

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ

Т.в.о. декана юридичного факультету

Надія МОСКАЛЮК

" 31 " 08 2023 р.



ЗАТВЕРДЖУЮ

В.о. проректора з науково-педагогічної роботи

Віктор ОСТРОВЕРХОВ

" 31 " 08 2023 р.



ЗАТВЕРДЖУЮ

Директор ННІНОТ

Святослав ПИТЕЛЬ

" 31 " 08 2023 р.



РОБОЧА ПРОГРАМА

з дисципліни "ІНТЕЛЕКТУАЛЬНА БЕЗПЕКА"

ступінь вищої освіти – магістр

галузь знань – 26 Цивільна безпека

спеціальність – 262 Правоохоронна діяльність

освітньо-професійна програма – «Економічна безпека та фінансові розслідування»

Кафедра безпеки та правоохоронної діяльності

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	ІРС (год.)	Тренінг, КПЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Зал. (сем.)
Денна	1	2	30	15	5	6	64	120	2
Заочна	1	2,3	8	4	-	-	108	120	3

Тернопіль: ЗУНУ, 2023

31.08.2023
[Signature]

Робочу програму склала к.е.н., доцент, доцент кафедри безпеки та правоохоронної діяльності
Юлія МУРАВСЬКА.

Робоча програма затверджена на засіданні кафедри безпеки та правоохоронної діяльності,
протокол № 1 від 29 серпня 2023 р.

В.о. завідувача кафедри
к.ю.н., старший викладач

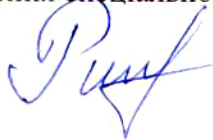


Ігор МЕТЕЛЬСЬКИЙ

Розглянуто та схвалено групою забезпечення спеціальності правоохоронна діяльність,
протокол № 1 від 30.08. 2023 р.

Голова групи забезпечення спеціальності

д.ю.н., доцент



Ніна РОГАТИНСЬКА

Гарант ОП



Роман ОЛІЙНИЧУК

**СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
„Інтелектуальна безпека”**

**1. Опис дисципліни
„Інтелектуальна безпека”**

Дисципліна „Інтелектуальна безпека”	Галузь, спеціальність, СВО	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 4	Галузь знань: 26 – <i>цивільна безпека</i>	Статус дисципліни (<u>вибіркова</u>) Мова навчання українська
Кількість залікових модулів – 3	Спеціальність 262 “Правоохоронна діяльність”	Рік підготовки : <i>денна – 1</i> <i>заочна – 1</i> Семестр: <i>денна – 2</i> <i>Заочна – 2,3</i>
Кількість змістових модулів – 2	Ступінь вищої освіти – <i>магістр</i>	Лекції: <i>Денна – 30 год.</i> <i>заочна – 8 год.</i> Практичні заняття: <i>Денна – 15 год.</i> <i>Заочна – 4 год.</i>
Загальна кількість годин – 120		Самостійна робота: <i>Денна – 70 год.</i> <i>(в т.ч. тренінг, КПІЗ – 6 год.)</i> <i>Заочна – 108 год.</i> <i>Індивідуальна робота – Денна – 5 год.</i>
Тижневих годин: 6 год. з них аудиторних – 2 год.		Вид підсумкового контролю - залік

2. Мета й завдання дисципліни „Інтелектуальна безпека”

2.1. Мета вивчення дисципліни

Предметом навчальної дисципліни „Інтелектуальна безпека” є розвиток системи інтелектуальної безпеки на усіх рівнях.

Мета навчальної дисципліни „Інтелектуальна безпека” — допомогти студентам, слухачам опанувати теоретичні основи та виробити вміння і практичні навички з планування та організації системи інтелектуальної безпеки, а також розвиток здібностей до логічного та алгоритмічного мислення, навичок використання сучасних напрямків, методів і засобів захисту об'єктів інтелектуальної власності.

Дисципліна «Інтелектуальна безпека» вивчає закономірності та організаційно-економічні механізми побудови й відтворення стану безпечного, захищеного розвитку сфери інтелектуальної власності на рівні держави і окремих суб'єктів господарювання.

Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами теоретичних знань з інтелектуальної безпеки.

Зміст навчальної дисципліни складають принципи інтелектуальної безпеки, теоретичні та практичні проблеми розроблення проекту вибору найбільш ефективної технології, засобів і методів інтелектуальної безпеки з урахуванням конкретної ситуації.

2.2. Завдання вивчення дисципліни

Завдання навчальної дисципліни „Інтелектуальна безпека” полягає в тому, щоб на основі теоретичних положень у сфері у сфері правоохоронної діяльності, безпекознавства й узагальнення практичного досвіду роботи розкрити зміст, організаційні форми та методи роботи у сфері інтелектуальної безпеки.

*Навчальна дисципліна „Інтелектуальна безпека” не є самоціллю, яка досягається у відриві від виробничої, соціальної та інших сторін діяльності організації. Виходячи з цього *одне з найважливіших завдань навчальної дисципліни* — визначення змісту і межі проблем, пов'язаних із прийняттям рішень щодо формування системи інтелектуальної безпеки в тісному взаємозв'язку з вирішенням інших питань у сфері правоохоронної діяльності. Це сприяє більш чіткому визначенню місця та підвищенню значення заходів із формування системи інтелектуальної безпеки в системі національної безпеки.*

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

- сутність інтелектуальної безпеки як складової національної економічної безпеки; національні інтереси в сфері інтелектуальної власності; інституційні умови та принципи управління інтелектуальною безпекою; видизагроз 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 інтелектуальної безпеки підприємства; поняття комерційної таємниці, конкурентної розвідки; завдання і функції служби економічної безпеки щодо захисту комерційної таємниці; переваги та недоліки забезпечення інтелектуальної власності через механізм комерційної таємниці; способи захисту комерційно цінної інформації при переговорах із потенційними партнерами; загрози та ризики для інтелектуальної безпеки 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 інтелектуальної безпеки.

