ПрАТ «ВНЗ» МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

Інститут Безпеки

Кафедра національної безпеки

Затверджую:
Директор Інституту Безпеки
_____
Сергій МАСЛЯНКО
“ ” _____ 2025 р.

Схвалено на засіданні кафедри
Національної безпеки
Протокол № 1 від 07.08 2025 р.
Заст. зав. кафедри
_____
Іван СЕРВЕЦЬКИЙ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕОРЕТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ»

Спеціальності: **256 Національна безпека (за окремими сферами забезпечення і видами діяльності)**

Освітнього рівня: **перший (бакалаврський) рівень**

Освітньої програми: **«Національна безпека (за окремими сферами забезпечення і видами діяльності)»**

Спеціалізація: _____

Київ МАУП 2025

Загальна інформація про навчальну дисципліну

Назва навчальної дисципліни	**Теоретичні основи захисту інформації**
Шифр та назва спеціальності	256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Рівень вищої освіти	перший (бакалаврський) рівень
Статус дисципліни	обов'язкова
Кількість кредитів і годин	**6 кредита/180 год** Лекції : **34** Семінарські заняття:**48** Самостійна робота студентів: **98**
Терміни вивчення дисципліни	III семестр
Мова викладання	українська
Вид підсумкового контролю	**екзамен**
Сторінка дисципліни на сайті	https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-b/vstup-do-specialnosti-nacionalna-bezpeka.pdf

Загальна інформація про викладача. Контактна інформація.

Лисенко Сергій Олексійович	
Науковий ступінь	доктор юридичних наук, доктор наук з державного управління
Вчене звання	професор
Посада	Професор кафедри
Дисципліни, які викладає НПП	Теоретичні основи захисту інформації
Напрями наукових досліджень	Інформаційна безпека
Посилання на реєстри ідентифікаторів для науковців	ORCID: https://orcid.org/0000-0002-7050-5536 Google Scholar: https://scholar.google.com.ua/citations?hl=ru&user=hXbTiEAAAAAJ
Контактна інформація викладача:	
E-mail:	crimeconsult@ukr.net
Контактний тел.	+380507417375
Телефон кафедри	
Портфоліо викладача на сайті кафедри/Інституту/Академії	https://maup.com.ua/ua/pro-akademiyu/instituti/institut-bezpeki-prat-vnz-maup/nacionalna-bezpeka/lisenko.html

1.1 Анотація курсу.

Курс «Теоретичні основи захисту інформації» є обов'язковою дисципліною для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 256 Національна безпека (за окремими сферами забезпечення і видами діяльності). Курс вивчається протягом ІІІ семестру обсягом 6 кредитів ECTS (лекції – 34 год., практичні та семінарські заняття – 48 год., самостійна робота студентів – 98 годин) та знайомить здобувачів із базовими категоріями захисту інформації, принципами конфіденційності, цілісності та доступності, загальними підходами до охорони інформаційних ресурсів і систем, а також з організаційними, технічними та правовими механізмами протидії сучасним інформаційним і кіберзагрозам.

1.2 Предмет вивчення курсу.

Предметом вивчення навчальної дисципліни є сукупність теоретичних положень, понять і підходів, а також норми й принципи, що визначають сутність та закономірності процесів захисту інформації, регулюють відносини у сфері забезпечення інформаційної та кібербезпеки, а також організаційно-технічні механізми охорони інформаційних ресурсів від несанкціонованого доступу, витоку, порушення цілісності чи блокування. Опрацювання змісту дисципліни спрямоване на формування у здобувачів належного рівня фахової правосвідомості та інформаційної культури, необхідних для розуміння ролі безпеки інформаційних систем у зміцненні національної стійкості, а також для коректного застосування базових положень захисту інформації у навчальних і практикоорієнтованих ситуаціях.

1.3 Метою викладання навчальної дисципліни «Теоретичні основи захисту інформації» є формування у здобувачів системи фундаментальних знань про принципи, методи та засоби захисту інформації, розуміння природи інформаційних і кібернетичних загроз, а також базових підходів до побудови комплексних систем інформаційної безпеки. Вивчення курсу має забезпечити набуття первинних професійних компетентностей, необхідних для подальшого опанування спеціальних дисциплін (зокрема, з управління інформаційною безпекою) , розуміння логіки функціонування механізмів кіберзахисту, орієнтації у базових стандартах і політиках безпеки, а також розвитку навичок критичного аналізу інформаційного простору та оцінювання вразливостей інформаційних систем.

1.4 Завдання: поглиблене засвоєння понятійно-категоріального апарату у сфері захисту інформації та ключових наукових підходів до розуміння інформаційної безпеки; забезпечення знань про сутність, принципи та механізми забезпечення конфіденційності, цілісності й доступності інформації в сучасних інформаційно-комунікаційних системах; розкриття основних методів, засобів та організаційно-правових засад захисту інформації (зокрема інформації з обмеженим доступом), а також особливостей їх застосування суб'єктами забезпечення національної безпеки; формування уявлення про сучасні кіберзагрози, інформаційно-психологічні впливи, вразливості інформаційних систем та загальні алгоритми їх виявлення, попередження і нейтралізації; набуття навичок аналізу політик безпеки, застосування базових концепцій управління інформаційними ризиками та використання отриманих знань під час розв'язання типових навчально-практичних ситуацій у сфері захисту даних.

1.5 Пререквізити і постреквізити навчальної дисципліни:

Пререквізити:

«Сучасна українська мова» засвоєння цієї дисципліни є необхідною передумовою, оскільки вивчення теоретичних основ захисту інформації вимагає високого рівня академічної грамотності, здатності коректно аналізувати й інтерпретувати складні нормативно-правові та технічні тексти, фахово оперувати специфічним термінологічним апаратом сфери національної та інформаційної безпеки, а також грамотно розробляти, формулювати і документувати політики безпеки державною мовою.

Постреквізити:

«Розвідувальна та контррозвідувальна діяльність» дисципліна тісно пов’язана з «Теоретичними основами захисту інформації», оскільки глибоке розуміння методів захисту даних, криптографії, каналів витоку та вразливостей інформаційних систем є фундаментальною основою для організації захищеної комунікації, а також для виявлення та нейтралізації спроб технічного проникнення чи несанкціонованого доступу з боку іноземних спецслужб у межах контррозвідувальних заходів.

«Протидія злочинності, корупції та тероризму» зв’язок зумовлений тим, що сучасні злочинні угруповання та терористичні організації активно використовують кіберпростір, зашифровані канали зв'язку та інформаційні технології для координації своєї діяльності; базові знання із захисту інформації надають здобувачам концептуальний інструментарій для аналізу цифрових слідів, розуміння механізмів кібертероризму та розробки комплексних заходів протидії високотехнологічним загрозам.

1.6 Програмні компетентності (загальні (ЗК); спеціальні (СК)):

ЗК6. Здатність до абстрактного мислення, пошуку, аналізу та синтезу.

Забезпечено дисципліною через системне опрацювання теоретичних моделей захисту інформації, логіки побудови комплексних систем безпеки та вивчення математико-алгоритмічних основ криптографії; у межах курсу здобувачі набувають здатності здійснювати пошук уразливостей, аналізувати моделі загроз і синтезувати отримані дані для розробки обґрунтованих рішень щодо захисту інформаційних ресурсів.

ЗК8. Здатність використовувати інформаційні та комунікаційні технології.

Забезпечено дисципліною, оскільки теоретичне вивчення принципів конфіденційності, цілісності та доступності невіддільне від практичного розуміння архітектури сучасних ІКТ; здобувачі засвоюють правила безпечної експлуатації комунікаційних систем, протоколи безпечного передавання даних та алгоритми використання технологій в умовах потенційних кіберризиків.

СК11. Здатність користуватися інформаційно-аналітичними системами, засобами зв’язку для ефективної комунікації, обміну та захисту інформації.

