МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА БЕЗПЕКИ ТА ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Юлія МУРАВСЬКА

Навчально-методичні матеріали

з дисципліни

ПРОТИДІЯ ПРОМИСЛОВОМУ ШПИГУНСТВУ

Тернопіль - 2023

УДК [65.012.8+343.534](072)
Н15

Протидія промисловому шпигунству : Навчально-методичні матеріали з дисципліни // Укладач: Ю.Є.Муравська. Тернопіль: ЗУНУ, 2023. 31 с.

Укладач:
Муравська Юлія Євгенівна – кандидат економічних наук, доцент, доцент кафедри безпеки та правоохоронної діяльності Західноукраїнського національного університету.

Відповідальна за випуск:
Канюка Валерій Євгенович, кандидат юридичних наук, в.о. завідувача кафедри безпеки та правоохоронної діяльності ЗУНУ.

Рецензенти:
Якубівський Ігор Євгенович – доктор юридичних наук, професор, професор кафедри цивільного права та процесу Львівського національного університету імені Івана Франка.
Слома Валентина Миколаївна – доктор юридичних наук, доцент, професор кафедри цивільного права і процесу Західноукраїнського національного університету.

Рекомендовано на засіданні кафедри безпеки та правоохоронної діяльності Юридичного факультету Західноукраїнського національного університету.
(протокол № 9 від "04" квітня 2023 р.).

ЗМІСТ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ДИСЦИПЛІНИ «ПРОТИДІЯ ПРОМИСЛОВОМУ ШПИГУНСТВУ»

«Протидія промисловому шпигунству» є дисципліною, яка сприяє підготовці фахівців у сфері безпеки та правоохоронної діяльності. Студенти отримують теоретичні знання і практичні навички захисту та боротьби з промисловим шпигунством. Фахівці з правоохоронної діяльності володіють системою знань, що пов'язана з цілеспрямованим впливом на працівників організацій та установ для забезпечення її ефективного функціонування та підвищення рівня безпеки інтелектуальної власності, планування та організації протидії промисловому шпигунству.

По завершенню вивчення дисципліни «Протидія промисловому шпигунству» студенти можуть обґрунтовано обрати найоптимальнішу форму визначення змісту і межі проблем, пов'язаних із прийняттям рішень щодо протидії промисловому шпигунству в тісному взаємозв'язку з вирішенням інших питань безпеки та правоохоронної діяльності, а також застосовувати спеціальні фахові знання з питань захисту прав інтелектуальної власності в контексті протидії промисловому шпигунству, інформаційно-пошукові системи та бази даних з метою захисту та боротьби з промисловим шпигунством, формувати систему превентивних заходів. Це сприяє більш чіткому визначенню місця та підвищенню значення заходів із протидії промисловому шпигунству в системі безпеки.

Предметом навчальної дисципліни «Протидія промисловому шпигунству» є розвиток системи захисту та боротьби з промисловим шпигунством.

Мета навчальної дисципліни «Протидія промисловому шпигунству» — допомогти студентам, слухачам опанувати теоретичні основи та виробити вміння і практичні навички з планування та організації протидії промисловому шпигунству, а також розвиток здібностей до логічного та алгоритмічного мислення, навичок використання сучасних напрямків захисту інтелектуальної власності від проявів промислового шпигунства, методів і засобів захисту об'єктів інформатизації.

Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами теоретичних знань з захисту та боротьби з промисловим шпигунством.

Зміст навчальної дисципліни складають принципи і методи протидії промисловому шпигунству, теоретичні та практичні проблеми розроблення проекту вибору найбільш ефективної технології, засобів захисту інтелектуальної власності від проявів промислового шпигунства і методів протидії промисловому шпигунству з урахуванням конкретної ситуації.

Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами теоретичних знань з формування методів протидії промисловому шпигунству.

Кожен студент повинен отримати певний набір компетентностей, формування яких здійснюється через результати навчання.