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 інтелектуальної безпеки 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 промислового шпигунству; виявляти потенційні шляхи втрати об'єктів інтелектуальної власності підприємства; враховувати специфіку управління безпекою за фазами життєвого циклу об'єктів інтелектуальної власності; розробляти та координувати заходи 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 інтелектуальної безпеки.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних питань щодо формування системи інтелектуальної безпеки в контексті національної безпеки; законодавчої та нормативної бази.
- сформуванні у студентів цілісну систему теоретичних знань з курсу „Інтелектуальна безпека”.

Завдання практичних занять

Мета проведення практичних занять полягає в тому, щоб виробити у студентів навички практично застосувати сучасні методи інтелектуальної безпеки, 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 інтелектуальної безпеки;
- практично вирішувати питання щодо класифікування методів та форм інтелектуальної безпеки;
- орієнтуватись на інтелектуальній безпеці;
- засвоїти методику та техніку виконання превентивних заходів формування системи інтелектуальної безпеки.

3. Програма навчальної дисципліни: „Інтелектуальна безпека”

Змістовний модуль 1. Інтелектуальна безпека: загальнотеоретичний аспект

Тема 1. Інтелектуальна безпека в системі національної економічної безпеки

1. Інтелектуальна безпека як складова національної економічної безпеки. Інтелектуальна безпека науково-технологічна (інноваційна) безпека держави.
2. Інституційні умови інтелектуальної безпеки. Друга економічна революція за Д. Норттом. Взаємозв'язок між інститутами та інтенсивністю і спрямованістю інновацій.
3. Принципи управління інтелектуальною безпекою. Рівні регулювання відносин інтелектуальної власності.
4. Роль держави в управлінні інтелектуальною безпекою.

Тема 2. Об'єкти та суб'єкти системи інтелектуальної безпеки

- 1 Об'єкти права інтелектуальної власності, що виступають об'єктами системи інтелектуальної безпеки
- 2 Суб'єкти інтелектуальної безпеки
- 3 Система законодавства у сфері інтелектуальної безпеки

Тема 3. Авторське право як елемент інтелектуальної безпеки

1. Поняття авторського права.
2. Об'єкти, що охороняються авторським правом.
3. Суб'єкти авторського права в контексті формування системи інтелектуальної безпеки
4. Виникнення авторського права.
5. Знак охорони авторського права та його значення в контексті формування системи інтелектуальної безпеки
6. Зміст суб'єктивного авторського права.
7. Вільне використання творів.
8. Строк охорони авторського права.
9. Перехід твору до суспільного надбання.

Тема 4. Правова охорона об'єктів промислової власності. Патентне право як механізм інтелектуальної безпеки

1. Еволюція промислової власності.
2. Поняття та об'єкти патентного права.
3. Суб'єкти прав на винаходи, корисні моделі і промислові зразки.
4. Патент як форма охорони прав на винаходи, корисні моделі і промислові зразки.
5. Суб'єктивні права на винаходи, корисні моделі та промислові зразки.
6. Обов'язки, що накладаються патентом.
7. Дії, що не визнаються порушенням прав власника патенту.
8. Захист прав патентовласника як механізм інтелектуальної безпеки.
9. Патентування винаходу, корисної моделі та промислового зразка в іноземних державах.

Тема 5. Правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг як механізм інтелектуальної безпеки

1. Засоби індивідуалізації учасників цивільного обороту, товарів і послуг та їх види.
2. Фірмове найменування (фірма) як елементи інтелектуальної безпеки.
3. Зазначення походження товарів як елементи інтелектуальної безпеки
4. Знаки для товарів і послуг як елементи інтелектуальної безпеки
5. Об'єкти знаків для товарів і послуг та їх види.
6. Права і обов'язки, що випливають зі свідоцтва на знак.
7. Захист прав на знаки для товарів і послуг.
8. Реєстрація кваліфікованого зазначення походження товару та права, що випливають з неї.
9. Міжнародно-правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг

Тема 6. Передача прав на об'єкти інтелектуальної власності як напрямок формування системи інтелектуальної безпеки

1. Суть торгівлі ліцензіями як передумова формування системи інтелектуальної безпеки.
2. Види ліцензій.
3. Ліцензійні договори як елементи інтелектуальної безпеки
4. Ліцензійні платежі.
5. Передача прав за авторськими договорами.

Тема 7. Захист прав інтелектуальної власності як механізм інтелектуальної безпеки

1. Захист як базовий елемент системи інтелектуальної безпеки. Форми захисту. Стратегічні напрями подолання загроз та нейтралізації ризиків у сфері інтелектуальної власності в Україні.
2. Дії, що визнаються порушеннями прав інтелектуальної власності.
3. Форми захисту прав інтелектуальної власності.
4. Способи захисту прав інтелектуальної власності.