Забезпечено дисципліною шляхом ґрунтовного вивчення механізмів криптографічного і технічного захисту даних, систем автентифікації та інфраструктури відкритих ключів; курс формує розуміння того, як надійно

налаштовувати канали зв'язку та застосовувати програмно-апаратні засоби для убезпечення процесів збору, обробки й обміну інформацією в інтересах національної безпеки.

СК12. Здатність аналізувати інформаційний простір, визначати та протидіяти інформаційно-психологічним загрозам та кіберзагрозам, шляхом використання кібернетичних, інформаційно-комунікаційних технологій, впровадження сучасних методів інформаційної безпеки та захисту інформації.

Забезпечено дисципліною, оскільки вона закладає концептуальний і методологічний фундамент для розуміння природи сучасних кіберзагроз, векторів атак на інформаційні системи та методів соціальної інженерії; курс надає здобувачам базовий інструментарій для ідентифікації несанкціонованих втручань та впровадження організаційно-правових і технічних методів захисту з метою мінімізації наслідків інформаційних і кібернетичних інцидентів..

1.7 Очікувані результати навчання (ПРН)

ПРН3. Застосовувати результати абстрактного мислення, самостійного пошуку, аналізу та синтезу, методів теорії інформації, теорії систем та системного аналізу для ефективного вирішення завдань професійної діяльності.

Забезпечено дисципліною «Теоретичні основи захисту інформації», оскільки у межах курсу здобувачі опановують фундаментальні методи теорії інформації та системного аналізу для оцінювання інформаційних ризиків. Дисципліна формує здатність абстрагуватися від конкретних апаратних реалізацій та аналізувати інформаційні системи як комплексні об'єкти захисту, синтезуючи теоретичні підходи (моделювання загроз, криптографічні алгоритми, політики доступу) для розв'язання складних професійних завдань у безпековій сфері.

ПРН5. Застосовувати знання державної та іноземних мов, інформаційно-аналітичних, інформаційно-комунікаційних технологій, комп’ютерної техніки для забезпечення професійної комунікації.

Забезпечено дисципліною через необхідність опрацювання фахової літератури, нормативно-правових актів та міжнародних стандартів інформаційної безпеки (зокрема сімейства ISO/IEC 27000). У процесі навчання здобувачі використовують комп'ютерну техніку та інформаційно-комунікаційні технології для моделювання захищених систем комунікації. Одночасно курс вимагає вільного володіння фаховою термінологією з кібербезпеки державною мовою, що є критично важливим для розробки політик безпеки та забезпечення коректної професійної взаємодії у державному та приватному секторах.

ПРН17. Протидіяти інформаційно-психологічним впливам під час адаптації та дій в умовах мирного часу та в особливий період, критично оцінювати достовірність джерел інформації, виявляти дезінформацію та маніпулятивний контент, що може впливати на національну безпеку, використовуючи методи верифікації та фактчекінгу.

Забезпечено дисципліною, оскільки курс розкриває не лише технічні аспекти криптографії та контролю доступу, але й механізми порушення цілісності та достовірності даних, включно з методами соціальної інженерії. Здобувачі набувають навичок верифікації інформації, розуміння критеріїв автентичності та захищеності

каналів передавання даних, що створює аналітичне підґрунтя для ідентифікації маніпулятивного контенту, виявлення дезінформації та ефективної протидії загрозам інформаційно-психологічного характеру в інтересах національної безпеки.

2. Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ЗАХИСТУ ІНФОРМАЦІЇ ТА МОДЕЛЮВАННЯ ЗАГРОЗ

Тема 1. Сутність та складові інформаційної безпеки: базові поняття та категорії. Тема спрямована на формування у здобувачів вищої освіти цілісного уявлення про інформацію як об’єкт захисту, розкриття базової тріади інформаційної безпеки (конфіденційність, цілісність, доступність), а також додаткових властивостей: автентичності, апелювальності (неможливості відмови) та спостережності. У процесі опанування теми здобувачі засвоюють понятійно-категоріальний апарат теорії захисту інформації та зв’язок інформаційної безпеки з національними інтересами держави.

Тема 2. Правові та організаційні засади захисту інформації в Україні. Вивчення цієї теми покликане забезпечити здобувачів знаннями про національну систему нормативно-правового регулювання у сфері захисту інформації (зокрема інформації з обмеженим доступом, державної таємниці, комерційної таємниці, персональних даних). Тема формує здатність орієнтуватися у вимогах законодавства та галузевих стандартів, а також розуміти розподіл повноважень між суб’єктами державного управління у сфері кібербезпеки та захисту інформації.

Тема 3. Класифікація загроз, вразливостей та атак на інформаційні системи. Тема спрямована на засвоєння здобувачами теоретичних підходів до класифікації дестабілізаційних факторів в інформаційному просторі. Опанування теми розвиває здатність систематизувати джерела загроз (природні, антропогенні, техногенні), аналізувати види вразливостей (архітектурні, програмні, організаційні) та розуміти базові класифікації кібератак, що є необхідним для подальшої розробки адекватних механізмів протидії.

Тема 4. Формальні моделі політик інформаційної безпеки. Тема формує у здобувачів математичне та логічне розуміння механізмів контролю доступу. Вивчення теми спрямоване на засвоєння дискреційних, мандатних та рольових моделей управління доступом, зокрема класичних формальних моделей Белла-ЛаПадули (для конфіденційності), Біба та Кларка-Вілсона (для цілісності), а також моделі Харрісона-Руццо-Ульмана.

Тема 5. Управління ризиками інформаційної безпеки: методологія та оцінювання. Тема дає можливість засвоїти ризик-орієнтований підхід до захисту інформації. Вивчення теми спрямоване на розвиток здатності ідентифікувати інформаційні активи, визначати їхню цінність, оцінювати ймовірність реалізації загроз та можливі збитки, а також здійснювати вибір стратегій обробки ризиків (прийняття, уникнення, передача, зниження) відповідно до міжнародних стандартів.

ЗМІСТОВИЙ МОДУЛЬ 2. МАТЕМАТИЧНІ ТА КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Тема 6. Теоретичні основи криптографії та симетричні криптосистеми. Тема спрямована на формування уявлення про криптографію як фундаментальний інструмент забезпечення конфіденційності. Опанування теми дає здобувачам можливість зрозуміти принципи потокового та блокового шифрування, вимоги Шеннона до криптостійкості (розсіювання та перемішування), а також базові алгоритми симетричного шифрування (AES, національні стандарти шифрування).

Тема 7. Асиметричні криптосистеми та інфраструктура відкритих ключів (PKI). Тема спрямована на засвоєння здобувачами математичних основ криптографії з відкритим ключем (алгоритми RSA, криптографія на еліптичних кривих). Вивчення теми формує уявлення про логіку розв'язання проблеми розподілу ключів, а також про архітектуру та компоненти інфраструктури відкритих ключів (PKI), сертифікати X.509 і діяльність центрів сертифікації ключів.

Тема 8. Криптографічні геш-функції та електронний підпис .Тема дає можливість зрозуміти механізми забезпечення цілісності та автентичності інформації. Вивчення теми спрямоване на формування здатності розуміти властивості стійких геш-функцій, алгоритми формування кодів автентифікації повідомлень та теоретичні засади створення і перевірки електронного цифрового підпису (ЕЦП/КЕП) як інструменту забезпечення юридичної значущості електронного документообігу.

Тема 9. Теорія автентифікації та управління доступом. Тема спрямована на формування цілісного бачення процесів ідентифікації, автентифікації та авторизації суб'єктів в інформаційних системах. Опанування теми дозволяє здобувачам зрозуміти класифікацію факторів автентифікації (знання, володіння, біометрія), принципи побудови систем строгої та багатофакторної автентифікації, а також протоколи єдиного входу.

Тема 10. Стеганографія та методи приховування інформації. Тема допомагає сформувати у здобувачів теоретичні знання щодо методів приховування самого факту існування та передачі інформації. Вивчення теми спрямоване на розуміння відмінностей між криптографією та стеганографією, засвоєння базових стеганографічних алгоритмів у цифрових медіафайлах, а також принципів стеганоаналізу та виявлення прихованих каналів передачі даних.

