**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 СЕРВЕЦЬКИЙ

# *СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ*
# «Управління інформаційною безпекою»

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:**

***Кукін Ігор В'ячеславович*** - доктор наук з державного управління, професор кафедри інформаційної безпеки

*(підпис)*

**Викладач:**

***Кукін Ігор В'ячеславович*** - доктор наук з державного управління, професор 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 | **Управління інформаційною безпекою** |
| 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**<br>Лекції : **26**<br>Семінарські заняття: **26**<br>Самостійна робота студентів: **98** |
| Терміни вивчення дисципліни | II 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.

| ***Кукін Ігор В'ячеславович*** | |
|---|---|
| **Науковий ступінь** | Доктор наук з державного управління, Доктор юридичних наук |
| **Вчене звання** | професор |
| **Посада** | Професор кафедри |
| **Дисципліни, які викладає НПП** | Управління інформаційною безпекою |
| **Напрями наукових досліджень** | Освіта, безпека освіти |
| **Посилання на реєстри ідентифікаторів для науковців** | ORCID: https://orcid.org/0000-0002-7050-5536<br>Google Scholar: https://scholar.google.com/citations?hl=uk&user=ZX9C_3UAAAAJ |
| Контактна інформація викладача: | |
| **E-mail:** | institutbezpeki@gmail.com |
| **Контактний тел.** | +380507417375 |
| **Телефон кафедри** | |
| **Портфоліо викладача на сайті кафедри/Інституту/Академії** | https://maup.com.ua/assets/files/kafedra/nacbezpeka/sylabus-2025/b/upravlinnya-informacijnoyu-bezpekoyu.pdf |

### 1.1 Анотація курсу.

Навчальна дисципліна «Управління інформаційною безпекою» спрямована на формування у здобувачів цілісного розуміння управлінської логіки побудови, підтримання та вдосконалення системи інформаційної безпеки в органах публічної влади, підприємствах і організаціях з урахуванням сучасних загроз цифрового середовища, гібридних впливів, інцидентів у інформаційних системах і ризиків порушення конфіденційності, цілісності та доступності даних. Зміст дисципліни (лекції – 26 год., семінарські заняття – 26 год., самостійна робота студентів – 98 год.) поєднує правові, організаційні та процедурні підходи до керування інформаційними ризиками, планування політик і контролів, визначення ролей та відповідальності, управління інцидентами, аудитів і безперервного вдосконалення, а також інтеграцію вимог відповідності із внутрішніми регламентами установи. У межах навчання акцент робиться на практичних інструментах управління: моделюванні загроз, оцінюванні ризиків, побудові політик доступу, організації моніторингу, реагуванні на інциденти, підготовці управлінських рішень на основі доказової бази та комунікації зі стейкхолдерами, що забезпечує здатність здобувачів застосовувати набуті знання в реальних управлінських ситуаціях.

### 1.2 Предмет вивчення курсу

Предметом дисципліни є принципи, методи та інструменти управління інформаційною безпекою в організаціях, включно з організаційно-правовими механізмами, процесами ризик-менеджменту, формуванням політик і процедур, системою контролів, управлінням інцидентами, аудитом і забезпеченням відповідності, а також управлінськими рішеннями, що спрямовані на захист інформаційних ресурсів і підтримання стійкості функціонування інформаційних систем.

**1.3 Метою викладання навчальної дисципліни «Управління інформаційною безпекою»** є формування у здобувачів компетентностей щодо планування, організації, координації та контролю процесів забезпечення інформаційної безпеки, здатності аналізувати загрози та ризики, будувати систему управління інформаційною безпекою на основі політик, процедур і контрольних заходів, а також ухвалювати управлінські рішення щодо запобігання інцидентам, реагування на них та відновлення, забезпечуючи належний рівень захищеності даних і безперервності діяльності.

### 1.4 Завдання

Завданнями дисципліни є формування у здобувачів здатності розуміти категоріальний апарат інформаційної безпеки та управління ризиками, інтерпретувати сучасні загрози і вразливості та оцінювати їхній вплив на діяльність організації, проєктувати й документувати політики та процедури інформаційної безпеки, визначати ролі та відповідальність учасників процесів захисту інформації, обґрунтовувати вибір організаційних і технічних контролів та планувати їх впровадження, організовувати процеси моніторингу та реагування на інциденти з формуванням належної доказової бази, здійснювати підготовку до аудитів і перевірок та підтримувати відповідність внутрішнім і зовнішнім вимогам, застосовувати підходи безперервного вдосконалення системи управління

інформаційною безпекою з опорою на аналіз інцидентів, результатів контролю та управлінської аналітики.

**1.5 Пререквізити і постреквізити навчальної дисципліни:**

**Пререквізити:**

Для успішного опанування навчальної дисципліни «Управління інформаційною безпекою» здобувач має попередньо засвоїти навчальну дисципліну **«Вступ до спеціальності “Національна безпека”»**, оскільки її зміст забезпечує базове розуміння предметної області національної безпеки, системи суб’єктів, загрозового середовища та місця інформаційної безпеки в загальній архітектурі безпекової політики й управління.

**Постреквізити:**

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

**ЗК7. Здатність застосовувати знання у практичних ситуаціях.**

Обґрунтування: Дисципліна орієнтована на прикладне управління інформаційною безпекою, де ключовим є вміння переносити теоретичні підходи на реальні управлінські кейси, пов’язані з ризиками, інцидентами, організацією доступу до даних, контролем виконання політик і процедур. Здобувач має навчитися діяти в умовах невизначеності та обмежених ресурсів, обираючи коректні управлінські рішення та забезпечуючи їх документальне оформлення, контроль і корекцію на підставі результатів аналізу.

