МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

ІНСТИТУТ ПРАВА, ЕКОНОМІКИ ТА МІЖНАРОДНИХ ВІДНОСИН

Кафедра кримінального права, процесу та криміналістики

« ЗАТВЕРДЖУЮ »

Ректор, проф.

_____ К.В. Громовенко

«02» вересня 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ОСНОВИ КІБЕРБЕЗПЕКИ»

Галузь **26- Цивільна безпека**
(шифр і назва напряму підготовки)

Спеціальності **262- Правоохоронна діяльність**
(шифр і назва спеціальності)

Назви освітньо-наукових програм: **Правоохоронна діяльність**

Інститут права, економіки та міжнародних відносин
(назва інституту, факультету)

Рівень вищої освіти: **перший (бакалаврський)**

ОДЕСА - 2021 рік

Робоча програма навчальної дисципліни «**Основи кібербезпеки»** для здобувачів наукового ступеня бакалавра за спеціальністю 262 – Правоохоронна діяльність. 24 с.

Розробник:

Слатвінська В.М., викладач кафедри кримінального права, процесу та криміналістики Міжнародного гуманітарного університету.

(підпис) **/ Слатвінська В. М. /**
(прізвище та ініціали)

Робоча програма затверджена на засіданні кафедри кримінального права, процесу та криміналістики

Протокол № 1 від «20» серпня 2021 року

Завідувач кафедри
д.ю.н., професор

(підпис) **/ Подобний О. О./**
(прізвище та ініціали)

«20» серпня 2021 р.

Гарант освітньо-професійної програми
д.ю.н., професор.

(підпис) **/ Подобний О. О./**
(прізвище та ініціали)

«30» серпня 2021 р.

Схвалено Вченою радою Міжнародного гуманітарного університету
Протокол № 1 від «31» серпня 2021 року

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-професійний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів – 3</td><td>Галузь знань
26 - Цивільна безпека
(шифр і назва)</td><td colspan="2">Вибіркова</td></tr>
<tr><td>Модулів – 1</td><td rowspan="4">Спеціальність
262- Правоохоронна діяльність</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 1</td><td>3-й</td><td>4-й</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 90</td><td colspan="2">Семестр</td></tr>
<tr><td>6-й</td><td>8-й</td></tr>
<tr><td rowspan="11">Тижневих годин
- для денної форми навчання:
аудиторних – 1
самостійної роботи –4,3;
- для заочної форми навчання:
аудиторних – 0.6
самостійної роботи –5</td><td rowspan="11">Освітньо-кваліфікаційний рівень:
перший (бакалаврський)</td><td colspan="2">Лекції</td></tr>
<tr><td>16 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>14 год.</td><td>8 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>немає</td><td>немає</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>60 год.</td><td>72 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання:</td></tr>
<tr><td colspan="2">Вид контролю: залік</td></tr>
</table>

Навчальний курс «Основи кібербезпеки» присвячений вивченню об'єктів інформатизації, до яких відносяться комп'ютерні, автоматизовані, інформаційні та телекомунікаційні системи, інформаційні ресурси та інформаційні технології в умовах існування кіберзагроз в інформаційної сфері; технологій забезпечення інформаційної та кібернетичної безпеки об'єктів різного рівня (системи, їх об'єкти та компоненти), які пов'язані з інформаційними технологіями; механізмів забезпечення веб-безпеки, банківських систем та систем електронної комерції; процесів управління інформаційної безпекою об'єктів, що захищаються; методів розслідування інцидентів, управління ризиками та аудит систем інформаційної та кібернетичної безпеки; методики захисту від негативного інформаційного впливу тощо.

У сучасній конкурентній боротьбі широко поширені різноманітні дії, на отримання інформації самими різними способами, з використанням сучасних технічних засобів кіберрозвідки. 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 кібербезпеки та захисту інформації в діяльності майбутніх фахівців правознавців.