Результати навчання повинні формулюватися таким чином, щоб досягати однієї чи декількох перерахованих нижче компетентностей:

Інтегральна компетентність:

Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі безпеки та правоохоронної діяльності під час практичної діяльності з охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку або у процесі навчання, що передбачає застосування теорій та методів правоохоронної діяльності, системного аналізу та планування операцій, прогнозування, оптимізації та прийняття рішень, проведення досліджень та/або здійснення інновацій у сфері правоохоронної діяльності і характеризується комплексністю та невизначеністю умов і вимог

Загальні компетентності:

Здатність до абстрактного мислення, аналізу та синтезу

Спеціальні (фахові) компетентності:

Здатність припиняти виявлені кримінальні та адміністративні правопорушення

Засвоєння основ базових знань з професії (у сфері правоохоронної діяльності)

Здатність застосовувати знання на практиці

На основі знань, отриманих в університеті, вміти протидіяти промисловому шпигунству.

Завдання навчальної дисципліни «Протидія промисловому шпигунству» 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 протидії промисловому шпигунству.

Навчальна дисципліна «Протидія промисловому шпигунству» 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 захисту інтелектуальної власності від проявів промислового шпигунства, протидії промисловому шпигунству в тісному взаємозв'язку з вирішенням інших питань у сфері правоохоронної діяльності. Це сприяє більш чіткому визначенню місця та підвищенню значення заходів із протидії промисловому шпигунству в системі економічної безпеки підприємства.

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

- поняття і завдання, мету і завдання захисту інтелектуальної власності від проявів промислового шпигунства, стратегію і тактику протидії промисловому шпигунству;
- зміст роботи служби безпеки, особливості протидії промисловому шпигунству, перепідготовки та підвищення кваліфікації працівників даної служби;
- специфіку планування і прогнозування впливу превентивних та реактивних заходів в контексті нейтралізації загроз виникнення промислового шпигунства;

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

- здійснювати професійне навчання, планування протидії промисловому шпигунству ;
- забезпечувати найповніше використання системи захисту інтелектуальної власності в контексті протидії промисловому шпигунству і в такий спосіб успішно протидіяти дестабілізуючим факторам зовнішнього та внутрішнього середовища.

Завдання лекційних занять

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із основними сучасними методами протидії промисловому шпигунству.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних питань щодо захисту інтелектуальної власності від проявів промислового шпигунства; законодавчої та нормативної бази.
- сформувати у студентів цілісну систему теоретичних знань з курсу «Протидія промисловому шпигунству».

Завдання практичних занять

Мета проведення практичних занять полягає в тому, щоб виробити у студентів навички практично застосувати сучасні методи протидії промисловому шпигунству, чинне законодавство України, які регулюють боротьбу з промисловим шпигунством для майбутнього використання в управлінській діяльності.

Завдання проведення практичних занять:

- розв’язувати конкретні питання стосовно використання сучасних форм захисту інтелектуальної власності від проявів промислового шпигунства;
- засвоїти методику та техніку виконання превентивних заходів протидії промисловому шпигунству;
- глибше засвоїти та закріпити теоретичні знання, одержані на

лекціях з питань захисту інтелектуальної власності від проявів промислового шпигунства.

ЗМІСТ ДИСЦИПЛІНИ «ПРОТИДІЯ ПРОМИСЛОВОМУ ШПИГУНСТВУ»

Змістовний модуль 1. Промислове шпигунство: загальнотеоретичний аспект

Тема 1. Промислове шпигунство: сутність, форми, прийоми та інструменти

1. Сутність промислового шпигунства
2. Джерела витоку інформації
3. Характерні риси промислового шпигунства
4. Найбільш поширені форми промислового шпигунства
5. Найбільш поширені прийоми промислового шпигунства
6. Інструменти промислового шпигунства
7. Виробництво підроблюваних товарів та піратських копій як результат промислового шпигунства.
8. Історія виникнення та розвитку промислового шпигунства
9. Розвиток промислового шпигунства в країнах Європи
10. Українська оборонна сфера і промислове шпигунство