Змістовий модуль 2. Інтелектуальна безпека: прикладний аспект

Тема 8. Відповідальність за порушення законодавства про комерційну таємницю та прояви недобросовісної конкуренції

1. Відповідальність за дії недобросовісної конкуренції
2. Комерційна таємниця як об'єкт посягання в процесі формування системи інтелектуальної безпеки
3. Відповідальність за порушення законодавства про комерційну таємницю
4. Завдання і функції служби економічної безпеки щодо захисту комерційної таємниці.

Тема 9. Технічний захист інформації як елемент інтелектуальної безпеки

1. Форми контролю за каналами витоку інформації.
2. Система технічного захисту інформаційних об'єктів. Кібербезпека.
3. Роль персоналу в захисті комерційної таємниці.
4. Захист комерційної таємниці в переговорних процесах, на виставках і ярмарках.
5. Особливості захисту комерційної таємниці у зовнішньоекономічній діяльності підприємства.

Тема 10. Загрози та ризики для національної економічної безпеки в сфері інтелектуальної власності

1. Моніторинг інтелектуальної безпеки. Критерії та показники оцінки інтелектуальної безпеки.
2. Загрози та ризики інтелектуальної безпеки.
3. Промислове шпигунство в системі світової конкуренції. Інтелектуальна власність як інструмент економічної агресії в умовах глобалізації.

Тема 11. Інтелектуальна безпека підприємства

1. Інтелектуальна безпека підприємства та її складові.
2. Шляхи втрати об'єктів інтелектуальної власності та інформації про них. Загрози безпеці інтелектуальної власності підприємства.
3. Механізм управління системою інтелектуальної безпеки на підприємстві залежно від виду підприємства.
4. Форми, напрями і механізми захисту інтелектуальної власності підприємства. Завдання служби економічної безпеки щодо убезпечення інтелектуальної власності.

Тема 12. Промислове шпигунство і конкурентна розвідка як загрози інтелектуальній безпеці

1. Відмінність промислового шпигунства від конкурентної розвідки
2. Методи, що використовуються в промисловому шпигунстві
3. Методи, що використовуються в конкурентній розвідці
4. Організаційні методи захисту від інтелектуальної безпеки на підприємстві

Тема 13. Убезпечення об'єктів права інтелектуальної власності

1. Сутність безпеки об'єктів права інтелектуальної власності. Загрози та ризики втрати, несанкціонованого копіювання, використання конкурентами інтелектуального продукту.
2. «Due Diligence» інтелектуальної власності у зниженні ризиків інтелектуальної безпеки організації.
3. Патентування як механізм захисту інтелектуальної власності. Сучасні патентні технології. Традиційна та міжнародна процедури патентування. Зарубіжне патентування.
4. Ноу-хау і комерційна таємниця. Переваги і недоліки охорони комерційно цінної інформації у режимі конфіденційності.
5. Захист авторських і суміжних прав в епоху Інтернет.
6. Засоби індивідуалізації учасників цивільного обороту товарів та послуг в убезпеченні інтелектуальної власності організації: сфера та особливості застосування.

Тема 14. Страхування об'єктів інтелектуальної власності як передумова формування ефективної системи інтелектуальної безпеки

1. Ризики та страхові інтереси в сфері відносин інтелектуальної власності.
2. Сутність та сфера застосування страхування інтелектуальної власності: зарубіжний досвід та практика в Україні.
3. Види страхування інтелектуальної власності.

Тема 15. Безпека інтелектуальних трудових ресурсів підприємства та руху знань як елемент інтелектуальної безпеки

1. Інтелектуальні трудові ресурси підприємства як носії знань
2. Специфічні та інтерспецифічні інтелектуальні трудові ресурси. Збитки підприємства внаслідок їх втрати
3. Інвестиції в робочі та проектні команди. Роль управління рухом знань в організації системи інтелектуальної безпеки.

**4. Структура залікового кредиту з дисципліни
„Інтелектуальна безпека”
денна форма навчання**

	Кількість годин				Контр. заходи
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	
Змістовий модуль 1 . Інтелектуальна безпека: загальнотеоретичний аспект					
<i>Тема 1. Інтелектуальна безпека в системі національної економічної безпеки</i>	2	1	6	2	Питання для обговорення
<i>Тема 2. Об'єкти та суб'єкти системи інтелектуальної безпеки</i>	2	1	8		Тести, питання
<i>Тема 3. Авторське право в системі захисту від інтелектуальної безпеки</i>	2	1	10		Тести, задачі, питання
<i>Тема 4. . Правова охорона об'єктів промислової власності. Патентне право як механізм інтелектуальної безпеки</i>	2	1	10		Тести, задачі, питання
<i>Тема 5. Правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг як механізм інтелектуальної безпеки</i>	2	1	10		Тести, задачі, питання
<i>Тема 6. Передача прав на об'єкти інтелектуальної власності як напрямок формування системи інтелектуальної безпеки</i>	2	1	10		Тести, питання
<i>Тема 7. Захист прав інтелектуальної власності як складова системи попередження інтелектуальної безпеки</i>	2	1			Тести, питання
Змістовий модуль 2 . Інтелектуальна безпека: прикладний аспект					
<i>Тема 8 Відповідальність за порушення законодавства про комерційну таємницю та прояви недобросовісної конкуренції</i>	2	1	10		Тести, кейси
<i>Тема 9. Технічний захист інформації як елемент інтелектуальної безпеки</i>	2	1	10	2	Тести, питання