Предметом навчальної дисципліни є загальні теоретичні основи, методи та практичні засобі інформаційної кібербезпеки і захисту інформації, які необхідно використовувати в професійної діяльності фахівця правознавця.

При вивчені курсу «Основи кібербезпеки» використовуються знання студентів, одержані під час вивчення таких дисциплін як «Комп'ютерна криміналістика», «Інформаційне забезпечення професійної діяльності», «Судові та правоохоронні органи» та ін.

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

У процесі реалізації програми дисципліни «Основи кібербезпеки» формуються наступні компетентності із передбачених освітньо-науковою 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.

Очікувані результати навчання (компетентності освітньої складової)

Метою навчальної дисципліни є 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.

Завданнями вивчення курсу «Основи кібербезпеки» є оволодіння студентами знаннями щодо:

1) інституційні та правові механізіми забезпечення кібербезпеки
2) законодавці новації в сфері кібербезпеки
3) співвідношення кіберзлочинів та кіберзлочинності

Вимоги до знань та умінь студентів

Знати:

1) поняття та типи загроз в кібербезпеці
2) аналіз та оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки
3) методику виявлення, ідентифікації, аналізу та реагування на інциденти кібербезпеки;
4) загрози кібербезпеки в Україні;
5) Загрози кібербезпека в ЄС.

Уміти:

1) забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

2) впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;

3) аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;

4) застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;

5) впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

6) вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів з інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної/або кібербезпеки.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМА 1. ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення.
2. Поняття та види кіберзлочинів.
3. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.
4. Законодавство в даній області низки країн (США, Австралія, Китай і ряд інших). Питання судового переслідування.
5. Конфіденційність особистої інформації. Міжнародні і національні стандарти і специфікації в області інформаційної безпеки.
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.

ТЕМА 2. ЗАХИСТ ІНФОРМАЦІЇ У ПЕРСОНАЛЬНИХ КОМП'ЮТЕРАХ ТА В АВТОМАТИЗОВАНИХ СИСТЕМАХ

1. Найпоширеніші методи викрадення інформації (зламу паролів).
2. Стадії зламу отримання ключів та паролів. Ознаки можливого злому комп'ютера та його зараження шкідливими програмами.
3. Рекомендації з безпеки Вашого комп'ютера. Виявлення шкідливих програм зі шкідливими функціями, які беруть участь в атаках.
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.
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 застосування.
6. Використовування програмних та апаратних засобів розмежування доступу до інформації у автоматизованих системах та антивірусних засобів захисту інформації у персональних комп'ютерах.

ТЕМА 3. ІНФОРМАЦІЙНА БЕЗПЕКА ПРИ РОБОТІ У МЕРЕЖІ ІНТЕРНЕТ ТА У ВІДКРИТИХ КАНАЛАХ ЗВ'ЯЗКУ

1. Основні чинники, що впливають на стан інформаційної безпеки у зв'язку із використанням загальнодоступних та соціально орієнтованих ресурсів мережі Інтернет.

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.

3. Рекомендації щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет і перелік іноземних веб-ресурсів, якими не рекомендовано користуватись.

4. Методи і системи захисту мовленнєвої інформації, що передається у відкритих каналах зв'язку.

5. Стеганографічні та криптографічні систем захисту письмової інформації, що передається у відкритих каналах зв'язку.

ТЕМА 4. ОРГАНІЗАЦІЙНО-ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ. КОМПЛЕКСНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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.

2. Види інформації, яка може стати об'єктом злочинних посягань.

3. Поняття технічних каналів витоку інформації та механізм їх утворення. Види та класифікація технічних каналів витоку інформації та способів несанкціонованого зняття інформації.

4. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні. Визначення можливих джерел витоку інформації з радіоканалу.

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.

6. Методики і засоби пошуку радіозакладних пристроїв.

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 технічних засобів захисту інформації.