**ЗК8. Здатність використовувати інформаційні та комунікаційні технології.**

Обґрунтування: Управління інформаційною безпекою неможливе без застосування інформаційно-аналітичних інструментів, засобів комунікації, систем обліку інцидентів, моніторингу, ведення реєстрів ризиків і активів, а також інструментів підтримки управлінської звітності. У межах дисципліни здобувачі опановують логіку використання ІКТ для організації процесів захисту інформації, координації взаємодії відповідальних осіб і забезпечення контрольованого обміну даними, що напряму підсилює здатність працювати з цифровими інструментами професійно й результативно.

**ЗК9. Здатність виявляти, ставити та вирішувати проблеми.**

Обґрунтування: Практика інформаційної безпеки постійно продукує проблемні ситуації, пов’язані з появою нових загроз, вразливостей, порушень регламентів, конфліктів доступу, помилок персоналу або організаційних прогалин. Дисципліна формує навички постановки проблеми через її управлінське “діагностування”, визначення причин і наслідків, вибір релевантних заходів реагування, а також оцінювання ефективності впроваджених рішень з опорою на факти, показники та доказову базу.

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

Обґрунтування: Інформаційна безпека є складовою національної безпеки, тому управлінські рішення в цій сфері мають узгоджуватися з цінностями захисту прав і свобод, інтересами держави та суспільства, а також із логікою функціонування безпекового сектору. Дисципліна закладає розуміння, що організаційні політики, розподіл повноважень і управління ризиками повинні будуватися не ізольовано, а в контексті загальної державної політики та системи забезпечення національної безпеки.

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

Обґрунтування: Управління інформаційною безпекою спирається на аналіз загроз як вихідну управлінську процедуру, оскільки саме від коректної ідентифікації загроз, джерел впливу та вразливостей залежить вибір контрольних заходів і пріоритетів. У дисципліні здобувачі опрацьовують підходи до класифікації загроз, оцінювання їх імовірності та наслідків, визначення критичності активів і залежностей, що дозволяє пов’язати управління інформаційними ризиками з ширшим контекстом загроз національній безпеці.

**СК8. Здатність формувати систему історичних, культурних, соціальних цінностей національної ідентичності, бути критичним, працювати автономно та в команді, під час організації та здійснення заходів забезпечення національної безпеки.**

Обґрунтування: Ефективна система інформаційної безпеки передбачає не лише технічні рішення, а й організаційну культуру відповідальності, критичного мислення та дотримання регламентів, де значну роль відіграє людський чинник. Дисципліна формує здатність працювати автономно з нормативними та внутрішніми документами, а також координувати дії в команді під час управління інцидентами, проведення аудитів, навчань і комунікації зі стейкхолдерами, що підсилює управлінську стійкість організації.

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

Обґрунтування: Управління інформаційною безпекою потребує коректної організації потоків інформації, побудови каналів повідомлення про інциденти, підготовки управлінської звітності та забезпечення контрольованого доступу до даних. У межах дисципліни відпрацьовується використання інформаційно-аналітичних систем і засобів зв’язку як інструментів управління, що дозволяє забезпечувати ефективну координацію, фіксацію подій, накопичення доказової бази та підтримання належного режиму захисту інформації.

**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.**

Обґрунтування: Дисципліна розглядає інформаційний простір як середовище ризиків і впливів, у якому загрози можуть мати як технічну, так і інформаційно-психологічну природу, а наслідки проявляються в порушенні стійкості управління,

компрометації даних або маніпуляції комунікаціями. Здобувачі опановують підходи до виявлення індикаторів загроз, організації моніторингу, управління інцидентами та впровадження комплексних методів захисту інформації, що забезпечує здатність протидіяти деструктивним впливам у межах управлінської компетенції.

### 1.7 Очікувані результати навчання (ПРН)

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

Управління інформаційною безпекою передбачає підготовку документів, звітів, повідомлень про інциденти, взаємодію з технічними й управлінськими підрозділами, а також роботу з профільними матеріалами й документацією, що часто потребує опрацювання термінології та джерел різними мовами. Дисципліна формує практику професійної комунікації із застосуванням ІКТ, що забезпечує точність передавання змісту, контрольованість обміну даними та відповідність внутрішнім правилам організації.

**ПРН9. Формулювати та аналізувати основні напрями політики забезпечення національної безпеки, включаючи основні пріоритети національних інтересів в державі, загрози національній безпеці та їх класифікацію за сферами людської діяльності, основи забезпечення національної безпеки в основних сферах життєдіяльності.**

Політики інформаційної безпеки в організаціях мають бути узгоджені з логікою безпекової політики держави та з пріоритетами захисту національних інтересів, особливо в умовах гібридних загроз. Дисципліна навчає пов'язувати внутрішні управлінські рішення з ширшими напрямами політики національної безпеки, щоб забезпечувати системність, адекватність пріоритетів і обґрунтованість заходів захисту.

**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.**

Інформаційна безпека впливає на права особи, сталість функціонування організаційних процесів та здатність держави забезпечувати управління і послуги, тому оцінювання стану безпеки вимагає врахування різних рівнів і сфер. У дисципліні формуються підходи до оцінювання стану захищеності через показники, критерії, аналіз ризиків та наслідків, що дозволяє робити обґрунтовані висновки й готувати управлінські рішення.