Тема 2. Об'єкти та суб'єкти права інтелектуальної власності в контексті захисту від промислового шпигунства

1 Об'єкти права інтелектуальної власності, що виступають об'єктами посягань в процесі промислового шпигунства

2 Суб'єкти права інтелектуальної власності

3 Система законодавства про інтелектуальну власність

Тема 3. Авторське право в системі захисту від промислового шпигунства

1. Поняття авторського права.
2. Об'єкти, що охороняються авторським правом.
3. Суб'єкти авторського права в контексті захисту від промислового шпигунства.
4. Виникнення авторського права.
5. Знак охорони авторського права та його значення як елементи захисту від промислового шпигунства.
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 в системі захисту від промислового шпигунства

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 від проявів промислового шпигунства.
9. Патентування винаходу, корисної моделі та промислового зразка в іноземних державах.

Тема 5. Правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг в контексті захисту від промислового шпигунства

1. Засоби індивідуалізації учасників цивільного обороту, товарів і послуг та їх види.
2. Фірмове найменування (фірма) як елементи захисту від промислового шпигунства.
3. Зазначення походження товарів як елементи захисту від промислового шпигунства.: загальна характеристика.
4. Знаки для товарів і послуг як елементи захисту від промислового шпигунства.: поняття, види та значення.
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 попередження промислового шпигунства

1. Суть торгівлі ліцензіями як передумова захисту від промислового шпигунства..
2. Види ліцензій.
3. Ліцензійні договори як елементи захисту від промислового шпигунства..
4. Ліцензійні платежі.
5. Передача прав за авторськими договорами.

Тема 7. Захист прав інтелектуальної власності як складова системи попередження промислового шпигунства

1. Поняття захисту прав інтелектуальної власності від проявів промислового шпигунства.
2. Дії, що визнаються порушеннями прав інтелектуальної власності.
3. Форми захисту прав інтелектуальної власності від проявів промислового шпигунства.
4. Способи захисту прав інтелектуальної власності.

Змістовий модуль 2. Промислове шпигунство: прикладний аспект

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

1. Відповідальність за дії недобросовісної конкуренції
2. Комерційна таємниця як об'єкт посягання в процесі промислового шпигунства
3. Відповідальність за порушення законодавства про комерційну таємницю

Тема 9. Хакерство в промисловому шпигунстві як загроза для економічної безпеки

1. Поняття категорії «хакер». Маніфест хакера
2. Хакерська етика
3. Типові кроки для отримання несанкціонованого доступу
4. Загрози в Інтернеті та методи боротьби з ними

Тема 10. Промислове шпигунство і конкурентна розвідка

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 промислового шпигунства на підприємстві

Тема 11. Служба безпеки підприємства: структура, особливості управління її діяльністю та забезпечення працівниками

1. Структура та особливості управління безпекою підприємства
2. Процес управління службою безпеки та захист від промислового шпигунства.
3. Особливості підбору персоналу для роботи у службі безпеки

Тема 12. Методика збору інформації про юридичну особу.

1. Мета заходу
2. Орієнтири для збору інформації
3. Де і як можна зібрати інформацію
4. Збір і аналіз реєстраційної інформації
5. Збір і аналіз інформації з відкритих джерел

6. Аналіз рекламної продукції компанії
7.Збір і аналіз закритої інформації

Тема 13. Збір інформації з закритих джерел.