Тема 10. <i>Загрози та ризики для національної економічної безпеки в сфері інтелектуальної власності</i>	2	1			Тести, питання
Тема 11. <i>Інтелектуальна безпека підприємства</i>	2	1	10	1	Тести, питання
Тема 12. <i>Промислове шпигунство і конкурентна розвідка як загрози інтелектуальній безпеці</i>	2	1	10		Тести, задачі, питання
Тема 13. <i>Збір інформації з закритих джерел</i>	2	1	10		Питання
Тема 14. <i>Страхування об'єктів інтелектуальної власності як передумова формування ефективної системи інтелектуальної безпеки</i>	2	1	10		Кейси
Тема 15. <i>Безпека інтелектуальних трудових ресурсів підприємства та руху знань як елемент інтелектуальної безпеки</i>	2	1			Тести, питання
Разом	30	15	64	5	

заочна форма навчання

	Кількість годин			
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота
Змістовий модуль 1 . Інтелектуальна безпека: загальнотеоретичний аспект				
Тема 1. <i>Інтелектуальна безпека в системі національної економічної безпеки</i>	1		10	
Тема 2. <i>Об'єкти та суб'єкти системи інтелектуальної безпеки</i>	1	1	10	
Тема 3. <i>Авторське право в системі захисту від інтелектуальної безпеки</i>			10	
Тема 4. <i>Правова охорона об'єктів промислової власності. Патентне право як механізм інтелектуальної безпеки</i>	1		10	
Тема 5. <i>Правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг як механізм інтелектуальної безпеки</i>	1	1	10	
Тема 6. <i>Передача прав на об'єкти інтелектуальної власності як напрямок формування системи інтелектуальної безпеки</i>	1		5	
Тема 7. <i>Захист прав інтелектуальної власності як складова системи попередження інтелектуальної безпеки</i>			5	

Змістовий модуль 2 . Інтелектуальна безпека: прикладний аспект				
Тема 8 <i>Відповідальність за порушення законодавства про комерційну таємницю та прояви недобросовісної конкуренції</i>			10	
Тема 9. <i>Технічний захист інформації як елемент інтелектуальної безпеки</i>	1	1	10	
Тема 10. <i>Загрози та ризики для національної економічної безпеки в сфері інтелектуальної власності</i>			5	
Тема 11. <i>Інтелектуальна безпека підприємства</i>	1		5	
Тема 12. <i>Промислове шпигунство і конкурентна розвідка як загрози інтелектуальній безпеці</i>	1	1	5	
Тема 13. <i>Збір інформації з закритих джерел</i>			5	
Тема 14. <i>Страхування об'єктів інтелектуальної власності як передумова формування ефективної системи інтелектуальної безпеки</i>			4	
Тема 15. <i>Безпека інтелектуальних трудових ресурсів підприємства та руху знань як елемент інтелектуальної безпеки</i>			4	
Разом	8	4	108	

5. Тематика практичних занять

Практичне заняття 1. Інтелектуальна безпека в системі національної економічної безпеки

Питання для обговорення:

1. Інтелектуальна безпека як складова національної економічної безпеки. Інтелектуальна безпека науково-технологічна (інноваційна) безпека держави.
2. Інституційні умови інтелектуальної безпеки. Друга економічна революція за Д. Нортон. Взаємозв'язок між інститутами та інтенсивністю і спрямованістю інновацій.
3. Принципи управління інтелектуальною безпекою. Рівні регулювання відносин інтелектуальної власності.
4. Роль держави в управлінні інтелектуальною безпекою.

Мета: Визначення поняття формування системи інтелектуальної безпеки в контексті національної безпеки

Література: 1, 2, 5, 7

Практичне заняття 2. Об'єкти та суб'єкти системи інтелектуальної безпеки

Питання для обговорення:

- 1 Об'єкти права інтелектуальної власності, що виступають об'єктами системи інтелектуальної безпеки
- 2 Суб'єкти інтелектуальної безпеки
- 3 Система законодавства у сфері інтелектуальної безпеки

Мета: засвоїти та закріпити теоретичні знання щодо питання сутності інституту інтелектуальної власності в системі інтелектуальної безпеки

Література: 1, 3, 7,12.

Практичне заняття 3. Авторське право як елемент інтелектуальної безпеки

Питання для обговорення:

1. Поняття авторського права.
2. Об'єкти, що охороняються авторським правом.
3. Суб'єкти авторського права в контексті формування системи інтелектуальної безпеки
4. Виникнення авторського права.
5. Знак охорони авторського права та його значення в контексті формування системи інтелектуальної безпеки
6. Зміст суб'єктивного авторського права.
7. Вільне використання творів.
8. Строк охорони авторського права.
9. Перехід твору до суспільного надбання.

Мета: засвоїти та закріпити теоретичні знання щодо питання сутності авторського права в системі інтелектуальної безпеки

Література: 1, 3, 7,12.

Практичне заняття 4. Правова охорона об'єктів промислової власності. Патентне право як механізм інтелектуальної безпеки

Питання для обговорення:

1. Еволюція промислової власності.
2. Поняття та об'єкти патентного права.
3. Суб'єкти прав на винаходи, корисні моделі і промислові зразки.
4. Патент як форма охорони прав на винаходи, корисні моделі і промислові зразки.
5. Суб'єктивні права на винаходи, корисні моделі та промислові зразки.
6. Обов'язки, що накладаються патентом.
7. Дії, що не визнаються порушенням прав власника патенту.
8. Захист прав патентовласника як механізм інтелектуальної безпеки.
9. Патентування винаходу, корисної моделі та промислового зразка в іноземних державах.