**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.**

Дисципліна безпосередньо спрямована на планування і організацію заходів інформаційної безпеки, включно з визначенням цілей, ресурсів, відповідальних осіб, регламентів і контрольних точок. Здобувачі опановують логіку управлінського циклу, що забезпечує вміння перетворювати вимоги безпеки на конкретні плани дій, узгоджувати їх з підрозділами та контролювати виконання.

**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.**

Управління інформаційною безпекою починається з інвентаризації активів і визначення їх критичності, а також з системного опису загроз і вразливостей, що можуть впливати на ці активи. У дисципліні відпрацьовуються методи класифікації загроз, ранжирування ризиків і встановлення пріоритетів контролів, що забезпечує основу для раціонального розподілу ресурсів і побудови ефективної системи захисту.

**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.**

Дисципліна розкриває систему управління інформаційною безпекою як сукупність ролей, процесів, регламентів і контрольних процедур, де важливо чітко визначити повноваження і відповідальність суб’єктів, а також механізми контролю й звітності. Здобувачі вчаться описувати таку систему у вигляді організаційної моделі, що є необхідним для впровадження політик, аудитів і забезпечення керованості процесів.

**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.**

Управління інформаційною безпекою включає компонент захисту інформаційного середовища організації від маніпуляцій, фейкових повідомлень, підміни даних і впливів, що здатні провокувати управлінські помилки й репутаційні втрати. У межах дисципліни здобувачі опановують практику верифікації, перевірки джерел і внутрішнього реагування на підозрілі інформаційні впливи, що посилює здатність підтримувати стійкість комунікації та ухвалювати рішення на основі перевіреної доказової бази.

## 2. Зміст навчальної дисципліни

### ЗМІСТОВИЙ МОДУЛЬ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: ПОНЯТТЯ, ПІДХОДИ, ЗАГРОЗИ, ВРАЗЛИВОСТІ, РИЗИКИ, УПРАВЛІНСЬКА АРХІТЕКТУРА

**Тема 1. Управління інформаційною безпекою: предмет, категорії, принципи та місце в системі національної безпеки**

Тема формує понятійно-категоріальний апарат дисципліни та пояснює інформаційну безпеку як управлінську функцію, що забезпечує захист даних і стійкість процесів організації. Розкривається логіка цілей захисту (конфіденційність, цілісність, доступність), законність і підзвітність управлінських рішень, а також взаємозв’язок управління інформаційною безпекою з цілями національної безпеки та публічної стійкості.

**Тема 2. Інформаційні активи та критичні функції: інвентаризація, класифікація, власники активів, критичність**

Тема забезпечує розуміння, що керування інформаційною безпекою починається з визначення активів (дані, системи, сервіси, канали зв'язку) і критичних функцій, від яких залежить діяльність організації. Формується здатність встановлювати власників активів, визначати рівні критичності та описувати залежності, які можуть спричиняти каскадні наслідки при порушеннях.

**Тема 3. Загрози і вразливості інформаційного середовища: джерела, механізми впливу, індикатори**

Тема розкриває типологію загроз (внутрішні/зовнішні, навмисні/ненавмисні, організаційні/технічні/соціальні) та логіку їх реалізації через вразливості процесів і систем. Окремо пояснюється, як визначаються індикатори загроз, як оцінюється їх актуальність і як формується аналітична основа для пріоритезації реагування.

**Тема 4. Ризик-орієнтований підхід в управлінні інформаційною безпекою: оцінювання ризиків, критерії прийнятності, пріоритети контролів**

Тема формує практичне розуміння ризику як поєднання ймовірності та наслідків і навчає застосовувати інструменти оцінювання для управлінського вибору. Розглядаються критерії прийнятності ризику, пріоритезація заходів, баланс між витратами і ефектом, а також вимога доказовості рішень у межах внутрішнього контролю.

**Тема 5. Управлінська модель та ролі: власники процесів, відповідальність, підзвітність, взаємодія підрозділів**

Тема формує розуміння системи управління як мережі ролей і повноважень, де визначається, хто ухвалює рішення, хто виконує, хто контролює та як здійснюється ескалація. Пояснюється, чому "розмита відповідальність" створює системні прогалини, і як узгодженість функцій підвищує керованість інформаційної безпеки.

**Тема 6. Нормативно-організаційні основи: політики, вимоги відповідності, регламенти, документація і доказова база**

Тема розкриває значення політик і регламентів як "правил гри" в організації та пояснює, як вимоги законодавства і внутрішніх процедур переводяться в контрольовані процеси. Формується здатність вибудовувати доказову базу виконання вимог через документування, протоколи, журнали, акти та управлінську звітність.

## ЗМІСТОВИЙ МОДУЛЬ 2. СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: ПОЛІТИКИ, КОНТРОЛІ, МОНІТОРИНГ, РЕАГУВАННЯ, СТІЙКІСТЬ І УДОСКОНАЛЕННЯ

**Тема 7. Політики і процедури доступу: ідентифікація, автентифікація, авторизація, права доступу та дисципліна виконання**

Тема пояснює логіку керування доступом як базового управлінського контролю: хто, до чого, за яких умов і з якою відповідальністю має доступ. Розглядаються принципи мінімальних привілеїв, розмежування повноважень, контроль змін доступів і роль процедур у запобіганні помилкам та зловживанням.

**Тема 8. Захист даних і комунікацій: класифікація інформації, режими обробки, зберігання, передавання, резервування**

Тема формує бачення захисту даних як процесу, який охоплює весь життєвий цикл інформації: створення, обробку, зберігання, обмін і знищення. Акцент робиться на правилах класифікації, режимах доступу, резервуванні та керуванні каналами обміну, щоб мінімізувати ризики витоків і втрати цілісності.