1. Зовнішнє спостереження
2. Збір інформації під прикриттям
3. Агентурна робота в рамках промислового шпигунства. Вербування агента
4. Аналіз телефонних (ТЛФ) переговорів
5. Прелюстрація пошти
6. Використання технічних каналів несанкціонованого отримання інформації з ціллю промислового шпигунства

Тема 14. Дезінформація у промисловому шпигунстві

1. Поняття дезінформації
2. Процес дезінформації в цілях промислового шпигунства
3. Виявлення дезінформації

ТЕМАТИКА ПРАКТИЧНИХ ЗАНЯТЬ ТА ПИТАННЯ ДЛЯ ОБГОВОРЕННЯ

Практичне заняття 1. Промислове шпигунство: сутність, форми, прийоми та інструменти

Питання для обговорення:

1. Сутність промислового шпигунства
2. Джерела витоку інформації
3. Характерні риси промислового шпигунства
4. Найбільш поширені форми промислового шпигунства
5. Найбільш поширені прийоми промислового шпигунства
6. Інструменти промислового шпигунства
7. Виробництво підроблюваних товарів та піратських копій як результат промислового шпигунства.
8. Історія виникнення та розвитку промислового шпигунства
9.Розвиток промислового шпигунства в країнах Європи
10. Українська оборонна сфера і промислове шпигунство

Мета: Визначення поняття протидії промисловому шпигунству в контексті економічної безпеки

Література: 1, 2, 5, 7

Практичне заняття 2. ***Об'єкти та суб'єкти права інтелектуальної власності в контексті захисту від промислового шпигунства***

Питання для обговорення:

1 Об'єкти права інтелектуальної власності, що виступають об'єктами посягань в процесі промислового шпигунства

2 Суб'єкти права інтелектуальної власності

3 Система законодавства про інтелектуальну власність

Мета: засвоїти та закріпити теоретичні знання щодо питання сутності інституту інтелектуальної власності в системі протидії промисловому шпигунству

Література: 1, 3, 7,12.

Практичне заняття 3. ***Авторське право в системі захисту від промислового шпигунства***

Питання для обговорення:

1. Поняття авторського права.
2. Об'єкти, що охороняються авторським правом.
3. Суб'єкти авторського права в контексті захисту від промислового шпигунства.
4. Виникнення авторського права.
5. Знак охорони авторського права та його значення як елементи захисту від промислового шпигунства.
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 протидії промисловому шпигунству

Література: 1, 3, 7,12.

Практичне заняття 4. ***Правова охорона об'єктів промислової власності. Патентне право в системі захисту від промислового шпигунства***

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 від проявів промислового шпигунства.

9. Патентування винаходу, корисної моделі та промислового зразка в іноземних державах.

Мета: засвоїти та закріпити теоретичні знання щодо питання сутності патентного права в системі протидії промисловому шпигунству

Література: 7,10,14,17.

Практичне заняття 5. ***Правова охорона засобів індивідуалізації учасників цивільного обороту, товарів і послуг в контексті захисту від промислового шпигунства***

Питання для обговорення:

1. Засоби індивідуалізації учасників цивільного обороту, товарів і послуг та їх види.

2. Фірмове найменування (фірма) як елементи захисту від промислового шпигунства.

3. Зазначення походження товарів як елементи захисту від промислового шпигунства.: загальна характеристика.

4. Знаки для товарів і послуг як елементи захисту від промислового шпигунства.: поняття, види та значення.

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

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 попередження промислового шпигунства***

Питання для обговорення:

1. Суть торгівлі ліцензіями як передумова захисту від промислового шпигунства..
2. Види ліцензій.
3. Ліцензійні договори як елементи захисту від промислового шпигунства..
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 попередження промислового шпигунства

Література: 10,14-18.

Практичне заняття 7. ***Захист прав інтелектуальної власності як складова системи попередження промислового шпигунства***

Питання для обговорення:

1. Поняття захисту прав інтелектуальної власності від проявів промислового шпигунства.
2. Дії, що визнаються порушеннями прав інтелектуальної власності.
3. Форми захисту прав інтелектуальної власності від проявів промислового шпигунства.
4. Способи захисту прав інтелектуальної власності.

