ПрАТ "ВНЗ "МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ"

Навчально-науковий інститут права та безпеки імені князя Володимира Великого

МАУП

Кафедра національної безпеки

Затверджую:
Директор Інституту безпеки

Сергій ЛИСЕНКО

"____" _____ 2025 р.

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

Іван СЕРВЕНЬКИЙ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Теорія безпеки організацій»

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

Розробник силабусу навчальної дисципліни:

Лисенко Сергій Олексійович - доктор юридичних наук, доктор наук з державного управління, професор, завідувач кафедри інформаційної безпеки

(підпис)

Викладач:

Лисенко Сергій Олексійович - доктор юридичних наук, доктор наук з державного управління, професор, завідувач кафедри інформаційної безпеки

(підпис)

Силабус розглянуто на засіданні кафедри національної безпеки

Протокол №1 від «07» 08 2025р.

Загальна інформація про навчальну дисципліну

Назва навчальної дисципліни	**Теорія безпеки організацій**
Шифр та назва спеціальності	К3 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Рівень вищої освіти	перший (бакалаврський) рівень
Статус дисципліни	обов'язкова
Кількість кредитів і годин	**5 кредита/150 год** Лекції : **26** Семінарські заняття: **26** Самостійна робота студентів: **98**
Терміни вивчення дисципліни	І семестр
Мова викладання	українська
Вид підсумкового контролю	**екзамен**
Сторінка дисципліни на сайті	https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-2025/b/osnovi-operativno-rozshukovoi-diyalnosti.pdf

Загальна інформація про викладача. Контактна інформація.

Лисенко Сергій Олексійович	
Науковий ступінь	Доктор наук з державного управління, Доктор юридичних наук
Вчене звання	професор
Посада	Завідувач кафедри
Дисципліни, які викладає НПП	Теорія безпеки організацій
Напрями наукових досліджень	Освіта, безпека освіти
Посилання на реєстри ідентифікаторів для науковців	ORCID: https://orcid.org/0000-0002-7050-5536 Google Scholar: https://scholar.google.com.ua/citations?hl=uk&user=SKvoZKIAAAAJ
Контактна інформація викладача:	
E-mail:	crimeconsult@ukr.net
Контактний тел.	+380507417375
Телефон кафедри	
Портфоліо викладача на сайті кафедри/Інституту/Академії	https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-2025/b/teoriya-bezpeki-organizacij.pdf

1.1 Анотація курсу.

Курс «Теорія безпеки організацій» є обов'язковою дисципліною для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю К3 Національна безпека (за окремими сферами забезпечення і видами діяльності). Курс вивчається обсягом 5 кредитів ECTS (лекції – 26 год., семінарські заняття – 26 год., самостійна робота студентів – 98 год.) та спрямований на формування у здобувачів цілісного розуміння безпеки організації як керованої системи, що охоплює виявлення загроз, оцінювання ризиків, планування та реалізацію заходів захисту, а також побудову й підтримання системи безпеки на рівні політик, процедур і контролю. Дисципліна розглядає взаємозв'язок внутрішніх і зовнішніх факторів ризику, логіку управління безпековими ситуаціями та практичні підходи до фізичної, інформаційної, кадрової та економічної складових безпеки організації.

1.2 Предмет вивчення курсу

Предметом вивчення навчальної дисципліни є теоретичні та прикладні засади формування системи безпеки організацій, класифікація загроз і вразливостей, методи аналізу ризиків, організаційні механізми управління безпекою, внутрішні регламенти та процедури контролю, а також підходи до забезпечення стійкості організації в умовах криз, конфліктів і комбінованих (гібридних) впливів. Опрацювання змісту дисципліни спрямоване на розвиток умінь систематизувати інформацію про ризики, формувати аналітичні висновки, готувати обґрунтовані управлінські рішення та узгоджувати заходи безпеки з цілями організації й вимогами доброчесності.

1.3 Метою викладання навчальної дисципліни «Теорія безпеки організацій» є формування у здобувачів комплексних знань і практичних навичок щодо побудови та управління системою безпеки організації, здатності аналізувати потенційні загрози, оцінювати ризики, планувати й реалізовувати заходи захисту та забезпечувати стійкість організаційних процесів. Вивчення курсу має забезпечити розуміння логіки безпекового менеджменту як циклу «ідентифікація загроз — оцінка ризиків — план заходів — реалізація — контроль — удосконалення», що дозволяє підтримувати результативність і керованість організації в умовах невизначеності.

1.4 Завдання

засвоєння базових понять і категорій теорії безпеки організацій та системного бачення безпеки як управлінської функції; формування навичок ідентифікації загроз, вразливостей і критичних процесів організації та оцінювання рівня ризику; опанування підходів до проектування системи безпеки (політики, процедури, контрольні механізми, розподіл відповідальності); розвиток умінь готувати аналітичні матеріали й управлінські рішення щодо запобігання інцидентам, мінімізації збитків і відновлення функціонування; формування здатності інтегрувати фізичну, інформаційну, кадрову та економічну складові безпеки в єдину модель, що підвищує стійкість організації та її спроможність діяти в кризових умовах.

1.5 Пререквізити і постреквізити навчальної дисципліни:

Пререквізити:

Основи оперативно-розшукової діяльності. Навчальна дисципліна «Теорія

безпеки організацій» спирається на результати опанування курсу «Основи оперативно-розшукової діяльності», оскільки потребує сформованих умінь працювати з інформацією про загрози, оцінювати її достовірність, здійснювати первинну верифікацію та формувати аналітичні висновки для управлінських рішень. Логіка ОРД щодо документування обставин, процедурної дисципліни та недопущення недоброчесних практик підсилює здатність будувати систему безпеки організації на основі контрольованих процесів, де ризики і вразливості фіксуються, аналізуються і перетворюються на план заходів. Додатково засвоєння підходів до розмежування оперативної інформації та доказів сприяє коректному управлінню інцидентами в організації, коли якість матеріалів і підстави рішень можуть бути предметом перевірки, а відповідальність і законність дій мають ключове значення.

