МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
Т.в.о. декана юридичного факультету

Валентина СЛОМА _____
“29” 08 2025 р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи

Віктор ОСТРОВЕРХОВ _____
“29” 08 2025 р.

ЗАТВЕРДЖУЮ
Директор Навчально-наукового
інституту новітніх освітніх технологій

Святослав ПИТЕЛЬ
“29” 08 2025 р.

РОБОЧА ПРОГРАМА
з дисципліни
“ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ”

ступінь вищої освіти – бакалавр
галузь знань – 25 Воєнні науки, національна безпека, безпека національного кордону
спеціальності 256 Національна безпека (за окремими сферами забезпечення та видами діяльності)
освітньо-професійна програма – «Національна безпека (за окремими сферами забезпечення та видами діяльності)»

Кафедра безпеки та правоохоронної діяльності

Форма навчання	Курс	Семе-стр	Лек-ції (год.)	Практ. (год.)	ІРС (год)	Тренінг (год.)	СРС (год.)	Разом (год.)	Залік (сем.)
Денна	2	2	30	30	4	8	78	150	2
заочна	2	3,4	8	4	-	-	138	150	4

29.08 гуд

Тернопіль – ЗУНУ
2025

Робочу програму розробила к.е.н., доцент, в.о. завідувача кафедри безпеки та правоохоронної діяльності Юлія МУРАВСЬКА.

Робоча програма затверджена на засіданні кафедри безпеки та правоохоронної діяльності, протокол № 2 від 26 серпня 2025 р.

В.о. завідувача кафедри
безпеки та правоохоронної діяльності
к.е.н., доцент Юлія МУРАВСЬКА

Гарант ОП Василь ОМЕЛЬЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
“Протидія кіберзлочинності”

1. Опис дисципліни
“Протидія кіберзлочинності”

Дисципліна „Протидія кіберзлочинності ”	Галузь, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 5	Галузь знань: 25 «Воєнні науки, національна безпека, безпека національного кордону»	Статус дисципліни (вибіркова) Мова навчання українська
Кількість залікових модулів – 4	Спеціальність 256 «Національна безпека (за окремими сферами забезпечення та видами діяльності)»	Рік підготовки : денна – 2 заочна – 2 Семестр: денна – 2 Заочна – 3,4
Кількість змістових модулів – 2	Ступінь вищої освіти – бакалавр	Лекції: Денна – 30 год. заочна – 8 год. Практичні заняття: Денна – 30 год. Заочна – 4 год.
Загальна кількість годин – 150		Самостійна робота: Денна – 78 год. Тренінг – 8 год. Заочна – 138 год. Індивідуальна робота – Денна – 4 год.
Тижневих годин: 10год. з них аудиторних – 2 год.		Вид підсумкового контролю - залік

2. Мета й завдання дисципліни
„ Протидія кіберзлочинності”

2.1. Мета вивчення дисципліни

Мета навчальної дисципліни полягає в формуванні комплексних знань про правове регулювання запобігання кіберзлочинності, вивченні національних і міжнародних підходів до забезпечення кібербезпеки, розвитку ключових навичок застосування національного законодавства, активізації аналітичної роботи студентів, проведенні наукових досліджень і формуванні практичних навичок правозастосування.

2.2. Завдання вивчення дисципліни

Завдання дисципліни:

- Формування теоретичних знань про інститут кібербезпеки та його зміст;
- Опанування інструментів для запобігання кіберзлочинам і базових понять кібербезпеки;
- Визначення поняття, видів та стану кіберзлочинності: рівня, структури, динаміки та інших характеристик;
- Аналіз та дослідження практичних проблем формування і реалізації державної політики у сфері кібербезпеки, орієнтованих на набуття і підтвердження суб’єктивних прав і обов’язків приватних осіб відповідно до закону;
- Опис характеристик, класифікацій і видів кіберзлочинів, аналіз їхньої структури, визначення стадій і етапів, а також повноважень суб’єктів запобігання кіберзлочинності;
- Розвиток навичок і умінь у запровадженні та застосуванні заходів протидії кіберзлочинам.

Виходячи з поставленого завдання навчальної дисципліни, студенти і слухачі повинні знати:

- сутність протидії кіберзлочинності як складової національної економічної безпеки; національні інтереси в сфері інформаційної безпеки; інституційні умови та принципи управління інтелектуальною безпекою; види загроз та ризиків для національної економічної безпеки у сфері інтелектуальної власності за умов глобалізації; основні організаційно-економічні механізми захисту інтелектуальної власності на рівні держави; сутність і складові протидії кіберзлочинності підприємства; поняття комерційної таємниці, конкурентної розвідки; завдання і функції служби економічної безпеки щодо захисту комерційної таємниці; переваги та недоліки убезпечення інтелектуальної власності через механізм комерційної таємниці; способи захисту комерційно цінної інформації при переговорах із потенційними партнерами; загрози та ризики для протидії кіберзлочинності об’єктів; поняття та цілі «Due Diligence»; ризики зарубіжного патентування; сутність патентного тролінгу; особливості захисту авторських та суміжних прав у мережі Інтернет; сутність, види страхування інтелектуальної власності;
- поняття і завдання, мету і завдання, стратегію і тактику формування системи протидії кіберзлочинності.