8. Комплексний підхід до забезпечення безпеки. Рекомендації щодо комплексного зміцнення інформаційної безпеки юридичного офісу.

ТЕМА 5. ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІАЛЬНОЇ РОБОТИ КОРИСТУВАЧА В ОС

1. Типи атак на інформаційні системи. Технології антивірусів та цілісності системи

2. Технології аудиту, моніторингу та менеджменту

3. Персональні дані і GDPR
4. Рекомендації в разі виявлення незаконного втручання в роботу електронно-обчислювальних машин фахівця.

ТЕМА 6. ПЕРЕХОПЛЕННЯ, ІДЕНТИФІКАЦІЯ І АНАЛІЗ ТРАФІКУ

1. Вимоги до кібербезпеки елементів телекомунікації
2. Методи і технології управління визначенням ідентичності

ТЕМА 7. АРХІТЕКТУРА КІБЕРБЕЗПЕКИ З КІНЦЯ В КІНЕЦЬ. МЕРЕЖЕВА МОДЕЛЬ КІБЕРБЕЗПЕКИ КІБЕРСЕРЕДОВИЩА

1. Системи захисту інформації та виявлення атак
2. Методи та технології забезпечення кібербезпеки
3. Інформаційна інфраструктура як об'єкт кібербезпеки
4. Проблеми кібербезпеки інформаційної інфраструктури

ТЕМА 8. КІБЕРРОЗВІДКА

1. Поняття, види та форми кіберрозвідки
2. Принципи кіберрозвідки
3. Засоби і способи кіберрозвідки

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		лекц.	прак	лаб	інд	сам. роб.		лекц	прак	лаб	інд	сам. роб.
1	2	3	4	5	6	7	8	9	10	11	12	13
Тема 1. Організаційно-правове забезпечення захисту інформації	11	2	2			7	6	2	2			6
Тема 2. Захист інформації у персональних комп'ютерах та в автоматизованих системах	11	2	2			7	6	2	-			6
Тема 3. Інформаційна безпека при роботі у мережі Інтернет та у відкритих каналах зв'язку	11	2	2			7	12	-	2			6
Тема 4. Організаційно-технічний захист інформації. Комплексне забезпечення інформаційної безпеки	11	2	2			7	12	2	-			6
Тема 5. Забезпечення конфіденціальної роботи користувача в ОС	11	2	2			7	12	2	-			6
Тема 6. Перехоплення, ідентифікація і аналіз трафіку	11	2	2			7	12	-	2			6
Тема 7. Архітектура кібербезпеки з кінця в кінець. Мережева модель кібербезпеки кіберсередовища	11	2				7	12	-	-			6
Тема 8. Кіберрозвідка	13	2	2			11	18	2	2			6
Усього годин	**90**	**16**	**14**			**60**	**90**	**10**	**8**			**72**

5. ТЕМИ СЕМІНАРСЬКИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин
1	**Тема 1. Організаційно-правове забезпечення захисту інформації** 1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення. 2. Поняття та види кіберзлочинів. 3. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності.	2 / 2
2	**Тема 2. Захист інформації у персональних комп'ютерах та в автоматизованих системах** 1. Найпоширеніші методи викрадення інформації (зламу паролів). 2. Стадії зламу отримання ключів та паролів. Ознаки можливого злому комп'ютера та його зараження шкідливими програмами. 3. Рекомендації з безпеки Вашого комп'ютера. Виявлення шкідливих програм зі шкідливими функціями, які беруть участь в атаках.	2 / -
3	**Тема 3. Інформаційна безпека при роботі у мережі Інтернет та у відкритих каналах зв'язку** 1. Основні чинники, що впливають на стан інформаційної безпеки у зв'язку із	- / 2

