

УМАНСЬКИЙ ДЕРЖАВНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ  
ІМЕНІ ПАВЛА ТИЧІНИ

КАФЕДРА ІНФОРМАТИКИ І  
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»

завідувач кафедри

 М.О.Медведєва

“27” серпня 2019 р.

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**ВВС3.2.01 ІНФОРМАЦІЙНА БЕЗПЕКА**

галузь знань 01 Освіта

Спеціальність 014.06 Середня освіта (Хімія)

Освітня програма Середня освіта (Хімія)

Факультет/інститут Природничо-географічний

2019–2020 навчальний рік

Робоча програма дисципліни інформаційна безпека для студентів спеціальності 014.06 Середня освіта ( Хімія)

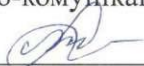
Розробники:

доцент кафедри інформатики і інформаційно-комунікаційних технологій, кандидат педагогічних наук Бондаренко Т.В.; викладач кафедри інформатики і інформаційно-комунікаційних технологій Троян С.О.

Робочу програму схвалено на засіданні кафедри інформатики і інформаційно-комунікаційних технологій

Протокол № 1 від «27» серпня 2019 року

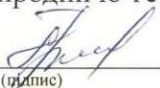
Завідувач кафедри інформатики і інформаційно-комунікаційних технологій

 (Медведєва М. О.)

Робочу програму розглянуто та затверджено на засіданні науково-методичної комісії природничо-географічного факультету.

Протокол № 1 від 29 серпня 2019 року

Голова науково-методичної комісії природничо-географічного факультету

 (Грабо́вська С.Л.)  
(прізвище та ініціали)

### 1. Опис навчальної дисципліни

Найменування показників	Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів - 4	Галузь знань 01 <i>Освіта</i>	Вибіркова
	<u>Спеціальність 014.06</u> <u>Середня освіта (Хімія)</u>	
Модулів - 2	Освітній ступінь: <b>магістр</b>	Рік підготовки: 1-й
Змістових модулів - 2		Семестр: 1
Загальна кількість годин - 120		Лекції: 16 год.
Тижневих годин: 2 аудиторних - 40 самостійної роботи студента - 80		Лабораторні роб.: 24 год. Практичні:
		Самостійна роб.: 80 год.
		Вид контролю: залік

**Примітка.**

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить:

для денної форми навчання - 1/3

## 2. Мета та завдання навчальної дисципліни

**Мета** вивчення дисципліни полягає у формуванні фундаментальних понять, методів, аналізу інформаційної безпеки; свідомого, активного та вмілого використання алгоритмів захисту інформації в комп'ютерних системах з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Основне **завдання** курсу «Інформаційна безпека» полягає у накопиченні знань з теорії та практики захисту інформації, а також набуття студентами відповідних умінь та навичок.

Відповідно до освітньої програми підготовки фахівця студенти повинні володіти наступними компетентностями:

**ФК 22.** Здатність будувати відповідні моделі природних явищ за допомогою комп'ютерної графіки, досліджувати їх для отримання нових висновків та поглиблення розуміння природи.

### Очікувані результати навчання:

У результаті вивчення навчальної дисципліни студент повинен:

**знати:** загальні поняття та положення щодо захисту даних; історичний аспект організації захисту даних; організаційно-правове забезпечення захисту інформації; основні методи захисту програмного забезпечення; технічні методи та засоби захисту інформації; методи захисту комп'ютерних систем від несанкціонованого доступу; особливості організації захисту в інформаційно-комунікаційних системах; методи захисту інформації в розподілених інформаційних системах; антивірусні засоби, міжмережні екрани та монітори безпеки; шифрування, цифровий підпис; криптографічні методи захисту інформації; методи та засоби створення комплексної системи захисту інформації.

**вміти:** добирати методи та засоби захисту даних; використовувати сучасний інструментарій захисту даних; виявляти погрози безпеці інформаційних систем; застосовувати алгоритми та методи захисту інформації у проектах комп'ютеризованих систем; обирати технології та методи захисту інформації в комп'ютеризованих системах та мережах.

У процесі освоєння курсу «Інформаційна безпека» передбачено такі форми навчальної роботи: аудиторна (лекції і лабораторні заняття) та позааудиторна (самостійна робота) студентів.