Одержані теоретичні знання дадуть змогу студентам та слухачам у майбутньому як фахівцям у сфері правоохоронної діяльності вміти вирішувати такі завдання:

- ідентифікувати внутрішні та зовнішні загрози, виявляти ризики протидії кіберзлочинності на рівні держави; прогнозувати наслідки реалізації загроз / ризиків для національної економіки;

обґрунтовувати напрями подолання загроз та нейтралізації ризиків національної економічної безпеки в сфері інтелектуальної власності; розробляти механізми узгодження інтересів суб'єктів відносин інтелектуальної власності, заходи з убезпечення інтелектуальної власності при міжнародному науково-технічному співробітництві, запобігання промисловому шпигунству; виявляти потенційні шляхи втрати об'єктів інтелектуальної власності підприємства; враховувати специфіку управління безпекою за фазами життєвого циклу об'єктів інтелектуальної власності; розробляти та координуватизаходи з попередження та нейтралізації опортуністичної поведінки працівників, визначати та застосовувати інструменти закріплення і збереження на підприємстві інтерспецифічних інтелектуальних трудових ресурсів; виявляти ознаки ведення конкурентної розвідки щодо підприємства, застосовувати систему раннього конкурентного попередження; ідентифікувати відомості, що складають комерційну таємницю; розробляти систему заходів щодо захисту комерційної таємниці; приймати рішення щодо доцільності укладення договору про конфіденційність, опціонної угоди; визначати найбільш ефективний вид патенту для захисту об'єктів права інтелектуальної власності, доцільність застосування міжнародної або традиційної процедури патентування; приймати управлінські рішення щодо вибору механізмів захисту об'єктів інтелектуальної власності.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із основними сучасними методами формування системи протидії кіберзлочинності.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних питань щодо формування системи протидії кіберзлочинності в контексті національної безпеки; законодавчої та нормативної бази.
- сформувати у студентів цілісну систему теоретичних знань з курсу „Протидія кіберзлочинності".

Завдання практичних занять

Мета проведення практичних занять полягає в тому, щоб виробити у студентів навички практично застосувати сучасні методи протидії кіберзлочинності, чинне законодавство України, які регулюють боротьбу з загрозами для майбутнього використання в правоохоронній діяльності.

Завдання проведення практичних занять:

- розв'язувати конкретні питання стосовно використання сучасних форм протидії кіберзлочинності;
- практично вирішувати питання щодо класифікування методів та форм протидії кіберзлочинності;
- орієнтуватись на інтелектуальній безпеці;
- засвоїти методику та техніку виконання превентивних заходів формування системи протидії кіберзлочинності.

3. Програма навчальної дисципліни:
„ Протидія кіберзлочинності"

Змістовний модуль 1. Протидія кіберзлочинності: загальнотеоретичний аспект

Тема 1. Протидія кіберзлочинності в системі забезпечення національної економічної безпеки
1. Протидія кіберзлочинності як складова національної економічної безпеки.
2. Напрями виявлення цифрових загроз у сфері забезпеченн кібербезпеки.
3. Оцінка ризиків у сфері забезпеченн кібербезпеки

Тема 2. Об'єкти та суб'єкти системи протидії кіберзлочинності
1 Об'єкти системи протидії кіберзлочинності в системі інформаційної безпеки
2 Суб'єкти протидії кіберзлочинності
3 Надійність пароля як інструмент забезпечення кібербезпеки

Тема 3. Кіберзлочини у системі Он-лайн
1. Безпека он-лайн екаунтів.
2. Умови, що сприяють вчиненню кіберзлочину у соціальних мережах
3. Умови, що сприяють вчиненню кіберзлочину у месенджерах
4. Безпека сайтів

Тема 4. Кіберзлочинність
1. Поняття кіберзлочинності
2. Вимірювання рівня кіберзлочинності.
3. Структура кіберзлочинності.

Тема 5. Фактори впливу на кіберзлочинність
1. Соціальні фактори
2. Правові фактори
3. Технічні фактори. Захист пристроїв від фізичного доступу

Тема 6. Ознаки кіберзлочинності в умовах воєнного стану
1. Географія кіберзлочинності.
2. Структура кіберзлочинності.
3. Латентність кіберзлочинності

Тема 7. Кіберзлочинець
1. Кіберзлочинець як базовий елемент системи кіберзагроз.
2. Соціально-демографічні ознаки особи кіберзлочинця.
3. Морально-психологічні якості і особистісно- рольові властивості особи кіберзлочинця.
4. Типологія кіберзлочинців.

Змістовий модуль 2. Протидія кіберзлочинності: прикладний аспект
Тема 8. Кіберзлочинність проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
1. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
2. Основні риси кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
3. Причини кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
4. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

Тема 9 . Кіберзлочинність, пов'язана з використанням комп'ютера як засобу скоєння злочинів
1. Комп'ютерне шахрайство.
2. Особистість кібершахрая, основні риси.

