# СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ»

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Лектор курсу** | | | **Мужанова Тетяна Михайлівна**, кандидат наук з держ.упр., доц., доцент кафедри управління інформаційною та кібербезпекою | | **Контактна інформація лектора (e-mail), сторінка курсу в Moodle** | **e-mail:**muzanovat@gmail.com; **сторінка курсу в Moodle –** https://dn.dut.edu.ua/course/view.php?id=398 | |
| **Галузь знань** | | | 12 «Інформаційні технології» | | **Рівень вищої освіти** | бакалавр | |
| **Спеціальність** | | | 125 «Кібербезпека» | | **Семестр** | 4 | |
| **Освітня програма** | | | «Управління інформаційною та кібербезпекою» | | **Тип дисципліни** | Основна | |
| **Обсяг:** | Кредитів ECTS | Годин | За видами занять: | | | | |
| | | | Лекцій | Семінарських занять | Практичних занять | Лабораторних занять | Самостійна підготовка |
| | 5 | 150 | 36 | - | 36 | - | 78 |

## АНОТАЦІЯ КУРСУ

| | |
|---|---|
| **Мета курсу:** | набуття студентами компетенцій, знань, умінь і навичок у галузі забезпечення інформаційної безпеки держави, суспільства та особи, зокрема його нормативно-правових та організаційних засад, напрямів виявлення та протидії загрозам в інформаційній сфері з метою подальшого використання зазначених знань та навиків у подальшій практичній діяльності. |

**Компетентності відповідно до освітньої програми**

| **Загальні компетентності (ЗК)** | **Фахові компетентності (ПП)** |
|---|---|
| **ЗК 2**. Здатність застосовувати отримані знання в практичних ситуаціях.<br>**ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації. | **ПП 2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки. |

**Програмні результати навчання (ПРН)**

**ПРН 6.** Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
**ПРН 12.** Розробляти моделі загроз та порушника.
**ПРН 19.** Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційнотелекомунікаційних системах.
**ПРН 29.** Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
**ПРН 31.** Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційнотелекомунікаційних систем.
**ПРН 32.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційнотелекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
**ПРН 48.** Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

## ОРГАНІЗАЦІЯ НАВЧАННЯ

| **Тема, опис теми** | **Вид заняття** | **Оцінювання за тему** | **Форми і методи навчання/питання до самостійної роботи** |
|---|---|---|---|

| ЗМІСТОВИЙ МОДУЛЬ **1 «ОСНОВНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ»** | | | |
|---|---|---|---|
| Тема 1. ***Теоретичні засади інформаційної безпеки держави***<br>***Знати***: теоретичні засади забезпечення ІБ держави, суспільства, особи, сутність основних понять за темою, отримати уявлення про історію розвитку ІБ держави.<br>***Вміти:*** використовувати теоретичні знання у практичних ситуаціях, оцінювати й прогнозувати загрози ІБ держави, суспільства відповідно до різних методів, в т.ч. за паспортом загрози.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 1,5,7. | Лекція 1 | 5,5* | Лекція-візуалізація, встановлення зв'язку з попередніми дисциплінами |
| | Лекція 2 | | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 1 | | Коротке повторення матеріалу попередніх лекцій, робота в малих групах щодо оцінювання й прогнозування розвитку потенційних загроз ІБ (за паспортом загрози). Підготовка презентацій за результатами роботи групи. |
| Тема 2***. Система забезпечення інформаційної безпеки України***<br>***Знати***: положення нормативно-правових актів із питань ЗІБ України, повноваження суб'єктів системи ЗІБ та принципами їх взаємодії, роль неурядових організацій у ЗІБ України<br>***Вміти***: застосовувати норми законодавства України щодо ЗІБ у практичних ситуаціях, оцінити повноваження органів державної влади у системі ЗІБ, встановити роль неурядових організацій у ЗІБ України.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 1,5,7. | Лекція 3 | 5,5* | Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача) |
| | Практичне заняття 2 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення положень законодавства України з питань ІБ. Представлення узагальненої схеми нормативно-правового ЗІБ України. |
| | Лекція 4 | | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 3 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення повноважень суб'єктів ЗІБ України. Представлення узагальненої схеми суб'єктів ЗІБ України. |
| Тема 3. ***Політика забезпечення інформаційної безпеки України***<br>***Знати***: загальні риси й особливості політики ЗІБ України, функції і напрями ЗІБ України, у т.ч. науково-методичного, інформаційно-аналітичного та кадрового забезпечення.<br>***Вміти***: аналізувати напрями й особливості державної політики ЗІБ України, застосовувати інформаційно-аналітичні методи для їх аналізу, оцінити наявні проблеми та визначити перспективні напрями кадрового забезпечення ІБ в Україні.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 1,5,7. | Лекція 5 | 5,5* | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 4 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення особливостей кадрового забезпечення ІБ. Розробка узагальнених рекомендацій. |
| | Практичне заняття 5 | | Проведення контрольної роботи № 1 «ОСНОВНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ» |
| **Тема 1**. Співвідношення понять: ризик, виклик, небезпека, загроза.<br>**Тема 2.** Зміна підходів до класифікації національних інтересів та загроз ІБ відповідно до законодавства України. | Самостійна робота | | 1. Ризик, виклик, небезпека, загроза: бачення вітчизняних науковців.<br>2. Концепція Уряду США щодо змісту понять ризик, виклик, |