	використанням загальнодоступних та соціально орієнтованих ресурсів мережі Інтернет. 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.	
4	**Тема 4. Організаційно-технічний захист інформації. Комплексне забезпечення інформаційної безпеки** 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. 2. Види інформації, яка може стати об'єктом злочинних посягань. 3. Поняття технічних каналів витоку інформації та механізм їх утворення. Види та класифікація технічних каналів витоку інформації та способів несанкціонованого зняття інформації. 4. Визначення можливих джерел витоку акустичної та електромагнітної інформації у приміщенні. Визначення можливих джерел витоку інформації з радіоканалу.	2 / -
5	**Тема 5. Забезпечення конфіденціальної роботи користувача в ОС** 1. Типи атак на інформаційні системи. Технології антивірусів та цілісності системи 2. Технології аудиту, моніторингу та менеджменту	2 / -
6	**Тема 6. Перехоплення, ідентифікація і аналіз трафіку** 1. Вимоги до кібербезпеки елементів телекомунікації 2. Методи і технології управління визначенням ідентичності	- / 2
7	**Тема 7. Архітектура кібербезпеки з кінця в кінець. Мережева модель кібербезпеки кіберсередовища** 1. Системи захисту інформації та виявлення атак 2. Методи та технології забезпечення кібербезпеки	- / -
8	**Тема 8. Кіберрозвідка** 1. Поняття, види та форми кіберрозвідки 2. Принципи кіберрозвідки	2 / 2

6. САМОСТІЙНА РОБОТА

Самостійна робота з дисципліни складається з опрацювання навчального матеріалу:

- опрацювання лекційного матеріалу;
- самостійне опрацювання окремих питань навчальної дисципліни;
- підготовка до семінарських занять;
- підготовка до підсумкового контролю.

Конспект із виконаним завданням подається викладачу на перевірку під час проведення відповідного семінарського заняття, або в інший, визначений викладачем час. Загальний підсумок самостійної роботи з вивчення курсу фіксується під час складення заліку.

№ з/п	Назва теми	Кількість годин
1	**Тема 1. Організаційно-правове забезпечення захисту інформації** 1. Законодавство в даній області низки країн (США, Австралія, Китай і ряд інших). Питання судового переслідування. 2. Конфіденційність особистої інформації. Міжнародні і національні стандарти і	7 / 6

	специфікації в області інформаційної безпеки. 3. 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.	
2	**Тема 2. Захист інформації у персональних комп'ютерах та в автоматизованих системах** 1. 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. 2. 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 застосування. 3. Використовування програмних та апаратних засобів розмежування доступу до інформації у автоматизованих системах та антивірусних засобів захисту інформації у персональних комп'ютерах.	7 / 6
3	**Тема 3. Інформаційна безпека при роботі у мережі Інтернет та у відкритих каналах зв'язку** 1. Рекомендації щодо забезпечення інформаційної безпеки при роботі в мережі Інтернет і перелік іноземних веб-ресурсів, якими не рекомендовано користуватись. 2. Методи і системи захисту мовленнєвої інформації, що передається у відкритих каналах зв'язку. 3. Стеганографічні та криптографічні систем захисту письмової інформації, що передається у відкритих каналах зв'язку.	7 / 6
4	**Тема 4. Організаційно-технічний захист інформації. Комплексне забезпечення інформаційної безпеки** 1. 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. 2. Методики і засоби пошуку радіозакладних пристроїв. 3. 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 технічних засобів захисту інформації. 4. Комплексний підхід до забезпечення безпеки. Рекомендації щодо комплексного зміцнення інформаційної безпеки юридичного офісу.	7 / 6
5	**Тема 5. Забезпечення конфіденціальної роботи користувача в ОС** 1. Персональні дані і GDPR 2. Рекомендації в разі виявлення незаконного втручання в роботу електронно-обчислювальних машин фахівця.	7 / 6
6	**Тема 6. Перехоплення, ідентифікація і аналіз трафіку** 1. Вимоги до кібербезпеки елементів телекомунікації 2. Методи і технології управління визначенням ідентичності	7 / 6
7	**Тема 7. Архітектура кібербезпеки з кінця в кінець. Мережева модель кібербезпеки кіберсередовища** 1. Інформаційна інфраструктура як об'єкт кібербезпеки 2. Проблеми кібербезпеки інформаційної інфраструктури	7 / 6
8	**Тема 8. Кіберрозвідка** 1. Засоби і способи кіберрозвідки	11 / 6

7. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальне завдання з навчальної дисципліни є формою самостійної обов'язкової роботи здобувача і виконується у вигляді реферативної роботи.