3. Причини і умови кіберзлочинності, пов’язаної з використанням комп’ютера
4. Запобігання кіберзлочинності, пов’язаної з використанням комп’ютера

Тема 10. Кіберзлочинність, пов’язана з з контентом (змістом даних), розміщених у комп’ютерних мережах.
1. Кіберзлочинність, пов’язана з контентом (змістом даних), розміщених у комп’ютерних мережах.
2. Характеристика кіберзлочинності, що пов’язана з контентом (змістом даних), розміщених у комп’ютерних мережах.
3. Особистість кіберзлочинця, що пов’язана з контентом (змістом даних), розміщених у комп’ютерних мережах.
4. Причини і умови кіберзлочинів, пов’язаних з контентом, розміщених у комп’ютерних мережах

Тема 11. Кіберзлочинність, пов’язана з порушенням авторського права і суміжних прав
1. Поняття авторського права і суміжних прав.
2. Об’єкти авторського права і суміжних прав
3. Суб’єкти авторського права і суміжних прав.
4. Запобігання кіберзлочинам пов’язаних з порушенням авторського права і суміжних прав

Тема 12. Інформаційне поле під час війни
1. Відмінність між внутрішніми та зовнішніми маніпуляторами
2. Ворожі інформаційні операції
3. ЗМІ в системі кіберзагроз.

Тема 13. Російська пропаганда
1. Сутність та принципи російської пропаганди
2. Анонімні канали та їх безпечність
3. Блогери-інсайдери як кіберзагроза.
4. Інформаційно-психологічні операції

Тема 14. Кіберзлочинність у сфері російської пропаганди. ІПСО
1. ІПСО «переселенці».
2. Складові інформаційного тероризму росії

Тема 15. Правила інформаційної гігієни в період введення воєнного стану
1. Маніпуляції в інформаційному полі
2. Шахрайства в мережі та методи їхнього запобігання

4. Структура залікового кредиту з дисципліни
„ Протидія кіберзлочинності”
денна форма навчання

	Кількість годин					
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	Гре нінг	Контр. заходи
Змістовий модуль 1 . Протидія кіберзлочинності: загальнотеоретичний аспект						

Тема 1. Протидія кіберзлочинності в системі забезпечення національної економічної безпеки	2	2	6			Питання для обговорення
Тема 2. Об’єкти та суб’єкти системи протидії кіберзлочинності	2	2	4			Тести, питання
Тема 3. Кіберзлочини у системі Он-лайн	2	2	6	1		Тести, задачі, питання
Тема 4. Кіберзлочинність	2	2	6	1		Тести, задачі, питання
Тема 5. Фактори впливу на кіберзлочинність	2	2	4	1		Тести, задачі, питання
Тема 6. Ознаки кіберзлочинності в умовах воєнного стану	2	2	6			Тести, питання
Тема 7. Кіберзлочинець	2	2	4			Тести, питання
Змістовий модуль 2 . Протидія кіберзлочинності: прикладний аспект						
Тема 8. Кіберзлочинність проти конфіденційності, цілісності та доступності комп’ютерних даних і систем	2	2	6			Тести, кейси
Тема 9 . Кіберзлочинність, пов’язана з використанням комп’ютера як засобу скоєння злочинів	2	2	4			Тести, питання
Тема 10. Кіберзлочинність, пов’язана з з контентом (змістом даних), розміщених у комп’ютерних мережах	2	2	4			Тести, питання
Тема 11. Кіберзлочинність, пов’язана з порушенням авторського права і суміжних прав	2	2	6		4	Тести, питання
Тема 12. Інформаційне поле під час війни	2	2	6			Тести, задачі, питання
Тема 13. Російська пропаганда	2	2	6	1	4	Питання
Тема 14. Кіберзлочинність у сфері російської пропаганди. ІПСО	2	2	6			Кейси
Тема 15. Правила інформаційної гігієни в період введення воєнного стану	2	2	4			Тести, питання
Разом	30	30	78	4	8	

заочна форма навчання

	Кількість годин			
	Лекції	Практичні заняття	Самостійна робота	
Змістовий модуль 1 . Протидія кіберзлочинності: загальнотеоретичний аспект				

Тема 1. Протидія кіберзлочинності в системі забезпечення національної економічної безпеки	1		10	
Тема 2. Об’єкти та суб’єкти системи протидії кіберзлочинності	1		8	
Тема 3. Кіберзлочин у системі Он-лайн	1	1	10	
Тема 4. Кіберзлочинність	1	1	10	
Тема 5. Фактори впливу на кіберзлочинність	1	1	10	
Тема 6. Ознаки кіберзлочинності в умовах воєнного стану			10	
Тема 7. Кіберзлочинець			5	
Змістовий модуль 2 . Протидія кіберзлочинності: прикладний аспект				
Тема 8. Кіберзлочинність проти конфіденційності, цілісності та доступності комп’ютерних даних і систем	1		5	
Тема 9. Кіберзлочинність, пов’язана з використанням комп’ютера як засобу скоєння злочинів			10	
Тема 10. Кіберзлочинність, пов’язана з з контентом (змістом даних), розміщених у комп’ютерних мережах			10	
Тема 11. Кіберзлочинність, пов’язана з порушенням авторського права і суміжних прав			10	
Тема 12. Інформаційне поле під час війни			10	
Тема 13. Російська пропаганда	1	1	10	
Тема 14. Кіберзлочинність у сфері російської пропаганди. ІПСО	1		10	
Тема 15. Правила інформаційної гігієни в період введення воєнного стану			10	
Разом	8	4	138	

