**Міжнародний гуманітарний університет**
**Інститут права, економіки та міжнародних відносин**
**Кафедра кримінального права, процесу та криміналістики**

ЗАТВЕРДЖЕНО
Ректор
Міжнародного гуманітарного університету
проф. Костянтин ГРОМОВЕНКО
«02» вересня 2021 р.

# СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

## Основи кібербезпеки

**Рівень вищої освіти** перший (бакалаврський) рівень вищої освіти
(назва рівня вищої освіти)

**Ступінь вищої освіти** бакалавр
(назва ступеня вищої освіти)

**Спеціальність** 262 «Правоохоронна діяльність
(код та найменування спеціальності)

**Освітня програма** «Правоохоронна діяльність»
(найменування освітньої програми)

| | |
|---|---|
| **Викладач** | Слатвінська Валерія Миколаївна |
| **Профайл викладачів** | ORCID : https://orcid.org/0000-0002-6082-981X |
| **Контактний тел.** | 067 122 39 12 |
| **E-mail:** | slatvinskaya_valeriya@ukr.net |
| **Сторінка курсу у Moodle** | |
| **Консультації** | Очні – кожен четвер у кабінеті 612 з 11-30 до 13-00. Онлайн-консультації – viber, zoom – за замовленням студентів. |

Силабус розглянуто та прийнято на засіданні кафедри кримінального права, процесу та криміналістики

Протокол № 1 від 20 серпня 2021 р.

Завідувач кафедри кримінального права, процесу та криміналістики _____ проф. Олександр ПОДОБНИЙ

Перевірено: Гарант освітньо-професійної програми _____ проф. Олександр ПОДОБНИЙ

Перевірено: Начальник навчального відділу _____ доц. Лариса РАЙЧЕВА

Погоджено: Проректор з науково-педагогічної роботи _____ проф. Анатолій ГОНЧАРУК

## 1. Анотація до курсу

У сучасній конкурентній боротьбі широко поширені різноманітні дії, на отримання інформації самими різними способами, з використанням сучасних технічних засобів розвідки. Близько половини охоронюваних відомостей видобувається з використанням методів промислового шпигунства. У цих умовах захисту інформації відводиться далеко не останнє місце. Актуальність курсу зумовлена необхідністю використання методів інформаційної безпеки та захисту інформації в діяльності майбутніх фахівців правознавців. Предметом вивчення навчальної дисципліни «Основи кібербезпеки» є загальні теоретичні основи, методи та практичні засобі інформаційної безпеки і захисту інформації, які необхідно використовувати в професійної діяльності фахівця правознавця. Формування у майбутніх фахівців загальних і професійних знань в сфері інформаційної та кібернетичної безпеки, що забезпечують здатність випускника виконувати професійну діяльність на первинній посаді, що здатні впроваджувати технології інформаційної та кібербезпеки у практичній діяльності. Об'єктами навчання є: об'єкти інформатизації, до яких відносяться комп'ютерні, автоматизовані, інформаційні та телекомунікаційні системи, інформаційні ресурси та інформаційні технології в умовах існування кіберзагроз в інформаційної сфері; технології забезпечення інформаційної та кібернетичної безпеки об'єктів різного рівня (системи, їх об'єкти та компоненти), які пов'язані з інформаційними технологіями; механізми забезпечення веб-безпеки, банківських систем та систем електронної комерції; процеси управління інформаційної безпекою об'єктів, що захищаються; методи розслідування інцидентів, управління ризиками та аудит систем інформаційної та кібернетичної безпеки; методики захисту від негативного інформаційного впливу тощо.

