

**ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД УКООПСПІАКИ  
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»**

Навчально-науковий інститут бізнесу та сучасних технологій  
Кафедра математичного моделювання та соціальної інформатики

**СИЛАБУС**

навчальної дисципліни  
**«Захист інформації»**  
на 2021-2022 навчальний рік

Курс та семестр вивчення	4 курс, 7 семестр
Освітня програма/спеціалізація	122 Комп'ютерні науки
Спеціальність	122 Комп'ютерні науки
Галузь знань	12 «Інформаційні технології»
Ступінь вищої освіти	бакалавр

ПІБ НПП, який веде дану дисципліну,  
науковий ступінь і вчене звання,  
посада

Парфьонова Т.О., к.ф.-м.н., доцент, доцент кафедри ММСІ

Контактний телефон	0532 509204
Електронна адреса	tpa.poltava@gmail.com
Розклад навчальних занять	<a href="http://schedule.puet.edu.ua/">http://schedule.puet.edu.ua/</a>
Консультації	он-лайн: електронною поштою
Сторінка дистанційного курсу	<a href="https://el.puet.edu.ua/">https://el.puet.edu.ua/</a>

**Опис навчальної дисципліни**

<b>Мета вивчення навчальної дисципліни</b>	Основною метою вивчення дисципліни «Захист інформації» є засвоєння основних понять та категорій комп'ютерної безпеки, вивчення принципів побудови комплексних систем захисту інформації, розробки, дослідження та застосування механізмів захисту інформації, що ґрунтуються на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій.
<b>Тривалість</b>	4 кредити ЄКТС/120 годин (лекції 24 год., практичні заняття 24 год., самостійна робота 72 год.)
<b>Форми та методи навчання</b>	Лекції та практичні заняття в аудиторії, самостійна робота поза розкладом
<b>Система поточного та підсумкового контролю</b>	Поточний контроль: відвідування занять; виконання РГР; поточна модульна робота Підсумковий контроль: ПМК (залік)
<b>Базові знання</b>	Вивчення дисципліни базується на знаннях, отриманих студентами при вивченні дисциплін "Дискретна математика", "Алгебра та геометрія", "Математичний аналіз", "Теорія ймовірностей та математична статистика", "Програмування", "Інформатика".
<b>Мова викладання</b>	Українська

**Перелік компетентностей, які забезпечує дана навчальна дисципліна, програмні результати навчання**

<b>Програмні результати навчання</b>		<b>Компетентності, якими повинен оволодіти здобувач</b>
Знання	Знання основних форм і законів абстрактно-логічного мислення, основ логіки, норм критичного підходу, основ методології наукового пізнання, форм і методів аналізу та синтезу.	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

Уміння	Здобувати систематичні знання в галузі комп'ютерних наук, аналізувати проблеми з точки зору сучасних наукових парадигм, осмислювати і робити обґрунтовані висновки з наукової і навчальної літератури та результатів експериментів	
Комунікація	Здійснення соціальних комунікацій в процесі спілкування з фахівцями та нефахівцями в галузі комп'ютерних наук, забезпечення обміну логічними аргументами з метою досягнення взаєморозуміння й згоди.	
Автономія та відповідальність	Відповідальність за доручену справу, самостійність в прийнятті рішень щодо розв'язання задач в галузі комп'ютерних наук	
Знання	Знання способів і методів навчання, методів самоосвіти, основ наукової та дослідницької діяльності, методів пошуку, збору, аналізу та обробки інформації.	ЗК 6. Здатність вчитися і оволодівати сучасними знаннями.
Уміння	Оцінювати предмет навчальної діяльності, визначати загальну мету і конкретні задачі, вибирати адекватні засоби їх розв'язання для досягнення результату, здійснювати необхідний самоконтроль, використовувати довідкову літературу і технічну документацію, розвивати та застосовувати у професійній діяльності свої творчі здібності, організовувати робоче місце, планувати робочий час.	
Комунікація	Використання комунікативної компетентності для ефективної взаємодії в різних сферах спілкування; відбір і систематизація інформаційних матеріалів з метою спілкування в професійній сфері, використання засобів масової комунікації для отримання, перероблення і створення актуальної інформації у вигляді документів, рефератів, доповідей, статей, інтерв'ю; вдосконалення особистісної комунікаційної компетентності на основі навичок і вмінь міжособистісної комунікації.	
Автономія та відповідальність	Відповідально ставитися до професійних обов'язків та виконуваної роботи, проявляти самостійність в здійсненні самостійних узагальнень, прийняття самостійних рішень і виконання самостійних дій у процесі подолання навчальних труднощів, спираючись на власний досвід творчого розв'язання поставлених проблем.	
Знання	Знання методів, способів та технологій збору інформації з різних джерел, контент-аналізу документів, аналізу та обробки даних.	
Уміння	Використовувати технології та інструментарії пошукових систем, методи інтелектуального аналізу даних і текстів, здійснювати опрацювання, інтерпретацію та узагальнення даних.	
Комунікація	Використання системи документно-інформаційних комунікацій для задоволення інформаційних потреб в галузі комп'ютерних наук та інформаційних технологій.	ЗК 7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
Автономія та відповідальність	Самостійність при опрацюванні, інтерпретації та узагальненні даних, відповідальність за оперативність, точність і достовірність подачі інформації.	
Знання	Знання принципів командної роботи, командних цінностей, основ конфліктології. Знання методології управління ІТ проектами, стандартів РМВОК, програмного інструментарію для управління ІТ проектами	
Уміння	Будувати зв'язки та відносини з людьми, враховувати точку зору колег, розуміти інших людей, виражати довіру команді, визнавати свої помилки, уникати та запобігати конфліктам, стримувати особисті амбіції. Здійснювати підбір і підготовку інформації та задач проектній команді, ставити цілі і формулювати завдання для реалізації проектів і програм	ЗК 10. Здатність бути критичним і самокритичним.