5. Тематика практичних занять

Практичне заняття 1. Протидія кіберзлочинності в системі забезпечення національної економічної безпеки

Питання для обговорення:

1. Протидія кіберзлочинності як складова національної економічної безпеки.
2. Напрями державної політики у сфері забезпеченн кібербезпеки.
3. Оцінка ризиків у сфері забезпеченн кібербезпеки

Мета: Визначення поняття та формування системи протидії кіберзлочинності в контексті національної безпеки

Література: 1, 2, 5, 7

Практичне заняття 2. Об’єкти та суб’єкти системи протидії кіберзлочинності

Питання для обговорення:

1 Об’єкти системи протидії кіберзлочинності в системі інформаційної безпеки

2 Суб'єкти протидії кіберзлочинності
3 Надійність пароля як інструмент забезпечення кібербезпеки
Мета: Засвоїти та закріпити теоретичні знання щодо питання сутності об'єктів та суб'єктів протидії кіберзлочинності в системі інформаційної безпеки

Література: 1, 3, 7,12.

Практичне заняття 3. Кіберзлочин у системі Он-лайн
Питання для обговорення:
1. Безпека он-лайн екаунтів.
2. Умови, що сприяють вчиненню кіберзлочину у соціальних мережах
3. Умови, що сприяють вчиненню кіберзлочину у месенджерах
4. Безпека сайтів Мета: Засвоїти та закріпити теоретичні знання щодо питання сутності кіберзлочину
Література: 1, 3, 7,12.

Практичне заняття 4. Кіберзлочинність
Питання для обговорення:
1. Поняття кіберзлочинності
2. Вимірювання рівня кіберзлочинності.
3. Структура кіберзлочинності.
Мета: Засвоїти та закріпити теоретичні знання щодо питання сутності кіберзлочинності
Література: 7,10,11.

Практичне заняття 5. Фактори впливу на кіберзлочинність
Питання для обговорення:
1. Соціальні фактори
2. Правові фактори
3. Технічні фактори. . Захист пристроїв від фізичного доступу
Мета: Навчитися аналізувати фактори впливу на кіберзлочинність
Література: 1, 3, 7,12.

Практичне заняття 6. Ознаки кіберзлочинності в умовах воєнного стану
Питання для обговорення:
1. Географія кіберзлочинності.
2. Структура кіберзлочинності.
3. Латентність кіберзлочинності
Мета: Глибше засвоїти та закріпити теоретичні знання щодо ідентифікації ознак кіберзлочинності в умовах воєнного стану
Література: 10

Практичне заняття 7. Кіберзлочинець
Питання для обговорення:
1. Кіберзлочинець як базовий елемент системи кіберзагроз.
2. Соціально-демографічні ознаки особи кіберзлочинця.
3. Морально-психологічні якості і особистісно- рольові властивості особи кіберзлочинця.
4. Типологія кіберзлочинців.
Мета: Ознайомлення з особливостями категорії «кіберзлочинець»
Література: 2, 4, 7,10

Практичне заняття 8. Кіберзлочинність проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Питання для обговорення:

1. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
2. Основні риси кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
3. Причини кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем
4. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

Мета: Вивчення особливостей кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем

Література: 1,4,7,12

Практичне заняття 9. . Кіберзлочинність, пов'язана з використанням комп'ютера як засобу скоєння злочинів

Питання для обговорення:

1. Комп'ютерне шахрайство.
2. Особистість кібершахрая, основні риси.
3. Причини і умови кіберзлочинності, пов'язаної з використанням комп'ютера
4. Запобігання кіберзлочинності, пов'язаної з використанням комп'ютера

Мета: Вивчення особливостей кіберзлочинності, пов'язаної з використанням комп'ютера як засобу скоєння злочинів

Література: 8, 9

Практичне заняття 10. Кіберзлочинність, пов'язана з з контентом (змістом даних), розміщених у комп'ютерних мережах.