Постреквізити:

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

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

Дисципліна «Теорія безпеки організацій» формує цілісне розуміння предметної області безпекового менеджменту на рівні організації, де безпека розглядається як керована система політик, процедур, ролей і контролю. Засвоєння понятійного апарату загроз, ризиків, вразливостей і стійкості дозволяє здобувачам усвідомлювати професійну діяльність у сфері безпеки як процес планування, реалізації та оцінювання заходів, а не як набір реакцій на інциденти.

СК1. Здатність осмислювати та застосовувати знання у сфері національної безпеки, її концепції, цінностей та досягнень.

Курс забезпечує прикладне осмислення концепцій національної безпеки через їх перенесення на рівень організації як об’єкта безпеки, де цінності законності, доброчесності, підзвітності та захисту прав людини проявляються у внутрішніх політиках і стандартах. Здобувачі вчаться застосовувати концептуальні засади національної безпеки для побудови організаційних механізмів захисту та стійкості в реальних умовах.

СК3. Здатність демонструвати та використовувати знання з теорії національної безпеки, виявляти та аналізувати загрози економічній, політичній, інформаційній, воєнній, соціальній та іншим напрямкам життєдіяльності держави.

Дисципліна розширює здатність аналізувати загрози через системну логіку «зовнішні і внутрішні фактори → вразливості → ризики → наслідки», яка застосовується як до держави, так і до організацій у різних секторах. Опрацювання міжсферних загроз формує навички визначати, як економічні, інформаційні чи соціальні впливи трансформуються у ризики для організації, її ресурсів, процесів і репутації.

СК13. Здатність систематизувати та оцінювати інформацію про людські ресурси об’єктів національної безпеки, враховувати антропогенний чинник

впливу на рівень безпеки та застосовувати основні методи та механізми кадрової безпеки в системі національної безпеки України.

Курс підсилює розуміння антропогенного чинника як одного з ключових джерел організаційних ризиків і вразливостей, оскільки розглядає кадрову складову безпеки у зв'язку з доброчесністю, дисципліною, доступом до інформації, помилками й конфліктами. Здобувачі набувають здатності систематизувати дані про персонал, визначати ризикові індикатори та проектувати механізми кадрової безпеки як частину загальної системи захисту організації.

1.7 Очікувані результати навчання (ПРН)

ПРН7. Розуміти і використовувати понятійно-категоріальний апарат теорії національної безпеки щодо структури національної безпеки, об'єктів, суб'єктів та принципів забезпечення національної безпеки.

Дисципліна закріплює понятійний апарат через практичне застосування категорій «об'єкт безпеки», «суб'єкт забезпечення», «загроза», «вразливість», «ризик», «стійкість», «контроль», що дозволяє описувати організацію як об'єкт у структурі національної безпеки. Здобувачі вчаться коректно використовувати ці поняття для аналізу ситуацій та побудови моделей забезпечення безпеки.

ПРН10. Моделювати окремі процеси забезпечення національної безпеки, у державній та недержавній складових, включаючи повноваження і функції суб'єктів, їх основні завдання, контроль за здійсненням ними заходів забезпечення національної безпеки.

Курс формує здатність моделювати організаційні процеси безпеки як цикли управління з визначеними ролями, повноваженнями, контрольними точками та показниками ефективності. Це дозволяє проектувати взаємодію суб'єктів безпеки всередині організації та узгоджувати її з зовнішніми вимогами і контролем, що забезпечує керованість і підзвітність.

ПРН11. Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності.

Дисципліна розвиває прикладні навички оцінювання стану безпеки через аналіз ризиків і вразливостей у конкретних видах діяльності організацій, що впливає і на безпеку персоналу, і на суспільні процеси. Здобувачі вчаться визначати критерії безпечного стану, оцінювати рівень загроз і пріоритети заходів для підтримання стійкості.

ПРН12. Планувати та організовувати професійну діяльність в окремих сферах забезпечення національної безпеки та видах діяльності для забезпечення безпеки окремої сфери і виду діяльності держави та організації.

Курс забезпечує здатність планувати безпекову діяльність через побудову політик, процедур і планів заходів, визначення відповідальних осіб, ресурсів і строків, а також організацію контролю виконання. Такий підхід формує управлінську дисципліну і дозволяє переводити аналіз загроз у практичні рішення, що забезпечують безпеку діяльності організації.

ПРН13. Аналізувати та упорядковувати основні властивості об'єктів безпеки окремих сфер забезпечення національної безпеки і видів діяльності та

здійснювати класифікацію загроз об’єктам безпеки, класифікацію та ранжирування джерел загроз і вразливостей безпеки.

Дисципліна формує здатність класифікувати загрози і вразливості за джерелами, механізмами впливу і наслідками, а також ранжирувати їх за ризиком для критичних процесів організації. Це підтримує аналітичну основу управління безпекою, коли заходи плануються не хаотично, а відповідно до пріоритетів і реальної критичності.

ПРН15. Характеризувати складові системи забезпечення безпеки за окремою сферою забезпечення національної безпеки і видом діяльності, включаючи повноваження і функції суб’єктів, їх основні завдання, контроль за здійсненням ними заходів забезпечення національної безпеки.

Курс дозволяє описувати систему безпеки організації як набір взаємопов’язаних складових (кадрова, інформаційна, фізична, економічна, організаційна), де кожна має суб’єктів, завдання та механізми контролю. Здобувачі вчаться визначати функції відповідальних підрозділів і посад, встановлювати контрольні механізми та пояснювати, як саме забезпечується стійкість системи в умовах загроз.