Згідно з вимогами освітньо-професійної програми студенти повинні володіти програмними результатами навчання:

**ПРН 30.** Знає вимоги до технічного і програмного забезпечення кабінету інформатики та інформаційних технологій.

## 3. Мова навчання

Мова навчання: Українська

#### **4. Програма навчальної дисципліни**

### **ЗМІСТОВИЙ МОДУЛЬ I. ОСНОВНІ ПОНЯТТЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ**

*Тема 1. Загальні питання безпеки інформаційних ресурсів*

Поняття інформаційної безпеки. Основні складові інформаційної безпеки. Визначення та загальні властивості інформації. Цінність та класифікація інформації. Інформація як об'єкт власності. Інформація як комерційна таємниця.

*Тема 2. Поняття про комп'ютерні злочини та віруси*

Проблеми захисту інформації в сучасних інформаційних системах. Види комп'ютерних злочинів. Причини поширення комп'ютерної злочинності. Поняття і класифікація комп'ютерних вірусів. Основні групи вірусів.

*Тема 3. Основні види шкідливого програмного забезпечення*

Основні типи шкідливого ПЗ. Вірусний маркетинг. Білий, сірий, чорний SEO. Комп'ютерні загрози та їх попередження. Поняття та зміст кібершпигунства.

*Тема 4. Сучасні загрози інформаційної безпеки*

Загрози безпеці під час роботи в Інтернеті. Соціальна інженерія. Фішинг. Скімінг.

### **ЗМІСТОВИЙ МОДУЛЬ II. ЗАСОБИ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ**

*Тема 5. Парольний захист та парольні зломцики*

Поняття про ідентифікацію користувача та її особливості. Апаратна ідентифікації користувачів. Біометрична ідентифікації користувачів. Парольна ідентифікація користувачів. Комбіновані системи захисту

*Тема 6. Створення оптимізованих веб-ресурсів та їх захист від копіювання*

Індексція сайту. Пошукова оптимізація сайту. Захист контенту сайту від незаконного копіювання.

*Тема 7. Ідентифікація та захист мультимедійних даних за допомогою водяних знаків, логотипу, іконки, фавікон, юзебару*

Захист інформації за допомогою технології цифрових водяних знаків. Електронний логотип як засіб аутентифікації та візуалізації. Ідентифікація Інтернет-ресурсу за допомогою фавікон, іконки, юзебару.

*Тема 8. Інформаційні загрози та безпека у віртуальному світі*

Основні загрози для безпеки сайту. Боти, тролі та їх діяльність. Проблеми конфіденційності в Інтернеті. Використання навичок критичного мислення при оцінюванні Інтернет-ресурсів.

### 5. Структура навчальної дисципліни

№ п/п	Назви змістових модулів і тем	Кількість годин				
		Усього	Лекції	Лаб.пр. заняття	Сам. робота.	Інд. робота
		2	3	4	5	6
<b>Модуль 1.</b>						
<b>Змістовий модуль 1. Основні поняття безпеки інформаційних ресурсів</b>						
T1	Загальні питання безпеки інформаційних ресурсів	15	2	2	10	
T2	Поняття про комп'ютерні злочини та віруси	15	2	2	10	
T3	Основні види шкідливого програмного забезпечення	15	2	4	10	
T4	Сучасні загрози інформаційної безпеки	15	2	4	10	
	Разом за змістовий модуль 1	<b>60</b>	<b>8</b>	<b>12</b>	<b>40</b>	
<b>Змістовий модуль 2. Засоби організації захисту інформаційних ресурсів</b>						
T5	Парольний захист та парольні зломщики	15	2	2	10	
T6	Створення оптимізованих веб-ресурсів та їх захист від копіювання	15	2	2	10	
T7	Ідентифікація та захист мультимедійних даних за допомогою водяних знаків, логотипу, іконки, фавікон, юзебару	15	2	4	10	
T8	Інформаційні загрози та безпека у віртуальному світі	15	2	4	10	
	Разом за змістовий модуль 2	<b>60</b>	<b>8</b>	<b>12</b>	<b>40</b>	
	<b>Усього годин:</b>	<b>120</b>	<b>16</b>	<b>24</b>	<b>80</b>	

### 6. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
1	Захист документів МБ Офісе та архівних даних.	2
2	ПРОФІЛЬ ОСОБИСТОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	2
3	Дослідження порушення безпеки та боротьба з фішингом	4
4	Критичне оцінювання ресурсів Інтернет, поняття про авторське право, використання ПППЗ для виявлення плагіату.	4
5	Захист контенту в мережі Інтернет за допомогою логотипу та фавікон.	4
6	створення унікальної іконки як авторського знаку для означення легітимності та захисту інформаційного ресурсу.	4
7	Веб-квест на тему: «Захист інформаційних ресурсів»	4
	Разом:	24