Комунікація	Планування комунікацій в команді та із замовниками, дотримання коректної поведінки, терпимості, порядку, визнання чужої думки і коректної дискусії, подоланню егоїстичних поглядів, принципів самокритичності, поширення інформації про хід виконання робіт	
Автономія та відповідальність	Вільне висловлювання своїх думок при роботі в команді, відповідальність за результати роботи команди, відповідальність лідера перед командою.	
Знання	Знання теоретичних і прикладних положень неперервного та дискретного аналізу, включаючи аналіз нескінчено малих, інтегральне числення, лінійну алгебру, аналітичну геометрію, диференціальні рівняння, функціональний аналіз, комбінаторику, теорію графів, бульову алгебру.	СК 1. Здатність до математичного та логічного мислення, формулювання та досліджування математичних моделей, зокрема дискретних математичних моделей, обґрунтування вибору методів і підходів для розв'язування теоретичних і прикладних задач в галузі комп'ютерних наук, інтерпретування отриманих результатів.
Уміння	Ефективно використовувати сучасний математичний апарат в професійній діяльності для розв'язання задач теоретичного та прикладного характеру в процесі аналізу, синтезу та проектування інформаційних систем за галузями	
Комунікація	Здатність ефективно формувати комунікаційну стратегію через точність аргументації в математичних викладеннях	
Автономія та відповідальність	Здатність самостійно розв'язувати професійні задачі, використовуючи сучасний математичний апарат і нести відповідальність за отримані розв'язки	
Знання	Знання концепції інформаційної безпеки, принципів безпечного проектування ІС а ІТ, методології безпечного програмування, погроз і атак, безпеки комп'ютерних мереж, методи криптографії.	СК 14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти та експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.
Уміння	Зберігати конфіденційність, цілісність та доступність інформації, забезпечувати автентичність, відстежуваність та надійність інформації в умовах неповноти та невизначеність вихідних даних, багатокритеріальності професійних задач.	
Комунікація	Здатність ефективно формувати комунікаційні стратегії у процесі формування концепції обміну інформацією, кодування та вибору каналу комунікації, передачі повідомлень і документів через канал, зберігання та добування документів, реалізації зворотного зв'язку.	
Автономія та відповідальність	Самостійно управляти повідомленнями та документами, нести відповідальність за зміст інформаційних ресурсів, що потребують забезпечення інформаційного захисту.	