2. Зміст навчальної дисципліни

ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ ОРГАНІЗАЦІЙ: ПОНЯТТЯ, ПІДХОДИ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, РИЗИКИ

Тема 1. Теорія безпеки організацій: предмет, категорії, принципи та місце в системі національної безпеки

Тема формує понятійно-категоріальний апарат дисципліни та пояснює, чому організація виступає об’єктом безпеки зі своїми ресурсами, процесами, цілями і обмеженнями. Розкривається логіка безпеки як управлінської функції, де ключовими є законність, доброчесність, підзвітність, стійкість і превентивність, а також показується зв’язок організаційної безпеки з ширшими цілями національної безпеки.

Тема 2. Організація як об’єкт безпеки: структура, процеси, критичні функції, ресурси і точки вразливості

Тема забезпечує розуміння того, що безпека залежить від ідентифікації критичних процесів і ресурсів, без яких організація не може виконувати свої функції. Формується здатність виділяти ключові активи, визначати їх властивості та вразливості, а також оцінювати, як порушення окремих елементів призводить до каскадних наслідків.

Тема 3. Загрози і вразливості: класифікація, джерела, механізми впливу, індикатори ризику

Тема розкриває типологію загроз (внутрішні/зовнішні, навмисні/ненавмисні, фізичні/інформаційні/кадрові/економічні) і логіку їх перетворення у ризики через наявні вразливості. Окремо пояснюється, як визначаються індикатори загроз, як оцінюється їх актуальність та як вибудовується пріоритезація реагування.

Тема 4. Ризик-орієнтований підхід: оцінювання ризиків, матриці, сценарії, прийнятність ризику та пріоритети заходів

Тема формує практичне розуміння ризику як поєднання ймовірності та наслідків і навчає застосовувати інструменти оцінювання для вибору пріоритетів. Розглядаються підходи до сценарного аналізу, визначення прийнятності ризику, а також логіка переходу від оцінки до управлінських рішень, де важлива доказовість і обґрунтованість.

Тема 5. Антропогенний чинник у безпеці організацій: кадрові ризики, дисципліна, доброчесність, помилки і конфлікти

Тема показує роль людського фактора як джерела як загроз, так і спроможностей організації, розкриває кадрові ризики (недоброчесність, конфлікт інтересів, витоки, вигорання, саботаж, помилки), а також механізми їх профілактики через кадрову політику, контроль доступу, навчання, мотивацію і культуру відповідальності.

Тема 6. Інформаційний простір організації та інформаційні ризики: дезінформація, маніпуляції, витоки, довіра до даних

Тема розкриває, як інформаційні впливи та спотворення даних змінюють управлінські рішення, підвищують ризики помилок і створюють репутаційні загрози. Формується здатність оцінювати достовірність джерел, будувати внутрішні процедури верифікації інформації, підтримувати цілісність управлінських даних і мінімізувати ризики витоків.

ЗМІСТОВИЙ МОДУЛЬ 2. СИСТЕМА БЕЗПЕКИ ОРГАНІЗАЦІЇ: ПОЛІТИКИ, ПРОЦЕДУРИ, КОНТРОЛЬ, СТІЙКІСТЬ ТА ВІДНОВЛЕННЯ

Тема 7. Архітектура системи безпеки організації: суб’єкти, функції, розподіл відповідальності, контроль і підзвітність

Тема формує розуміння структури системи безпеки як мережі ролей і повноважень, де визначаються відповідальні підрозділи, порядок взаємодії, контрольні точки і механізми підзвітності. Пояснюється, як система запобігає хаотичним діям і чому узгодженість функцій підвищує керованість і стійкість.

Тема 8. Політики і процедури безпеки: стандарти, регламенти, інструкції, документування і дисципліна виконання

Тема розкриває значення політик як «правил гри» в організації і процедур як практичних механізмів реалізації цих правил. Розглядаються вимоги до якості документів (однозначність, контрольованість, доказовість), способи забезпечення дисципліни виконання та роль комунікації у впровадженні стандартів безпеки.

Тема 9. Моніторинг, аудит і показники безпеки: оцінка ефективності заходів, контроль змін і безперервне удосконалення

Тема формує здатність оцінювати безпеку не декларативно, а через показники, моніторинг і перевірку виконання заходів. Пояснюються різниця між процесними і результатними індикаторами, логіка аудиту, контроль змін, аналіз інцидентів та цикл удосконалення, який підтримує актуальність системи безпеки.

Тема 10. Управління інцидентами: реагування, документування, розслідування причин і профілактичні заходи

Тема забезпечує розуміння інциденту як управлінської події, що потребує швидкого реагування, коректної фіксації обставин, аналізу причин і плану профілактики. Розглядається логіка встановлення безпосередніх і системних

причин, контроль виконання коригувальних дій і забезпечення підзвітності без підміни аналізу «пошуком винного».

Тема 11. Стійкість і безперервність діяльності: кризове управління, резерви, відновлення функцій, сценарне планування

Тема розкриває підходи до забезпечення стійкості організації через планування резервів, визначення критичних функцій, сценарне моделювання криз і підготовку планів відновлення. Формується здатність будувати організаційну стійкість як систему, що зменшує наслідки загроз і скорочує час відновлення.

Тема 12. Інтеграція складових безпеки: фізична, інформаційна, кадрова, економічна безпека як єдина модель управління ризиками

Тема узагальнює міжсферний характер безпеки організації і показує, як різні складові взаємопов'язані, впливають одна на одну і потребують єдиного підходу до ризик-менеджменту. Акцент робиться на інтегрованому плануванні заходів, узгодженості відповідальності та управлінських рішень, що підвищує ефективність системи безпеки в умовах комбінованих загроз.