Реферат повинен мати титульний лист, вступ, основні розділи (2–4), висновки, список використаних джерел. Цитати, фактичні і статистичні матеріали, наведені в тексті, обов'язково мають супроводжуватися посиланнями на використані джерела.

При написанні реферату слід дотримуватися наступних вимог:

1. Обов'язковою умовою написання реферату є план, що складається не менше, ніж з 3-х пунктів, а також вступ та висновки, які повинні виражати власне ставлення студента до обраної теми.

2. Робота має мати обсяг не менш 10-ти друкованих сторінок тексту

3. Друкування тексту - за допомогою комп'ютера здійснюється через 1,5 міжрядкових інтервали, 14 кегль, шрифт Times New Roman. Поля: зліва - 30 мм; праворуч - 10-15 мм; вгорі і знизу - 20 мм.

Теми рефератів

1. Окремі аспекти інформаційно-аналітичного забезпечення правоохоронної діяльності
2. Правове регулювання основних термінів щодо систем обробки інформації у сфері забезпечення кібербезпеки в Україні
3. Освітні заходи превенції кіберзлочинності в Україні
4. Правове регулювання захисту інформації
5. Кіберзагрози Європи та боротьба з ними на прикладі Німеччини
6. Сучасний стан наукового забезпечення та перспективи формування методики розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку
7. Правове регулювання феномену цифрової людини як фактор забезпечення кібербезпеки
8. Запобігання та протидія торгівлі людьми в мережі Інтернет
9. Стан і актуальні задачі кіберзахисту в системах розрахунків та платіжних системах України
10. Захист персональних даних в інформаційному суспільстві
11. Кібербезпека як складова інформаційної безпеки у сфері охорони державного кордону України
12. Хмарний шлюз інтернет-безпеки cisco umbrella
13. Використання систем відеоспостереження, як джерела доказової інформації
14. Вдосконалення біометричних інформаційних систем ідентифікації осіб як чинник у протидії торгівлі людьми

15. Сучасні проблеми забезпечення підготовки персоналу по боротьбі з кіберзлочинністю в Україні

16. Значення інформаційно-аналітичної розвідки у діяльності спеціальних служб

17. Проблеми підготовки іт-фахівців в Україні

18. Нормативно-правове регулювання протидії правоохоронних органів загрозам у кіберпросторі в Україні

19. Інформаційно-аналітична діяльність як запорука підвищення ефективності роботи Національної поліції у протидії злочинності

20. Проблеми кваліфікації та криміналізації фішингу

21. Кібербезпека та інтелектуальна власність: питання правового забезпечення

22. Актуальні аспекти підготовки кадрів з попередження кіберзлочинності в Україні

23. Місце аналітиків в правоохоронній системі України

24. Психологічні особливості осіб, які вчиняють злочини у сфері високих технологій

25. Проблеми взаємодії слідчого з оперативними та інформаційно-аналітичними підрозділами Національної поліції України

26. Кібербезпека – важливий напрям діяльності органів державної влади щодо захисту суспільства

27. Інформаційно-аналітичне забезпечення та особливості здійснення пошуку осіб, які становлять оперативний інтерес у злочинах, пов'язаних з торгівлею людьми

8. МЕТОДИ КОНТРОЛЮ

Система оцінювання та вимоги

Контроль знань і умінь здобувачів (поточний і підсумковий) з дисципліни «Основи кібербезпеки» здійснюється відповідно до «Положення про організацію освітнього процесу у Міжнародному гуманітарному університеті» та «Положення про порядок оцінювання результатів навчальної діяльності здобувачів передвищої та вищої освіти». Рейтинг здобувача із засвоєння дисципліни визначається за 100 бальною шкалою.