## 2. Мета та цілі курсу

*Мета*: оволодіння теоретичними основами інформаційної безпеки та захисту інформації, необхідними для розв'язання практичних задач; набуття вміння самостійно знаходити, вивчати і застосовувати літературу та інші інформаційні джерела з інформаційної безпеки та захисту інформації; напрацювання навичок з дослідження прикладних задач, а саме, вміння вирішувати практичні задачі фахівця із застосуванням методів інформаційної безпеки та захисту інформації; вивчення досвіду окремих європейських країн із гарантування інформаційної безпеки; знання сучасного стану законодавчої бази і сучасних технологій в області інформаційної безпеки та розробка, на цій основі, відповідних пропозицій, необхідних для використання у практиці фахівця.

## 3. Формат курсу

Головними формами вивчення курсу «Основи кібербезпеки» є лекції, семінарські заняття, індивідуальні заняття та самостійна робота студентів.

Кращому опануванню здобувачами вищої освіти навчальним матеріалом може слугувати проведення певної частини лекційного заняття у форматі: а) бесіди, що передбачає активізацію інтелектуальної діяльності здобувачів вищої освіти, мотивування їх до вивчення певної теми навчальної дисципліни, постановку «бінарних» та «небінарних» запитань для виявлення ставлення, думки, рівня ознайомлення та готовності здобувачів вищої освіти, визначення міри сприйняття ними матеріалу, що викладається. Адекватна оцінка психоемоційного стану слухачів, фахова та етична реакція на їхні репліки – загальна вимога до проведення будь-якого публічного виступу – за такого формату набуває особливого значення; б) дослідження, що передбачає формулювання здобувачами вищої освіти за участі викладача певної теоретичної позиції, виявлення закономірностей або аномалій у конституційно-правовому регулюванні, шляхом «мозкового штурму» (метод спільного пошуку ідей і рішень, шляхів вирішення проблем або нестандартних ситуацій, що на має на меті спершу запропонувати

якнайбільшу кількість варіантів, не вдаючись до їхнього аналізу та критики, а потім відібрати перспективні пропозиції, обговоривши й оцінивши кожен варіант); б) ситуаційного аналізу (кейс-метод), що передбачає вивчення здобувачами вищої освіти реальної конкретної політико-правової ситуації (події), визначення за участі викладача суті проблеми, причин та наслідків причин, формулювання можливих варіантів її вирішення; в) «бінарної» лекції, що передбачає виклад певного навчального матеріалу з протилежних позицій (прихильника – противника; теоретика – практика тощо) і спрямована на демонстрацію різних підходів до розуміння певного конституційно-правового явища або процесу. Така технологія викладання спонукає слухачів порівнювати й оцінювати різні точки зору, використовувати у подальшому нові ідеї замість традиційних чи очікуваних.

## 4. Компетентності та програмні результати навчання

**У процесі реалізації програми дисципліни «Основи кібербезпеки» формуються наступні компетентності із передбачених освітньою програмою:**

**Інтегральна компетентність.** Здатність вирішувати складні спеціалізовані задачі та практичні проблеми у сфері правоохоронної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів правоохоронної діяльності і характеризується комплексністю та невизначеністю умов.

**Загальні компетентності:**

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

**Спеціальні (фахові) компетентності**

СК3. Здатність професійно оперувати категоріально-понятійним апаратом права і правоохоронної діяльності.

СК4. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань та навичок у професійній діяльності.

СК5. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.

СК6. Здатність аналізувати та систематизувати одержані результати, формулювати аргументовані висновки та рекомендації.

СК9. Здатність ефективно застосовувати сучасні техніку і технології захисту людини, матеріальних цінностей і суспільних відносин від проявів криміногенної обстановки та обґрунтовувати вибір засобів та систем захисту людини і суспільних відносин.

СК12. Здатність систематизувати закономірності злочинності, визначати особу злочинця, причини і умови злочинності та її окремих видів, реалізовувати напрями і заходи її запобігання.

СК18. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури.

Навчальна дисципліна «Основи кібербезпеки» забезпечує досягнення програмних результатів навчання, передбачених освітньою програмою:

РН1. Розуміти історичний, економічний, технологічний і культурний контексти розвитку правоохоронної діяльності.