## 7. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Загальні питання безпеки інформаційних ресурсів	10
2	Поняття про комп'ютерні злочини та віруси	10
	Основні види шкідливого програмного забезпечення	10
	Сучасні загрози інформаційної безпеки	10
	Парольний захист та парольні зломщики	10
	Створення оптимізованих веб-ресурсів та їх захист від копіювання	10
	Ідентифікація та захист мультимедійних даних за допомогою водяних знаків, логотипу, іконки, фавікон, юзебару	10
	Інформаційні загрози та безпека у віртуальному світі	10
	Разом	80

### ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

1. Дослідити найбільш відомі віруси та заповнити таблицю:

НАЗВА ВІРУСУ	РІК ЗАСНУВАННЯ	ГЕОЛОКАЦІЯ	ТИП ВІРУСУ	ДІЯ ВІРУСУ
Хробак Morrisa				
Хробак Heartbleed				
Хробак Sasser				
Вірус WIN.CIH				
Melissa				
Хробак Stuxnet				
Code Red				
Slammer				
Nimda				
ILOVEYOU				

2. Написати наукову статтю про історію комп'ютерних вірусів в Україні.

3. Дослідити такі об'єкти захисту інформації як іконка та фавікон. Описати їх та заповнити таблицю:

№п/п	Ресурс	Іконка

4. Користуючись програмним забезпеченням на зразок ЕІКОКАшагк дослідити зображення з цифровим водяним знаком на наявність авторства. Проаналізувати 10 зображень та провести ідентифікацію на предмет конкретного ідентифікаційного номера та конкретного автора.

5. Прослідкувати розвиток науково-практичних основ інформаційної безпеки.

6. Проаналізувати процес ліцензування програм та надання патентів.

7. Загальні питання захисту інформації в автоматизованих системах обробки даних (АСОД).

8. Проаналізувати процес отримання електронних підписів та сертифікатів а

також дію їхніх повноважень.

### **8. Індивідуальні завдання**

#### **Виконати завдання на такі теми:**

1. Захист інформації в мережі INTERNET за допомогою брандмауерів.
2. Вивчити аналіз механізмів захисту додатків та їх блокування.
3. Ознайомитись з основними методами шифрування даних.
4. Побудувати корпоративну мережу з використанням засобів доступу до регіональних мереж.
5. Забезпечення безпеки зберігання даних в операційній системі.
6. Навчитись використовувати утиліти для перевірки комп'ютера на підозрілі дії.

### **9. Методи навчання**

Класичні лекції та лекції із застосуванням мультимедійного проектора, лабораторні роботи, робота у системі Moodle, робота з глосарієм. Розв'язування задач квесту, самостійна робота.

### **10. Методи контролю**

Поточне оцінювання результатів роботи, виконаної за комп'ютером, усна відповідь під час захисту лабораторної роботи; виступ під час організації квесту «Інформаційна безпека»; модульний і підсумковий контроль - тести і контрольні роботи.

1. Виконання та захист звіту лабораторного заняття - 6 - 8 балів.
2. Підсумкове модульне тестування (контрольна робота) - 10, 15 балів.
3. Оцінка за реферат - 10 балів.
4. Інші види діяльності - 20

### **11. Критерії оцінювання результатів навчання**

При визначенні оцінки знань студентів викладач керується критеріями і положеннями, які розроблені Міністерством освіти України. Крім цього, при оцінюванні засвоєння знань студентів проводиться після вивчення модуля модульний контроль, результати, якого оцінюються за нижче наведеними критеріями та заносяться в академічний журнал окремим рядком.

Оцінки «відмінно» заслуговують відповіді студентів, що показали глибокі знання програми курсу, засвоїли основну літературу, набули визначеного програмою кола необхідних знань та мають визначені практичні навички. Крім того, враховується вміння грамотно, чітко і послідовно викласти питання, що розглядається. Швидко виконувати поставлені практичні задачі.

Оцінки «добре» заслуговують відповіді студентів, які виявили тверді знання навчального матеріалу в обсязі навчальної програми, не допустили суттєвих помилок при відповіді на всі питання, чітко виклали матеріал та показали здібності і вміння застосовувати одержані знання у своїй практичній діяльності при використанні натяків на виконання практичних завдань.

Оцінки «задовільно» виставляється студентам, які показали знання основного матеріалу в обсязі навчальної програми, але допустили при відповіді



помилки, невірність окремих формулювань, положень, або які показали поверхові знання з питань, не чітко і не аргументовано дали відповідь на поставлені запитання. Виконувати практичні завдання можуть виконувати лише при додаткових вказівках.

Оцінки «незадовільно» заслуговують відповіді студентів, які показали недостатні знання навчально-програмового матеріалу, не знають основних понять та положень дисципліни, не вміють виконувати елементарні практичні завдання і зовсім не орієнтуються в питаннях до практичної роботи, чим виявили непридатність до професійної діяльності.