| | | | |
|---|---|---|---|
| **Тема 3**. Зарубіжний досвід кадрового забезпечення у сфері інформаційної та кібербезпеки: досвід для України. | | | загроза.<br>3. Класифікації національних інтересів в інформаційній сфері відповідно до ЗУ «Про основи нац.безпеки» 2003 р. та «Про національну безпеку» 2018 р.<br>4. Види загроз ІБ відповідно до Доктрин ІБ України 2009 та 2017 рр., Стратегій нац.безпеки України 2007 та 2020 рр.<br>5. Досвід підготовки фахівців у сфері інформаційної та кібербезпеки США.<br>6. Європейська практика кадрового забезпечення інформаційної та кібербезпеки. |
| **ЗМІСТОВИЙ МОДУЛЬ 2 «ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ, ІНФРАСТРУКТУРИ ТА РЕСУРСІВ УКРАЇНИ»** | | | |
| Тема 4. ***Безпека інформаційного простору держави***<br>***Знати***: основні засади забезпечення інформаційної безпеки інформаційних ресурсів, інфраструктури держави та національного інформаційного простору, проблеми національного інформаційного простору та напрями забезпечення його ІБ.<br>***Вміти***: застосовувати отримані знання для аналізу й прогнозування тенденцій у забезпеченні безпеки національного інформаційного простору, інформаційної інфраструктури та ресурсів України, класифікувати види інформації обмеженого доступу відповідно до вимог вітчизняного законодавства.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 1-4. | Лекція 6 | 5,5* | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 6 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення питань щодо засад забезпечення безпеки інформаційних ресурсів та інфраструктури України. Формування висновків з теми. |
| | Лекція 7 | | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 7 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення питань щодо методів та напрямів забезпечення безпеки інформаційного простору України, визначення засад стратегічних комунікацій в Україні. Дискусія. |
| Тема 5. ***Інформаційний простір як середовище інформаційного протиборства***<br>***Знати***: сутність основних понять у сфері інформаційного протиборство, вимоги до структури системи ІП держави як складової системи ЗІБ, форми і методи ІП. специфіку сучасного етапу ІП на рівні держави тощо.<br>***Вміти:*** на основі отриманих знань виявити й проаналізувати факти, | Лекція 8 | 5,5* | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 8 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення форм і методів ІП з обов'язковим наведенням і оцінкою конкретних прикладів ІП з української та світової практики. |
| | Лекція 9 | | Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача) |