РН3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.

РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.

РН18. Застосовувати штатне озброєння підрозділу (вогнепальну зброю, спеціальні засоби, засоби фізичної сили); інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності.

РН21. Організовувати заходи щодо режиму секретності та захисту інформації.

## 5. Обсяг курсу

| Загалом | | Вид заняття (денне відділення) | | |
|---|---|---|---|---|
| ЄКТС | годин | Лекційні заняття | Практичні заняття | Самостійна робота |
| 3 | 90 | 16 | 14 | 60 |

## 6. Ознаки курсу

| Рік викладання | Семестр | Курс, (рік навчання) | Обов'язкова / вибіркова |
|---|---|---|---|
| 2021 - 2022 | 6 | 4 | Вибіркова |

## 7. Технічне й програмне забезпечення /обладнання

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи онлайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою.

## 8. Політика курсу

У процесі викладання навчальної дисципліни застосовуються інтерактивні методи навчання, відбувається активне залучення студентів до обговорення кожного з питань курсу, що сприяє досягненню такого кваліфікаційного рівня підготовки випускників, при якому вони повинні бути здатними до вирішення професійних задач діяльності, пов'язаних з ефективним забезпеченням прав і свобод людини і громадянина. Критерієм вибору методів навчання є їхня відповідність дидактичним меті та завданням навчального заняття, конкретним

РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.

РН18. Застосовувати штатне озброєння підрозділу (вогнепальну зброю, спеціальні засоби, засоби фізичної сили); інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності.

РН21. Організовувати заходи щодо режиму секретності та захисту інформації.

## 5. Обсяг курсу

| **Загалом** | | **Вид заняття (денне відділення)** | | |
|---|---|---|---|---|
| **ЄКТС** | **годин** | **Лекційні заняття** | **Практичні заняття** | **Самостійна робота** |
| 3 | 90 | 16 | 14 | 60 |

## 6. Ознаки курсу

| **Рік викладання** | **Семестр** | **Курс, (рік навчання)** | **Обов'язкова / вибіркова** |
|---|---|---|---|
| **2021 - 2022** | 6 | 3 | **Вибіркова** |

## 7. Технічне й програмне забезпечення /обладнання

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи онлайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань, тощо, студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою.

## 8. Політика курсу

У процесі викладання навчальної дисципліни застосовуються інтерактивні методи навчання, відбувається активне залучення студентів до обговорення кожного з питань курсу, що сприяє досягненню такого кваліфікаційного рівня підготовки випускників, при якому вони повинні бути здатними до вирішення професійних задач діяльності, пов'язаних з ефективним забезпеченням прав і свобод людини і громадянина. Критерієм вибору методів навчання є їхня відповідність дидактичним меті та завданням навчального заняття, конкретним

обставинам – умовам і часу навчання, психоемоційному стану здобувачів вищої освіти, рівню їхню базової підготовки та мотивації тощо. При цьому слід врахувати не лише потребу надання здобувачам вищої освіти нових знань, а й формування у них вмінь та навичок, необхідних для подальшого самостійного здобуття й оновлення інформації, професійного й фахового застосування набутих знань.

Вирішення практичних завдань з основ кібербезпеки дозволить студентам певною мірою оволодіти практикою застосування норм кібер-законодавства, усвідомити рівень законодавчого регулювання у цій сфері та спрямувати свої зусилля на захист прав людини, громадян, підприємств, організацій, держави та інших суб'єктів правовідносин.

Тому специфіка практичних занять по даній дисципліні полягає в тому, що на цих заняттях відводиться час не тільки для обговорення теоретичних питань основ кібербезпеки, усній перевірці знань студентів, але й для вирішення практичних ситуацій.

На практичних заняттях можуть використовуватись різні форми та методи контролю знань студентів: доповіді, експрес-опитування, доповнення відповіді, вільна дискусія, співбесіда, обговорення рефератних повідомлень, розв'язання казусів та задач, індивідуальні завдання та інші. Рівень знань, підготовленості, ерудиції, активності студентів на семінарах оцінюється викладачем самостійно.