### **Тематичний план навчальної дисципліни**

<b>Назва теми</b>	<b>Види робіт</b>	<b>Завдання самостійної роботи у розрізі тем</b>
<b>Модуль 1. Модульна арифметика. Сучасне шифрування</b>		
Тема 1. Модульна арифметика. Тема 2. Шифри із симетричним ключем. Тема 3. Сучасне шифрування Тема 4. Стандарти шифрування.	відвідування занять; опитування на заняттях; розв'язування практичних завдань біля дошки; перевірка виконання РГР; опитування в процесі індивідуально-консультативних занять для перевірки засвоєння матеріалу пропущених занять; перевірка виконання модульних контрольних робіт.	підготувати РГР, опрацювати лекційний матеріал, готуватись до практичних занять, виконувати домашні завдання, опрацювати дистанційний курс, готуватися до модульної контрольної роботи

### **Інформаційні джерела**

1. Алферов А.П. Основы криптографии. Уч. пос. / А.П. Алферов, А.Ю.Зубов, А.С.Кузьмин, А.В.Черемушкин – 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. – 480с.
2. Баричев С.Г. Основы современной криптографии. / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов – 2-е изд., испр. и доп. – М.: Горячая линия–Телеком, 2002. – 175с.
3. Безруков Н.Н. Компьютерная вирусология: Справ. руководство. / Н.Н. Безруков – К.: УРЕ, 1991. – 416с.
4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. / В.В. Домарев – К.: ТИД «ДС», 2001. – 688с.
5. Складар Д.В. Искусство защиты и взлома информации. / Д.В. Складар – СПб.: БХВ-Петербург, 2004. – 288с.
6. Галатенко В.А. Стандарты информационной безопасности / В.А. Галатенко. Под редакцией В.Б. Бетелина – М.: ИНТУИТ. РУ «Интернет-университет Информационных технологий», 2004. – 328с.
7. Кузьменко Б.В. Захист інформації. Навчальний посібник. Ч.1. (Організаційно-правові засоби забезпечення інформаційної безпеки) / Б.В. Кузьменко, О.А. Чайковська – К., 2009. – 83 с.
8. Кукина Е.Г. Сборник задач и упражнений к учебнику В.А.Романькова «Введение в криптографию». Курс лекций 2-е издание, испр. и доп.– Омск: Изд-во Омского государственного университета, 2009. / Е.Г. Кукина, В.А.Романьков. – Москва: Форум, 2012.
9. Харин Ю.С. Математические основы криптологии: Учеб.пособие / Ю.С. Харин, В.И. Берник, Г.В. Матвеев. – Мн.:БГУ, 1999. – 319 с.:ил.
10. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, В.А. Чекатков – К.: Юниор, 2003. – 504с.

### **Програмне забезпечення навчальної дисципліни**

- Пакет програмних продуктів Microsoft Office.

### **Політика вивчення навчальної дисципліни та оцінювання**

- Політика щодо термінів виконання та перескладання: завдання, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. Перескладання модулів відбувається із дозволу провідного викладача за наявності поважних причин (наприклад, лікарняний).
- Політика щодо академічної доброчесності: списування під час виконання поточних модульних робіт та тестування заборонено (в т. ч. із використанням мобільних девайсів). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття.
- Політика щодо відвідування: відвідування занять є обов'язковим компонентом. За об'єктивних причин (наприклад, хвороба, працевлаштування, стажування) навчання може відбуватись в он-лайн формі (Moodle) за погодженням із провідним викладачем.
- Політика зарахування результатів неформальної освіти: <http://puet.edu.ua/uk/publiczna-informaciya>

### **Оцінювання**

Підсумкова оцінка за вивчення навчальної дисципліни розраховується через поточне оцінювання

Форма навчальної роботи	Вид навчальної роботи	Бали
1. Аудиторна	1. Відвідування занять	20
	2. Правильна відповідь при опитуванні (2 бали за відповідь (5 відповідей в семестр)), $2*5 = 10$ б.	10
2. Самостійна та індивідуально-консультативна робота.	1. Виконання розрахунково-графічного завдання 1, 2 (кожне), - за виконання в термін	25
	- за виконання з порушенням в тиждень	23
	- за виконання з порушенням більше тижня	21
3. Підсумковий контроль.	Модульна контрольна робота	20
4. Підсумковий контроль.	1. ПМК	-

### **Шкала оцінювання здобувачів вищої освіти за результатами вивчення навчальної дисципліни**

<b>Сума балів за всі види навчальної діяльності</b>	<b>Оцінка за шкалою ЄКТС</b>	<b>Оцінка за національною шкалою</b>
90-100	A	Відмінно
82-89	B	Дуже добре
74-81	C	Добре
64-73	D	Задовільно
60-63	E	Задовільно достатньо
35-59	FX	Незадовільно з можливістю повторного складання
0-34	F	Незадовільно з обов'язковим повторним вивченням навчальної дисципліни