| | | | |
|---|---|---|---|
| що свідчать про використання ІП у вітчизняному та світовому інформаційному просторі, встановити форми і методи ІП, застосувати теоретичні знання для оцінювання й прогнозування ситуації у сфері ІП в Україні.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 1-4,7,9. | Практичне заняття 9 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення інформаційно-технічної та інформаційно-психологічної зброї з обов'язковим наведенням і оцінкою конкретних фактів її використання. Обговорення і підведення підсумків. |
| | Практичне заняття 10 | | Проведення контрольної роботи № 2 «ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ, ІНФРАСТРУКТУРИ ТА РЕСУРСІВ УКРАЇНИ» |
| **Тема 4**. Підходи до встановлення та класифікації об'єктів критичної інформаційної інфраструктури держави в Україні та ЄС.<br>**Тема 5.** Особливості сучасного етапу ІП. | Самостійна робота | | 1. Класифікація об'єктів критичної інфраструктури відповідно до нормативної бази ЄС.<br>2. Нормативно-правові засади забезпечення безпеки критичної інфраструктури в Україні (ЗУ «Про основні засади забезпечення кібербезпеки України», Постанова КМУ від 09.10.2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», Постанова КМУ від 19.06.2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури».<br>3. Положення проекту ЗУ «Про критичну інфраструктуру та її захист».<br>4. Гібридний характер ІП.<br>5. Мережеві принципи ІП.<br>6. Особливості інформаційного тероризму. |
| **ЗМІСТОВИЙ МОДУЛЬ 3 «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ»** | | | |
| Тема 6. ***Засади забезпечення кібернетичної безпеки держави***<br>***Знати***: теоретичні засади забезпечення кібербезпеки держави, категорійний апарат у цій сфері, норми законодавства України з питань кібербезпеки, особливості побудови державних стратегій кібербезпеки провідних країн світу (США та ЄС, РФ та Китаю).<br>***Вміти:*** на основі теоретичних знань аналізувати підходи до забезпечення кібербезпеки провідних держав світу, оцінювати актуальну ситуацію й прогнозувати перспективи забезпечення кібербезпеки в Україні.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 1-4. | Лекція 10 | 5,5* | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 11 | | Індивідуальні виступи за результатами самостійного вивчення положень Будапештської конвенції про кіберзлочинність, інших нормативно закріплених підходів до класифікації кіберзлочинів. Обговорення і підведення підсумків. |
| | Лекція 11 | | Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача) |
| | Практичне заняття 12 | | Підготовка індивідуальних доповідей та узагальнених схем структури та/або основних принципів систем забезпечення кібербезпеки провідних країн світу (США та ЄС, РФ та Китаю) та пропозицій щодо їх застосування в Україні. |
| | Лекція 12 | | Лекція-візуалізація, експрес-опитування студентів |

| | | | |
|---|---|---|---|
| Тема 7. ***Інтернет як об'єкт забезпечення ІБ.***<br>***Знати***: риси Інтернету як об'єкта інформаційної безпеки, засоби захисту від кіберзлочинності та тероризму.<br>***Вміти***: застосовувати отримані знання для аналізу й прогнозування загроз ІБ держави, суспільства, особи в мережі Інтернет, вести наукову дискусію, аргументовано виражати свою позицію з фахових питань.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 1-4,8. | Лекція 13 | 5,5* | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 13 | | Індивідуальна самостійна підготовка до заняття з проблем безпеки та управління глобальною мережею Інтернет. Дискусія про шляхи її вирішення. Підведення підсумків щодо перспектив упорядкування й безпеки Інтернету. |
| | Практичне заняття 14 | | Проведення контрольної роботи № 3 «ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ» |
| **Тема 6**. Міжнародні ініціативи США та РФ-КНР у сфері кібербезпеки.<br>**Тема 7.** Загрози ІБ в мережі Інтернет. Інтернет-цензура. | Самостійна робота | | 1. Основні положення Міжнародної стратегії щодо дій у кіберпросторі (США).<br>2. Конвенція про забезпечення міжнародної інформаційної безпеки (концепція) (РФ).<br>3. Види інформації, які підлягають цензуруванню в Інтернеті.<br>4. Методи цензури в Інтернеті.<br>5. Моделі систем цензурування |
| **ЗМІСТОВИЙ МОДУЛЬ 4 «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУСПІЛЬСТВА І ОСОБИ»** | | | |
| Тема 8. ***Особливості забезпечення ІБ суспільства й особи. Забезпечення інформаційно-психологічної безпеки***<br>***Знати***: основні засади забезпечення інформаційної безпеки особи, зокрема дотримання прав і свобод людини і громадянина, захисту персональних даних, виявлення та протидії загрозам інформаційно-психологічного характеру.<br>***Вміти***: аналізувати і прогнозувати загрози, а також тенденції забезпечення ІБ суспільства та особи в умовах глобалізації і цифровізації, застосовувати отримані знання для захисту інформаційних прав і свобод людини і громадянина.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 6,7. | Лекція 14 | 5,5* | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 15 | | Індивідуальні виступи за результатами самостійного вивчення інформаційних прав і свобод людини і громадянина в Україні. Підготовка узагальненої схеми за темою. |
| | Лекція 15 | | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 16 | | Індивідуальна самостійна підготовка до заняття щодо особливостей інформаційно-психологічного впливу. Формування класифікації інформаційно-психологічних впливів. |
| Тема 9. ***Технології маніпулятивного інформаційно-психологічного впливу***<br>***Знати***: види деструктивних впливів на психіку людину та засоби їх запобігання і протидії, особливості здійснення маніпулятивних впливів у ЗМІ, політичній сфері, міжособистісному спілкуванні та методи їх протидії.<br>***Вміти:*** виявляти й аналізувати факти негативного психологічного | Лекція 16 | 5,5* | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 17 | | Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення форм і методів маніпулятивних технологій у ЗМІ з обов'язковим наведенням і оцінкою конкретних фактів їх застосування. Обговорення і підведення підсумків. |