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 «Вступ до спеціальності «Національна безпека» 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

2-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. Теорія безпеки організацій: предмет, категорії, принципи та місце в системі національної безпеки** Завдання: • Визначити ключові категорії: об’єкт безпеки, загроза, вразливість, ризик, стійкість, контроль, підзвітність, доброчесність. • Розібрати ситуацію «організація як об’єкт безпеки» і описати, чому безпека є управлінською функцією. • Скласти коротку схему циклу безпекового менеджменту: загрози → ризики → план → виконання → контроль → удосконалення. Очікуваний результат: • Вміння коректно використовувати понятійний апарат і пояснювати

	логіку управління безпекою. • Здатність показувати зв’язок між організаційною та національною безпекою. Дискусія: • Чи може «формальна система» безпеки бути ефективною без культури відповідальності? • Де межа між ризиком, який приймають, і ризиком, який не можна прийняти? **Тема 2. Організація як об’єкт безпеки: структура, процеси, критичні функції, ресурси і точки вразливості** Завдання: • Визначити 5–7 критичних процесів організації (на вибір) і пояснити, чому вони критичні. • Побудувати просту карту активів: люди, інформація, майно, процеси, репутація. • Виявити точки вразливості та описати можливі наслідки порушення критичної функції. Очікуваний результат: • Вміння виділяти критичні функції й активи та описувати їх уразливості. • Здатність переходити від структури організації до безпекових висновків. Дискусія: • Що важливіше в кризі: захист активів чи збереження безперервності процесів? • Чи завжди найбільший актив — люди, і як це проявляється в ризиках? **Тема 3. Загрози і вразливості: класифікація, джерела, механізми впливу, індикатори ризику** Завдання: • Класифікувати загрози для обраної організації: внутрішні/зовнішні, навмисні/ненавмисні, за сферами (кадрові, інформаційні, економічні,

	фізичні). • Визначити 10 індикаторів ризику (ознаки, що загроза активується). • Розібрати 2 кейси та показати ланцюг: загроза → вразливість → інцидент → наслідок. Очікуваний результат: • Вміння формувати класифікацію загроз і виділяти індикатори ризику. • Здатність пояснювати механізм впливу загроз через вразливості. Дискусія: • Чи може загроза існувати без вразливості? • Коли індикатори ризику стають «хибною тривогою»? **Тема 4. Ризик-орієнтований підхід: оцінювання ризиків, матриці, сценарії, прийнятність ризику та пріоритети заходів** Завдання: • Заповнити матрицю ризиків для 6 загроз: ймовірність × наслідки → рівень ризику → пріоритет. • Скласти 2 сценарії розвитку подій і визначити, які рішення змінюють наслідки. • Обґрунтувати поріг прийнятності ризику для організації. Очікуваний результат: • Вміння оцінювати ризики і пріоритезувати заходи на основі доказовості. • Здатність аргументувати рішення щодо прийнятності ризику. Дискусія: • Чи можна «закрити ризик» документом без реальних змін? • Коли низька ймовірність не зменшує критичності загрози? **Тема 5. Антропогенний чинник: кадрові ризики, дисципліна, доброчесність, помилки і конфлікти**

	Завдання: • Скласти карту кадрових ризиків: недоброчесність, конфлікт інтересів, витік, вигорання, саботаж, помилки. • Розібрати кейс внутрішнього конфлікту і визначити, як він перетворюється на безпековий ризик. • Запропонувати 5 запобіжників кадрової безпеки (процедури, контроль доступу, навчання, мотивація, культура). Очікуваний результат: • Вміння пов'язувати людський фактор з ризиками і планувати профілактику. • Здатність бачити доброчесність як елемент системи безпеки, а не «моральну опцію». Дискусія: • Що ефективніше: контроль чи культура? • Як не перетворити кадрову безпеку на недовіру до всіх? **Тема 6. Інформаційний простір організації та інформаційні ризики: дезінформація, маніпуляції, витоки, довіра до даних** Завдання: • Виявити 5 типових інформаційних ризиків для організації та їх наслідки (управлінські помилки, репутація, витоки). • Розібрати приклад маніпулятивного повідомлення та визначити, що є фактом, а що — впливом. • Скласти алгоритм внутрішньої верифікації даних для управлінського рішення. Очікуваний результат: • Вміння оцінювати достовірність інформації та будувати процедури перевірки. • Здатність зменшувати ризик рішень, заснованих на спотворених даних.

	Дискусія: • Чи можна «швидко» і «якісно» перевіряти дані одночасно? • Де межа між прозорістю і ризиком витоку? **Тема 7. Архітектура системи безпеки: суб'єкти, функції, розподіл відповідальності, контроль і підзвітність** Завдання: • Побудувати модель структури безпеки організації: ролі, повноваження, взаємодія. • Визначити контрольні точки та порядок ескалації рішень у разі інциденту. • Проаналізувати, як підзвітність знижує ризик недоброчесних рішень. Очікуваний результат: • Вміння проектувати систему ролей і відповідальності як основу керованості безпеки. • Здатність описувати механізми контролю та підзвітності. Дискусія: • Чи може система бути ефективною без незалежного контролю? • Як уникнути «розмитої відповідальності»? **Тема 8. Політики і процедури безпеки: стандарти, регламенти, інструкції, документування і дисципліна виконання** Завдання: • Проаналізувати приклад політики/процедури та визначити, що робить документ контрольованим і однозначним. • Скласти коротку процедуру (1 стор.) для обраного ризику: ціль, кроки, відповідальні, контроль, фіксація. • Виявити типові помилки формалізації (коли «є документ, але немає виконання») і запропонувати рішення.