Мета: засвоїти та закріпити теоретичні знання щодо питання сутності патентного права в системі інтелектуальної безпеки

Література: 7,10,14,17.

Практичне заняття 5. Правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг як механізм інтелектуальної безпеки

Питання для обговорення:

1. Засоби індивідуалізації учасників цивільного обороту, товарів і послуг та їх види.
2. Фірмове найменування (фірма) як елементи інтелектуальної безпеки.
3. Зазначення походження товарів як елементи інтелектуальної безпеки
4. Знаки для товарів і послуг як елементи інтелектуальної безпеки
5. Об'єкти знаків для товарів і послуг та їх види.
6. Права і обов'язки, що випливають зі свідоцтва на знак.
7. Захист прав на знаки для товарів і послуг.

8. Реєстрація кваліфікованого зазначення походження товару та права, що впливають з неї.

9. Міжнародно-правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг

Мета: навчитися досліджувати охорону засобів індивідуалізації учасників цивільного обороту, товарів і послуг

Література: 1, 3, 7,12,13.

Практичне заняття 6. Передача прав на об'єкти інтелектуальної власності як напрямок формування системи інтелектуальної безпеки

Питання для обговорення:

1. Суть торгівлі ліцензіями як передумова формування системи інтелектуальної безпеки.
2. Види ліцензій.
3. Ліцензійні договори як елементи інтелектуальної безпеки
4. Ліцензійні платежі.
5. Передача прав за авторськими договорами.

Мета: глибше засвоїти та закріпити теоретичні знання щодо питання передачі прав на об'єкти інтелектуальної власності як напрямку інтелектуальної безпеки

Література: 10,14-18.

Практичне заняття 7. Захист прав інтелектуальної власності як механізм інтелектуальної безпеки

Питання для обговорення:

1. Захист як базовий елемент системи інтелектуальної безпеки. Форми захисту. Стратегічні напрями подолання загроз та нейтралізації ризиків у сфері інтелектуальної власності в Україні.
2. Дії, що визнаються порушеннями прав інтелектуальної власності.
3. Форми захисту прав інтелектуальної власності.
4. Способи захисту прав інтелектуальної власності.

Мета: Ознайомлення з особливостями захисту прав інтелектуальної власності як складової системи інтелектуальної безпеки

Література: 2, 4, 7,10

Практичне заняття 8. Відповідальність за порушення законодавства про комерційну таємницю та прояви недобросовісної конкуренції

Питання для обговорення:

1. Відповідальність за дії недобросовісної конкуренції
2. Комерційна таємниця як об'єкт посягання в процесі інтелектуальної безпеки
3. Відповідальність за порушення законодавства про комерційну таємницю 1. Відповідальність за дії недобросовісної конкуренції
2. Комерційна таємниця як об'єкт посягання в процесі формування системи інтелектуальної безпеки
3. Відповідальність за порушення законодавства про комерційну таємницю
4. Завдання і функції служби економічної безпеки щодо захисту комерційної таємниці.

Мета: Вивчення особливостей несення відповідальності за порушення законодавства про комерційну таємницю

Література: 1,4,7,12

Практичне заняття 9. Технічний захист інформації як елемент інтелектуальної безпеки

Питання для обговорення:

1. Форми контролю за каналами витоку інформації.
2. Система технічного захисту інформаційних об'єктів. Кібербезпека.
3. Роль персоналу в захисті комерційної таємниці.
4. Захист комерційної таємниці в переговорних процесах, на виставках і ярмарках.
5. Особливості захисту комерційної таємниці у зовнішньоекономічній діяльності підприємства.

Мета: Характеристика технічного захисту інформаційних об'єктів.

Література: 8, 9

Практичне заняття 10. Загрози та ризики для національної економічної безпеки в сфері інтелектуальної власності

Питання для обговорення:

1. Моніторинг інтелектуальної безпеки. Критерії та показники оцінки інтелектуальної безпеки.
2. Загрози та ризики інтелектуальної безпеки.
3. Промислове шпигунство в системі світової конкуренції. Інтелектуальна власність як інструмент економічної агресії в умовах глобалізації.

Мета: Характеристика показників оцінки інтелектуальної безпеки.

Література: 5,7,9

Практичне заняття 11. Інтелектуальна безпека підприємства

Питання для обговорення:

1. Інтелектуальна безпека підприємства та її складові.
2. Шляхи втрати об'єктів інтелектуальної власності та інформації про них. Загрози безпеці інтелектуальної власності підприємства.
3. Механізм управління системою інтелектуальної безпеки на підприємстві залежно від виду підприємства.
4. Форми, напрями і механізми захисту інтелектуальної власності підприємства. Завдання служби економічної безпеки щодо забезпечення інтелектуальної власності.