| | | | |
|---|---|---|---|
| впливу на психіку людини (в т.ч. через ЗМІ), його мотиви та цілі, запобігати і протидіяти маніпулятивним технологіям на рівні особи.<br>***Формування компетенцій:*** ЗК2, ЗК5, ПП2<br>***Результати навчання:*** ПРН6, ПРН12, ПРН19, ПРН29, ПРН31, ПРН32, ПРН48<br>***Рекомендовані джерела:*** 6,7,8,9. | Лекція 17 | | Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача) |
| | Лекція 18 | | Лекція-візуалізація, експрес-опитування студентів |
| | Практичне заняття 18 | | Проведення контрольної роботи № 4 «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУСПІЛЬСТВА І ОСОБИ» |
| **Тема 8**. Інформаційно-психологічна безпека особи та засоби її забезпечення.<br>**Тема 9.** Медіаосвіта як засіб запобігання маніпулюванню суспільною свідомістю у ЗМІ. | Самостійна робота | | 1. Засоби забезпечення інформаційно-психологічної безпеки особи та суспільства на рівні держави.<br>2. Ментальність, суспільна мораль як об'єкти забезпечення інформаційно-психологічної безпеки.<br>3. Соціально-вікові, освітні, гендерні, національні особливості забезпечення інформаційно-психологічної безпеки.<br>4. Медіаосвіта та медіаграмотність: сутність понять.<br>5. Концепції медіаосвіти провідних країн світу та України.<br>6. Шляхи формування медіаграмотності. |

**МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ**

- Мультимедійний проектор;
- Комп'ютерний клас для проведення практичних занять.

**ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ**


1. Мужанова Т.М. Інформаційна безпека держави : посібник. Київ: ДУТ, 2019. 131 с. URL: http://www.dut.edu.ua/uploads/l_1856_97597210.pdf
2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : Підручник. К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.
3. Бурячок В. Л., Толюпа С.В., Семко В.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник. К. : ДУТ-КНУ, 2016. 178 с. URL: http://www.dut.edu.ua/uploads/p_303_92597962.pdf
4. Бурячок, В.Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/l_1209_69915296.pdf
5. Биченок Н.Н., Савченко В.А., Дзюба Т.М. Основи забезпечення інформаційної безпеки держави у воєнній сфері : Підручник. 2017. URL: http://www.dut.edu.ua/ua/lib/1/category/742/view/2011
6. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Вид-во Ліра-К, 2021. 412 с.
7. Інформаційно-психологічне протиборство: підручник / В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін. ; за заг. ред. В. М. Петрика ; Ін-т спец. зв'язку та захисту інформації НТУ України «КПІ ім. І. Сікорського». Київ : ІСЗЗІ КПІ ім. І. Сікорського, 2018. 387 с. URL: https://mil.univ.kiev.ua/files/8_367228400.pdf
8. Забезпечення інформаційної безпеки держави : Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с. URL: http://vlp.com.ua/files/170227_zmist.pdf
9. Бібліотека Центру практичної психології «Псі-фактор». URL: https://psyfactor.org/lybr.htm
10. Мужанова Т.М., Якименко Ю.М. Досвід Європейського Союзу з протидії деструктивній інформаційній діяльності в мережі Інтернет. Сучасний захист інформації. 2019. № 2. С.37-41. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2314

**ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)**

- Курс передбачає роботу індивідуально і в групах.
- Середовище в аудиторії є інтерактивним, творчим, відкритим до дискусії та взаємодопомоги.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій та практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем, які не ввійшли в теоретичний курс, або були розглянуті коротко, їх поглиблене опрацювання на основі рекомендованої літератури, практичне оволодіння навичками аналітичного характеру, методами роботи з літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він надає викладачу виконані завдання в індивідуальному порядку.
- Під час роботи над завданнями не допустимо порушення вимог академічної доброчесності: при використанні Інтернет-ресурсів та інших джерел інформації студент має посилатися на використане джерело. Не допускається підказування й допомога студенту з боку одногрупників під час виконання індивідуальних завдань. У разі виявлення факту плагіату студент отримує за завдання 0 балів, аналогічну оцінку отримують автори тотожних робіт.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- Використання телефонів і комп'ютерних засобів без дозволу викладача забороняється.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

| Форми контролю | Види навчальної роботи | Оцінювання |
|---|---|---|
| **ПОТОЧНИЙ КОНТРОЛЬ** | ***Робота на заняттях,*** *у т.ч.:* | |
| | • присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу) | за кожне відвідування 0,55 бала |
| | • опитування за результатами вивчення теми, перевірка знання термінології | за кожну правильну відповідь 0,25 бала |
| | • індивідуальний виступ за результатами самостійного вивчення навчального матеріалу | за кожен виступ максимум 2 бали |
| | • доповідь з презентацією за темою, в тому числі вивченою самостійно (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності презентації і доповіді) | за кожну доповідь максимум 3 бали |
| | • підготовка повідомлення, ессе, порівняльної характеристики, аналіз положень законодавства, публікації тощо | за кожну правильну відповідь 2 бали |
| | • участь у дискусії, обговоренні положень нормативних актів, положень законодавства тощо | за кожну участь 1 бал |
| **РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)** | Модульний контроль № 1 «ОСНОВНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ» | максимальна оцінка – 10 балів |
| | Модульний контроль № 2 «ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ, ІНФРАСТРУКТУРИ ТА РЕСУРСІВ УКРАЇНИ» | максимальна оцінка – 10 балів |
| | Модульний контроль № 3 ««ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ ЗАСАДИ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ»» | максимальна оцінка – 10 балів |
| | Модульний контроль № 4 «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУСПІЛЬСТВА І ОСОБИ» | максимальна оцінка – 10 балів |
| **Додаткова оцінка** | Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю тощо. | Звільняється від заліку |
| **ПІДСУМКОВЕ ОЦІНЮВАННЯ** ***Залік*** | Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків.<br>Залік проходить у письмовій формі. | 30 балів |

| ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ | | | |
|---|---|---|---|
| **бали** | **Критерії оцінювання** | **Рівень компетентності** | **Оцінка** */запис у заліковій відомості* |
| **90-100** | Студент демонструє повні й міцні знання навчального матеріалу, що відповідає робочій програмі дисципліни, правильно й обґрунтовано відповідає на поставлені запитання за темою. Студент уміє реалізувати теоретичні положення дисципліни у ході виконання практичних завдань аналітичного характеру, що свідчить про високий рівень засвоєння навчального матеріалу, показує здатність застосовувати знання із суміжних дисциплін. Знає сучасні напрями, методи і тенденції забезпечення інформаційної та кібербезпеки держави, набуті в рамках даної дисципліни.<br>За час навчання при проведенні практичних занять та виконанні індивідуальних/ контрольних завдань студент проявляє вміння самостійно опрацьовувати наукову літературу та нормативні документи, активно долучатися до обговорення проблем забезпечення інформаційної безпеки держави та шляхів їх вирішення.<br>Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки обсягів матеріалу, передбаченого робочою програмою, або невпевненістю у тлумаченні окремих теоретичних положень. | **Високий**<br>Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.<br>Власні пропозиції студента щодо виконання практичних завдань підвищують його вміння використання знань, отриманих при вивченні інших дисциплін, а також знань, набутих при самостійному поглибленому вивченні питань у межах дисципліни, яка вивчається. | Відмінно / Зараховано (A) |
| **82-89** | Студент демонструє гарні знання змісту навчальних матеріалів, підходів до оцінювання й аналізу ситуацій у сфері інформаційної безпеки, що відповідає робочій програмі дисципліни, вміє застосовувати набуті знання та вміння для самостійної роботи, але допускає одиничні неточності. Вміє самостійно виправляти допущені помилки, число яких є незначним. Показує володіння аналітичними методами та вміє застосовувати їх для оцінки ситуацій у сфері інформаційної безпеки на достатньому рівні.<br>За час навчання при проведенні практичних занять, виконанні індивідуальних/ контрольних завдань студент проявляє хорошу здатність самостійно виконувати поставлені завдання, долучатися до обговорення шляхів вирішення проблем за напрямом із незначними прогалинами у володінні практичними навичками. | **Достатній**<br>На достатньо високому рівні забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни.<br>Забезпечує студенту самостійне виконання практичних завдань у разі незначної зміни умов, порівняно з наданими у матеріалах дисципліни | Добре / Зараховано (B) |
| **75-81** | Студент загалом добре володіє навчальним матеріалом, знає основні теоретичні положення відповідно до робочої програми дисципліни, вміє застосовувати набуті вміння для виконання практичних завдань аналітичного характеру з питань забезпечення інформаційної безпеки держави, але допускає окремі неточності, вміє пояснити основні положення виконаних завдань та дати правильні відповіді у ході опитування. Помилки у відповідях не є системними.<br>Студент знає основні положення матеріалу, що мають визначальне значення при виконанні індивідуальних/контрольних завдань та поясненні представлених думок в межах дисципліни, що вивчається. | **Достатній**<br>На достатньому рівні забезпечує вимоги до знань, умінь і навичок вивченим матеріалом робочої програми дисципліни.<br>Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення. | Добре / Зараховано (C) |
| **64-74** | Студент засвоїв більшу частину теоретичного матеріалу та в основному вивчив підходи до оцінювання й аналізу ситуацій у сфері інформаційної безпеки**,** передбачених робочою програмою дисципліни, розуміє постановку стандартних завдань, має уявлення щодо способів їх виконання. | **Середній**<br>Забезпечує помірний рівень відтворення основних положень дисципліни | Задовільно / Зараховано (D) |

| | | | |
|---|---|---|---|
| | У ході виконання завдань допускає значну кількість неточностей і грубих помилок, які може усунути з допомогою викладача. | | |
| **60-63** | Студент володіє певними неґрунтовними знаннями, передбаченими в робочій програмі дисципліни, на мінімально допустимому рівні. З використанням основних теоретичних положень студент з труднощами виконує поставлені завдання щодо опрацювання літератури, оцінювання й аналізу ситуацій у сфері інформаційної безпеки**.**<br>У ході виконання практичних/ індивідуальних/ контрольних завдань демонструє формальне ставлення, відсутність глибокого розуміння роботи та взаємозв'язків з іншими темами. | **Середній**<br>Забезпечує мінімально допустимий рівень у всіх складових навчальної програми з дисципліни | Задовільно / Зараховано (E) |
| **35-59** | Студент може відтворити окремі фрагменти матеріалів курсу, показати слабкі аналітичні навички**.** Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, якість виконання практичних завдань в більшості є низькою, відповіді невірними, необґрунтованими.<br>Цілісність розуміння матеріалу з дисципліни та володіння необхідними вміннями у студента відсутні. | **Низький**<br>Не забезпечує практичної реалізації завдань, що формуються при вивченні дисципліни | Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється* |
| **1-34** | Студент повністю не виконав вимог робочої програми навчальної дисципліни.<br>Його знання на підсумкових етапах навчання є фрагментарними.<br>Студент не допущений до здачі заліку. | **Незадовільний**<br>Студент не підготовлений до самостійного вирішення завдань, які встановляє програма дисципліни | Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється* |