	Очікуваний результат: • Вміння перетворювати вимоги безпеки на виконувані процедури і стандарти. • Здатність забезпечувати дисципліну виконання через контрольні механізми. Дискусія: • Чи може «надлишок процедур» знижувати безпеку? • Як зробити процедури живими, а не бюрократичними? **Тема 9. Моніторинг, аудит і показники безпеки: оцінка ефективності заходів, контроль змін і безперервне удосконалення** Завдання: • Запропонувати 6–8 KPI/індикаторів безпеки (процесні й результатні) для організації. • Скласти короткий план аудиту: що перевіряється, як фіксуються результати, як формуються коригувальні дії. • Пояснити, як контроль змін впливає на стабільність системи безпеки. Очікуваний результат: • Вміння оцінювати ефективність заходів через показники і аудит, а не через «враження». • Здатність формувати цикл безперервного удосконалення. Дискусія: • Які показники найбільш чесні: ті, що легко зібрати, чи ті, що відображають реальність? • Чи може аудит бути корисним без реальних коригувальних дій? **Тема 10. Управління інцидентами: реагування, документування, розслідування причин і профілактичні заходи** Завдання: • Розібрати кейс інциденту і побудувати ланцюг причин: подія →

	безпосередні причини → системні причини. • Скласти план реагування: хто що робить, у які строки, як фіксується інформація. • Запропонувати 5–7 профілактичних заходів і описати контроль їх виконання. Очікуваний результат: • Вміння керувати інцидентом як процесом із фіксацією, аналізом і профілактикою. • Здатність відрізняти «пошук винного» від аналізу причин. Дискусія: • Чи завжди прозорість розслідування підвищує довіру? • Як уникнути повторення інцидентів без «посилення паперів»? **Тема 11. Стійкість і безперервність діяльності: кризове управління, резерви, відновлення функцій, сценарне планування** Завдання: • Визначити 3–5 критичних функцій і допустимий час простою для кожної. • Скласти сценарій кризи і план відновлення: ресурси, відповідальні, комунікація. • Запропонувати резерви (персонал, дані, інфраструктура) і оцінити їх достатність. Очікуваний результат: • Вміння планувати безперервність діяльності та відновлення функцій на основі сценаріїв. • Здатність оцінювати готовність організації до кризи. Дискусія: • Чи варто інвестувати в резерви, якщо криза «може не настати»?

	• Як не перетворити план безперервності на формальний документ? **Тема 12. Інтеграція складових безпеки: фізична, інформаційна, кадрова, економічна безпека як єдина модель управління ризиками** Завдання: • Побудувати інтегровану карту ризиків: як один ризик у сфері кадрів/інформації може запустити економічні чи фізичні наслідки. • Розібрати кейс комбінованої загрози і визначити узгоджений пакет заходів у різних підсистемах безпеки. • Скласти короткий план інтеграції: хто координує, які документи потрібні, які показники контролю. Очікуваний результат: • Вміння бачити міжсферні зв'язки та планувати заходи комплексно, а не фрагментарно. • Здатність забезпечувати узгодженість рішень і підзвітність у системі безпеки. Дискусія: • Чи можлива «ідеальна інтеграція», чи завжди будуть конфлікти цілей? • Як уникнути розпорошення відповідальності при комплексному підході?
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. Теорія безпеки організацій: предмет, категорії, принципи та місце в системі національної безпеки**	Презентація результатів

	Підготувати короткий «профіль безпеки організації» (1 стор.): що є об’єктом безпеки, які базові категорії (загроза, вразливість, ризик, стійкість, контроль), як вони пов’язані між собою і як відображаються у професійній діяльності. Скласти глосарій із 20 ключових термінів дисципліни з короткими визначеннями (об’єкт/суб’єкт безпеки, загроза, вразливість, ризик, інцидент, стійкість, безперервність, контроль, підзвітність, політика, процедура, аудит, KPI, антропогенний чинник, доброчесність, конфлікт інтересів, інформаційний ризик, економічний ризик, фізична безпека, інтеграція).	
2	**Тема 2. Організація як об’єкт безпеки: структура, процеси, критичні функції, ресурси і точки вразливості** Побудувати карту активів (1 стор.) для умовної організації: люди, інформація, інфраструктура, фінанси, процеси, репутація, визначивши критичність кожного активу. Описати 5 ключових точок вразливості (½–1 стор.) і пояснити, як вони можуть перетворитися на інцидент і які наслідки матиме порушення критичної функції.	Презентація результатів
3	**Тема 3. Загрози і вразливості: класифікація, джерела, механізми впливу, індикатори ризику** Скласти класифікацію загроз для обраної сфери діяльності (не менше 15): внутрішні/зовнішні, навмисні/ненавмисні, за сферами (кадрові, інформаційні, економічні, фізичні). Підготувати перелік 10 індикаторів ризику (1 стор.) з коротким поясненням: що саме сигналізує про загрозу і які перевірки потрібні.	Презентація результатів
4	**Тема 4. Ризик-орієнтований підхід: оцінювання ризиків, матриці, сценарії, прийнятність ризику та пріоритети заходів** Заповнити матрицю ризиків для 8 загроз: ймовірність, наслідки, рівень ризику, пріоритет, рекомендований захід. Написати коротке обґрунтування (½–1 стор.), як визначено прийнятність ризику і чому обрані заходи є пріоритетними.	Презентація результатів
5	**Тема 5. Антропогенний чинник: кадрові ризики, дисципліна, доброчесність, помилки і конфлікти** Скласти «карту кадрових ризиків» (1 стор.): недоброчесність, конфлікт інтересів, витоки, вигорання, саботаж, помилки, конфлікти; для кожного — індикатори і запобіжники. Проаналізувати 1 кейс конфлікту в колективі (1–1,5 стор.): причини, стадія, ризики для безпеки, план деескалації і управлінські рішення.	Презентація результатів
6	**Тема 6. Інформаційний простір організації та інформаційні ризики: дезінформація, маніпуляції, витоки, довіра до даних** Підготувати алгоритм внутрішньої верифікації інформації (1 стор.) для управлінських рішень: джерела, підтвердження,	Презентація результатів