Мета: Набуття практичних навичок з планування системи захисту службою безпеки підприємства

Література: 3,5, 9

Практичне заняття 12. Промислове шпигунство і конкурентна розвідка як загрози інтелектуальній безпеці

Питання для обговорення:

1. Відмінність промислового шпигунства від конкурентної розвідки
2. Методи, що використовуються в промисловому шпигунстві
3. Методи, що використовуються в конкурентній розвідці

4. Організаційні методи захисту від інтелектуальної безпеки на підприємстві

Мета: Характеристика методів та форм шпигунства та конкурентної розвідки

Література: 8, 9

Практичне заняття 13. Убезпечення об'єктів права інтелектуальної власності

Питання для обговорення:

1. Сутність безпеки об'єктів права інтелектуальної власності. Загрози та ризики втрати, несанкціонованого копіювання, використання конкурентами інтелектуального продукту.
2. «Due Diligence» інтелектуальної власності у зниженні ризиків інтелектуальної безпеки організації.
3. Патентування як механізм захисту інтелектуальної власності. Сучасні патентні технології. Традиційна та міжнародна процедури патентування. Зарубіжне патентування.
4. Ноу-хау і комерційна таємниця. Переваги і недоліки охорони комерційно цінної інформації у режимі конфіденційності.
5. Захист авторських і суміжних прав в епоху Інтернет.
6. Засоби індивідуалізації учасників цивільного обороту товарів та послуг в забезпеченні інтелектуальної власності організації: сфера та особливості застосування.

Мета: Вивчення питань безпеки об'єктів права інтелектуальної власності в контексті технічного захисту інформаційних об'єктів інтелектуальної безпеки

Література: 2,5,6

Практичне заняття 14. Страхування об'єктів інтелектуальної власності як передумова формування ефективної системи інтелектуальної безпеки

Питання для обговорення:

1. Ризики та страхові інтереси в сфері відносин інтелектуальної власності.
2. Сутність та сфера застосування страхування інтелектуальної власності: зарубіжний досвід та практика в Україні.
3. Види страхування інтелектуальної власності.

Мета: Дослідження процесу страхування інтелектуальної власності

Література: 2,5,6

Практичне заняття 15. Безпека інтелектуальних трудових ресурсів підприємства та руху знань як елемент інтелектуальної безпеки

Питання для обговорення:

1. Інтелектуальні трудові ресурси підприємства як носії знань
2. Специфічні та інтерспецифічні інтелектуальні трудові ресурси. Збитки підприємства внаслідок їх втрати
3. Інвестиції в робочі та проектні команди. Роль управління рухом знань в організації системи інтелектуальної безпеки.

Мета: Дослідження системи формування інтелектуальних трудових іресурсів.

Література: 2,5,6

6 Самостійна робота

Метою виконання самостійної роботи є глибоке вивчення методів формування системи інтелектуальної безпеки. 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. Кількість годин вказана для денної та заочної форми відповідно).

1. Сучасні підходи до визначення сутності інтелектуальної безпеки
2. Структура та властивості системи економічної безпеки держави
3. Сутнісні характеристики інтелектуальної безпеки в системі економічної безпеки держави
4. Структурно-функціональні параметри системи інтелектуальної безпеки
5. Методологічні засади дослідження технічного захисту інформаційних об'єктів в системі економічної безпеки
6. Методичні підходи до оцінювання системи інтелектуальної безпеки
7. Роль вищої освіти у формуванні системи інтелектуальної безпеки
8. Активізація наукової діяльності як передумова розвитку інтелектуальної безпеки
9. Оцінювання рівня та ефективності використання інтелектуальної безпеки України

7. Комплексне практичне індивідуальне завдання.

Комплексне практичне індивідуальне завдання з дисципліни " **Інтелектуальна безпека** " виконується самостійно кожним студентом. Мета виконання комплексного практичного індивідуального завдання полягає у глибокому самостійному вивченні формування системи інтелектуальної безпеки.

Виконання комплексного практичного індивідуального завдання необхідно починати з вивчення відповідних розділів підручників, навчальних посібників, тощо, що наведена у переліку рекомендованої літератури, а також додаткової літератури, практичних матеріалів, які студент повинен знайти і опрацювати самостійно.

Робота може пропонуватися студентам в якості написання практичного завдання (в якості формування стратегії), доповіді-реферату та підготовки презентації на обрану тему. Робота повинна бути написана студентом самостійно, своїми словами. Забороняється переписувати підручники, нормативні акти тощо. Цитування робіт окремих авторів необхідно наводити з посилання на джерела їх опублікування, який наводиться в кінці роботи у списку використаної літератури. Обсяг роботи повинен становити 20-25 сторінок печатного тексту через 1,5 інтервали.

У випадку підготовки презентації, вона повинна включати від 10 до 15 слайдів та бути продемонстрованою в присутності інших студентів. У тих випадках, коли робота повертається студенту для виправлення помилок, нова робота повинна представляти для перевірки разом з поверненою.

Завдання:

Підготувати реферативну доповідь (презентацію РРТ)

1. Інтелектуальна безпека як складова національної економічної безпеки.
2. Роль інтелектуальної безпеки у формуванні інноваційної моделі розвитку.
3. Суб'єкти інтелектуальної безпеки та їх інтереси.
4. Суперечності інтересів суб'єктів відносин інтелектуальної власності.
5. Інституційні умови інтелектуальної безпеки.
6. Сучасні трансформації інституційних основ сфери інтелектуальної власності.
7. Загрози та ризики інтелектуальної безпеки як складової національної економічної безпеки.