### **12. Розподіл балів, які отримують студенти**

Поточне тестування та самостійна робота									Сума
Змістовий модуль 1					Змістовий модуль 2				
T1	T2	T3	T4	T5	T6	T7	T8	Інші ВД	100
10	10	10	10	10	10	10	10	20	

T1, T2 ... T6 - теми змістових модулів.

### **Шкала оцінювання: національна та ЄКТС**

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, курсової роботи, практики	для заліку
90-100	відмінно	зараховано
82-89	добре	
75-81		
69-74	задовільно	
60-68		
35-59	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

### **13. Методичне забезпечення**

1. Опорні конспекти лекцій
2. Електронний курс в системі Моосіе.
3. Інтерактивний комплекс навчально-методичного забезпечення дисципліни (ІКНМЗД) (паперовий та електронний варіант).
4. Ілюстративні матеріали (презентації лекцій).
5. Методичні рекомендації до виконання лабораторних робіт.
6. Навчальні підручники та посібники.

### **14. Рекомендована література**

**Основна**

1. Захист інформаційних ресурсів [Текст] : навч.-метод. посіб. до курсу «Захист інформаційних ресурсів» / МОН Молодьспорту України, Уманський державний педагогічний ун-т імені Павла Тичини ; уклад. С. О. Троян ; [рец. В. Д. Дербенцев, О. В. Малишевський]. - Умань : [б.в.], 2012. - 120 с.
2. Смалько О.А. Захист інформаційних ресурсів: Монографія. - Кам'янець-Подільський: ІІІІ Буйницький О А, 2011. - 704 с.
3. Франчук В.М. Захист інформаційних ресурсів / Василь Франчук. - К.: Редакції газет природничо-математичного циклу, 2012. - 112 с.
4. Сажієнко О. П., Троян С. О. Захист інформації в комп'ютерних системах [Текст] : навчально-методичний посібник / [рец. С. І. Ткачук, С. В. Бесєдіна]. - Умань : Візаві, 2014. - 155, [5] с.
5. Бабак В. П., Корченко А. Г. Інформаційна безпека та сучасні мережеві технології [Текст] = Information security and modern network technology : англо-українсько-російський словник термінів / МОН України, Національний авіаційний ун-т. - К. : НАУ, 2003. - 667с.
6. Коваленко М.М. Комп'ютерні віруси і захист інформації : Навчальний посібник. - К. : "Наукова думка", 1999. - 272 с.
7. Кочарян А. Б., Гущина Н. І. Виховання культури користувача Інтернету. Безпека у всесвітній мережі : навчально-методичний посібник / А. Б. Кочарян, Н. І. Гущина. - Київ, 2011. - 100 с.

#### **Допоміжна**

1. Грайворонський, М. В. Безпека інформаційно-комунікаційних систем : підручник / М. В. Грайворонський, О. М. Новіков ; за заг. ред. М. З. Згуровського. - К. : Видавнича група ВНУ, 2009. - 608 с.
2. Рибальський О. В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / О. В. Рибальський, В. М. Смаглюк, В. Г. Хахановський - К.: НАВС, 2013. - 255 с.
3. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко.- Под ред. В.А. Хорошко. - К.: Арий, 2008. - Том 1. Несанкционированное получение информации. - 464 с.
4. Ленков С. В. Методы и средства защиты информации. В 2-х томах / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. - Под ред. В. А. Хорошко. - К.: Арий, 2008. - Том 2. Информационная безопасность. - 344 с.
5. Інформаційні технології; Методи захисту. Геш-функції / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид - К. : Держспоживстандарт України, 2004. - (Національний стандарт України). - Бібліогр.: с. 5 : ДСТУ ISO/IEC . - IV, 6с.
6. Інформаційні технології; Методи захисту; Цифрові підписи з доповненнями / А. Анісімов (пер.і наук.-техн.ред.). - Офіц. вид. - К. : Держспоживстандарт України, 2006. - (Національний стандарт України) : ДСТУ ISO/IEC 14888-1:2002; Загальні положення (ISO/IEC 14888- 1:1998, IDT). - IV, 14с.
7. Есин В. И., Кузнецов А. А., Сорока Л. С. Безопасность информационных систем и технологий - Х.: ООО «ЭДЭНА», 2010. - 656с.
8. Горбенко І. Д. Гриненко Т. О. Захист інформації в інформаційно-телекомунікаційних системах: Навч. посібник. Ч.1. Криптографічний захист інформації. - Харків: ХНУРЕ, 2004 - 368 с.
9. Василюк В. Я., Климчук С. О. Інформаційна безпека держави: курс

лекцій для студентів, які навчаються за спеціальностями «Організація захисту інформації з обмеженим доступом», «Правознавство». - К. : КНТ, Скіф, 2008. - 135 с.