ЗМІСТОВИЙ МОДУЛЬ 3. КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ТЕХНІЧНА ПРОТИДІЯ

Тема 11. Технічний захист інформації: канали витоку та методи протидії. Тема дає можливість засвоїти фізичні принципи витоку інформації акустичними, віброакустичними, оптичними та побічними електромагнітними каналами . Вивчення теми спрямоване на розуміння методів інженерно-технічного захисту, екранування, зашумлення та організаційних заходів щодо створення виділених приміщень для циркуляції інформації з обмеженим доступом.

Тема 12. Мережева безпека та криптографічні протоколи зв'язку. Тема спрямована на формування уявлення про вразливості стека протоколів TCP/IP та теоретичні основи захисту периметра мережі. Вивчення теми дозволяє здобувачам

усвідомити логіку роботи міжмережевих екранів, систем виявлення та запобігання вторгненням, а також застосування захищених протоколів для створення віртуальних приватних мереж.

Тема 13. Шкідливе програмне забезпечення: механізми дії та основи протидії. Тема спрямована на формування у здобувачів розуміння еволюції та класифікації шкідливого програмного забезпечення (віруси, хробаки, трояни, руткіти, програми-вимагачі). Вивчення теми забезпечує усвідомлення теоретичних методів виявлення шкідливого коду (сигнатурний, евристичний, поведінковий аналіз) та принципів побудови антивірусних систем і пісочниць.

Тема 14. Інформаційно-психологічні впливи та соціальна інженерія. Тема спрямована на вивчення "людського фактору" як найуразливішої ланки інформаційної безпеки. Вивчення теми забезпечує розуміння психологічних механізмів, що лежать в основі атак соціальної інженерії (фішинг, претекстінг, бейттінг), а також формує здатність розробляти організаційні заходи протидії, проводити верифікацію даних та підвищувати рівень інформаційної гігієни персоналу.

Тема 15. Побудова комплексних систем захисту інформації та аудит безпеки. Тема спрямована на систематизацію отриманих знань та інтеграцію правових, організаційних, криптографічних і технічних заходів у єдину комплексну систему захисту інформації. Вивчення теми допомагає здобувачам зрозуміти етапи створення КСЗІ, принципи проведення аудиту інформаційної безпеки, сертифікації систем захисту та забезпечення їх безперервного функціонування в умовах сучасних викликів національній безпеці.

3. Технічне й програмне забезпечення/обладнання

В освітньому процесі використовуються навчальні аудиторії, бібліотека, мультимедійний проектор та комп'ютер для проведення аудиторних занять з елементам презентацій Microsoft PowerPoint. Вивчення окремих тем і виконання практичних завдань потребує доступу до інформації зі всесвітньої мережі Інтернет, який забезпечується безкоштовною мережею Wi-Fi.

4. Форми і методи навчання

Основними формами занять із навчальної дисципліни «Теоретичні основи захисту інформації є практичні заняття та самостійна робота здобувачів вищої освіти.

При проведенні практичних занять передбачено поєднання таких форм і методів навчання, як-то: робота у малих групах, рольові ігри, дискусія, публічні виступи, групові проєкти та кейс-завдання.

Здобувачі освіти опрацьовують інформацію з наукових, навчальних та лекційних джерел, в тому числі за допомогою всесвітньої мережі Інтернет і бібліотек, під час занять виконують усні та письмові завдання, виступають із доповідями та презентаціями, що можуть бути підготовленими як у групі, так і індивідуально.

Програмою курсу також передбачено **індивідуальні завдання.**

5. Система оцінювання та вимоги (критерії оцінювання результатів навчання здобувачів освіти та розподіл балів, які вони отримують)

Оцінювання знань здійснюється відповідно до:

1. Положення про організацію освітнього процесу в ПрАТ «ВНЗ «МАУП» https://surl.li/bpxlbj
2. Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ «ВНЗ «МАУП» http://surl.li/fkfyye

3-й семестр.

№ тем	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Заг.сума балів**
Робота на сем.занятті	4	4	4	4	4	4	4	4	4	36
Сам.робота	1	1	1	1	1	1	1	1	1	9
Всього										**45**

Підсумкове оцінювання	Сума балів за семінари	Сума балів за самостійні роботи	Модульна контрольна робота	Сума балів за екзамен	Загальна сума
	36	9	15	40	100

5.1 Відвідування та робота на семінарських (практичних) заняттях та критерії їх оцінювання

Під час вивчення курсу виконується *робота на семінарських (практичних) заняттях по кожній з тем***.**

Критерії оцінювання:

правильність відповідей та розрахунків – від 0 до 3 балів;
відповідність оформлення практичних робіт вимогам – 1 бал.
(враховуються лише за умови нарахування балів за правильність відповідей).

Робота на семінарському занятті оцінюється у **4 бали**.

Максимальна кількість балів за семінарські (практичні) заняття по курсу – **36 балів.**

Зміст практичних занять

№ з/п	**Назва теми**
1	**Тема 1. Сутність та складові інформаційної безпеки: базові поняття та категорії** **Завдання:** Проаналізувати базову тріаду інформаційної безпеки (конфіденційність, цілісність, доступність) та пояснити її взаємозв'язок із додатковими властивостями (автентичність, апелювальність). Скласти схему: властивість інформації — можливі наслідки її порушення — механізм базового захисту. Розглянути приклади відомих кіберінцидентів (обраних викладачем) та визначити, які саме складові інформаційної безпеки були скомпрометовані.

	Результат: Здобувачі зможуть систематизувати уявлення про сутність захисту інформації та базові принципи побудови безпечного середовища. Вміння розмежовувати об’єкти захисту та коректно класифікувати наслідки порушення безпеки. Формування навичок узагальнення теоретичних знань і використання фундаментального понятійно-категоріального апарату. **Дискусія:** Обговорити проблему пошуку балансу між надійністю захисту інформації та зручністю її використання (Security vs. Usability). Порівняти пріоритетність конфіденційності та доступності в різних типах систем (наприклад, у медичних базах даних та фінансових установах). Розглянути ситуації, коли вимоги щодо забезпечення безпеки можуть конфліктувати з інтересами користувача чи бізнес-процесами організації. **Тема 2. Правові та організаційні засади захисту інформації в Україні** **Завдання:** Проаналізувати базові вимоги національного законодавства щодо захисту інформації з обмеженим доступом (державна таємниця, комерційна таємниця, персональні дані). Скласти порівняльну таблицю: категорія інформації — суб'єкти захисту — правова відповідальність за розголошення. Розглянути кейс несанкціонованого витоку персональних даних з державної установи та визначити правові наслідки й алгоритм організаційного реагування. **Результат:** Здобувачі зможуть орієнтуватися в нормативно-правовій базі України у сфері захисту інформації та кібербезпеки. Вміння класифікувати інформацію за режимами доступу та визначати відповідні правові вимоги щодо її обробки. Формування здатності здійснювати правовий аналіз інформаційних інцидентів. **Дискусія:** Обговорити межі державного контролю та втручання у приватну комунікацію з міркувань національної безпеки. Порівняти вітчизняні стандарти захисту персональних даних із європейськими (зокрема, GDPR). Розглянути проблеми притягнення до відповідальності за кіберзлочини в умовах транскордонності інформаційного простору. **Тема 3. Класифікація загроз, вразливостей та атак на інформаційні системи** **Завдання:** Визначити типові загрози для інформаційних систем та здійснити їх класифікацію (за джерелом, мотивацією, способом реалізації). Скласти структурну схему: джерело загрози — вразливість системи — вектор атаки — наслідок. Проаналізувати сценарій типової мережевої атаки (наприклад, DDoS або