Питання для обговорення:

1. Кіберзлочинність, пов'язана з контентом (змістом даних), розміщених у комп'ютерних мережах.
2. Характеристика кіберзлочинності, що пов'язана з контентом (змістом даних), розміщених у комп'ютерних мережах.
3. Особистість кіберзлочинця, що пов'язана з контентом (змістом даних), розміщених у комп'ютерних мережах.
4. Причини і умови кіберзлочинів, пов'язаних з контентом, розміщених у комп'ютерних мережах

Мета: Вивчення особливостей кіберзлочинності, пов'язаної з контентом (змістом даних), розміщених у комп'ютерних мережах

Література: 5,7,9

Практичне заняття 11. Кіберзлочинність, пов'язана з порушенням авторського права і суміжних прав

Питання для обговорення:

1. Поняття авторського права і суміжних прав.
2. Об'єкти авторського права і суміжних прав
3. Суб'єкти авторського права і суміжних прав.
4. Запобігання кіберзлочинам пов'язаних з порушенням авторського права і суміжних прав

Мета: Вивчення особливостей кіберзлочинності, пов'язаної з порушенням авторського права і суміжних прав
Література: 3,5, 9

Практичне заняття 12. . Інформаційне поле під час війни
Питання для обговорення:

1. Сутність та принципи російської пропаганди
2. Анонімні канали та їх безпечність
3. Блогери-інсайдери як кіберзагроза.
4. Інформаційно-психологічні операції

Мета: Вивчення особливостей кіберзлочинності під час війни, зафіксованої в окремому протоколі
Література: 8, 9

Практичне заняття 13 Російська пропаганда
Питання для обговорення:

1. Сутність та принципи російської пропаганди
2. Анонімні канали та їх безпечність
3. Блогери-інсайдери як кіберзагроза.
4. Інформаційно-психологічні операції

Мета: Вивчення особливостей російської пропаганди
Література: 2,5,6,10,12

Практичне заняття 14. Кіберзлочинність у сфері російської пропаганди. ІПСО
Питання для обговорення:

1. ІПСО «переселенці».
2. Складові інформаційного тероризму росії

Мета: Вивчення особливостей кіберзлочинності у сфері російської пропаганди. ІПСО
Література: 2,5,6,-8

Практичне заняття 15. Правила інформаційної гігієни в період введення воєнного стану
Питання для обговорення:

1. Маніпуляції в інформаційному полі
2. Шахрайства в мережі та методи їхнього запобігання

Мета: Вивчення особливостей кіберзлочинності та гібридних воєн в інформаційному полі
Література: 2,5,6,11

6 Самостійна робота

Метою виконання самостійної роботи є глибоке вивчення методів формування системи протидії кіберзлочинності. Виконання самостійної роботи необхідно починати з вивчення відповідних розділів підручників, навчальних посібників, наукових джерел тощо, що наведені у переліку рекомендованої літератури, а також додаткової літератури і практичних матеріалів, які студент повинен знайти і опрацювати самостійно.

Оцінка за самостійну роботу визначається як середнє арифметичне з оцінок, отриманих наступних завдань:

- написання наукового есе на актуальну для воєнного стану тематику (тематика додається).

- опрацювання розділів програми, які не виносяться на лекції та підготовка відповідно до них наукових заміток (до 3 сторінок) в презентацією роботи перед групою (тематика додається).

Опрацювання окремих розділів програми, які не виносяться на лекції включає:

1. Корупція у віртуальному середовищі: визначення як соціального явища та її зв'язок з новітніми технологіями, різновиди корупційних проявів у кіберпросторі.
2. Характеристика кіберзлочинності, пов'язаної з корупцією: причини, умови виникнення і способи запобігання.
3. Аналіз злочинності неповнолітніх у віртуальному середовищі: особливості особистості неповнолітнього кіберзлочинця, основні характеристики.
4. Причини та умови кіберзлочинності серед неповнолітніх та способи її запобігання.

Критерії оцінювання опрацювання окремих розділів програми, які не виносяться на лекції:

- Актуальність інфорації (30 балів)
- Посилання на провідних науковців (30 балів)
- Виявлення правових колізій, якщо такі наявні (10 балів)
- Якість викладу та аргументації (30 балів)

Тематика есе, що пропонуються студентам для виконання самостійної роботи (рекомендовано використовувати актуальну інформацію, з аналізом особливостей воєнного стану в Україні):

Завдання:

1. Протидія кіберзлочинності як складова національної економічної безпеки.
2. Роль протидії кіберзлочинності у формуванні інноваційної моделі розвитку.
3. Суб'єкти протидії кіберзлочинності та їх інтереси.
4. Суперечності інтересів суб'єктів відносин інтелектуальної власності.
5. Інституційні умови протидії кіберзлочинності в період воєнного стану.
6. Сучасні трансформації інституційних основ сфери інтелектуальної власності.
7. Загрози та ризики протидії кіберзлочинності як складової національної економічної безпеки.
8. Внутрішні та зовнішні загрози в період воєнного стану.
9. Протидія кіберзлочинності підприємства.
10. Складові протидії кіберзлочинності підприємства.
11. Шляхи втрати об'єктів інтелектуальної власності та інформації про них.
12. Система технічного захисту інформаційних об'єктів.
13. Кібербезпека України в період воєнного стану.

8. Тренінг з дисципліни (8 год.).

Тренінг з дисципліни пропонує 2 завдання різного змісту на кожного студента (Виконання завдань: №1-5 ((на вибір), Студенти отримують одне із завдань (на вибір), формуючи групи. Критерії оцінювання залежать від окремо взятого завдання. Оцінка за тренінг визначається як середнє арифметичне з відповідностей критеріям виконання.
Результати виконання тренінгу подаються у вигляді презентації або відеоролику.