**Тема 9. Моніторинг, аудит і показники: контроль ефективності, вимірювання, управлінська звітність, контроль змін**

Тема формує здатність оцінювати інформаційну безпеку не декларативно, а через показники, моніторинг і перевірку виконання контролів. Пояснюється різниця між процесними та результатними індикаторами, логіка аудиту, контроль змін у системах і процедурах, формування управлінських висновків та коригувальних дій.

**Тема 10. Управління інцидентами: виявлення, реагування, документування, розслідування причин і профілактика**

Тема забезпечує розуміння інциденту як управлінської події, що потребує швидкого реагування та коректної фіксації обставин. Розглядається підхід до аналізу безпосередніх і системних причин, побудова плану профілактики, контроль виконання коригувальних дій і підтримання підзвітності без підміни аналізу “пошуком винного”.

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

Тема розкриває підходи до забезпечення стійкості організації у випадку порушень роботи інформаційних систем і процесів. Формується здатність визначати критичні функції, допустимий час простою, планувати резерви, організовувати відновлення та будувати сценарії криз, що зменшують наслідки і скорочують час повернення до нормального режиму.

**Тема 12. Людський фактор і культура безпеки: навчання, обізнаність, протидія маніпуляціям та інформаційно-психологічним впливам**

Тема показує роль персоналу як ключового елемента системи управління інформаційною безпекою, де помилки, недоброчесність або маніпулятивні впливи можуть створювати критичні ризики. Формується здатність організовувати навчання і комунікацію, критично оцінювати джерела інформації, виявляти дезінформацію та вибудовувати практики фактчекінгу як частину управлінської стійкості.

## 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**

| **№** | **Назва теми** |
|---|---|

| з/п | |
|---|---|
| 1 | **Практичне заняття 1. Управління інформаційною безпекою як управлінська функція: постановка цілей, меж системи, критерії результативності**<br><br>Завдання: визначити цілі управління інформаційною безпекою для заданої організації, окреслити межі системи (процеси, підрозділи, інформаційні системи), сформувати перелік ключових показників результативності та підзвітності.<br><br>Очікуваний результат: підготовлений короткий управлінський профіль системи інформаційної безпеки з визначеними цілями, межами, відповідальними ролями та показниками контролю.<br><br>Дискусія: що є пріоритетом — мінімізація ризиків чи забезпечення безперервності; як уникати формального підходу до політик і показників.<br><br>**Практичне заняття 2. Інвентаризація інформаційних активів і визначення критичності: реєстр активів та власники**<br><br>Завдання: скласти реєстр інформаційних активів (дані, системи, сервіси, канали), визначити власників активів, класифікувати активи за критичністю та встановити залежності між ними.<br><br>Очікуваний результат: сформований реєстр активів із класифікацією критичності та коротким поясненням залежностей і потенційних каскадних наслідків.<br><br>Дискусія: як визначати критичність у випадку конфлікту між підрозділами; чому відсутність “власника активу” створює управлінську прогалину.<br><br>**Практичне заняття 3. Аналіз загроз і вразливостей: побудова карти загроз та індикаторів**<br><br>Завдання: визначити актуальні загрози для вибраного периметра, описати можливі вразливості процесів і систем, запропонувати індикатори загроз для моніторингу та ескалації.<br><br>Очікуваний результат: карта загроз і вразливостей з описом джерел загроз, механізмів реалізації та набором індикаторів для спостереження.<br><br>Дискусія: як відрізняти “гіпотетичну” загрозу від “актуальної”; що робити, якщо даних для оцінювання недостатньо.<br><br>**Практичне заняття 4. Оцінювання ризиків і пріоритезація контролів:** |

| | |
|---|---|
| | **матриця ризиків та план обробки**<br><br>Завдання: побудувати матрицю ризиків (ймовірність/наслідки), визначити критерії прийнятності, пріоритезувати заходи обробки ризиків та сформувати короткий план впровадження.<br><br>Очікуваний результат: матриця ризиків із визначеними пріоритетами та план обробки ризиків з управлінськими рішеннями щодо прийняття, зменшення, уникнення або перенесення ризику.<br><br>Дискусія: як обґрунтовувати витрати на захист; чи можливий “нульовий ризик” у реальній організації.<br><br>**Практичне заняття 5. Політики та регламенти інформаційної безпеки: структура документа і доказова база виконання**<br><br>Завдання: підготувати структуру політики інформаційної безпеки та одного регламенту (наприклад, управління доступом або реагування на інциденти), визначити, які документи та записи формують доказову базу виконання.<br><br>Очікуваний результат: проєкт структури політики та регламенту з переліком контрольних точок, відповідальних осіб і документів підтвердження.<br><br>Дискусія: чому політики “не працюють”, коли вони відокремлені від процесів; як досягти виконання без надмірної бюрократії.<br><br>**Практичне заняття 6. Управління доступом: моделювання ролей, прав доступу та сценаріїв порушень**<br><br>Завдання: описати рольову модель доступу до інформаційних ресурсів, визначити правила надання/зміни/скасування доступу, змоделювати типові порушення та управлінські заходи реагування.<br><br>Очікуваний результат: рольова матриця доступу та процедура керування доступом з описом точок контролю й відповідальності.<br><br>Дискусія: як збалансувати зручність користування й принцип мінімальних привілеїв; як керувати “винятками” без руйнування системи.<br><br>**Практичне заняття 7. Моніторинг і аудит: план перевірки, показники, управлінська звітність**<br><br>Завдання: розробити план внутрішньої перевірки (аудиту) для одного процесу, визначити показники, джерела даних, форму управлінської |