	Ransomware) та окреслити життєвий цикл атаки (Cyber Kill Chain). **Результат:** Здобувачі зможуть класифікувати та аналізувати загрози й вразливості в інформаційній сфері. Вміння встановлювати причинно-наслідкові зв'язки між наявністю вразливості та успішністю реалізації кібератаки. Формування навичок системного бачення поверхні атаки (Attack Surface) та архітектурних недоліків. **Дискусія:** Обговорити, що становить більшу небезпеку для організації: цілеспрямована зовнішня атака (APT) чи випадкова помилка інсайдера. Порівняти наслідки експлуатації апаратних вразливостей і програмних помилок. Розглянути етичні аспекти пошуку вразливостей (White-hat hacking) та проблему своєчасного випуску патчів. **Тема 4. Формальні моделі політик інформаційної безпеки** **Завдання:** Проаналізувати принципи функціонування класичних моделей безпеки (Белла-ЛаПадули, Біба, HRU) та пояснити їхнє математичне підґрунтя. Скласти матрицю доступу для гіпотетичної організації, застосувавши принципи рольового управління доступом (RBAC). Розглянути практичний кейс призначення прав доступу в інформаційній системі та виявити порушення принципу найменших привілеїв. **Результат:** Здобувачі зможуть пояснювати логіку функціонування мандатних, дискреційних та рольових моделей контролю доступу. Вміння розробляти базові матриці доступу та уникати конфліктів повноважень. Формування навичок опису та формалізації політик безпеки для інформаційних систем різних рівнів критичності. **Дискусія:** Обговорити переваги та недоліки жорстких мандатних моделей у порівнянні з гнучкими дискреційними. Порівняти застосування рольової моделі (RBAC) та моделі управління на основі атрибутів (ABAC) у сучасних хмарних середовищах. Розглянути типові помилки адміністраторів при делегуванні повноважень. **Тема 5. Управління ризиками інформаційної безпеки: методологія та оцінювання** **Завдання:** Провести ідентифікацію та оцінку цінності інформаційних активів на прикладі навчального кейсу підприємства. Скласти матрицю ризиків: ідентифікована загроза — ймовірність реалізації — рівень впливу — пріоритет. Запропонувати стратегії обробки для виявлених критичних ризиків (прийняття, уникнення, передача, зниження) із обґрунтуванням обраних заходів захисту.

Результат:

Здобувачі зможуть здійснювати базову оцінку інформаційних ризиків та пояснювати їхній вплив на стійкість організації.

Вміння застосовувати методологію ризик-менеджменту та обґрунтовано обирати інструменти реагування.

Формування навичок ранжирування загроз і оптимізації витрат на систему захисту інформації.

Дискусія:

Обговорити проблему суб'єктивності в якісному оцінюванні ризиків та можливості переходу до кількісних метрик.

Порівняти підходи до управління ризиками в умовах обмеженого бюджету.

Розглянути, як правильно комунікувати рівень інформаційних ризиків вищому керівництву (бізнесу/командуванню) для обґрунтування інвестицій у безпеку.

Тема 6. Теоретичні основи криптографії та симетричні криптосистеми

Завдання:

Проаналізувати принципи роботи симетричних криптосистем та пояснити фундаментальні вимоги до криптостійкості (принципи розсіювання та перемішування Шеннона).

Скласти схему процесу шифрування та дешифрування повідомлення з використанням єдиного секретного ключа.

Розглянути навчальний кейс із перехопленням зашифрованого трафіку та визначити потенційні вектори атак на симетричні шифри (атака повним перебором, лінійний та диференціальний криптоаналіз).

Результат:

Здобувачі зможуть пояснювати теоретичні основи та логіку функціонування потокових і блокових симетричних шифрів.

Вміння оцінювати криптографічну стійкість алгоритмів та коректно обирати довжину ключа відповідно до сучасних стандартів (наприклад, AES).

Формування базових навичок аналізу загроз, пов’язаних із компрометацією секретного ключа.

Дискусія:

Обговорити проблему безпечного розподілу секретних ключів (Key distribution problem) у великих мережах.

Порівняти пріоритети: висока швидкодія симетричних алгоритмів чи складність управління ключами.

Розглянути ризики використання застарілих алгоритмів (наприклад, DES) у сучасних інформаційних системах.

Тема 7. Асиметричні криптосистеми та інфраструктура відкритих ключів (PKI)

Завдання:

Визначити математичне підґрунтя асиметричної криптографії (на прикладі задачі факторизації великих чисел в RSA або дискретного логарифмування).

Скласти алгоритмічну схему безпечного обміну даними між двома суб'єктами з використанням відкритих та закритих ключів.

Проаналізувати структуру та призначення інфраструктури відкритих ключів (PKI), розібрати життєвий цикл цифрового сертифіката формату X.509.

Результат:

Здобувачі зможуть пояснювати механізми розв'язання проблеми розподілу

	ключів за допомогою асиметричної криптографії. Вміння описувати ролі центрів сертифікації (CA) та центрів реєстрації (RA) у побудові довірчого цифрового середовища. Формування навичок проєктування захищених каналів зв'язку з використанням криптографії з відкритим ключем. **Дискусія:** Обговорити "квантову загрозу" (Post-quantum cryptography) та її потенційний вплив на сучасні асиметричні криптосистеми. Розглянути наслідки компрометації кореневого центру сертифікації (Root CA) для національної безпеки. Порівняти ефективність алгоритму RSA та криптографії на еліптичних кривих (ECC) у мобільних системах зв'язку. **Тема 8. Криптографічні геш-функції та електронний підпис** **Завдання:** Проаналізувати базові властивості криптографічних геш-функцій (односторонність, стійкість до колізій першого та другого роду). Скласти алгоритмічну схему накладання та валідації кваліфікованого електронного підпису (КЕП). Розглянути практичний кейс порушення цілісності фінансового або управлінського документа та визначити, як застосування геш-функції з КЕП дозволяє виявити несанкціоновані зміни. **Результат:** Здобувачі зможуть обґрунтовувати необхідність використання геш-функцій для контролю цілісності даних. Вміння застосовувати концепцію електронного підпису для забезпечення автентичності та апелювальності (неможливості відмови від авторства). Формування навичок інтеграції механізмів КЕП у процеси юридично значущого електронного документообігу. **Дискусія:** Обговорити правовий статус кваліфікованого електронного підпису в Україні та його відповідність європейським стандартам (eIDAS). Порівняти наслідки використання вразливих алгоритмів хешування (MD5, SHA-1) у державних реєстрах. Розглянути межі відповідальності власника особистого ключа у разі його втрати або крадіжки. **Тема 9. Теорія автентифікації та управління доступом** **Завдання:** Класифікувати базові фактори автентифікації (знання, володіння, невід'ємна властивість/біометрія) та пояснити їхні вразливості. Скласти архітектурну схему суворої багатофакторної автентифікації (MFA) для доступу до критичної інформаційної інфраструктури. Проаналізувати методи атак на системи парольного захисту (Brute-force, Dictionary attack, Credential stuffing) та запропонувати політики парольного захисту для організації. **Результат:** Здобувачі зможуть чітко розмежовувати процеси ідентифікації, автентифікації та авторизації. Вміння проєктувати надійні процедури доступу, що мінімізують ризики несанкціонованого проникнення. Формування навичок аргументованого вибору методів автентифікації залежно

від моделі порушника та рівня критичності активів.

Дискусія:

Обговорити дилему використання біометрії: високий рівень зручності проти неможливості зміни скомпрометованих біометричних даних.

Порівняти ефективність апаратних токенів і програмних автентифікаторів (OTP-додатків) у корпоративному середовищі.

Розглянути конфлікт між жорсткими політиками безпеки (часта зміна складних паролів) та поведінкою користувачів (записування паролів на стікерах).

Тема 10. Стеганографія та методи приховування інформації

Завдання:

Визначити концептуальні відмінності між криптографією (приховування змісту) та стеганографією (приховування факту передачі повідомлення).

Розглянути базовий стеганографічний алгоритм (наприклад, метод найменшого значущого біта — LSB) на прикладі вбудовування текстового повідомлення у графічний або аудіофайл.

Проаналізувати кейс інсайдерського витоку даних за допомогою прихованих каналів та окреслити принципи роботи систем протидії витокам інформації (DLP).

Результат:

Здобувачі зможуть пояснювати сутність методів стеганографії та розуміти ризики існування прихованих каналів комунікації.

Вміння ідентифікувати цифрові контейнери, що потенційно можуть містити стеганограми.