8. Внутрішні та зовнішні загрози.
9. Промислове шпигунство в системі світової конкуренції.
10. Інтелектуальна власність як інструмент економічної агресії в умовах глобалізації.
11. Стратегічні напрями подолання загроз та нейтралізації ризиків у сфері інтелектуальної власності в Україні.
12. Превентивні і захисні заходи щодо забезпечення економічної безпеки в сфері інтелектуальної власності.
13. Державне регулювання трансферу технологій як складова забезпечення інтелектуальної власності.
14. Попередження несанкціонованих форм запозичення науково-технічних рішень, запобігання промислому шпигунству.
15. Інтелектуальна безпека підприємства.
16. Складові інтелектуальної безпеки підприємства.
17. Шляхи втрати об'єктів інтелектуальної власності та інформації про них.
18. Загрози безпеці інтелектуальної власності підприємства. Ризики та збитки.
19. Механізм управління системою інтелектуальної безпеки на підприємстві.
20. Управління безпекою відповідно до фаз життєвого циклу об'єктів інтелектуальної власності.
21. Напрями забезпечення інтелектуальної безпеки підприємства. Технічна, організаційна, мотиваційна підсистеми.
22. Основні механізми захисту інтелектуальної власності на підприємстві.
23. Завдання служби економічної безпеки щодо забезпечення інтелектуальної власності. Підрозділ конкурентної розвідки.
24. Інтелектуальні трудові ресурси підприємства як носії знань.
25. Перетворення інтелектуального продукту найманих працівників на об'єкти інтелектуальної власності підприємства.
26. Специфічні та інтерспецифічні інтелектуальні трудові ресурси.
27. Збитки підприємства внаслідок їх втрати.
28. Інструменти закріплення і збереження на підприємстві інтерспецифічних інтелектуальних трудових ресурсів.
29. Поняття комерційної таємниці.
30. Комерційна таємниця і конкуренція. Конкуренти і партнери.
31. Ознаки ведення щодо підприємства конкурентної розвідки.
32. Система раннього конкурентного попередження.
33. Методика виявлення відомостей, що складають комерційну таємницю.
34. Завдання і функції служби економічної безпеки щодо захисту комерційної таємниці. Форми контролю за каналами витоку інформації.
35. Система технічного захисту інформаційних об'єктів.
36. Кібербезпека.
37. Криптографічні засоби захисту.
38. Роль персоналу в захисті комерційної таємниці.
39. Управління працівниками, що працюють із комерційною таємницею.
40. Переговори з потенційними партнерами.
41. Договір про конфіденційність інформації.
42. Опціонана угода.
43. Сутність безпеки об'єктів права інтелектуальної власності підприємства.

44. Загрози та ризики втрати, несанкціонованого копіювання, використання конкурентами інтелектуального продукту.
45. «Due Diligence» інтелектуальної власності у зниженні ризиків інтелектуальної безпеки підприємства.
46. Патентування як механізм захисту інтелектуальної власності.
47. Запобігання передчасному розкриттю секретів при патентуванні.
48. Сучасні патентні технології: сутність, потенціал щодо забезпечення інтелектуальної власності підприємства.
49. Ноу-хау і комерційна таємниця.

8. Тренінг з дисципліни

Тренінг включає в себе:

1. Тематика: Оцінка рівня інтелектуальної безпеки

Мета: набуття навичок оцінки якісних параметрів Інтернет-ресурсів як джерела інформації для підготовки і прийняття управлінських рішень.

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

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

Оцінка має здійснюватися зважаючи на:

- зміст понять «загроза» і «безпека» по відношенню до систем «природа», «суспільство», «людина»;
- зміст понять «інтелектуальна безпека» (інтелектуальна безпека вважається складовою економічної 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 інтелектуальної безпеки в Україні;
- складові, функції, критерії, рівні та умови інтелектуальної безпеки;
- функції окремих рівнів інтелектуального захисту;
- способи та методи збереження інтелектуальної безпеки;
- особливості організації інтелектуально безпечного середовища.

Література: 13, 14, 25.

9. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Інтелектуальна безпека» використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

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

10. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни “Інтелектуальна безпека ” визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Заліковий модуль 1	Заліковий модуль 2 (ректорська контрольна робота)	Заліковий модуль 3 (підсумкова оцінка за КПІЗ)	Разом
40 %	40%	20 %	100 %
1. Усне опитування (тестування) на заняттях: Теми 1-7 по 10 балів – мах 70 балів. 2. Письмова робота – мах 30 балів.	1. Усне опитування (тестування) на заняттях: Теми 8-15 по 10 балів – мах 70 балів. 2. Письмова робота – мах 30 балів.	1. Підготовка КПІЗ – мах 40 балів. 2. Захист КПІЗ – мах 40 балів. 3. Участь у тренінгах – мах 20 балів	

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)

11. Перелік наочних матеріалів та методичних вказівок

№	Найменування	Номер теми
1	Мультимедійний проектор	1-11
2	Нормативні матеріали	1-11

3	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-11
4	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-11
5.	Програмне забезпечення: ОС Windows	1-11
6.	Інструменти Microsoft Office (Word, Power Point і т. і.)	1-11

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. 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.
2. 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>
3. Муравська Ю. Поняття та сутність економічної розвідки в контексті її відмінності від бізнес-аналітики. Російсько-українська війна: право, безпека, світ [Матеріали V Міжнародної науково-практичної конференції, м. Тернопіль, Західноукраїнський національний університет, 29-30 квітня 2022 р.]. Тернопіль: ЗУНУ, 2022. С. 245-248.
4. 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/>
DSPACE: <http://dspace.tneu.edu.ua/handle/316497/19378>
5. Мельник В. Конкурентна розвідка та промислове шпигунство як засоби конкурентної боротьби / Вікторія Мельник, Ірина Кисельова, Марина Пучкова // Інноваційне підприємництво: стан та перспективи розвитку [Електронний ресурс] : зб. матеріалів II Всеукр. наук.-практ. конф., 29–30 берез. 2017 р. / М-во освіти і науки України, ДВНЗ «Київ. нац. екон. ун-т ім. В. Гетьмана» [та ін.] ; оргком.: Г. О. Швиданенко (голова) [та ін.]. – Електрон. текст. дані. – Київ : КНЕУ, 2017. – С. 84–87. – Назва з титул. екрану.
DSPACE: <http://dspace.tneu.edu.ua/handle/316497/19381>
6. 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.
DSPACE: <http://dspace.tneu.edu.ua/handle/316497/19380>
7. 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.