Тренінг включає в себе:

1. Тематика: Оцінка рівня кіберзлочинності

Мета: набуття навичок оцінки якісних параметрів Інтернет-ресурсів як джерела інформації.

Завдання: здійснити інформаційний пошук ресурсів та оцінити їх якість і придатність для аналізу з метою аналізу рівня кіберзлочинності:

1. Оцініть рівень кіберзлочинності в своєму колі за десятибальною шкалою. Прокоментуйте результат.
2. Оцініть рівень кіберзлочинності в якості глядача одного з телевізійних каналів (на вибір).
3. Оцініть рівень кіберзлочинності в якості слухача одної з радіостанцій.
4. Оцініть рівень кіберзлочинності в якості одного з читачів інформаційного інтернет –сайту.
5. Прокоментуйте телешоу (на вибір) з точки зору наявності критеріїв кіберзлочинності.

Оцінка має здійснюватися зважаючи на:

- зміст понять «загроза» і «безпека» по відношенню до систем «природа», «суспільство», «людина»;
- зміст понять «Протидія кіберзлочинності» (Протидія кіберзлочинності вважається складовою національної безпеки України, складовою інформаційної безпеки України, провідним складником у системі національної економічної безпеки, системоутворюючим елементом економічної безпеки держави; стан стійкості та здатності до розвитку власника, рівень володіння сучасними знаннями, впровадження новацій у розвиток персоналу, захищеність інтелектуальних ресурсів соціально-економічного розвитку, захищеність економічних інтересів підприємства від впливу несприятливих умов зовнішнього середовища) і «інтелектуальний захист» (комплекс організаційних заходів, спрямованих на захист прав і законних інтересів);
- засади правового забезпечення протидії кіберзлочинності в Україні;
- складові, функції, критерії, рівні та умови протидії кіберзлочинності;
- функції окремих рівнів інформаційного захисту;
- способи та методи протидії кіберзлочинності;
- особливості організації інтелектуально безпечного середовища.

Література: 13, 14, 25.

Критерії оцінювання:

- Здатність ефективно збирати та аналізувати докази (40 балів)
- Виявлення джерел витоку інформації (30 балів)
- Якість звіту з висновками та рекомендаціями (20 балів)
- Командна робота та комунікативні навички (10 балів)

8. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни “Протидія кіберзлочинності” використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- стандартизовані тести;
- поточне опитування;
- залікове модульне тестування;
- презентації результатів виконаних завдань та досліджень;
- студентські презентації та виступи на наукових заходах;
- інші види індивідуальних та групових завдань.

9. Критерії, форми поточного та підсумкового контролю

У процесі вивчення дисципліни «Протидія кіберзлочиннисті» використовуються такі засоби оцінювання та методи демонстрування результатів навчання: поточне опитування, тестування; презентації результатів виконаних завдань; результати модульного контролю; оцінювання результатів самостійної роботи; інші види індивідуальних і групових завдань; екзамен.

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань студентами і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу студент може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими студентами, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування тощо) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Підсумковий бал (за 100-бальною шкалою) з дисципліни "Протидія кіберзлочинності" визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2		Модуль 3	Модуль 4
20%	20%	20%	20%	5%	15%
Усне опитування (тестування) на заняттях: Теми 1-7. Поточне оцінювання Оцінка за поточне оцінювання визначається як середнє арифметичне з оцінок отриманих під час занять	Модульний контроль 1 включає 20 тестів. Теми 1-7. Модульний контроль 1 планувати на проведених занять. Модульний контроль проводити в системі Мудл	Усне опитування (тестування) на заняттях: Теми 8-15. Поточне оцінювання Оцінка за поточне оцінювання визначається як середнє арифметичне з оцінок отриманих під час занять	Модульний контроль 2 включає 20 тестів. Теми 8-15. Модульний контроль 2 планувати на проведених занять. Модульний контроль проводитться в системі Мудл	Тренінги Тренінг з дисципліни пропонує 2 завдання різного змісту на кожного студента (Виконання завдань: №1-5 ((на вибір), Студенти отримують одне із завдань (на вибір), формуючи групи. Критерії оцінювання залежать від окремо взятого завдання та описані в розділі Тренінг. Оцінка за тренінг визначається як середнє арифметичне з відповідностей критеріям виконання. Результати виконання тренінгу подаються у вигляді презентації або відеоролику.	Визначається як середнє арифметичне з оцінок, отриманих під час вивчення дисципліни за самостійну роботу: - наукового есе на актуальну для воєнного стану тематику. - Опрацювання розділів програми, які не виносяться на лекції (тематика подана у розділі Самостійна робота).

Поточне оцінювання під час заняття:

90-100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань.

75-89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки.

65-74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки.

60-64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань, допускаючи при цьому суттєві неточності.

1-59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань.

Тестування під час заняття:

10 тестів, правильна відповідь на кожен із яких оцінюється у 10 балів.

Модульний контроль 1 (підсумкове тестування):

20 тестів, правильна відповідь на кожен із яких оцінюється у 5 балів.

Модульний контроль 2:

20 тестів, правильна відповідь на кожен із яких оцінюється у 5 балів.