Мета: Ознайомлення з особливостями захисту прав інтелектуальної власності як складової системи попередження промислового шпигунства

Література: 2, 4, 7,10

Практичне заняття 8. ***Відповідальність за порушення законодавства про комерційну таємницю та прояви недобросовісної конкуренції в промисловому шпигунстві***

Питання для обговорення:

1. Відповідальність за дії недобросовісної конкуренції
2. Комерційна таємниця як об’єкт посягання в процесі промислового шпигунства
3. Відповідальність за порушення законодавства про комерційну таємницю

Мета: Вивчення особливостей несення відповідальності за дії промислового шпигунства та за порушення законодавства про комерційну таємницю

Література: 1,4,7,12

Практичне заняття 9. ***Хакерство в промисловому шпигунстві як загроза для економічної безпеки***

Питання для обговорення:

1. Поняття категорії «хакер». Маніфест хакера
2. Хакерська етика
3. Типові кроки для отримання несанкціонованого доступу
4. Загрози в Інтернеті та методи боротьби з ними
5. Хто такі хакери і які загрози вони несуть?.
6. Поняття й етапи отримання несанкціонованого доступу.
7. Зміст хакерської етики
8. Система протидії хакерським атакам.
9. Сутність боротьби з загрозами в Інтернеті, рекомендації щодо використання їх на практиці.

Мета: Характеристика методів та форм хакерства

Література: 8, 9

Практичне заняття 10. ***Промислове шпигунство і конкурентна розвідка***

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 промислового шпигунства на підприємстві

Мета: Характеристика методів та форм промислового шпигунства та конкурентної розвідки в розрізі пошуку їх відмінних рис

Література: 5,7,9

Практичне заняття 11. ***Служба безпеки підприємства: структура, особливості управління її діяльністю та забезпечення працівниками***

Питання для обговорення:

1. Структура та особливості управління безпекою підприємства

2. Процес управління службою безпеки та захист від промислового шпигунства.

3. Особливості підбору персоналу для роботи у службі безпеки

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

Література: 3,5, 9

Практичне заняття 12. ***Методика збору інформації про юридичну особу.***

Питання для обговорення:

1. Мета заходу
2. Орієнтири для збору інформації
3. Де і як можна зібрати інформацію
4. Збір і аналіз реєстраційної інформації
5. Збір і аналіз інформації з відкритих джерел
6. Аналіз рекламної продукції компанії
7. Хто збирає інформацію про юридичну особу і які загрози вони несуть?.
8. Поняття й етапи отримання несанкціонованого доступу.
9. Зміст реєстраційної інформації
10. Збір і аналіз інформації з відкритих джерел

Мета: Характеристика методів та форм збору інформації про юридичну особу

Література: 8, 9

Практичне заняття 13. ***Збір інформації з закритих джерел.***

Питання для обговорення:

1. Зовнішнє спостереження
2. Збір інформації під прикриттям
3. Агентурна робота в рамках промислового шпигунства. Вербування агента
4. Аналіз телефонних (ТЛФ) переговорів
5. Прелюстрація пошти
6. Використання технічних каналів несанкціонованого отримання інформації з ціллю промислового шпигунства

Мета:Вивчення питань збору інформації в контексті протидії промисловому шпигунству

Література: 2,5,6

Практичне заняття 14. ***Дезінформація у промисловому шпигунстві***

Питання для обговорення:

1. Поняття дезінформації
2. Процес дезінформації в цілях промислового шпигунства
3. Виявлення дезінформації

Мета:Дослідження процесу дезінформування

Література: 2,5,6

КОМПЛЕКСНЕ ПРАКТИЧНЕ ІНДИВІДУАЛЬНЕ ЗАВДАННЯ: МЕТА, ЗМІСТ, ВАРІАНТИ ЗАВДАНЬ

Комплексне практичне індивідуальне завдання з дисципліни «Протидія промисловому шпигунству» виконується самостійно кожним студентом. Мета виконання комплексного практичного індивідуального завдання полягає у глибокому самостійному вивченні методів забезпечення надійності персоналу.

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 представлятись для перевірки разом з поверненою.