Підсумковою формою контролю знань є залік наприкінці 6-го семестру, що має на меті перевірити теоретичні знання та вміння застосовувати їх, вирішуючи конкретні завдання, а також уміння студентів самостійно працювати з науковою та навчальною літературою. До заліку допускаються ті студенти, які відпрацювали всі пропущені заняття, виправили незадовільні оцінки, отримані на семінарських заняттях, набрали мінімальну кількість балів.

## 9. Схема курсу
### 6 семестр

| № | Тема, план, короткі тези | Форма діяльності (заняття) / Формат | Матеріали | Література, інформаційні ресурси | Завдання, години | Кількість годин денна | заочна |
|---|---|---|---|---|---|---|---|
| 1 | **Тема 1. Організаційно-правове забезпечення захисту інформації.**<br>1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення.<br>2. Поняття та види кіберзлочинів.<br>3. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.<br>4. Законодавство в даній області низки країн (США, Австралія, Китай і ряд інших). Питання судового переслідування. | Лекція | Презентація | 1 – 4, 6 - 8. | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття. | 2 акад. год. | 2 акад. год. |
| | | Практичне | доповіді | 6, 7, 9, 10, 15 | Передивитись презентації | 2 акад. | 2 акад. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 5. Конфіденційність особистої інформації. Міжнародні і національні стандарти і специфікації в області інформаційної безпеки.<br>6. Системи захисту інформації в провідних світових компаніях. Практика компанії IBM в області захисту. Практика компанії Cisco Systems в розробці політики розвитку мереж безпеки. Практика компанії Microsoft в області інформаційної безпеки. | заняття | студентів | | доповідей, *2 год* | год. | год. |
| 2 | **Тема 2. Захист інформації у персональних комп'ютерах та в автоматизованих системах.**<br>1. Найпоширеніші методи викрадення інформації (зламу паролів).<br>2. Стадії зламу отримання ключів та паролів. Ознаки можливого злому комп'ютера та його зараження шкідливими програмами.<br>3. Рекомендації з безпеки Вашого комп'ютера. Виявлення шкідливих програм зі шкідливими функціями, які беруть участь в атаках.<br>4. Захист інформації з обмеженим доступом у захищеній комп'ютерній мережі. Розмежування доступу до інформації в залежності від повноважень користувача. Використання паролів. Шифрування інформації у комп'ютерах при її зберіганні.<br>5. Програмні засоби захисту інформації. Вибір програм розмежування доступу до інформації. Вибір програм автоматичного шифрування інформації при її збереженні на дисках та відпрацювання практичних навичок їх | Лекція | Презентація | 1 – 4, 6 - 8 | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття | 2 акад. год. | 2 акад. год. |
| | | Практичне заняття | доповіді студентів | 6, 7, 9, 10, 15 | Передивитись презентації доповідей, *2 год* | 2 акад. год. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | застосування.<br>6. Використовування програмних та апаратних засобів розмежування доступу до інформації у автоматизованих системах та антивірусних засобів захисту інформації у персональних комп'ютерах. | | | | | | |
| 3 | **Тема 3. Інформаційна безпека при роботі у мережі Інтернет та у відкритих каналах зв'язку.**<br>1. Основні чинники, що впливають на стан інформаційної безпеки у зв'язку із використанням загальнодоступних та соціально орієнтованих ресурсів мережі Інтернет.<br>2. Характеристика ключових факторів ризику при роботі у мережі Інтернет та рекомендації щодо їх нейтралізації: зберігання та передача даних; соціальні мережі; використання іноземних соціально орієнтованих ресурсів мережі Інтернет; використання додатків до смартфонів; вихід до мережі Інтернет.<br>3. Рекомендації щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет і перелік іноземних веб-ресурсів, якими не рекомендовано користуватись.<br>4. Методи і системи захисту мовленнєвої інформації, що передається у відкритих каналах зв'язку.<br>5. Стеганографічні та криптографічні систем захисту письмової інформації, що передається у відкритих каналах зв'язку.<br><br>Доповіді студентів за темою заняття та їх обговорення. | Лекція | Презентація | 1 – 4, 6 - 8 | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття | 2 акад. год. | |