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповідей, глибоко та всебічно розкриває зміст теоретичних питань, тестових та практичних завдань.

75–89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки.

65–74 балів – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки.

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності.

1-59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичних питань та практичних завдань.

Тренінг:

90–100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його використовує під час виконання завдань тренінгу, виявляє творчий підхід до виконання завдань.

75–89 балів – достатньо повно володіє навчальним матеріалом, але при виконанні окремих завдань тренінгу не вистачає достатньої глибини та аргументації його

використання, допускаються при цьому окремі несуттєві неточності та незначні помилки, загалом виявляє творчий підхід до виконання завдань.

65–74 бали – в цілому володіє навчальним матеріалом та загалом його використовує при виконанні завдань тренінгу, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому суттєві неточності та помилки, в окремих моментах виявляє творчий підхід до виконання завдань.

60–64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його використовує, недостатньо розкриває зміст завдань тренінгу, допускаючи при цьому суттєві неточності, не виявляє творчого підходу до виконання завдань.

1-59 – не володіє навчальним матеріалом, не розкриває зміст завдань тренінгу, не бере участі у колективних завданнях підчас проведення тренінгу.

Активність під час тренінгу:

Оцінюється у діапазоні від 1 до 10 балів, де 1 бал – найнижча активність (студент практично не виявляє інтересу до завдань тренінгу), 10 балів – найвища активність (студент активно залучений у виконання завдань тренінгу, виявляє творчу ініціативу, ґрунтовне знання навчального матеріалу).

встановленим вимогам, містить елементи самостійного дослідження, свідчить про високий рівень опанування навчального матеріалу, студент на високому рівні виявляє творчий підхід до виконання завдань.

75–89 балів – зміст самостійної роботи в основному відповідає встановленим вимогам, можуть бути несуттєві недопрацювання за окремими завданнями, свідчить про належний рівень опанування навчального матеріалу, студент належно виявляє творчий підхід до виконання завдань.

60–74 балів – поставлені завдання виконані на недостатньому рівні; наведені авторські напрацювання є загальними і слабко обґрунтованими, свідчать про недостатній рівень опанування навчального матеріалу; студент припускається значних помилок у виконанні завдань, в окремих моментах виявляє творчий підхід до виконання завдань.

1-59 балів – завдання практично не виконані; відсутні авторські напрацювання; грубі помилки у вирішенні завдань роботи, що свідчать про низький рівень опанування навчального матеріалу; студент не виявляє творчого підходу до виконання завдань.

Залік: Визначається як середнє арифметичне з оцінок, отриманих під час вивчення дисципліни за самостійну роботу:

- наукового есе на актуальну для воєнного стану тематику.

Критерії оцінювання есе:

- Глибина аналізу актуальної на сьогодні ситуації, зважаючи на воєнний стан (30 балів)
- Виявлення ключових проблем (30 балів)
- Пропозиції щодо стратегії реагування та запобігання (30 балів)
- Якість викладу та аргументації (10 балів)

- Опрацювання розділів програми, які не виносяться на лекції (тематика подана у розділі Самостійна робота), що оцінюється в діапазоні:

90-100 балів – у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час відповіді, глибоко та всебічно розкриває зміст теоретичного питання.

75-89 балів – достатньо повно володіє навчальним матеріалом, але при викладанні питання не вистачає достатньої глибини та аргументації, допущені окремі несуттєві неточності та незначні помилки.

65-74 бали – в цілому володіє навчальним матеріалом та викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації, допускаючи при цьому окремі суттєві неточності та помилки.

60-64 бали – не в повному обсязі володіє навчальним матеріалом, фрагментарно (без аргументації та обґрунтування) його викладає, недостатньо розкриває зміст теоретичного питання, допускаючи при цьому суттєві неточності.

1-59 балів – не володіє навчальним матеріалом, не розкриває зміст теоретичного питання.

Шкала оцінювання:

За шкалою ЗУНУ	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

10. Перелік наочних матеріалів та методичних вказівок

№	Найменування	Номер теми
1	Мультимедійний проектор	1-15
2	Нормативні матеріали	1-15
3	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-15
4	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-15
5.	Програмне забезпечення: ОС Windows	1-15
6.	Інструменти Microsoft Office (Word, Power Point і т. і.)	1-15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Нормативно-правові акти:

1. Кримінальний кодекс України: Закон України від 05. 04. 2001 р. № 2341-III із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду. Електрон. дан. (1 файл). URL : https://zakon.rada.gov.ua/laws/show/2341-14.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text
3. «Про інформацію»: Закон України від від 02.10.1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
4. «Про захист персональних даних»: Закон України від 01.06.2010 р. № 2297-VI URL : // https://zakon.rada.gov.ua/laws/show/2297-17
5. «Про електронні довірчі послуги»: Закон України від 05.10.2017 р. № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
6. «Про основні засади забезпечення кібербезпеки України»: Закону України від 05.10.2017 р. № 2163-VIII URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
7. «Про національну безпеку України»: Закон України від 21.06.2018 р. № 2469-VIII URL : https://zakon.rada.gov.ua/laws/show/2469- 19#Text
8. «Про кіберзлочинність»: Конвенція ратифіковано із застереженнями і заявами Законом N 2824-IV ( ) від 07.09.2005, URL : https://zakon.rada.gov.ua/laws/show/994_575#Text
9. «Про Стратегію кібербезпеки України»: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