| | |
|---|---|
| | звітності та порядок коригувальних дій.<br><br>Очікуваний результат: короткий план аудиту з KPI/індикаторами, шаблоном звіту та переліком коригувальних дій.<br><br>Дискусія: як уникати “паперового” аудиту; що важливіше — відповідність чи реальна стійкість.<br><br>**Практичне заняття 8. Управління інцидентами: сценарій, хронологія, документування та аналіз причин**<br><br>Завдання: відпрацювати сценарій інциденту, скласти хронологію подій, підготувати пакет документування, визначити першопричини та профілактичні заходи.<br><br>Очікуваний результат: оформлена картка інциденту з хронологією, доказовою базою, висновками та планом профілактики.<br><br>Дискусія: як зберігати доказову базу без порушення правил доступу; чому аналіз причин має бути системним, а не персоналізованим.<br><br>**Практичне заняття 9. Забезпечення стійкості та безперервності: сценарне планування і план відновлення**<br><br>Завдання: визначити критичні функції та допустимі межі простою, розробити сценарій порушення роботи, сформувати базовий план відновлення та комунікації зі стейкхолдерами.<br><br>Очікуваний результат: короткий план безперервності для одного процесу/сервісу з описом відповідальних, ресурсів і порядку відновлення.<br><br>Дискусія: що є “реалістичним” планом для організації з обмеженими ресурсами; як перевіряти готовність без формальності.<br><br>**Практичне заняття 10. Людський фактор і протидія інформаційно-психологічним впливам: тренінг обізнаності та фактчекінг**<br><br>Завдання: розробити міні-програму підвищення обізнаності персоналу, підібрати інструменти верифікації, описати порядок дій при підозрі на дезінформацію або маніпулятивний контент у робочих каналах.<br><br>Очікуваний результат: проєкт програми навчання та короткий протокол фактчекінгу/верифікації для організації з визначенням ролей і каналів повідомлення.<br><br>Дискусія: як не перетворити навчання на “формальність”; де межа між |

| | |
|---|---|
| | відкритою інформацією та службовою інформацією в процесі перевірки. |
| 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 | **СРЗ 1. Понятійно-категоріальна база управління інформаційною безпекою та її місце в системі національної безпеки**<br>Форма завдання: опрацювання навчальних матеріалів і підготовка стислого аналітичного конспекту з визначенням ключових категорій (цілі захисту, активи, загрози, вразливості, ризики, політики, контролі, інциденти) та поясненням їх взаємозв'язку в управлінському циклі.<br>Форма контролю: перевірка конспекту, співбесіда за термінами та логікою управлінських рішень. | Презентація результатів |
| 2 | **СРЗ 2. Аналіз інформаційних активів організації: інвентаризація, класифікація, критичність**<br>Форма завдання: складання реєстру активів для умовної або реальної організації з визначенням власників активів, рівнів критичності та залежностей між активами і процесами.<br>Форма контролю: оцінювання реєстру активів і короткий захист із поясненням критичності та залежностей. | Презентація результатів |
| 3 | **СРЗ 3. Оцінювання загроз і вразливостей: підготовка карти загроз та індикаторів**<br>Форма завдання: підготовка карти загроз для вибраної сфери діяльності, опис механізмів впливу та вразливостей, формування переліку індикаторів для моніторингу й ескалації.<br>Форма контролю: презентація карти загроз і відповідь на запитання щодо обґрунтованості вибору індикаторів. | Презентація результатів |
| 4 | **СРЗ 4. Ризик-аналіз: матриця ризиків і план обробки**<br>Форма завдання: побудова матриці ризиків за заданим кейсом, визначення критеріїв прийнятності та розроблення плану обробки ризиків з пріоритетами впровадження заходів.<br>Форма контролю: перевірка матриці ризиків, оцінювання плану обробки та його захист у форматі короткої управлінської доповіді. | Презентація результатів |
| 5 | **СРЗ 5. Проєкт політики інформаційної безпеки: структура, принципи, відповідальність і доказова база** | Презентація результатів |

| | | |
|---|---|---|
| | Форма завдання: підготовка проєкту структури політики інформаційної безпеки для організації з визначенням принципів, ролей, відповідальності, порядку контролю виконання та переліку документів, які формують доказову базу.<br>Форма контролю: рецензування проєкту політики, тестові питання з ключових положень і процедур. | |
| 6 | **СРЗ 6. Управління доступом: модель ролей і процедура керування доступами**<br>Форма завдання: розроблення рольової моделі доступу та опис процедури надання/зміни/скасування доступу, включаючи винятки, ескалацію та контрольні точки.<br>Форма контролю: перевірка матриці доступів, аналіз сценарних завдань на порушення доступу. | Презентація результатів |
| 7 | **СРЗ 7. Моніторинг і аудит: підготовка плану внутрішнього контролю та набору показників**<br>Форма завдання: розроблення плану внутрішнього контролю (перевірки) одного процесу, визначення показників, джерел даних, форм звітності та порядку коригувальних дій.<br>Форма контролю: оцінювання плану контролю та усне обговорення логіки показників і висновків. | Презентація результатів |
| 8 | **СРЗ 8. Управління інцидентами: алгоритм реагування та шаблони документування**<br>Форма завдання: підготовка алгоритму реагування на інцидент і пакета шаблонів документування (картка інциденту, журнал подій, протокол ескалації, підсумковий звіт із аналізом причин і профілактики).<br>Форма контролю: перевірка комплекту документів, розв’язання кейсу з формуванням доказової бази. | Презентація результатів |
| 9 | **СРЗ 9. Стійкість і безперервність: базовий план відновлення для критичного процесу**<br>Форма завдання: визначення критичного процесу, встановлення допустимих меж простою, опис ресурсів, резервів і порядку відновлення, а також плану комунікації у кризовій ситуації.<br>Форма контролю: захист плану відновлення та оцінювання його реалістичності і керованості. | Презентація результатів |
| 10 | **СРЗ 10. Людський фактор: план підвищення обізнаності та протокол верифікації інформації**<br>Форма завдання: розроблення короткої програми навчання персоналу з акцентом на правилах поводження з інформацією, виявленні маніпуляцій, дезінформації та використанні фактчекінгу; підготовка протоколу внутрішньої верифікації повідомлень.<br>Форма контролю: перевірка програми та протоколу, тестування з кейсами на виявлення маніпулятивного контенту. | Презентація результатів |