Види контролю: поточний, підсумковий.

Методи контролю: спостереження за навчальною діяльністю здобувачів, усне опитування, письмовий 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:

«зараховано» A - від 90 до 100 балів. Здобувач виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

«зараховано» B - здобувач володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, розрахунків, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;

«зараховано», C - від 74 до 81 балів. Здобувач відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;

«зараховано», D - від 64 до 73 балів. Здобувач був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);

«зараховано» E - від 60 до 63 балів. Здобувач був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.

«не зараховано» FX – від 35 до 59 балів. Здобувач володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.

«не зараховано» F – від 0 до 34 балів. Здобувач не володіє навчальним матеріалом.

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).

Навчальна дисципліна «Основи кібербезпеки» викладається за кредитно-модульною системою організації навчального процесу (КМСОНП). Дана система запроваджується з метою удосконалення системи контролю якості знань студентів, сприяння формуванню системних та систематичних знань, ритмічної самостійної роботи впродовж семестру, підвищення об'єктивності оцінювання знань та адаптації до вимог, визначених Європейською системою залікових кредитів (ECTS).

Оцінювання знань здобувачів повинно сприяти реалізації низки завдань, зокрема:

- підвищення мотивації здобувачів до системного навчання впродовж семестру та навчального року, переорієнтація їх цілей з отримання позитивної оцінки на формування системних, стійких знань, умінь та навичок;
- відкритість контролю, яка базується на ознайомленні здобувачів на початку вивчення дисципліни переліком, формами та змістом контрольних завдань, критеріями та порядком їх оцінювання;
- розширення можливостей для всебічного розкриття здібностей здобувачів, розвитку їх творчого мислення, та підвищення ефективності навчального процесу.

У випадку відсутності здобувача на лекції або семінарському занятті він ***зобов'язаний*** відпрацювати пропущене заняття через усне опитування в поза аудиторний час (час консультацій викладача) або відпрацювати пропущене заняття протягом одного тижня з моменту його появи. Невідпрацьовані заняття вважаються незданими і за них не нараховується оцінка в балах. За 10 днів до початку сесії викладач припиняє приймати відпрацювання.

9. КРИТЕРІЇ ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ ЗДОБУВАЧІВ

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	**40**
Виконання модульних завдань			
1.2. Підготовка до модульного контролю знань	-//-	Перевірка правильності виконання модульних завдань	**35**
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 ІКР1, перевірка конспектів навчальних текстів тощо	**10**
Разом балів за обов'язкові види РС			**85**

ІІ. Вибіркові			
Виконання індивідуальних завдань			
2.1. Підготовка реферату (есе) за заданою тематикою	Відповідно до графіку ІКР	Обговорення (захист) матеріалів реферату (есе) під час ІКР	**5**
2.2. Аналітичний (критичний) огляд наукових публікацій, судової практики тощо	-//-	Перевірка та обговорення результатів проведеної роботи під час ІКР	**5**
2.3. Інші види індивідуальних завдань	-//-	Обговорення результатів проведеної роботи під час аудиторних занять або ІКР	**5**

1 Індивідуально-консультативна робота викладача зі студентами

Разом балів за вибіркові види РС			**15**
Всього балів за РС			**100**
Заочна форма навчання			
Види самостійної роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальна кількість балів**
І. Обов'язкові			
За виконання модульних (контрольних) завдань			
1.1. Підготовка до модульного контролю знань	Відповідно до розкладу	Перевірка правильності виконання модульних завдань	**70**
Разом балів за обов'язкові види СРС			**70**
ІІ. Вибіркові			
Виконання індивідуальних завдань (за бажанням 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	-//-	Обговорення результатів проведеної роботи під час ІКР	**10**
Разом балів за вибіркові види СРС			**30**
Всього балів за РС			**100**