Основні джерела інформації:

1. Муравська Ю. Побудова ефективної системи національної безпеки України як передумова євроінтеграції. Наукові заходи Юридичного факультету Західноукраїнського національного університету. 2022: Пріоритети зміцнення безпеки держави та підвищення ефективності правоохоронної діяльності: національні та міжнародні контексти (Тернопіль, 6 травня 2022 р.) http://confuf.wunu.edu.ua/index.php/confuf/article/view/829
2. Муравська (Якубівська) Ю. Є. Інформаційна безпека суспільства: концептуальний аналіз / Ю. Є. Муравська (Якубівська) // Економіка та суспільство [Електронне наукове фахове видання]. - № 9. – Мукачево : Мукачівський державний університет, 2017. Режим доступу: http://www.economyandsociety.in.ua/
3. Муравська (Якубівська) Ю. Є. Формування понятійного апарату у сфері кібербезпеки: іноземний досвід та нормативно-правова регламентація / Ю. Є. Муравська (Якубівська) // Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід: [Матеріали II Міжнародній науково-практичній конференції, м. Тернопіль, 21-22 квітня 2017 р.]. – Тернопіль: Економічна думка, 2017. – С.362-365.
4. Муравська (Якубівська) Ю. Є. Термінологічна та нормативно-правова невизначеність у сфері кібербезпеки / Ю. Є. Муравська (Якубівська) // Збірник тез доповідей всеукраїнської науково-практичної конференції «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави», м. Тернопіль, 21 квітня 2017 р., ТНЕУ. – Тернопіль, 2017. – С. 56-59.
5. Карапетян О.М., Будник Л.А., Метельський І.Д. Кіберзлочини: типології, фінансова розвідка, використання спеціальних знань. Актуальні проблеми правознавства. 2022. Вип. 3. С. 115-120.
6. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи / Тарасюк А. В. : монографія / А. В. Тарасюк. – Київ; Одеса : Фенікс, 2020. – 404 с.
7. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.
8. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.

9. Muravska Yuliia. Theoretical and conceptual approaches to defining the concept and forms of economic intelligence.in the Ukrainian scientific practice. Osteuropa-Recht. 2022. Vol. 4. P. 476-485.
10. Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, OleksiiV. Tavolzhanskyi, Roman I. Tashian Protection of ownership right in the court: the essence and particularities (Захист права власності в суді) // Asia life science, Supplement 21(2), December 2019. Iss. 2. P. 863-879. Філіпини. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0- 85077221643&origin=resultslist
11. Tsypko V., Alieksieieva K. I., Venger I. A., Tavolzhanskyi O. V., Galunets N. I., Klyuchnik A. V. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction () // Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0- 85087468504&origin=resultslist

Додаткова література

1. Таволжанський О.В. Інформаційна безпека України: стан правового забезпечення в контексті глобалізаційних процесів.// Журнал східноєвропейського права. – 2018. - № 56. – С. 90-105. (0,71 д.а). Таволжанський О.В. (у співавт.) International Experience of the Process of Re- Socialization of Convicts // Журнал східноєвпроейського права. – 2019. - № 63. – С. 125-136.
2. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. Ю. Шостко та ін.; за ред. Б. М. Головкіна. – Харків : Право, 2020
3. Карчевський М.В. Правове регулювання соціалізації штучного інтелекту. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Науково-теоретичний журнал. 2017. С. 99-08.
4. Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація / О. В. Таволжанський // Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія : Право. - 2017. - № 4. - С. 158-164. - Режим доступу: http://nbuv.gov.ua/UJRN/Nivif_2017_4_27
5. Гладка Н. М. Боротьба з кіберзлочинністю: напрями вдосконалення кримінального законодавства України [Електронний ресурс] / Н. М. Гладка // Науковий вісник Ужгородського національного університету. Серія : Право. - 2020. - Вип. 60. - С. 139-142.
6. Леонов Б. Д. Методичне забезпечення заходів з класифікації ідентифікації та фіксації кіберзлочинів [Електронний ресурс] / Б. Д. Леонов, В. С. Серьогін // Інформація і право. - 2021. - № 1. - С. 99-105
7. Саєнко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству [Електронний ресурс] / М. І. Саєнко, Є. А. Савела, Ю. Ю. Тополянський // Науковий вісник Ужгородського національного університету. Серія : Право. - 2021. - Вип. 64. - С. 386-391.
8. Волощук В., Заєць К., Муравська Ю. Національна безпека як інструмент збереження української державності. Актуальні проблеми правознавства. 2 (38)/2024. С. 111-117.
9. Zaiets K., Muravska Yu., Slipchenko T., Kaniuka V., Melnyk I. The etymology of the concept “military conflict” as a determinant of political orientation. Law, Policy and Security, 2(2), 39-51.