



## Силабус курсу ОСНОВИ ІНФОРМАЦІЙНІ БЕЗПЕКИ

Ступінь вищої освіти – бакалавр

Галузь знань – 02 Культура і мистецтво

Спеціальність – 028 «Менеджмент соціокультурної діяльності»

Освітньо-професійна програма – «Менеджмент соціокультурної діяльності»

Рік навчання: 3 Семестр: 6

Кількість кредитів: 5 Мова викладання: українська

### Керівник курсу

ПП

Аліна Давлетова

Контактна інформація

a.davletova@wunu.edu.ua

### Опис дисципліни

Курс «Основи інформаційної безпеки» покликаний дати студентам теоретичні знання та практичну підготовку, зокрема сучасних загроз інформаційної безпеки, антивірусної індустрії, безпеки електронних фінансів, принципів поведінки з персональною інформацією, правил безпеки в умовах інформаційної війни. Метою курсу є формування комплексу знань щодо основ інформаційної безпеки, набуття теоретичних знань та практичних навичок щодо методів та засобів підвищення рівня захисту інформації.

### Структура курсу

Тема	Результати навчання	Завдання
Історія комп'ютерних вірусів. Основні види шкідливого програмного забезпечення	Знання основних типів шкідливого програмного забезпечення та основних джерел зараження персональних комп'ютерів. Розуміння чим персональний комп'ютер цікавий зловмисникам. Вміння формувати портрет сучасного хакера.	Усне опитування, тестування
Сучасні загрози інформаційної безпеки	Знати етапи еволюції загроз інформаційної безпеки. Володіти поняттям соціальної інженерії, фітінг, скімінг. Вміти визначати загрози платіжних систем, основні джерела зараження.	Поточне опитування, тестування
Загрози для мобільних пристроїв.	Знання загроз сучасним мобільним пристроям, можливостей троянських програм для них, класичних кіберзагроз для смартфонів та вірусів для iOS. Вміння використовувати моделі роботи з платними послугами.	Ситуаційне опитування
Антивірусна індустрія.	Володіти поняттям технології, індустрії антивірусного програмного забезпечення та вміння практичного їх застосування.	Поточне опитування, тестування
Безпека електронних фінансів	Зняття загроз електронних фінансів та вміння використовувати можливості захисту фінансової інформації, застосовувати практики захисту.	Усне опитування
Захист персональної інформації	Знати та вміння визначати причини втрати інформації, використовувати методи та	Поточне опитування,

	засоби захисту даних від крадіжки, відновлення видаленої інформації, захисту від програмних помилок.	тестування
Безпечна робота з мобільними пристроями	Вміти визначати загрози та забезпечувати захист Android-пристроїв, iOS-пристроїв, та інших мобільних операційних систем.	Ситуаційне опитування
Безпека в умовах інформаційної війни та кібервійни.	Розуміти взаємозв'язок інформаційних війн та кібервійн. Володіти поняттями бот, троль, бот-мережа. Вміти виявити коментар від бота та тролінг.	Усне опитування
Управління інформаційною безпекою	Знання загальних положень управління інформаційною безпекою. Вміння застосовувати принципи управління безпекою інформації.	Усне опитування
Стратегія захисту інформації	Володіння поняттями інформаційна гігієна, точність у словах, правда і фейки. Розуміти алгоритми роботи мережі інтернет. Вміти безпечно використовувати цифровий простір.	Поточне опитування
Сумнівні джерела інформації.	Вміння визначити маніпуляції та дезінформація. Знання алгоритмів роботи Google. YouTube. Telegram. Viber. Facebook. Twitter.	Ситуаційне опитування
Безпечна комунікація.	Вміння безпечного використання електронної пошти та месенджерів Розуміння небезпек соціальних мереж.	Усне опитування

### Літературні джерела

1. Закон України «Про інформацію». URL: <https://zakon.rada.gov.ua/laws/show/2657-12>
2. Закон України Про захист інформації в інформаційно-телекомунікаційних системах № 80/94-ВР від 05.07.1994 р. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>
3. Захист конфіденційну інформацію – персональних даних. URL: <https://cutt.ly/iuggGRH>
4. Бобало Ю.Я., Горбатий І.В. Інформаційна безпека. Львів: Видавництво Львівської політехніки, 2019. 580 с.
5. Шумейко О.О. Інформаційна безпека. Дніпро: Дніпровський державний технічний університет, 2019. 155 с.
6. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.
7. Andress J. Foundations of Information Security: A Straightforward Introduction. No StarchPress, 2019. 248 p.
8. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах. Навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
9. Easttom Chuck. Computer Security Fundamentals. 4th Edition. Pearson Education Inc., 2020. 512 p.
10. Browning P., Drinan M. 101 Labs - CompTIA Security+. Independently published, 2021.680 p.

### Політика оцінювання

**Політика щодо дедлайнів та перескладання:** Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання модулів відбувається із дозволу деканату за наявності поважних причин (наприклад, лікарняний).

**Політика щодо академічної доброчесності:** Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%. Списування під час контрольних робіт та екзаменів заборонені (в т.ч. із використанням мобільних девайсів).

**Політика щодо відвідування:** Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба,

міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.

### Оцінювання

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КППЗ, враховуючи поточне опитування)	Разом
30%	40%	30%	100%
1. Усне опитування - тах 20 балів. 2. Письмова робота – тах 40 балів. 3. Практичне завдання - тах 40 балів.	1. Усне опитування - тах 20 балів. 2. Письмова робота - тах 40 балів. 3. Практичне завдання - тах 40 балів	1. Підготовка КППЗ - тах 40 балів. 2. Захист КППЗ - тах 40 балів. 3. Участь у тренінгах - тах 20 балів	

### Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)