	контроль якості даних, відповідальні. Розібрати 2 приклади маніпулятивної інформації (1–1,5 стор.): що є фактом, що є впливом, які ризики для рішень, які заходи нейтралізації.	
7	**Тема 7. Архітектура системи безпеки: суб'єкти, функції, розподіл відповідальності, контроль і підзвітність** Побудувати модель структури безпеки організації (1 стор.): ролі, повноваження, порядок взаємодії, порядок ескалації інцидентів. Скласти перелік контрольних точок (не менше 8) і пояснити, які документи/дані підтверджують виконання вимог.	Презентація результатів
8	**Тема 8. Політики і процедури безпеки: стандарти, регламенти, інструкції, документування і дисципліна виконання** Розробити коротку процедуру (1–1,5 стор.) для одного обраного ризику: ціль, кроки, відповідальні, строки, контроль, фіксація результатів. Проаналізувати приклад «формальної процедури» (½–1 стор.): чому вона не працює, які зміни потрібні, щоб процедура стала виконуваною.	Презентація результатів
9	**Тема 9. Моніторинг, аудит і показники безпеки: оцінка ефективності заходів, контроль змін і безперервне удосконалення** Запропонувати 8–10 KPI/індикаторів безпеки (процесні і результатні) та коротко пояснити, як кожен збирається і що означає. Скласти план аудиту (1 стор.): об'єкти перевірки, методи збору даних, форма звіту, коригувальні дії і контроль виконання.	Презентація результатів
10	**Тема 10. Управління інцидентами: реагування, документування, розслідування причин і профілактичні заходи** Проаналізувати 1 інцидент (1–1,5 стор.): опис події, безпосередні та системні причини, порушені запобіжники, пропозиції профілактики. Скласти пакет профілактичних заходів (7–10) із відповідальними, строками і показниками виконання.	Презентація результатів
11	**Тема 11. Стійкість і безперервність діяльності: кризове управління, резерви, відновлення функцій, сценарне планування** Побудувати перелік критичних функцій (3–5) і визначити допустимий час простою (RTO) та критичні ресурси для відновлення (1 стор.). Скласти сценарний план відновлення (1–1,5 стор.): дії, відповідальні, комунікація, резерви, контроль готовності.	Презентація результатів
12	**Тема 12. Інтеграція складових безпеки: фізична, інформаційна, кадрова, економічна безпека як єдина**	Презентація результатів

	модель управління ризиками Побудувати інтегровану карту ризиків (1 стор.): як ризик у одній сфері запускає наслідки в іншій, де «вузькі місця» і контрольні точки. Підготувати коротку інтеграційну записку (½–1 стор.): які зміни потрібні в ролях, документах і показниках, щоб система працювала як єдине ціле.	

Реферат є формою самостійної роботи здобувача, метою якої є поглиблення та засвоєння знань з дисципліни «Теорія безпеки організацій».

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

1. Теорія безпеки організацій: предмет, категорії та місце в системі національної безпеки

2. Організація як об’єкт безпеки: активи, процеси, критичні функції та вразливості

3. Поняття загрози, вразливості та ризику: співвідношення і практичне застосування
4. Класифікація загроз організації: внутрішні/зовнішні, навмисні/ненавмисні, міжсферні
5. Джерела загроз і вразливостей: як формуються ризики для організації
6. Індикатори ризику: ранні ознаки загроз і методи їх перевірки
7. Ризик-орієнтований підхід у безпековому менеджменті: логіка та переваги
8. Матриця ризиків: принцип побудови, інтерпретація і обмеження
9. Сценарний аналіз ризиків: методика та роль у плануванні заходів
10. Прийнятність ризику: критерії та управлінські рішення щодо ризику
11. Пріоритезація заходів безпеки: як вибирати найефективніші дії
12. Критичні процеси організації: виявлення, оцінка наслідків, захист
13. Стійкість організації: поняття, фактори та практичні механізми забезпечення
14. Безперервність діяльності: принципи, RTO/RPO, планування відновлення
15. Кризове управління в організації: структура, ролі, сценарії, комунікація
16. Архітектура системи безпеки організації: ролі, повноваження, підзвітність
17. Розподіл відповідальності в системі безпеки: як уникати “розмитої” відповідальності
18. Контроль і підзвітність як інструменти зниження ризиків недоброчесності
19. Політики безпеки: призначення, структура, вимоги до якості документів
20. Процедури безпеки: як перетворювати політики на виконувані механізми
21. Документування у системі безпеки: однозначність, контрольованість, доказовість
22. Моніторинг безпеки: показники, джерела даних, інтерпретація результатів
23. Аудит безпеки: види, етапи, звітність, коригувальні дії
24. Процесні та результатні KPI безпеки: порівняння і практична цінність
25. Безперервне удосконалення системи безпеки: цикл змін і контроль ефекту
26. Управління інцидентами: реагування, документування, ескалація, уроки
27. Аналіз причин інцидентів: безпосередні та системні причини, “root cause”
28. Профілактичні заходи після інциденту: планування і контроль виконання
29. Антропогенний чинник у безпеці: людський фактор як джерело ризиків
30. Кадрові ризики в організації: недоброчесність, помилки, вигорання, саботаж
31. Конфлікт інтересів як фактор ризику: виявлення та управління
32. Доброчесність і етика як елементи системи безпеки організації
33. Кадрова безпека: механізми профілактики ризиків і контроль доступу
34. Мотивація і дисципліна як фактори керованості ризиками
35. Психологічні ризики праці: стрес і вигорання як загроза безпеці процесів
36. Комунікація в системі безпеки: стандарти, бар’єри, управління інформацією
37. Інформаційні ризики організації: дезінформація, маніпуляції, викривлення даних
38. Верифікація інформації для управлінських рішень: алгоритми і відповідальні
39. Ризики витоку інформації: причини, індикатори, запобіжники
40. Репутаційна безпека організації: фактори ризику та заходи захисту
41. Економічні ризики організації: збитки, шахрайство, фінансова стійкість
42. Фізична безпека об’єктів організації: загальні принципи та вразливості