Підсумковий контроль знань по даній дисципліні проводиться у формі *заліку (усні питання та письмове завдання)*. Питання, що включаються програми заліку є вузловими, узагальненими, комплексними, потребують творчого підходу при побудові відповіді та уміння синтезувати отриманні знання. Питання до заліку формуються в межах змісту програми дисципліни. Програмні питання доводяться до студентів на початку навчального семестру. Підсумкове оцінювання знань студентів здійснюється з урахуванням результатів оцінювання поточної роботи в семестрі та результатів заліку за 100-бальною системою.

10. ПИТАННЯ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ ЗНАНЬ

1. Сучасні типи кіберзагроз
2. Ризики та кібебезпека в умовах пандемії
3. Білий хакінг як новий інститут для підтримки кібербезпеки
4. Сучасні підходи до поняття «кіберзлочин» та «кіберзлочинність»
5. Проблеми кіберпростору в Україні
6. Розслідування кіберзлочинів: вітчизняний та міжнародний досвід
7. Сутність та підходи до визначення кібербезпеки
8. Видова характеристика кібербезпеки
9. Космічна фрактальність як важливий критерій кібербезпеки
10. Методи вивчення кібербезпеки
11. Міжнародні аспекти кібербезпеки в умовах глобалізації
12. Кіберзлочинність як глобальна загроза економічній безпеці
13. Правовий потенціал безпечного функціонування кіберпростору
14. Концептуальні нормативно-правові засади забезпечення кібернетичної безпеки в Україні
15. Проблемні питання кіберзлочинності в Україні
16. Протидія кіберзлочинності, як один із основних напрямів діяльності держави
17. Питання правового регулювання протидії кіберзлочинності на теренах України
18. Стан кібербезпеки україни: нормативно-правового аспект
19. Правові основи кібербезпеки в Україні
20. Основні аспекти профілактики та запобігання кіберзлочинності, як загрози українському суспільству
21. Міжнародне законодавство у сфері протидії кіберзлочинності
22. Кіберзлочинність: основні заходи запобігання
23. Підходи до розробки програмного забезпечення систем кібербезпеки
24. Запровадження криміналістичного профайлінгу у діяльність органів національної поліції україни
25. Кіберзлочинність у відмиванні коштів
26. Боротьба з кіберзлочинністю вітчизняний і зарубіжний досвід
27. Загальні основи виявлення кіберзлочинів
28. Соціально-психологічні підходи до профілактики кіберзлочинності
29. Особливості здійснення досудового розслідування кіберзлочинів
30. Особливості використання технологій кримінального аналізу у протидії кіберзлочинності
31. Інформаційно-аналітична діяльність підрозділів кримінальної поліції з протидії організованій злочинності