Завдання:

А. Підготувати реферативну доповідь (презентацію PPT) про приклади промислового шпигунства в різних країнах / компаніях світу (країна/компанія/підприємство надається викладачем). На основі викладеного матеріалу сформуйте можливу стратегію протидії промисловому шпигунству на підприємстві

АБО

Б. Підготувати презентацію з дослідження конкретного виду інструментів промислового шпигунства :

- спеціальна звукозаписуюча апаратура;
- прилади для зняття інформації з телефонних ліній зв'язку;
- міні-радіозакладки;
- апаратура для зняття інформації з вікон за допомогою лазерних випромінювачів;
- навідні мікрофони;
- спеціальні системи спостереження і передача відеозображення;
- спеціальна фотоапаратура;
- прилади спостереження;
- прилади нічного бачення;
- апаратура для виявлення радіоактивного та іншого випромінювання тощо)

з використанням блок–схем, за наступними розділами:

1.Дати характеристику приладу. Оцінити рівень небезпеки на підприємстві. В яких країнах використовується найчастіше?
2.Визначити основні загрози безпеки на підприємстві, де такий прилад встановлено.

САМОСТІЙНА РОБОТА З ДИСЦИПЛІНИ «ПРОТИДІЯ ПРОМИСЛОВОМУ ШПИГУНСТВУ»

Метою виконання самостійної роботи є глибоке вивчення методів забезпечення надійності персоналу.

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 Всесвітня організація інтелектуальної власності - результативність впливу в контексті протидії промисловому шпигунству.

2. Міжнародна служба безпеки і розслідувань злочинів у сфері промислового шпигунства.

3. Концепція «Протидія промисловому шпигунству» і її вплив на економічну систему.

4. Створення умов для підготовки та проведення терористичних і диверсійних акцій.

5. Моніторинг персоналу як механізм протидії промисловому шпигунству.

6. Підробка товарів.

7. Маркетинг персоналу, його роль, місце в протидії промисловому шпигунству.

8. Інструментарій промислового шпигунства.

9. Легальне промислове шпигунство.

10. Загальна характеристика психологічних прийомів, технік, які використовуються при протидії промисловому шпигунству.

11. Діяльність конкурентної розвідки на підприємстві.

ОРГАНІЗАЦІЯ ТА ПРОВЕДЕННЯ ТРЕНІНГУ З ДИСЦИПЛІНИ «ПРОТИДІЯ ПРОМИСЛОВОМУ ШПИГУНСТВУ»

Тренінг включає в себе:

1. Тематика: Оцінка якості Web-ресурсу як джерела інформації

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 прийняття управлінських рішень.

Оцінка має здійснюватися за такими критеріями:

- компетентність і репутація авторів (власників) сайту (на основі вихідних даних – інформації про авторів, контактної інформації, адреси email і т. ін.);
- мета (визначення мети створення сайту з чіткою орієнтованістю на цільову групу; зосередженість на основній проблемі);
- розкриття теми (міра розкриття тих чи інших тем, прагматична цінність інформації, її об’єктивність і достовірність);
- актуальність;
- достовірність інформації та використаних джерел (наявність посилань на джерела інформації, опис відповідних методик);
- оригінальність матеріалів;
- інтерактивність;
- належність до пріоритетних сфер.

Література: 13, 14, 25.

ПРАКТИЧНІ ЗАВДАННЯ З ПОПЕРЕДЖЕННЯ ПРОЯВІВ ПРОМИСЛОВОГО ШПИГУНСТВА НА ПІДПРИЄМСТВІ

1. Дати коротку характеристику стану українського законодавства в галузі захисту від промислового шпигунства. Які доповнення до українського законодавства з цього питання Ви запропонували б?