Реферат є формою самостійної роботи здобувача, метою якої є поглиблення та засвоєння знань з дисципліни «Управління інформаційною безпекою».

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. Управління інформаційною безпекою як елемент системи національної безпеки: управлінські підходи та пріоритети.
2. Принципи конфіденційності, цілісності та доступності як основа управлінських рішень у сфері інформаційної безпеки.
3. Інформаційні активи організації: класифікація, критичність і відповідальність власників активів.
4. Реєстр інформаційних активів як управлінський інструмент: структура, порядок ведення, контроль якості даних.
5. Типологія загроз інформаційній безпеці: внутрішні та зовнішні джерела, навмисні й ненавмисні впливи.
6. Вразливості організаційних процесів як чинник ризику: причини виникнення та управлінські наслідки.
7. Ризик-орієнтоване управління інформаційною безпекою: методи оцінювання ризиків і критерії прийнятності.
8. Матриця ризиків в управлінні інформаційною безпекою: можливості, обмеження, типові помилки застосування.

9. Управлінська модель системи інформаційної безпеки: ролі, повноваження, підзвітність і ескалація.

10. Політика інформаційної безпеки: зміст, структура, механізми виконання та відповідальність.

11. Регламентація процесів інформаційної безпеки: стандарти операційних процедур і доказова база виконання.

12. Управління доступом до інформації: принцип мінімальних привілеїв і розмежування повноважень у практиці організації.

13. Життєвий цикл доступів: надання, зміна, скасування, періодичний перегляд і контроль винятків.

14. Класифікація інформації в організації: режими обробки, зберігання, передавання та знищення даних.

15. Захист даних при обміні інформацією: управління каналами зв’язку та контрольоване поширення відомостей.

16. Резервне копіювання як управлінський процес: політики, відповідальність, контроль результативності.

17. Моніторинг інформаційної безпеки: організаційні моделі спостереження та ескалації подій.

18. Показники (KPI) інформаційної безпеки: побудова системи вимірювання й управлінська аналітика.

19. Внутрішній контроль і аудит інформаційної безпеки: підходи, планування, документування результатів.

20. Управління змінами в інформаційних системах: ризики, контрольні процедури, управлінська відповідальність.

21. Інцидент інформаційної безпеки як управлінська подія: критерії, класифікація, пріоритети реагування.

22. Процес реагування на інциденти: хронологія, доказова база, управлінські рішення та координація.

23. Аналіз першопричин інцидентів: методологія, системні фактори, профілактичні заходи.

24. Документування інцидентів: журнали, акти, протоколи та їх значення для доказової бази.

25. Сталість і безперервність діяльності: роль інформаційної безпеки у забезпеченні стійкості організації.

26. Планування відновлення після інцидентів: сценарії, ресурси, комунікація зі стейкхолдерами.

27. Кризові комунікації під час інцидентів: управлінська дисципліна, прозорість і контроль повідомлень.

28. Людський фактор у інформаційній безпеці: типові порушення, ризики помилок персоналу та управлінські відповіді.

29. Культура інформаційної безпеки в організації: інструменти формування, мотивація, контроль виконання.

30. Навчання і підвищення обізнаності персоналу: ефективні моделі та оцінка результативності.

31. Соціальна інженерія як загроза: організаційні заходи протидії та управлінська профілактика.

32. Фактчекінг і верифікація інформації в організації: правила, процедури, відповідальні ролі.

33. Протидія дезінформації у внутрішніх і зовнішніх комунікаціях організації: управлінський аспект.

34. Інформаційно-психологічні впливи як фактор ризику: виявлення індикаторів і протидія в управлінських рішеннях.

35. Управління інформаційними ризиками в умовах воєнного стану: пріоритети, ресурси, стійкість процесів.

36. Інформаційна безпека критичних функцій організації: критерії критичності та управлінська відповідальність.

37. Взаємодія підрозділів у системі інформаційної безпеки: координація, конфлікти інтересів, підзвітність.

38. Роль керівництва у забезпеченні інформаційної безпеки: політика “tone at the top” і контроль виконання.

39. Режим доступу до службової інформації: управлінська регламентація та відповідальність за порушення.

40. Управління підрядниками та постачальниками: інформаційні ризики третіх сторін і контрольні заходи.

41. Управління безпекою під час впровадження нових цифрових сервісів: ризики, контрольні точки, відповідальність.

42. Комплаєнс у сфері інформаційної безпеки: узгодження внутрішніх вимог із зовнішніми стандартами та перевірками.