DSPACE: <http://dspace.tneu.edu.ua/handle/316497/24969>

8 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.

9. Москаленко Н.В. Теоретичні аспекти запровадження комплаєнсконтролю в Україні. Економічний вісник серія: фінанси, облік, оподаткування. УДФСУ. 2018. Вип. №2. С. 106-113

10. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. Верховна Рада України. Відомості Верховної Ради України. 2017. № 45. Ст. 403

11. Barrachina, Alex and Tauman, Yair. 2014. Entry and espionage with noisy signals: Games and economic behavior: Elsevier, N 83, p. 127-146.

12. Charkiewicz, Szymon i Chmura, Aneta. 2008. Znaki towarowe w działalności małych i średnich przedsiębiorstw. Warszawa: Urząd patentowy Rzeczypospolitej Polskiej. (40 s.).

13. Chmielarz, Wojciech. 2011. Szpiegostwo przemysłowe: duży zysk, niskie kary: Niwserwis : <<http://niwserwis.pl/artykuly/szpiegostwo-przemyslowe-duzy-zysk-niskie-kary>>

14. Ciecierski, Marek. 2019. Szpiegostwo przemysłowe opanowało cyberprzestrzeń: InteriaBiznes:<<http://biznes.interia.pl/wiadomosci/news/szpiegostwo-przemyslowe-opanowalo-cyberprzestrzen,1885978,4199>>

15. Ciecierski, Marek. 2018. Wkroczyliśmy w erę wywiadu gospodarczego : InteriaBiznes: <<http://praca.interia.pl/news-wkroczyliśmy-w-ere-wywiadu-gospodarczego,nId,723996>>

16. Commission proposes rules to help protect against the theft of confidential business information : European Commission, Press release: Brussels, 28 November 2013 : <http://europa.eu/rapid/press-release_IP-13-1176_en.htm>

17. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights: <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:EN:PDF>>

18. Dyrektywa 2005/29/WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. o nieuczciwych praktykach handlowych dotycząca nieuczciwych praktyk handlowych stosowanych przez przedsiębiorstwa wobec konsumentów na rynku wewnętrznym oraz zmieniająca inne dyrektywy, Dz. Urz. UE L z 2005 r. Nr 149, s. 22.

19. Elliott, Sharon Mollman . 2007. The threat from within: trade secret theft by employees: Patents, Nature Publishing Group: Wisconsin, Vol. 25, N 3, p. 293-295.

20. Everett, Bernet. 2013. Optically transparent: the rise of industrial espionage and statesponsored hacking: Feature, InfoGuard, p. 13-17.

21. Glenny, Misha and Kavanagh, Camino. 2012. 800 Titles but No Policy—Thoughts on Cyber Warfare. American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy: NCAFP, p. 287-294.

22. Hare, Forrest and Goldstein, Jnathan. 2010. The independent security problem in the defense industrial base: An agent-based model on a social network: Critical infrastructure protection, Elsevier, ScienceDirect, N 3, p. 128-139.

23. Kaczmarek, Jarosław i Kwieciński, Mirosław. 2010. Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu. Toruń : Towarzystwo Naukowe Organizacji i Kierownictwa "Dom Organizatora. (313 s.)

24. Lee, Chang-Moo. 2014. The Strategic Measures for the Industrial Security of Small and Medium Business: Hindawi Publishing Corporation, Scientific World Journal, p. 1-4.
25. Ludziejewski, Zdzisław. 2013. Bezpieczeństwo informacyjne w instytucjach gospodarczych. Zeszyty naukowe WSOWL, nr. 4 (170), s. 5-58.
26. Miller, Lesley Ellis. 1999. Innovation and Industrial Espionage in Eighteenth-Century France: An Investigation of the Selling of Silks through Samples: Journal of Design History, Vol. 12, No. 3, p. 271-292.
27. Minott, Nathaniel. 2018. The Economic Espionage Act: is the law all bark and no bite? : Information & Communications Technology Law: Routledge, Vol. 20, No. 3, October 2011, p. 201–224.
28. Morris, Mel. 2010. Intelligence, knowledge and organised crime: Computer Fraud & Security: CEO, Prevx, p. 13-15.
29. CcCallion, Jane. 2013. New EU rules on industrial espionage issued: ITPro : <<http://www.itpro.co.uk/hacking/20163/new-eu-rules-industrial-espionage-issued>>
30. Rid, Thomas and McBurney, Peter. 2012. Cyber-Weapons: The RUSI Journal, p. 6-13.
31. Rosenfeld, Steven. 2019. Corporate Espionage Tactics Used Against Leading Progressive Groups, Activists and Whistleblowers: Alternet: <<http://www.alternet.org/activism/corporate-espionage-against-progressive-nonprofits>>
32. Turaliński, Kazimierz. 2018. Wywiad gospodarczy i polityczny. metodyka, taktyka i źródła pozyskiwania. Radom: "Media Polskie". (446 s.).