Формування первинних аналітичних навичок у сфері стеганоаналізу та виявлення аномалій у мережевому трафіку.

Дискусія:

Обговорити використання методів стеганографії у шпигунській діяльності, кібертероризмі та розповсюдженні шкідливого програмного забезпечення (Stegware).

Розглянути складнощі виявлення стеганограм у сучасному зашифрованому мультимедійному трафіку.

Порівняти легітимне використання стеганографії (цифрові водяні знаки для захисту авторських прав) із деструктивним.

Тема 11. Технічний захист інформації: канали витоку та методи протидії

Завдання:

Проаналізувати фізичну природу утворення технічних каналів витоку інформації (акустичні, віброакустичні, оптичні канали та побічні електромагнітні випромінювання і наведення — ПЕМІН).

Скласти схему: джерело випромінювання — середовище поширення (канал витоку) — метод перехоплення — інженерно-технічний засіб захисту.

Розглянути практичний кейс обладнання виділеного приміщення для проведення конфіденційних переговорів (захист від закладних пристроїв та лазерних мікрофонів).

Результат:

Здобувачі зможуть класифікувати канали витоку мовної та видової інформації, а також інформації, що обробляється технічними засобами.

Вміння обґрунтовувати необхідність застосування методів екранування, зашумлення та організаційних режимних заходів.

Формування навичок первинного оцінювання захищеності об'єктів інформаційної діяльності.

Дискусія:

Обговорити економічну доцільність впровадження дороговартісних засобів

	технічного захисту (ТЗІ) у порівнянні з цінністю самої інформації. Порівняти ризики використання співробітниками власних мобільних пристроїв (BYOD) на об'єктах з підвищеними вимогами до безпеки. Розглянути межі ефективності технічного захисту, якщо не нейтралізовано загрозу інсайдерського витоку. **Тема 12. Мережева безпека та криптографічні протоколи зв'язку** **Завдання:** Визначити ключові вразливості стека протоколів TCP/IP та класифікувати типові мережеві атаки (Spoofing, MITM, DoS/DDoS). Скласти архітектурну схему захищеного периметра корпоративної мережі , визначивши місце та функції міжмережевих екранів (Firewall), систем виявлення/запобігання вторгненням (IDS/IPS) та демілітаризованої зони (DMZ). Проаналізувати кейс організації безпечного віддаленого доступу співробітників за допомогою віртуальної приватної мережі (VPN) на базі протоколів IPsec або OpenVPN. **Результат:** Здобувачі зможуть пояснювати теоретичні засади захисту інформації під час її передачі відкритими каналами зв'язку. Вміння розробляти базові топології захищених мереж та розуміти логіку маршрутизації і фільтрації трафіку. Формування навичок інтеграції криптографічних протоколів у мережеву інфраструктуру. **Дискусія:** Обговорити перехід від концепції «захищеного периметра» до парадигми «Нульової довіри» (Zero Trust Architecture). Порівняти вплив шифрування трафіку на забезпечення конфіденційності та на ускладнення роботи систем виявлення вторгнень (IDS). Розглянути проблеми використання анонімних мереж (наприклад, Tor) з погляду національної безпеки та правоохоронної діяльності. **Тема 13. Шкідливе програмне забезпечення: механізми дії та основи протидії** **Завдання:** Класифікувати сучасне шкідливе програмне забезпечення (віруси, хробаки, троянські програми, руткіти, програми-вимагачі) за способом поширення та деструктивним впливом. Скласти схему життєвого циклу зараження (Infection Lifecycle) та визначити на кожному етапі можливі методи виявлення (сигнатурний, евристичний, поведінковий аналіз). Проаналізувати кейс атаки вірусу-вимагача (Ransomware) на критичну інфраструктуру та запропонувати алгоритм локалізації загрози і відновлення даних. **Результат:** Здобувачі зможуть розпізнавати патерни поведінки шкідливого коду та розуміти механізми його закріплення в системі. Вміння формувати організаційні та технічні політики антивірусного захисту на рівні підприємства чи державної установи. Формування навичок планування резервного копіювання (Backup) як ультимативного заходу протидії програмам-вимагачам. **Дискусія:** Обговорити етичні та правові аспекти виплати викупу хакерам під час атак Ransomware (чи фінансує це подальшу злочинну діяльність?). Порівняти ефективність традиційних антивірусів (AV) та систем класу EDR

	(Endpoint Detection and Response) проти загроз нульового дня (Zero-day). Розглянути перспективи використання штучного інтелекту як для створення поліморфного шкідливого коду, так і для його виявлення. **Тема 14. Інформаційно-психологічні впливи та соціальна інженерія** **Завдання:** Проаналізувати психологічні тригери (страх, цікавість, авторитет, жадібність), які найчастіше експлуатуються в атаках соціальної інженерії. Скласти анатомію цільової фішингової атаки (Spear-phishing): збір інформації (OSINT) — формування претексту — доставка вектора атаки — експлуатація. Розробити базовий план тренінгу з підвищення обізнаності (Security Awareness) для нетехнічного персоналу державної установи. **Результат:** Здобувачі зможуть ідентифікувати ознаки маніпулятивного контенту та спроб соціальної інженерії в цифровому просторі. Вміння застосовувати методи верифікації інформації, перевірки автентичності відправників та виявлення дезінформації. Формування здатності мінімізувати вплив «людського фактора» на загальний рівень інформаційної безпеки. **Дискусія:** Обговорити межі етичності проведення навчальних фішингових розсилок власному персоналу з боку відділу безпеки. Порівняти ефективність технологічних засобів захисту (спам-фільтри, антифішинг) та рівня критичного мислення співробітників. Розглянути механізми захисту від атак з використанням технологій глибокого підроблення (Deepfake) та синтезу голосу керівництва (CEO Fraud). **Тема 15. Побудова комплексних систем захисту інформації (КСЗІ) та аудит безпеки** **Завдання:** Узагальнити правові, організаційні, інженерно-технічні та криптографічні заходи, інтегрувавши їх у єдину концепцію Комплексної системи захисту інформації (КСЗІ) . Скласти дорожню карту етапів створення КСЗІ (від обстеження інформаційного середовища до державної експертизи). Розглянути кейс проведення внутрішнього аудиту інформаційної безпеки: визначити об'єкти аудиту, критерії перевірки та формат звітності. **Результат:** Здобувачі зможуть інтегрувати знання з усіх модулів курсу в цілісну архітектуру управління інформаційною безпекою (ISMS). Вміння формулювати технічні завдання на створення КСЗІ та орієнтуватися у процедурах оцінки відповідності. Формування готовності до системного управління безпековими процесами та забезпечення їхньої безперервності. **Дискусія:** Обговорити проблему «паперової безпеки»: чи гарантує наявність атестата відповідності на КСЗІ реальну захищеність системи від сучасних кібератак? Порівняти вимоги національних нормативних документів (НД ТЗІ) із міжнародними стандартами серії ISO/IEC 27000. Розглянути життєвий цикл безпеки як безперервний процес вдосконалення, а не одноразовий проєкт.
Усього за навчальною дисципліною	

5.2 Завдання для самостійної роботи та критерії її оцінювання.

Під час вивчення курсу виконуються завдання для самостійних робіт до 19 тем.

Критерії оцінювання:

Змістовність, відповідність темі та вимогам оформлення – 1 бал.
Максимальна кількість балів за одиницю самостійної роботи – 1 бал.
Максимальна кількість балів за самостійну роботу по курсу – 19 балів.

