захист інформації в комп'ютерних системах [Електронний ресурс] : підручник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест та ін. — Чернігів, 2020. — 236 с. https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.2269749
4. Вишняков, Володимир Михайлович. Захист інформації в комп'ютерних системах [Електронний ресурс] : навч. посіб. / В. М. Вишняков ; Київ. нац. ун-ет будівництва і архітектури. — Київ, 2022. — 120 с. https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.2204149
5. GDPR: Посібник з виживання [Електронний ресурс] / Артем Кобрін, Дмитро Корчинський, Владіслав Некрутенко ; під ред. Д. Іванова ; Privacy HUB. — Одеса : Гельветика, 2022. — 228 с. https://elc.library.ontu.edu.ua/library-w/DocumentDescription?docid=OdONAHT.2049828

Додаткові:

1. Закон України "Про інформацію". [Онлайн]. Доступно: https://zakon.rada.gov.ua/laws/show/2657-12#Text
2. НД ТЗІ 1.1-003-99 № 22, Термінологія в області захисту інформації в комп’ютерних системах від несанкціонованого доступу. [Онлайн]. Доступно: https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
3. Офіційний веб-портал «Законодавство України» https://zakon.rada.gov.ua/laws
4. Урядовий портал https://www.kmu.gov.ua/

9. Політика освітнього компоненту

Політика всіх освітніх компонент в ОНТУ є уніфікованою та визначена з урахуванням законодавства України, Корпоративному кодексу ОНТУ, Кодексу академічної доброчесності ОНТУ, Положення про організацію освітнього процесу ОНТУ, Положення про порядок перезарахування результатів навчання (навчальних дисциплін) в ОНТУ, вимог ISO 9001:2015 та роботодавців.

Викладач /ПІДПИСАНО/ Валентина ВЛАДІМІРОВА

Викладач /ПІДПИСАНО/ Олена БОДЮЛ

Розглянуто та затверджено на засіданні кафедри Інформаційних технологій та кібербезпеки

Протокол від «17» листопада 2023 р. № 3

Завідувач кафедри /ПІДПИСАНО/ Павло ЛОМОВЦЕВ

ПОГОДЖЕНО:

Гарант ОП ІУСТ
доцент, ІТтаКБ /ПІДПИСАНО/ Алла СЕЛІВАНОВА