10. Горобцов В. О., Костецька Т. А., Кресіна І. О., Петренко В. М., Погорілко В. Ф., Чиж І. С. Інформаційне законодавство України: науково-практичний коментар / за заг. ред. Ю. С. Шемшученка ; Ін-т держави і права імені В. М. Корецького НАН України, Державний комітет телебачення і радіомовлення України. - К. : Юридична думка, 2006. - 230 с.

11. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу : навч. посібник. - К. : КНТ, 2007. - 255 с.

12. Домарєв В. В., Домарєв Д. В. Управління інформаційною безпекою в банківських установах : (теорія і практика впровадження стандартів серії ІБО 27к). - Донецьк : Велстар, 2012. - 143 с.

13. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції : навч. посібник / Київський нац. ун-т внутрішніх справ, Каф. міжнародних відносин та нац. безпеки. - К. : КНТ, 2006. - 279 с.

14. Марущак А. І. Інформаційне право : підручник : затв. МОН України. - К. : Дакор, 2011. - 340 с.

15. Марущак А. І. Інформаційне право: доступ до інформації : навч. посібник : рек. МОН України як навч. посіб. для студ. ВНЗ. - К. : КНТ, 2007. - 531 с.

16. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності: навч. посібник, рек. МОН України. - К. : Скіф : КНТ, 2008. - 342 с.

17. Марущак А. І. Правові основи захисту інформації з обмеженим доступом : (курс лекцій). - К. : КНТ, 2007. - 207 с.

18. Марущак А.І. Правомірні засоби доступу громадян до інформації : Науково-практичний посібник. - Біла Церква : Вид-во «Буква», 2006. - 432 с.

19. Сідак В. С., Артемов В. Ю. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. : рек. МОН України як навч. посіб. для студ. ВНЗ / МОН України. - К. : КНТ, 2007. - 158 с.

20. Суська О. О. Інформаційний імунітет : проблеми психологічного захисту в інформаційному просторі : монографія. - К. : [б. в.], 2008. - 107 с.

21. Фролов П. Д. Технології і методики прогнозування наслідків інформаційного впливу на політичні настанови старшокласників : методичний посібник. - К. : Міленіум, 2008. - 94 с.

### 15. Інформаційні ресурси

<a href="http://www.president.gov.ua">www.president.gov.ua</a>	Офіційне представництво Президента України
<a href="http://www.mon.gov.ua">www.mon.gov.ua</a>	Міністерство освіти і науки України
<a href="http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi">http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi</a>	Сайт Верховної Ради України

Електронні наукові бібліотеки:

<a href="http://catalog.udpu.org.ua">http://catalog.udpu.org.ua</a>	Електронний каталог УДПУ
---	--------------------------

<a href="http://www.library.kr.ua/libworld/elib.html">http://www.library.kr.ua/libworld/elib.html</a>	Бібліотеки в інтернет
<a href="http://www.nbu.gov.ua">http://www.nbu.gov.ua</a>	Національна бібліотека України ім. Вернадського
<a href="http://www.nbu.gov.ua/libdoc">http://www.nbu.gov.ua/libdoc</a>	Комп'ютерні технології в бібліотеці (Київ)
<a href="http://www.nbu.gov.ua/eb/ep.html">http://www.nbu.gov.ua/eb/ep.html</a>	Електронний фонд наукових публікацій (Київ)
<a href="http://www.infocity.kiev.ua">http://www.infocity.kiev.ua</a>	ІнфоСіті (Київ) Тексти з комп'ютерних технологій
<a href="http://lib.meta.ua">http://lib.meta.ua</a>	Библиотека на <a href="http://meta.ua">Meta.Ua</a> (Харьков)
<a href="http://www.utoronto.ca/elul">http://www.utoronto.ca/elul</a>	Електронна бібліотека української літератури (Канада)
<a href="http://www.library.edu-ua.net">http://www.library.edu-ua.net</a>	Державна науково-педагогічна бібліотека України імені В.О. Сухомлинського (Київ)
<a href="http://www.gntb.n-t.org">http://www.gntb.n-t.org</a>	Державна науково-технічна бібліотека України (Київ)
<a href="http://www.4uth.gov.ua">http://www.4uth.gov.ua</a>	Державна бібліотека України для юнацтва (Київ)