43. Інформаційна безпека як складова системи безпеки організації: взаємозв’язки
44. Інтегрована модель безпеки: поєднання фізичної, кадрової, інформаційної та економічної складових
45. Каскадні наслідки загроз: як один ризик запускає інші
46. Управління змінами і безпека: як зміни створюють нові вразливості
47. Ризики цифровізації в організації: контроль доступу, помилки, залежності
48. Система раннього попередження загроз: індикатори, моніторинг, реагування
49. Безпекова культура організації: формування, підтримання, роль керівника
50. Ефективність системи безпеки організації: критерії оцінювання і управлінські висновки

5.3 Форми проведення модульного контролю та критерії оцінювання

Проведення модульного контролю з дисципліни «Теорія безпеки організацій».

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. Поняття «безпека організації» та її місце у системі національної безпеки
2. Предмет і завдання теорії безпеки організацій
3. Основні категорії дисципліни: загроза, вразливість, ризик, інцидент, стійкість
4. Відмінність між загрозою і ризиком у практичному аналізі
5. Організація як об’єкт безпеки: активи, процеси, ресурси, репутація
6. Критичні функції організації: критерії визначення та наслідки порушення
7. Класифікація активів організації та їх значення для безпеки

8. Поняття вразливості: типи та способи виявлення
9. Загрози організації: внутрішні і зовнішні, навмисні і ненавмисні
10. Міжсферні (комбіновані) загрози та каскадні наслідки
11. Джерела загроз: середовище, персонал, техніка, інформація, процеси
12. Механізми впливу загроз на активи та процеси організації
13. Індикатори ризику: поняття, види, значення раннього попередження
14. Ризик-орієнтований підхід: сутність і переваги для управління безпекою
15. Оцінювання ризиків: етапи, вхідні дані, правила інтерпретації
16. Матриця ризиків: принцип побудови та використання для пріоритезації
17. Сценарний аналіз ризиків: поняття, етапи, приклади застосування
18. Прийнятність ризику: критерії, пороги, управлінські рішення
19. Пріоритезація заходів безпеки: принципи вибору найефективніших ді
20. Стратегії управління ризиками: уникнення, зменшення, перенесення, прийняття
21. Ризик-менеджмент як цикл: аналіз → рішення → реалізація → контроль
22. Антропогенний чинник у безпеці: поняття та роль людського фактора
23. Кадрові ризики організації: типологія та індикатори
24. Недоброчесність як кадровий ризик: механізми виникнення і наслідки
25. Конфлікт інтересів: поняття, приклади, підходи до мінімізації
26. Витік інформації як наслідок людського фактора: профілактика і контроль
27. Помилки персоналу: причини, фактори стресу, профілактика
28. Професійне вигорання як ризик для безпеки процесів
29. Внутрішні конфлікти як безпекова загроза: стадії, деескалація
30. Доброчесність і етика як елементи системи безпеки
31. Інформаційний простір організації: поняття і значення для управління
32. Інформаційні ризики: дезінформація, маніпуляції, викривлення даних
33. Довіра до даних і якість управлінських рішень: взаємозв’язок
34. Верифікація інформації: критерії та алгоритми перевірки
35. Ризики витоку інформації: джерела, ознаки, запобіжники
36. Репутаційні ризики організації: джерела та наслідки
37. Економічні ризики організації: збитки, шахрайство, фінансова стійкість
38. Фізичні ризики організації: загальна характеристика та типові вразливості
39. Архітектура системи безпеки організації: суб’єкти, функції, взаємодія
40. Розподіл відповідальності: ролі, повноваження, уникнення «розмиття»
41. Контроль і підзвітність: механізми і їх роль у зниженні ризиків
42. Політики безпеки: призначення, структура, вимоги до якості
43. Процедури безпеки: відмінність від політик, вимоги до виконуваності
44. Документування у системі безпеки: однозначність, контрольованість, доказовість
45. Моніторинг безпеки: мета, інструменти, джерела даних
46. Показники безпеки: процесні та результатні KPI, їх переваги й обмеження
47. Аудит безпеки: поняття, види, етапи та результати
48. Контроль змін: чому зміни створюють нові вразливості
49. Безперервне удосконалення системи безпеки: логіка циклу та приклади
50. Управління інцидентами: поняття, етапи, ескалація
51. План реагування на інцидент: ролі, строки, комунікація