43. Оцінювання ефективності системи управління інформаційною безпекою: підходи до безперервного вдосконалення.

44. Управління журналюванням і обліком подій: значення для розслідувань та доказової бази.

45. Політика роботи з носіями інформації: ризики витоків, порядок використання, контроль та облік.

46. Управління мобільними пристроями та віддаленою роботою: загрози, регламенти, контроль доступу.

47. Захист персональних даних як компонент інформаційної безпеки: управлінська організація процесів і відповідальність.

48. Етика й правомірність управлінських рішень у сфері інформаційної безпеки: баланс безпеки та прав людини.

49. Управління інформаційною безпекою в державних органах: специфіка процесів, підзвітність, контроль.

50. Типові помилки побудови системи управління інформаційною безпекою та шляхи їх усунення.

### 5.3 Форми проведення модульного контролю та критерії оцінювання

***Проведення модульного контролю*** з дисципліни «Управління інформаційною безпекою».

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. Розкрийте зміст поняття «управління інформаційною безпекою» та його відмінність від окремих заходів захисту інформації.
2. Визначте місце управління інформаційною безпекою в системі національної безпеки та в системі управління організацією.
3. Поясніть значення цілей захисту (конфіденційність, цілісність, доступність) для управлінських рішень.
4. Охарактеризуйте основні принципи управління інформаційною безпекою (підзвітність, системність, безперервність, доказовість, пропорційність).
5. Розкрийте поняття інформаційного активу та наведіть приклади активів у діяльності організації.
6. Поясніть, що таке «критична функція» організації та як вона пов’язана з інформаційними активами.
7. Опишіть порядок інвентаризації інформаційних активів та типові помилки під час її проведення.
8. Поясніть мету та структуру реєстру інформаційних активів.
9. Розкрийте поняття «власник активу» та його роль у системі управління інформаційною безпекою.
10. Охарактеризуйте підходи до класифікації інформації та визначення критичності активів.
11. Розкрийте поняття загрози інформаційній безпеці та назвіть основні джерела загроз.
12. Поясніть різницю між внутрішніми та зовнішніми загрозами й наведіть приклади.
13. Поясніть різницю між навмисними та ненавмисними загрозами.

14. Розкрийте поняття «вразливість» та охарактеризуйте її види (організаційні, технічні, поведінкові).
15. Опишіть взаємозв’язок «актив — загроза — вразливість — наслідки».
16. Поясніть, що таке індикатори загроз і для чого вони використовуються в управлінні.
17. Охарактеризуйте інформаційний простір організації як середовище ризиків і впливів.
18. Поясніть поняття «інформаційно-психологічні загрози» та їх управлінські наслідки.
19. Визначте поняття «ризик» у сфері інформаційної безпеки та його складові.
20. Поясніть відмінність між ризиком і загрозою та чому їх не можна підміняти.
21. Опишіть ризик-орієнтований підхід в управлінні інформаційною безпекою та його переваги.
22. Розкрийте етапи процесу оцінювання ризиків.
23. Поясніть, як визначаються ймовірність та наслідки ризику, які критерії можуть застосовуватися.
24. Охарактеризуйте матрицю ризиків як інструмент управління: можливості та обмеження.
25. Поясніть поняття «прийнятність ризику» та як вона встановлюється в організації.
26. Назвіть і поясніть способи обробки ризиків (прийняття, зменшення, уникнення, перенесення).
27. Опишіть порядок пріоритезації заходів (контролів) за результатами оцінювання ризиків.
28. Поясніть, що таке «залишковий ризик» та як він враховується.
29. Розкрийте значення управлінської доказової бази у прийнятті рішень щодо ризиків.
30. Охарактеризуйте типові помилки оцінювання ризиків та їх наслідки для управління.
31. Поясніть, що таке система управління інформаційною безпекою та які її складові.
32. Охарактеризуйте управлінські ролі та відповідальність у системі інформаційної безпеки.
33. Поясніть важливість розмежування повноважень та уникнення конфлікту інтересів.
34. Розкрийте поняття підзвітності та ескалації в управлінні інцидентами й ризиками.
35. Поясніть взаємодію підрозділів у питаннях інформаційної безпеки та типові проблеми координації.
36. Охарактеризуйте роль керівництва в забезпеченні інформаційної безпеки та контролі виконання політик.
37. Розкрийте зміст політики інформаційної безпеки та її місце в системі внутрішніх документів.
38. Поясніть різницю між політикою, стандартом, процедурою та інструкцією у внутрішній документації.