Зміст завдань для самостійної роботи здобувача (СРЗ)

№ п/п	Зміст самостійної роботи здобувача вищої освіти	Форми контролю СРЗ
1	**Тема 1. Сутність та складові інформаційної безпеки: базові поняття та категорії** Завдання для самостійної роботи: Проаналізувати еволюцію концепцій інформаційної безпеки та підготувати огляд сучасних міжнародних стандартів (наприклад, ISO/IEC 27000). Скласти порівняльну таблицю властивостей інформації та можливих наслідків їх порушення для державних і комерційних структур.	Презентація результатів
2	Тема 2. Правові та організаційні засади захисту інформації в Україні Завдання для самостійної роботи: Дослідити міжнародний досвід правового регулювання кібербезпеки (на прикладі NIS2 Директиви ЄС або GDPR) та порівняти його з національним законодавством України. Визначити прогалини та напрями імплементації європейських норм.	Презентація результатів
3	Тема 3. Класифікація загроз, вразливостей та атак на інформаційні системи Завдання для самостійної роботи: Розглянути класифікацію загроз та тактик кібератак за матрицею MITRE ATT&CK. Скласти профіль типової цілеспрямованої атаки (APT) на об'єкт критичної інфраструктури з описом етапів (Cyber Kill Chain).	Презентація результатів
4	Тема 4. Формальні моделі політик інформаційної безпеки Завдання для самостійної роботи:	Презентація результатів

	Проаналізувати практичне застосування мандатної моделі доступу в сучасних операційних системах з підвищеним рівнем безпеки (наприклад, SELinux або Trusted Solaris). Підготувати короткий аналітичний висновок щодо доцільності їх використання в органах державної влади.	
5	Тема 5. Управління ризиками інформаційної безпеки: методологія та оцінювання Завдання для самостійної роботи: Провести якісну оцінку ризиків для гіпотетичного інформаційного активу (база даних громадян) з використанням методології NIST SP 800-30 або OCTAVE. Сформувати реєстр ризиків із визначенням пріоритетів реагування.	Презентація результатів
6	Тема 6. Теоретичні основи криптографії та симетричні криптосистеми Завдання для самостійної роботи: Дослідити історію стандартизації алгоритму AES та порівняти режими його роботи (ECB, CBC, GCM) щодо криптостійкості та продуктивності. Пояснити, чому режим ECB не рекомендований для шифрування великих обсягів даних.	Презентація результатів
7	Тема 7. Асиметричні криптосистеми та інфраструктура відкритих ключів (PKI) Завдання для самостійної роботи:Описати процес генерації ключів та формування сертифіката формату X.509. Проаналізувати загрози компрометації центрів сертифікації ключів та механізми відкликання сертифікатів (CRL, OCSP).	Презентація результатів
8	Тема 8. Криптографічні геш-функції та електронний підпис Завдання для самостійної роботи: Дослідити проблему колізій у геш-функціях на історичному прикладі алгоритмів MD5 та SHA-1. Обґрунтувати необхідність переходу на стандарти SHA-256 / SHA-3 у державних інформаційних системах.	Презентація результатів
9	Тема 9. Теорія автентифікації та управління доступом Завдання для самостійної роботи: Проаналізувати сучасні протоколи федеративної автентифікації та авторизації (OAuth 2.0, OpenID Connect,	Презентація результатів

	SAML) та пояснити логіку їх використання у хмарних середовищах і системах електронного урядування (на прикладі інтеграції з "Дія.Підпис").	
10	Тема 10. Стеганографія та методи приховування інформації Завдання для самостійної роботи: Розглянути методи протидії стеганографії (стеганоаналіз) у корпоративних мережах. Підготувати короткий огляд інструментів та підходів до виявлення прихованих каналів зв'язку та запобігання витокам даних (DLP-системи).	Презентація результатів
11	Тема 11. Технічний захист інформації: канали витоку та методи протидії Завдання для самостійної роботи: Здійснити огляд сучасних засобів виявлення закладних пристроїв (нелінійні локатори, аналізатори спектра, індикатори електромагнітного поля) та описати фізичні принципи їх роботи під час проведення пошукових заходів.	Презентація результатів
12	Тема 12. Мережева безпека та криптографічні протоколи зв'язку Завдання для самостійної роботи: Дослідити архітектуру «Мережі з нульовою довірою» (Zero Trust Network Access - ZTNA) як еволюційну альтернативу традиційним VPN-рішенням. Визначити переваги цієї концепції для захисту критичної інфраструктури.	Презентація результатів
13	Тема 13. Шкідливе програмне забезпечення: механізми дії та основи протидії Завдання для самостійної роботи: Проаналізувати еволюцію програм-вимагачів (Ransomware) та концепцію "Ransomware-as-a-Service" (RaaS). Дослідити роль криптовалют і тіньового сегмента інтернету (Dark Web) у фінансуванні кіберзлочинності.	Презентація результатів
14	Тема 14. Інформаційно-психологічні впливи та соціальна інженерія Завдання для самостійної роботи: Дослідити використання технологій штучного інтелекту та Deepfake у цільових фішингових атаках і схемах соціальної інженерії (наприклад, CEO Fraud).	Презентація результатів

	Окреслити ризики для корпоративної та національної безпеки й методи верифікації контенту.	
15	Тема 15. Побудова комплексних систем захисту інформації (КСЗІ) та аудит безпеки Завдання для самостійної роботи:Скласти типову структуру Політики інформаційної безпеки організації відповідно до вимог міжнародного стандарту ISO/IEC 27001. Визначити ключові розділи документа та розподіл відповідальності між підрозділами.	Презентація результатів

Реферат є формою самостійної роботи здобувача, метою якої є поглиблення та засвоєння знань з дисципліни «Теоретичні основи захисту інформації».

Тему реферату здобувач визначає за першою буквою за списком групи.

В окремих випадках здобувач може самостійно запропонувати та розробити тему реферату, попередньо обговоривши її з викладачем.

Структура, зміст і тема рефератів визначаються програмою курсу, що зумовлює таку послідовність роботи:

вибір теми;

розробка плану;

ознайомлення з рекомендованою літературою;

написання та оформлення роботи.

При написанні реферату та його оформленні варто керуватися такими критеріями:

обґрунтування вибраної теми;

опрацювання відповідної літератури;

наявність авторського розділу;

наявність списку використаних джерел.

Цитати та статистичні матеріали слід обов’язково супроводжувати посиланнями на джерела інформації, які мають бути відображені у списку використаних джерел. Посилання на інформаційні джерела необхідно подавати по тексту у квадратних дужках, наприклад [15, с. 74], 15 – це порядковий номер джерела у списку літератури, а 74 – сторінка із вказаного джерела.

Реферат має складатися із вступу (актуальність теми, предмет, об’єкт, мета, завдання), основної частини (визначення проблеми та послідовне її розкриття), висновків та списку використаних літературних джерел.

Загальний обсяг реферату – до 20 машинописних сторінки формату А4 з 14 шрифтом та інтервалом 1,5, із полями (верхнє/нижнє – 2 см, ліве – 3 см, праве –

1 см.).

Слід мати на увазі, що головною вимогою до реферату є розкриття суті питань, а не кількість сторінок.

Теми рефератів

Теми рефератів:

1 Еволюція концепцій інформаційної безпеки в умовах цифрової трансформації держави.
2 Національні інтереси України в інформаційній сфері: загрози та механізми реалізації.
3 Правовий режим інформації з обмеженим доступом: порівняльний аналіз законодавства.
4 Моделі управління доступом: від дискреційної до атрибутивно-орієнтованої.
5 Ризик-орієнтований підхід у побудові систем інформаційної безпеки.
6 Математичні засади криптографії: історія, сучасний стан та постквантові виклики.
7 Інфраструктура відкритих ключів як основа довірчих електронних послуг в Україні.
8 Кваліфікований електронний підпис: правові гарантії та криптографічні механізми.
9 Біометрична автентифікація: переваги, вразливості та питання захисту приватності.
10 Стеганографія та приховані канали передавання даних у сучасному кібершпигунстві.
11 Фізична безпека об'єктів інформаційної діяльності та протидія технічним розвідкам.
12 Побічні електромагнітні випромінювання і наведення як канал витоку інформації.
13 Концепція нульової довіри у забезпеченні безпеки корпоративних та державних мереж.
14 Віртуальні приватні мережі: архітектура, протоколи та застосування.
15 Еволюція шкідливого програмного забезпечення: від класичних вірусів до цілеспрямованих атак.
16 Програми-вимагачі як загроза національній безпеці та критичній інфраструктурі.
17 Соціальна інженерія у кіберпросторі: психологічні аспекти та методи протидії.
18 Фішингові атаки та використання технологій глибинних підробок: нові виклики для безпеки.
19 Стандартизація у сфері кібербезпеки: роль міжнародних стандартів управління безпекою.
20 Організаційні етапи побудови комплексної системи захисту інформації.
21 Аудит інформаційної безпеки: методологія проведення та критерії оцінювання.
22 Інформаційна безпека систем електронного урядування та державних реєстрів.
23 Захист персональних даних великих обсягів: правові та технічні рішення.
24 Застосування технології розподілених реєстрів для забезпечення цілісності та автентичності інформації.
25 Системи запобігання витоку даних як інструмент боротьби з інсайдерськими загрозами.
26 Глобальні кіберзагрози та їх вплив на міжнародну та національну безпеку.
27 Роль кіберрозвідки у попередженні цілеспрямованих кібератак.
28 Конфіденційність у соціальних мережах: загрози розкриття особистої інформації розвідувальними методами.