Підказка: Законодавче визначення промислового шпигунства в сучасному законодавчому полі України обумовлене наступними законодавчими актами:

Господарський Кодекс України;

Кримінальний Кодекс України;

Цивільний Кодекс України;

Закон України “Про інформацію”;

Закон України “Про захист від недобросовісної конкуренції”;

Згідно з “Господарським Кодексом України”:

Стаття 32. Недобросовісна конкуренція

2. Поясніть як за допомогою спостереження за підприємством можна визначити, що воно виробляє.

Підказка: При зовнішньому контактному спостереженні, якщо дозволяють умови, найбільший обсяг інформації про підприємство та його продукцію можна дізнатися :

а) при бесідах в відділі кадрів про можливе працевлаштування;

б) при наявності доступу в відділ збуту продукції – проведення спеціальних бесід по можливому придбанні продукції підприємства;

в) при аналізі запрошення на роботу (об’яви);

г) при підслуховуванні та вступі в неформальний контакт з працівниками підприємства;

д) при працевлаштуванні охоронником чи ремонтником в гаражний кооператив працівників підприємства та вступі в неформальний контакт;

е) при спробі купити крадену готову продукцію у працівників підприємства.

3. Як потрібно було б захистити від промислового шпигунства Ваше підприємство?

Підказка: Для захисту підприємства необхідно:

провести детальне обстеження циркуляції на підприємстві інформації з обмеженим доступом – ІОД (комерційної таємниці) та розробити модель загроз для інформації для об’єкта інформаційної діяльності;

провести детальне обстеження технологічних процесів поставки сировини, виготовлення виробів та їх складування і транспортування

споживачам, розробити модель загроз для розголошення інформації про вхідні компоненти, обладнання та технологічні процеси, несанкціоноване заволодіння готовою продукцією;

на основі виявлених загроз матеріальним об'єктам та технологічним процесам розробити плани територіального захисту фізичних об'єктів підприємства (план контрольованої зони та технологічних пристроїв контролю в ній – захисні інженерні споруди, сигналізація, освітлення, відеоспостереження, контрольно-пропускна система, металошукачі на КПП, камера схову габаритних та нестандартних речей відвідувачів підприємства);

на основі виявлених загроз зняття чи розголошення комерційної інформації обмеженого доступу розробити плани захисту мовної інформації від радіоелектронної розвідки, захисту інформації, що циркулює в телекомунікаціях та лініях провідного зв'язку, використання шифраторів мобільного зв'язку, захисту інформації в комп'ютерних системах класу АС-1 (автономні комп'ютери) та класу АС-2 (локальна обчислювальна мережа) від доступу через мережу класу АС-3 (глобальні системи Інтернет) та радіоелектронних систем дистанційного зняття інформації при обробці сигналів побічних електромагнітних віпромінювань апаратури (екранування та радіозашумлення приміщень з важливими системами обробки ІОД)

4. Як можна організувати захист провідних фахівців вашого підприємства від нападу та промислового шпигунства?

Підказка: Повсякденна практика показує, що до погроз фізичної безпеки особистості належать наступні:

- викрадення й погрози викрадення співробітників, членів їхніх родин і близьких родичів;
- психологічний терор, погрози, залякування, шантаж, вимагання;
- напад з метою заволодіння коштами, цінностями й документами, убивство або погроза його здійснення.

Можна виділити чотири етапи в організації злочину проти особистості. Вони розділені в часі, відбуваються послідовно протягом тривалого періоду й застосовуються майже в будь-яких злочинах, якщо звичайно він не відбувається спонтанно. Тому що ці етапи проявляються незмінно, знання їх послідовності дає потенційній жертві досить часу для усвідомлення реальності погрози й вживанню заходів для її запобігання:

5. Провести комплексний аналіз конкурента з використанням інформації, яка друкується і подається у засобах масової інформації.

Підказка: На сьогодні найбільш інформативним джерелом інформації для економічної розвідки з використанням відкритих джерел інформації є:

- Інтернет- сайт власне підприємства, яке, наслідуючи маркетингову політику розширення ринку збуту, дає основні характеристики свого підприємства;

- Інтернет- сайт http://www.smida.gov.ua – Державної комісії по цінним паперам та фондовому ринку, на якому наведені формалізовані економічні звіти емітентів цінних паперів (акціонерних товариств).