| | | Практичне заняття | доповіді студентів | 6, 7, 9, 10, 15 | Передивитись презентації доповідей, *2 год* | 2 акад. год. | 2 акад. год. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 4 | **Тема 4. Організаційно-технічний захист інформації. Комплексне забезпечення інформаційної безпеки.**<br>1. Місце організаційно-технічного захисту інформації у системі інформаційної безпеки. Організаційні та технічні засоби захисту. Основні поняття, терміни та визначення організаційного та технічного захисту інформації.<br>2. Види інформації, яка може стати об'єктом злочинних посягань.<br>3. Поняття технічних каналів витоку інформації та механізм їх утворення. Види та класифікація технічних каналів витоку інформації та способів несанкціонованого зняття інформації.<br>4. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні. Визначення можливих джерел витоку інформації з радіоканалу.<br>5. Методи та засоби блокування технічних каналів витоку інформації. Методи пасивного та активного захисту інформації. Методи та засоби захисту акустичної інформації. Методи та засіб захисту електромагнітної інформації. Методи захисту від ВЧ-нав'язування.<br>6. Методики і засоби пошуку радіозакладних пристроїв.<br>7. Організація роботи щодо виявлення і блокування технічних каналів витоку інформації; здійснювання ефективний контроль робіт із захисту інформації; здійснювання ефективний вибір комп'ютерних систем захисту; дотримування правил безпечної роботи з інформацією; використовування спеціальних | Лекція | Презентація | 1 – 4, 6 - 8 | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття | 2 акад. год. | 2 акад. год. |
| | | Практичне заняття | доповіді студентів | 6, 7, 9, 10, 15 | Передивитись презентації доповідей, *2 год* | 2 акад. год. | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | технічних засобів захисту інформації.<br>8. Комплексний підхід до забезпечення безпеки. Рекомендації щодо комплексного зміцнення інформаційної безпеки юридичного офісу.<br><br>Доповіді студентів за темою заняття та їх обговорення. | | | | | | |
| 5 | **Тема 5. Забезпечення конфіденціальної роботи користувача в ОС.**<br><br>1. Типи атак на інформаційні системи. Технології антивірусів та цілісності системи<br>2. Технології аудиту, моніторингу та менеджменту<br>3. Персональні дані і GDPR<br>4. Рекомендації в разі виявлення незаконного втручання в роботу електронно-обчислювальних машин фахівця.<br><br>Доповіді студентів за темою заняття та їх обговорення. | Лекція | Презентації, доповіді студентів | 1 – 4, 6 - 8 | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття | 2 акад. год. | 2 акад. год. |
| | | Практичне заняття | Презентація | 6, 7, 9, 10, 15 | Передивитись презентації доповідей, *2 год* | 2 акад. год. | |
| 6 | **Тема 6. Перехоплення, ідентифікація і аналіз трафіку.**<br>1. Вимоги до кібербезпеки елементів телекомунікації<br>2. Методи і технології управління визначенням ідентичності<br><br>Доповіді студентів за темою заняття та їх обговорення. | Лекція | доповіді студентів | 1 – 4, 6 - 8 | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття | 2 акад. год. | |
| | | Практичне | Презентація | 6, 7, 9, 10, 15 | Передивитись презентації | 2 акад. | 2 акад. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | заняття | | | доповідей, *2 год* | год. | год. |
| 7 | **Тема 7. Архітектура кібербезпеки з кінця в кінець. Мережева модель кібербезпеки кіберсередовища.**<br><br>1. Системи захисту інформації та виявлення атак<br>2. Методи та технології забезпечення кібербезпеки<br>3. Інформаційна інфраструктура як об'єкт кібербезпеки<br>4. Проблеми кібербезпеки інформаційної інфраструктури<br><br>Доповіді студентів за темою заняття та їх обговорення. | Лекція | Презентація | 1 – 4, 6 - 8 | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття | 2 акад. год. | |
| | | Практичне заняття | доповіді студентів | 6, 7, 9, 10, 15 | Передивитись презентації доповідей, *2 год* | 2 акад. год. | |
| 8 | **Тема 8. Кіберрозвідка**<br><br>1. Поняття, види та форми кіберрозвідки<br>2. Принципи кіберрозвідки<br>3. Засоби і способи кіберрозвідки<br><br>Доповіді студентів за темою заняття та їх обговорення. | Лекція | Презентація | 1 – 4, 6 - 8 | Передивитись презентацію, *2 год*<br>Розподіл тем індивідуальних завдань серед студентів. Підготувати індивідуальне завдання та відповідну доповідь на наступне заняття | 2 акад. год. | 2 акад. год. |
| | | Практичне заняття | доповіді студентів | 6, 7, 9, 10, 15 | Передивитись презентації доповідей, *2 год* | 2 акад. год. | 2 акад. год. |