29 Захист інформації в хмарних середовищах: моделі відповідальності та спеціалізовані інструменти.
30 Проблема атрибуції кібератак у міжнародному праві та безпековому середовищі.
31 Захист критичної інформаційної інфраструктури в умовах гібридної війни.
32 Інформаційний тероризм: сутність, загрози та шляхи організаційно-технічної протидії.
33 Штучний інтелект у кібербезпеці: як інструмент захисту та зброя атаки.
34 Механізми забезпечення безпеки Інтернету речей на державному та корпоративному рівнях.
35 Правові та етичні аспекти діяльності фахівців з пошуку вразливостей.
36 Управління інцидентами інформаційної безпеки: алгоритми реагування.
37 Безпека мобільних пристроїв: загрози, вразливості та політики управління корпоративними пристроями.
38 Цифрова криміналістика: методи збору та аналізу електронних доказів.
39 Моделювання загроз при розробці захищеного програмного забезпечення.
40 Атаки на ланцюги постачання: наслідки та методи мінімізації ризиків.
41 Європейські директиви з кібербезпеки: імплементація вимог в національне законодавство України.
42 Проблема управління паролями: від традиційних політик до безпарольної автентифікації.
43 Захист інформації в бездротових мережах: стандарти, протоколи шифрування та вразливості.
44 Соціальна інженерія через канали телефонного та текстового зв'язку.
45 Криптографічні протоколи: еволюція, вразливості та сучасний стан захисту вебтрафіку.
46 Використання технологій цифрових пасток для виявлення кібершпигунства.
47 Кібергігієна як ключовий елемент формування безпекової культури персоналу.
48 Технічні та організаційні аспекти резервного копіювання даних та аварійного відновлення систем.
49 Інформаційні операції в кіберпросторі: психологічний вплив та маніпулювання суспільною свідомістю.
50 Роль державних органів спеціального зв'язку у забезпеченні національної кібербезпеки.

5.3 Форми проведення модульного контролю та критерії оцінювання

Проведення модульного контролю з дисципліни «Теоретичні основи захисту інформації».

здійснюється у формі тестового завдання.

Тестові завдання стосуються термінології, функцій, принципів та особливостей адміністративного судочинства.

Запитання формулюються з урахуванням принципів:

Лаконічність: чіткі та стислі формулювання.

Завершеність: відповіді охоплюють всі аспекти запитання.

Гомогенність: правильні та неправильні варіанти відповіді логічно та граматично подібні.

Вибірковість: питання стосуються суттєвих аспектів вивченого матеріалу.

Завдання передбачають вибір одного правильного варіанта з трьох запропонованих.

Кожне тестове завдання оцінюється в **1 бал**. (**1 бал** – відповідь правильна; **0** балів – відповідь неправильна).

Загальна максимальна можлива кількість балів за модульну контрольну роботу - 15 балів.

Час на виконання.

На виконання всього контрольного завдання відводиться **30 хвилин.**

Мінімальний поріг.

Для успішного складання модульного контролю здобувач повинен набрати не менше 10 балів (60% від максимальної кількості).

Загальні критерії оцінювання тестових завдань:

Бали	Процент виконання	Результат
14-15	-100%	Зараховано
13	83-90%	
12	76-82%	
11	60-75%	
10	60-67%	
0-9	< 60%	Не зараховано

5.4 Індивідуальні завдання та критерії їх оцінювання

До додаткових (індивідуальних) видів навчальної діяльності відносять участь здобувачів у роботі наукових конференцій, наукових гуртків здобувачів і проблемних груп, підготовці публікацій, участь у Всеукраїнських олімпіадах і конкурсах та Міжнародних конкурсах тощо понад обсяги завдань, які встановлені відповідною робочою програмою навчальної дисципліни.

За рішенням кафедри здобувачам освіти, які брали участь у науково-дослідній роботі та виконували певні види додаткових (індивідуальних) видів навчальної діяльності, можуть присуджуватися заохочувальні (бонусні) бали за визначену освітню компоненту.

Також, заохочувальні бали можуть нараховуватися, якщо здобувач освіти, наприклад, виконав і захистив певні види робіт, відвідував всі лекції, семінарські й практичні заняття, має власний рукописний конспект лекцій та опрацьований додатковий навчальний матеріал, немає пропусків занять без поважних причин, відвідував додаткові консультації за участі лектора тощо.

Сума заохочувальних балів враховується при виставленні підсумкових балів в заліково-екзаменаційну відомість (але не більше **89 балів** в загальному підсумку) і може бути автоматично зарахована при виставленні підсумкової семестрової оцінки з відповідної освітньої компоненти.

Заохочувальні бали не є нормативними і не входять до таблиці розподілу балів, які отримують здобувачі вищої освіти та основної шкали системи оцінювання.

Один захід може бути підставою для виставлення заохочувальних балів лише за однією найбільш релевантною освітньою компонентою.

5.5 Форми проведення семестрового контролю та критерії оцінювання

Екзамен. Відбувається згідно з «Положення про оцінювання навчальних досягнень здобувачів вищої освіти у ПрАТ ВНЗ МАУП» https://maup.com.ua/assets/files/yakist/studcentr/polozhennya-pro-sistemu-ocinyuvannya-rezultativ-navchannya-zdobuvachiv-vishhoi-osviti.pdf

Орієнтовний перелік питань для комплексного контролю:

1 Сутність та складові інформаційної безпеки держави.
2 Базові властивості інформації як об'єкта захисту.
3 Принципи забезпечення конфіденційності інформації.
4 Принципи забезпечення цілісності інформації.
5 Принципи забезпечення доступності інформації.
6 Додаткові властивості інформаційної безпеки: автентичність та апелювальність.
7 Правові засади захисту інформації в Україні.
8 Нормативно-правове регулювання захисту державної таємниці.
9 Нормативно-правове регулювання захисту комерційної таємниці.
10 Правові механізми захисту персональних даних.
11 Суб'єкти державного управління у сфері кібербезпеки України.
12 Класифікація загроз інформаційній безпеці за джерелом походження.
13 Класифікація загроз інформаційній безпеці за способом реалізації.
14 Поняття вразливості інформаційної системи та їх класифікація.
15 Архітектурні та програмні вразливості інформаційних систем.
16 Вектори кібератак та поняття поверхні атаки.
17 Життєвий цикл цілеспрямованої кібератаки.
18 Поняття політики інформаційної безпеки організації.
19 Дискреційна модель управління доступом.
20 Мандатна модель управління доступом.
21 Рольова модель управління доступом.
22 Атрибутивно-орієнтована модель управління доступом.
23 Формальна модель безпеки Белла-ЛаПадули.
24 Формальна модель безпеки Біба.
25 Формальна модель безпеки Кларка-Вілсона.
26 Управління ризиками інформаційної безпеки: основні поняття.