52. Документування інцидентів: що фіксувати і навіщо
53. Розслідування інцидентів: мета і принципи об’єктивності
54. Безпосередні та системні причини інцидентів: відмінність
55. Аналіз «root cause»: значення для профілактики повторення
56. Коригувальні та попереджувальні дії: зміст і контроль виконання
57. Профілактичні заходи після інциденту: як визначати пріоритети
58. Стійкість організації: поняття, фактори, критерії оцінки
59. Безперервність діяльності (BCP): зміст і призначення
60. Критичні функції та допустимий час простою: поняття RTO (загально)
61. Резерви і дублювання ресурсів: користь і межі
62. План відновлення функцій: етапи і показники готовності
63. Сценарне планування криз: як формувати і перевіряти сценарії
64. Кризове управління: структура, комунікація, прийняття рішень
65. Кризові комунікації: роль достовірності, ясності і дисципліни повідомлень
66. Інтеграція складових безпеки: чому фрагментарний підхід не працює
67. Взаємозв’язок фізичної, кадрової, інформаційної та економічної безпеки
68. Каскадні наслідки загроз: типові приклади у організаціях
69. Управління комплексними загрозами: координація і узгодженість рішень
70. Ризики цифровізації: залежність від систем, контроль доступу, помилки
71. Контроль доступу як елемент організаційної безпеки: принципи (загально)
72. Показники ефективності системи безпеки: підходи до оцінювання
73. «Паперова безпека» і реальна безпека: відмінність та ознаки
74. Безпекова культура організації: ознаки, механізми формування
75. Роль керівника у формуванні культури безпеки і дисципліни
76. Мотивація персоналу і безпека: як уникати «хибних стимулів»
77. Баланс між прозорістю і конфіденційністю в управлінні безпекою
78. Взаємодія підрозділів у забезпеченні безпеки: координація і конфлікти
79. Управлінські помилки в безпекових рішеннях: типові причини
80. Як зменшувати ризик помилкових рішень: дані, верифікація, контроль
81. Порівняння процесних і результатних KPI: коли які застосовувати
82. Підготовка аналітичних матеріалів з безпеки: структура і вимоги доказовості
83. Роль документування у підзвітності й перевірці виконання заходів
84. Адаптація системи безпеки до нових загроз: механізми оновлення
85. Вплив зовнішнього середовища на безпеку організації: регуляторні та соціальні фактори
86. Економічні інтереси та безпека: конфлікти цілей і баланс рішень
87. Ризики недоброчесності у системі контролю: як вони виникають і нейтралізуються
88. Роль внутрішніх перевірок у підтриманні керованості системи безпеки
89. Інтегрована карта ризиків: як її будувати і використовувати
90. Практичне значення теорії безпеки організацій для фахівця з національної безпеки

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 Теорія безпеки організацій 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):

Основні джерела:

1. Франчук В. І. Теорія безпеки соціальних систем: підручник. 2-ге вид., перероб. і допов. Львів; Одеса: Фенікс, 2020. 224 с. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3462/1/%D1%84%D1%80%D0%B0%D0%BD%D1%87%D1%83%D0%BA%20%D1%82%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D0%BF%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA.pdf
2. Отенко І. П., Москаленко Н. О., Азаренков Г. Ф. Теорія управління безпекою соціальних систем: навчальний посібник. Харків: ХНЕУ ім. С. Кузнеця, 2014. 220 с.
3. Живко З. Б., Баворовська О. Б., Занора В. О. Організація та управління системою економічної безпеки підприємства: навчально-методичний посібник. Черкаси: видавець Чабаненко Ю. А., 2019. 120 с.
4. Монастирський Г. Л. Теорія організації: підручник. Тернопіль: ТНЕУ, 2014. 288 с. URL: https://elcat.pnpu.edu.ua/docs/%D0%A2%D0%B5%D0%BE%D1%80%D1%96%D1%8F%20%D0%BE%D1%80%D0%B3%D0%B0%D0%BD%D1%96%D0%B7%D0%B0%D1%86%D1%96%D0%B9.pdf
5. Гриненко В. В. Основи безпеки бізнесу: навчальний посібник. Харків: ХНУМГ ім. О. М. Бекетова, 2020. URL: https://eprints.kname.edu.ua/59074/1/2020%20%D0%BF%D0%B5%D1%87%20100%D0%9B%20%D0%9A%D0%9B%20%D0%BE%D1%81%D0%BD%D0%BE%D0%B2%D0%B8%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8%20%D0%B1%D1%96%D0%B7%D0%BD%D0%B5%D1%81%D1%83%20%D0%93%D1%80%D0%B8%D0%BD%D0%B5%D0%BD%D0%BA%D0%BE.pdf

Додаткові:

Коломієць Б. С. Еволюція поняття безпеки: від класичних теорій до сучасних підходів. Economics: Time Realities. 2024. № 6(76). С. 47–55.

Олійник П. П. Організаційно-правові аспекти забезпечення безпеки підприємства: монографія. Тернопіль: ТНЕУ, 2016.

Резнікова О. С. Національна стійкість: монографія. Гарміш-Партенкірхен: Центр Джорджа К. Маршалла, 2021.

Корж І. Методологічні підходи до визначення поняття «безпека». Юридичний науковий електронний журнал. 2019. № 4. URL: https://www.jurnaluljuridic.in.ua/archive/2019/4/part_1/14.pdf

Стиценко Т. Є., Пронюк Г. В., Сердюк Н. М., Хондак І. І. Безпека життєдіяльності: навчальний посібник. Харків: ХНУРЕ, 2018. 336 с. URL: https://os.nure.ua/wp-content/uploads/2021/04/posibnik-bgd_2018.pdf

Інформаційні ресурси:

1.Бібліотека ім. В. І. Вернадського – http://www.nbuv.gov.ua
2. Верховна Рада України – http://zakon.rada.gov.ua
3. Президент України – http://www.president.gov.ua
4. Кабінет Міністрів України – http://www.kmu.gov.ua
5. Міністерство юстиції України – http://www.minjust.gov.ua
6. Офіційний веб портал судової влади в Україні URL: https://court.gov.ua/
7. Єдиний реєстр судових рішень в Україні. URL: https://reyestr.court.gov.ua/
8. Prozorro: система публічних закупівель. URL: https://prozorro.gov.ua
9. Сайт Національної бібліотеки України ім. В. І. Вернадського. Ресурси. URL: http://www.nbuv.gov.ua/