## 10. Система оцінювання та вимоги

Контроль знань і умінь студентів (поточний і підсумковий) з дисципліни «Основи кібербезпеки» здійснюється відповідно до «Положення про організацію освітнього процесу у Міжнародному гуманітарному університеті». Рейтинг студента із засвоєння дисципліни визначається за 100 бальною шкалою.

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю студентів, усне опитування, письмовий контроль, тестовий контроль.

Форма контролю: залік.

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в навчально-методичній карті. Розподіл балів між видами занять (лекції, практичні заняття, самостійна робота) можливий шляхом спільного прийняття рішення викладача і студентів на першому занятті. Рівень знань оцінюється:

«відмінно» – студент дає вичерпні, обґрунтовані, теоретично і практично правильні відповіді не менш ніж на 90% запитань, рішення задач та виконання вправ є правильними, демонструє знання матеріалу підручників, посібників, інструкцій, проводить узагальнення і висновки, акуратно оформлює завдання, був присутній на лекціях, має конспект лекцій чи реферати з основних тем курсу, проявляє активність і творчість у виконанні групових завдань;

«добре» – коли студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій і розрахунків, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді, був присутній на лекціях, має конспект лекцій чи реферати з основних тем курсу, проявляє активність у виконанні групових завдань;

«задовільно» – коли студент дає правильну відповідь не менше ніж на 60% питань, або на всі запитання дає недостатньо обґрунтовані, невичерпні відповіді, допускає грубі помилки, які виправляє за допомогою викладача. При цьому враховується наявність конспекту за темою завдань та самостійність, участь у виконанні групових завдань;

«незадовільно з можливістю повторного складання» – коли студент дає правильну відповідь не менше ніж на 35% питань, або на всі запитання дає необґрунтовані, невичерпні відповіді, допускає грубі помилки, має неповний конспект лекцій, індиферентно або негативно проявляє себе у виконанні групових завдань.

Підсумкова (загальна оцінка) курсу навчальної дисципліни є сумою рейтингових оцінок (балів), одержаних за окремі оцінювані форми навчальної діяльності: поточне та підсумкове тестування рівня засвоєння теоретичного матеріалу під час аудиторних занять та самостійної роботи (модульний контроль); оцінка (бали) за виконання практичних індивідуальних завдань. Підсумкова оцінка виставляється після повного вивчення навчальної дисципліни, яка виводиться як сума проміжних оцінок за усіма видами робіт, зазначені у таблиці нижче.