27 Методика ідентифікації та оцінювання інформаційних активів.
28 Якісні та кількісні методи оцінювання інформаційних ризиків.
29 Стратегії обробки ризиків інформаційної безпеки.
30 Матриця ризиків та її використання у плануванні безпеки.
31 Теоретичні основи криптографічного захисту інформації.
32 Вимоги Шеннона до криптографічних систем: розсіювання та перемішування.
33 Принципи функціонування симетричних криптосистем.
34 Потокові та блокові алгоритми симетричного шифрування.
35 Проблема розподілу ключів у симетричній криптографії.
36 Математичні основи асиметричної криптографії.
37 Принципи функціонування асиметричних криптосистем.
38 Алгоритми шифрування на основі факторизації великих чисел.
39 Алгоритми шифрування на основі еліптичних кривих.
40 Архітектура та компоненти інфраструктури відкритих ключів.
41 Роль центрів сертифікації у забезпеченні довірчих послуг.
42 Життєвий цикл цифрового сертифіката відкритого ключа.
43 Криптографічні геш-функції: визначення та базові властивості.
44 Стійкість геш-функцій до колізій першого та другого роду.
45 Застосування геш-функцій для контролю цілісності повідомлень.
46 Теоретичні засади створення електронного цифрового підпису.
47 Процедура перевірки валідності кваліфікованого електронного підпису.
48 Ідентифікація, автентифікація та авторизація суб'єктів в інформаційних системах.
49 Класифікація факторів автентифікації користувачів.
50 Системи суворої багатофакторної автентифікації.
51 Вразливості парольних систем захисту та методи атак на них.
52 Біометрична автентифікація: методи, переваги та недоліки.
53 Протоколи єдиного входу в корпоративних системах.
54 Сутність стеганографії та її відмінність від криптографії.
55 Методи вбудовування прихованої інформації у цифрові зображення.
56 Методи вбудовування прихованої інформації в аудіофайли.
57 Стеганоаналіз та виявлення прихованих каналів комунікації.
58 Використання цифрових водяних знаків для захисту авторських прав.
59 Загрози використання стеганографії у розповсюдженні шкідливого коду.
60 Управління ключовою інформацією: генерація, зберігання та знищення ключів.
61 Фізична природа утворення технічних каналів витоку інформації.
62 Акустичні та віброакустичні канали витоку мовної інформації.
63 Оптичні канали витоку видової інформації.
64 Побічні електромагнітні випромінювання і наведення як канал витоку.
65 Інженерно-технічні методи захисту акустичної інформації.
66 Екранування та зашумлення як засоби протидії витоку інформації.
67 Організація захисту інформації у виділених приміщеннях.
68 Архітектура мережевої безпеки та концепція захищеного периметра.
69 Вразливості стека мережевих протоколів передавання даних.
70 Типові мережеві атаки: підміна адрес, перехоплення трафіку, відмова в обслуговуванні.

71 Принципи функціонування та класифікація міжмережевих екранів.
72 Системи виявлення та запобігання мережевим вторгненням.
73 Технології віртуальних приватних мереж та захист віддаленого доступу.
74 Мережі з нульовою довірою: концептуальні засади та архітектура.
75 Класифікація сучасного шкідливого програмного забезпечення.
76 Життєвий цикл комп'ютерних вірусів та мережевих хробаків.
77 Програми-вимагачі: механізми дії та стратегії протидії.
78 Методи виявлення шкідливого коду: сигнатурний, евристичний, поведінковий.
79 Соціальна інженерія як загроза інформаційній безпеці організації.
80 Психологічні маніпуляції у кіберпросторі та їх інструментарій.
81 Фішингові атаки: різновиди, етапи реалізації та способи захисту.
82 Захист від цілеспрямованих інформаційно-психологічних впливів.
83 Поняття та структура комплексної системи захисту інформації.
84 Організаційні етапи створення комплексної системи захисту інформації.
85 Державна експертиза та сертифікація комплексних систем захисту.
86 Аудит інформаційної безпеки: види, цілі та методологія проведення.
87 Міжнародні стандарти управління інформаційною безпекою серії двадцять сім тисяч.
88 Системи запобігання витоку даних та контроль дій користувачів.
89 Забезпечення безперервності бізнес-процесів та аварійне відновлення систем.
90 Управління інцидентами інформаційної безпеки: виявлення, реагування, розслідування.

Шкала відповідності оцінок

Сума балів за всі види навчальної діяльності	**Оцінка ECT8**	**Оцінка за національною шкалою**	
		для екзамену, курсового проекту (роботи),	**для заліку**
90 – 100	A	відмінно	Зараховано
82-89	B	добре	
75-81	C		
68-74	D	задовільно	
60-67	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного
0-34	F	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

6. Політика курсу:

Курс Теоретичні основи захисту інформації» передбачає засвоєння та дотримання принципів етики та академічної доброчесності згідно Кодексу академічної доброчесності МАУП та Положення про запобігання та виявлення плагіату в наукових та академічних текстах у ПрАТ ВНЗ МАУП, зокрема орієнтації на запобігання плагіату у будь-яких його проявах: всі роботи, доповіді, есе, реферати та презентації мають бути оригінальними та авторськими, не переобтяженими цитатами, що мають супроводжуватися посиланнями на першоджерела. Порушеннями академічної доброчесності вважаються: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво, необ'єктивне оцінювання.

Оцінювання здобувача освіти орієнтовано на отримання балів за активність на семінарських (практичних) заняттях, а також виконання завдань для самостійної роботи.

Відпрацювання семінарського заняття може здійснюватися у формі опитування, тестування, виконання практичного завдання, розв'язання задачі з відповідної теми.

В кінці вивчення курсу проводиться модульна контрольна робота 1. Результат модульної контрольної роботи для здобувача, який не з'явився на контрольні заходи, є нульовим. У такому разі, здобувач має можливість повторно виконати модульну контрольну роботи.

Не допустимо: пропуск занять без поважних причин; запізнення на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття (за винятком дозволу викладача при зверненні до текстів нормативно-правових актів); списування та плагіат.

Рекомендовані джерела (література):

Базова література:

1 Верховна Рада України. (1992). *Про інформацію: Закон України від 02.10.1992 № 2657-XII*. https://zakon.rada.gov.ua/laws/show/2657-12

2 Верховна Рада України. (1994). *Про державну таємницю: Закон України від 21.01.1994 № 3855-XII*. https://zakon.rada.gov.ua/laws/show/3855-12

3 Верховна Рада України. (1994). *Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР*. https://zakon.rada.gov.ua/laws/show/80/94-вр

4 Верховна Рада України. (2010). *Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI*. https://zakon.rada.gov.ua/laws/show/2297-17

5 Верховна Рада України. (2017). *Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII*. https://zakon.rada.gov.ua/laws/show/2163-19

6 Верховна Рада України. (2018). *Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII*. https://zakon.rada.gov.ua/laws/show/2469-19

7 Богуш, В. М., & Юдін, О. К. (2005). *Інформаційна безпека держави*. МК-Прес.

8 Гавловський, В. (2000). Інформаційна безпека: захист інформації в автоматизованих системах. У *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні* (с. 50-52).

9 Костюк, Ю. В., Складанний, П. М., Гулак, Г. М., Бебешко, Б. Т., Хорольська, К. В., & Рзаєва, С. Л. (2025). *Системи захисту інформації*. Київський столичний університет імені Бориса Грінченка.

Допоміжна література:

1 Кавун, С. В. (2008). *Інформаційна безпека* (Ч. 2). Харківський національний економічний університет.

2 Ковтун, С. В. (2009). *Інформаційна безпека*. ХНЕУ.

3 Стичинська, А. (2021). Теоретичні основи політики інформаційної безпеки. *Науково-теоретичний альманах Грані*, 24(6), 100-108. https://doi.org/10.15421/172164

Інформаційні ресурси:

4 Офіційний вебпортал парламенту України. Законодавство України. https://zakon.rada.gov.ua

5 Офіційне інтернет-представництво Президента України. https://www.president.gov.ua

6 Офіційний сайт Державної служби спеціального зв’язку та захисту інформації України. https://cip.gov.ua

7 Національна бібліотека України імені В. І. Вернадського. Електронний каталог. http://www.nbuv.gov.ua