39. Охарактеризуйте вимоги до документування процесів інформаційної безпеки та до підтримання доказової бази.
40. Поясніть, як організовується контроль виконання політик і регламентів у практиці організації.
41. Розкрийте сутність управління доступом як базового контролю інформаційної безпеки.
42. Поясніть зміст принципу мінімальних привілеїв та наведіть приклади його застосування.
43. Охарактеризуйте рольову модель доступу та її значення для керованості системи.
44. Опишіть життєвий цикл доступів: надання, зміна, скасування, періодичний перегляд.
45. Поясніть порядок керування «винятками» в доступах та ризики, що виникають через винятки.
46. Розкрийте поняття контрольованого обміну інформацією та правила передачі даних.
47. Охарактеризуйте режим зберігання інформації та підходи до резервування як управлінського процесу.
48. Поясніть значення журналювання подій та обліку дій користувачів для управління й розслідувань.
49. Розкрийте принципи захисту інформації під час віддаленої роботи та використання мобільних пристроїв.
50. Охарактеризуйте основні ризики витоку інформації та управлінські заходи їх мінімізації.
51. Поясніть, що таке моніторинг у системі інформаційної безпеки та які його цілі.
52. Охарактеризуйте процес виявлення подій і їх перетворення на управлінську інформацію для реагування.
53. Розкрийте відмінність між подією та інцидентом та критерії ескалації.
54. Опишіть типові джерела даних для моніторингу та вимоги до їх якості.
55. Поясніть поняття KPI/індикаторів інформаційної безпеки та відмінність між процесними й результатними показниками.
56. Охарактеризуйте внутрішній контроль і аудит інформаційної безпеки: мета, підхід, результат.
57. Поясніть порядок планування внутрішньої перевірки та формування програми аудиту.
58. Опишіть структуру аудиторського звіту та вимоги до фіксації висновків і доказів.
59. Поясніть зміст коригувальних дій, превентивних дій та механізмів відстеження їх виконання.
60. Охарактеризуйте управління змінами в інформаційних системах і чому воно важливе для безпеки.
61. Розкрийте поняття «інцидент інформаційної безпеки» та його типові категорії.
62. Поясніть основні етапи управління інцидентом: виявлення, реагування, локалізація, відновлення, аналіз.

63. Охарактеризуйте вимоги до документування інцидентів та ведення хронології подій.
64. Поясніть значення доказової бази в процесі реагування та розслідування інциденту.
65. Розкрийте підходи до аналізу першопричин інцидентів та відмінність між симптомами й причинами.
66. Поясніть зміст плану профілактики після інциденту та порядок контролю виконання.
67. Охарактеризуйте кризові комунікації під час інцидентів: принципи, ризики, дисципліна повідомлень.
68. Поясніть роль ескалації та взаємодії підрозділів у реагуванні на інциденти.
69. Опишіть типові управлінські помилки під час реагування на інциденти та їх наслідки.
70. Поясніть, як забезпечується безперервне вдосконалення на основі уроків інцидентів.
71. Розкрийте поняття стійкості організації та роль інформаційної безпеки в забезпеченні стійкості.
72. Поясніть зміст безперервності діяльності та відмінність між планом безперервності й планом відновлення.
73. Охарактеризуйте поняття допустимого часу простою та його визначення для критичних функцій.
74. Опишіть сценарне планування як інструмент підготовки до кризових ситуацій.
75. Поясніть підходи до визначення ресурсів і резервів для відновлення критичних процесів.
76. Розкрийте порядок організації відновлення після порушень роботи інформаційних систем.
77. Поясніть роль тестування готовності планів (навчання, навчальні інциденти) та критерії ефективності.
78. Охарактеризуйте людський фактор як ключову змінну інформаційної безпеки та джерело ризиків.
79. Поясніть, як формується культура інформаційної безпеки та як оцінюється її результативність.
80. Опишіть підходи до навчання персоналу та підвищення обізнаності, які дозволяють уникати формалізму.
81. Розкрийте сутність соціальної інженерії та її значення для управління інформаційними ризиками.
82. Поясніть, як організація може протидіяти маніпуляціям і дезінформації у внутрішніх комунікаціях.
83. Охарактеризуйте методи верифікації та фактчекінгу, які можуть застосовуватися в організації.
84. Поясніть, як визначається достовірність джерел інформації та як працювати з маніпулятивним контентом.
85. Розкрийте зміст управління інформаційними ризиками третіх сторін (постачальники, підрядники) та механізми контролю.

86. Поясніть значення комплаєнсу у сфері інформаційної безпеки та його інтеграцію у внутрішні процеси.
87. Охарактеризуйте етичні межі управлінських рішень у сфері інформаційної безпеки та баланс із правами людини.
88. Поясніть специфіку управління інформаційною безпекою в органах публічної влади та вимоги підзвітності.
89. Розкрийте типові причини неефективності системи управління інформаційною безпекою та способи їх усунення.
90. Охарактеризуйте підхід безперервного вдосконалення системи управління інформаційною безпекою на основі контролю, аудиту та аналізу інцидентів.

**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 Управління інформаційною безпекою 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. Про інформацію : Закон України від 02.10.1992 № 2657-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2657-12
2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2297-17
3. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2939-17
4. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/3855-12
5. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2469-19
6. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2155-19
7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19
8. ISO/IEC 27001:2022 Information security management systems — Requirements. ISO. URL: https://www.iso.org/standard/27001
9. ISO/IEC 27002:2022 Information security controls. ISO. URL: https://www.iso.org/standard/75652.html

10. The NIST Cybersecurity Framework (CSF) 2.0 : NIST CSWP 29. 26.02.2024. NIST. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

**Додаткові:**

1. Security and Privacy Controls for Information Systems and Organizations : NIST SP 800-53 Rev.5. NIST. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
2. SP 800-61 Rev.2 Computer Security Incident Handling Guide. NIST (архівний документ). URL: https://csrc.nist.gov/pubs/sp/800/61/r2/final
3. Good Practice Guide for Incident Management. ENISA. URL: https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
4. Directive (EU) 2022/2555 (NIS2) of the European Parliament and of the Council of 14 December 2022. EUR-Lex. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555
5. Regulation (EU) 2022/2554 (DORA) of the European Parliament and of the Council of 14 December 2022. EUR-Lex (PDF). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554
6. ISO/IEC 27001:2022/Amd 1:2024 Information security management systems — Requirements — Amendment 1. ISO. URL: https://www.iso.org/standard/88435.html
7. Cybersecurity Framework (ресурсний центр та супровідні матеріали). NIST. URL: https://www.nist.gov/cyberframework

**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/