Виконання навчальних завдань і робота за дисципліною має відповідати вимогам «Положення про академічну доброчесність у Міжнародному гуманітарному університеті» (затверджене ректором наказом № 112 від 01.11.2018 року).

## КРИТЕРІЇ ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ СТУДЕНТІВ З ПІДСУМКОВИМ КОНТРОЛЕМ У ФОРМІ ЗАЛІКУ / ІСПИТУ

| *Денна форма навчання* | | | |
|---|---|---|---|
| **Види роботи** | **Планові терміни виконання** | **Форми контролю та звітності** | **Максимальна кількість балів** |

| | | | |
|---|---|---|---|
| **І. Обов'язкові** | | | |
| ***Систематичність і активність роботи на семінарських (практичних) заняттях*** | | | |
| 1.1. Підготовка до семінарських (практичних) занять | Відповідно до робочої програми та розкладу занять | Перевірка обсягу та якості засвоєного матеріалу під час семінарських (практичних) занять | **30** |
| ***Виконання модульних завдань*** | | | |
| 1.2. Підготовка до модульного контролю знань | -//- | Перевірка правильності виконання модульних завдань | **10** |
| ***Виконання завдань для самостійного опрацювання*** | | | |
| 1.3. Підготовка програмного матеріалу (тем, питань), що виноситься на самостійне вивчення | -//- | Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо | **10** |
| **Разом балів за обов'язкові види РС** | | | **50** |
| **ІІ. Вибіркові** | | | |
| ***Виконання індивідуальних завдань (науково-дослідна робота студента)*** | | | |
| 2.1. Підготовка реферату (есе) за заданою тематикою | Відповідно до графіку ІКР | Обговорення (захист) матеріалів реферату (есе) під час ІКР | **10** |
| 2.2. Аналітичний (критичний) огляд наукових публікацій, судової практики тощо | -//- | Перевірка та обговорення результатів проведеної роботи під час ІКР | **10** |
| 2.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо. | -//- | Обговорення результатів проведеної роботи під час аудиторних занять або ІКР, наукових конференцій та круглих столів. | **30** |
| **Разом балів за вибіркові види РС** | | | **50** |
| **ІІІ. Підсумковий контроль**<br>залік | | | **50** |
| **Всього балів за РС** | | | **100** |
| | | | |

[1] Індивідуально-консультативна робота викладача зі студентами

| *Заочна форма навчання* | | | |
|---|---|---|---|
| **Види самостійної роботи** | **Планові терміни виконання** | **Форми контролю та звітності** | **Максимальна кількість балів** |
| **І. Обов'язкові** | | | |
| ***Систематичність і активність роботи під час аудиторних занять*** | | | |
| 1.1. Підготовка до аудиторних занять | Відповідно до розкладу | Перевірка обсягу та якості засвоєного матеріалу під час аудиторних занять | **10** |
| ***За виконання модульних (контрольних) завдань*** | | | |
| 1.2. Підготовка до модульного контролю знань | -//- | Перевірка правильності виконання модульних завдань | **10** |
| ***Виконання завдань для самостійного опрацювання*** | | | |
| 1.3. Підготовка програмного матеріалу (тем, питань), що виноситься на самостійне вивчення | -//- | Розгляд відповідного матеріалу під час аудиторних занять або ІКР[2], перевірка конспектів навчальних текстів тощо | **30** |
| **Разом балів за обов'язкові види СРС** | | | **50** |
| **ІІ. Вибіркові** | | | |
| ***Виконання індивідуальних завдань (науково-дослідна робота студента)*** | | | |
| 2.1. Підготовка реферату (есе) за заданою тематикою | Відповідно до графіку ІКР | Обговорення (захист) матеріалів реферату (есе) під час ІКР | **10** |