32. Організаційні аспекти взаємодії суб'єктів боротьби з тероризмом щодо кібербезпеки
33. Особливості роботи правоохоронних органів щодо протидії кібератаки в умовах проведення операції об'єднаних сил
34. Діяльність СБ України щодо захисту критичної інфраструктури від кібератак
35. Інформаційно-аналітична складова пред'явлення для впізнання в умовах тактичного ризику
36. Європейський досвід правового регулювання забезпечення кібербезпеки
37. Запобігання кіберзлочинності в Україні: актуальна кримінологічна проблема
38. Використання знань про особливості криптовалют у протидії злочинності
39. Кримінальна відповідальність за злочини вчиненні у сфері кібепростору
40. Кібершпіонаж - загроза сучасному інформаційному суспільству
41. Національне законодавство із забезпечення кібербезпеки в Україні
42. Правові засади забезпечення кібербезпеки держоргану «Національне агентство з питань запобігання корупції»
43. Використання електронних доказів при розслідувані кіберзлочинів
44. Кібертероризм: поняття та шляхи протидії
45. Кіберзлочинність: поняття, види, загрози та ризики
46. Актуальні засади захисту інформації, що обробляється в автоматизованих системах державної прикордонної служби України
47. Стандарти управління інформаційною безпекою
48. Кіберзлочинність в Україні: види, наслідки таспособи боротьби
49. Система забезпечення кібербезпеки в Україні: сутність та призначення
50. Забезпечення кібербезпеки в управлінні організацією праці на підприємстві
51. Протидія комп'ютерній злочинності в кібернетичному просторі
52. Способи та методи попередження та протидії легалізації доходів, одержаних у сфері кіберзлочинності
53. Роль спеціаліста у технічному забезпеченні проведення слідчих (розшукових) дій
54. Особливості діяльності правоохоронних органів України в рамках сучасних інформаційних технологій
55. Використання сучасних технологій відеоаналітики в органах Національної поліції
56. SRS Femida – сучасна система технічної фіксації судового процесу
57. Використання інформаційних технологій під час розслідування злочинів
58. Особливості співробітництва правоохоронних органів країн ЄС у сфері протидії кібертероризму

59. Проблемні питання захисту персональних даних при використанні інформаційних систем та технологій в боротьбі зі злочинністю
60. Криміналістичний моніторинг як метод боротьби з кіберзлочинністю
61. Стан кібербезпеки в Україні
62. Кібервійна проти України
63. Кібервійни та протидія зовнішній кібернетичній агресії
64. Кіберзахист критичної інфраструктури
65. Кібербезпека Інтернет речей
66. Кіберзлочинність та кібертероризм
67. Операції правоохоронних органів та судові справи проти кіберзлочинців
68. Технічні та програмні рішення для протидії кібернетичним загрозам
69. Вірусне та шкідливе програмне забезпечення в кіберпросторі

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІПВіП 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 жовтня 2017 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. С. 63-65.

7. Подобний О. О., Слатвінська В.М. Основні завдання інформатизації правоохоронної діяльності. Юридичний науковий електронний журнал. № 9. 2021. С. 180-182. DOI https://doi.org/10.32782/2524-0374/2021-9/43

8. Бойко В. Д., Василенко М. Д., Слатвінська В. М. Живучість та стійкість функціонування компонентів інформаційних систем розумного міста. Науково-технічний збірник «Комунальне господарство міст». Серія: технічні науки та архітектура. Том. 6 № 166. 2021. С. 20-27.

9. Dmytro Kabachenko, Olena Churikanova, Svitlana Oneshko, Ruslan Avhustyn, Valeria Slatvinska. Application of information technologies for management quality decision making in the conditions of the instability of the external economic space. International journal for Quality research. V 16 n 4 2022. DOI: 10.24874/IJQR16.04-11 Scopus

10. Слатвінська В. М. Штучний інтелект інструмент чи загроза кібербезпеки? Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (випуск 65) (м. Тернопіль, 8 лютого 2022 р). 2022. http://www.konferenciaonline.org.ua/ua/articles/year-2/rozdil-11/pidrozdil-32/pidrozdil2-0/

11. Інтелектуальні системи захисту інформації в кіберпросторі : навчально-методичні рекомендації (в допомогу до самостійної роботи для здобувачів вищої освіти кваліфікації бакалавр факультету кібербезпеки та інформаційних технологій) / М. Д. Василенко, В. О. Рачук, В. М. Слатвінська. Одеса : Видавничий дім «Гельветика», 2021. - 32 с. https://hdl.handle.net/11300/14945

Інформаційні ресурси

http://zakon2.rada.gov.ua/laws/show/2163	Про основні засади кібербезпеки України : Закон України
https://zakon.rada.gov.ua/laws/show/994_575	Конвенція про кіберзлочинність
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