[2] Індивідуально-консультативна робота викладача зі студентами

| | | | |
|---|---|---|---|
| 2.2. Аналітичний (критичний) огляд наукових публікацій, судової практики тощо | -//- | Перевірка та обговорення результатів проведеної роботи під час ІКР | **10** |
| 2.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо. | -//- | Обговорення результатів проведеної роботи під час ІКР, наукових конференцій та круглих столів. | **30** |
| Разом балів за вибіркові види СРС | | | **50** |
| **ІІІ. Підсумковий контроль**<br>залік | | | **50** |
| **Всього балів за РС** | | | **100** |

## 11. Рекомендована література

### Основна


1. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.
2. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Humanitarian vision. 2016. Vol. 2, Num. 1. С. 27-32.
3. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 // Офіційний вісник Президента України. 2017. № 5. С. 15. Ст. 102.
4. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII
5. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 р. № 96/2016// Офіційний вісник України. 2016. № 23. С. 69. Ст. 899.
6. Козлов С.Н. Защита информации: устройства несанкционированного съема информации и борьба с ними: Учебно-практическое пособие.— 2-е изд. — М.: Академический проект, 2018. 286 с.
7. Кібербезпека та системи захисту інформації: виклики сьогодення: збірник матеріалів круглого столу, м. Маріуполь, 26 жовтня2017 р. / Маріупольський державний університет; Кафедра математичних методів та системного аналізу; уклад. Тимофєєва І. Б. – Маріуполь.: МДУ, 2017. – 104 с.
8. Василенко М.Д., Новіков В.П., Рачук В.О., Слатвінська В.М. Кібербезпека в проявах ризиків у період пандемії: стан та генеза. Вісник Черкаського державного технологічного університету. 2020. Вип. 3. С. 30-39. DOI: 10.24025/2306-4412.3.2020.214774.
9. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. –Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.


### Допоміжна


1. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних. — К. : «Центр навчальної літератури», 2018. 558 с.
2. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки
3. ДСТУ ISO/IEC 27005:2015 (ISO/IEC 27005:2011, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки
4. Слатвінська В.М. Різновиди кібератак на судні в контексті управління кібербезпекою. Пріоритетні напрями розвитку науки та техніки: Матеріали LXII Міжнародної інтернет-конференції (м. Чернігів, 1 березня 2021 р.). 2021. С. 125-128.
5. Василенко М.Д., Рачук В.О., Слатвінська В.М. Шкідливі програми в контексті розуміння комп'ютерної вірусології та техніко-правової змагальності: міждисциплінарне дослідження. Наукові праці Національного університету «Одеська юридична академія». 2021. Т. 28. С. 28-36.
6. Слатвінська В. М. Особливості навчання правоохоронців основам кібербезпеки. Науково-педагогічне стажування Прикладні науково-технічні дослідження: європейський досвід і напрями розвитку (м. Прага, Чеська Республіка, 13 вересня – 24 жовтня 2021 року). 2021. Друк.


### Інформаційні ресурси

| | |
|---|---|
| 1. http://zakon2.rada.gov.ua/laws/show/2163-Про основні засади кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // Сайт «Законодавство України»<br>2. https://zakon.rada.gov.ua/laws/show/994_575 – Конвенція про кіберзлочинність | Офіційний веб-сайт Верховної Ради України |
| www.dsszzi.gov.ua. | Державна служба спеціального зв'язку та захисту інформації України |
| https://remontka.pro/virtualbox/ | віртуальна машина VirtualBox |
| https://zillya.ua/antivirusnalaboratoriya | Українська антивірусна лабораторія. / Єдиний український розробник інноваційних технологій кіберзахисту |
| https://securelist.com | Огляд різноманітних шкідливих програмних засобів |
| https://khm.gov.ua/uk/content/informaciyna-bezpeka-pry-roboti-u-merezhi-internet | Інформаційна безпека при роботі у мережі Інтернет |
| http://www.nbuv.gov.ua | Національна бібліотека України імені В.І. Вернадського |

Розробник:

викладач кафедри кримінального права, процесу та криміналістики _____ В. М. Слатвінська