- Інтернет- сайт http://www.pfts.com.ua – ПФТС – першої фондової торгової системи, на якому наведені поточні курси та динаміка котирування акцій підприємств та формалізовані економічні звіти емітентів цінних паперів (акціонерних товариств).

СИТУАЦІЙНІ ЗАВДАННЯ З ПИТАНЬ ПРОТИДІЇ ТА БОРОТЬБИ З ПРОМИСЛОВИМ ШПИГУНСТВОМ НА ПІДПРИЄМСТВІ

ЗАВДАННЯ 1

Український виноробний завод власності підпорядкований Держсадвинпрому України. Асортимент продукції, що випускається: тихі вина (ординарні і марочні), міцні напої, шампанські вина та вермути. Продукція виноробного заводу відома в багатьох країнах світу. Сировинною базою підприємства є Закарпатська, Одеська, Херсонська та Миколаївська області. До 2014 року – також Автономна Республіка Крим.

На заводі два основних цехи (марочних вин і ординарних вин) і два допоміжних (автотранспортний і склотарний). У цеху марочних вин встановлено 2 лінії з денним випуском продукції – 2 350 шт. за зміну; в цеху ординарних вин встановлено 2 лінії по випуску тихих вин (випуск 2 600 шт. за зміну) і 1 лінія по виробництву шипучих вин (випуск 1 400 шт. за зміну). Головними конкурентами заводу є: Київський, Харківський, Одеський, Артемівський заводи шампанських вин, Інкерманський винзавод, АТ "Масандра", АТ "Київський виробничий завод "Укрвино".

Нині завдяки талановитим та енергійним спеціалістам розроблено й освоєно групу нових марок ароматизованих вин. Налагоджено також виробництво ігристих (шампанських) вин, які на міжнародних конкурсах завоювали численні почесні нагороди. Це результат співпраці з науково-дослідними, проектно-конструкторськими інститутами й фірмами багатьох країн світу.

Необхідно:

обґрунтувати склад осіб, які будуть залучені в групу з розробки положення про режим доступу до інформації підприємства;

обґрунтувати склад відомостей, які будуть віднесені до категорій конфіденційної та таємної інформації.

ЗАВДАННЯ 2

Львівське підприємство "Модна галичанка" займає провідне місце на українському ринку з виготовлення і продажу трикотажної продукції. Підприємство є відносно молодим, але за короткий проміжок часу здобуло прихильність великої кількості споживачів. "Модна галичанка" спеціалізується на виробництві жіночого, чоловічого та дитячого трикотажу. Його продукція набула високої популярності та попиту, що обумовлено: якістю, широким спектром асортиментної групи для задоволення різновікових категорій споживачів. В асортиментну групу товарів входять: жіночі ділові та святкові костюми, сукні, светри, брюки, пальто, шарфи, хустки.

Необхідно:

визначити осіб, зацікавлених у діяльності підприємства та спроможних порушити його економічну безпеку, а також коло їх інформаційних потреб;

обґрунтувати склад джерел інформації, якими можливо скористатися з метою порушення економічної безпеки підприємства;

аргументувати перелік економічних рішень, які будуть обґрунтовані за допомогою зібраної інформації.

Результати роботи доцільно оформити у вигляді табл.:

Зацікавлені особи, їх інформаційні потреби та економічні рішення, що порушують безпеку підприємства

Зацікавлена особа	Інформаційні потреби	Джерела інформації (спосіб отримання)	Економічні рішення, що порушують економічну безпеку підприємства

ЗАВДАННЯ 3

Фірма, головний офіс і заводи якої розташовані у Великобританії, займається виробництвом парфумерних товарів. 70 % прибутку фірма отримує від реалізації оригінальної зубної пасти в різних її модифікаціях. Протягом останніх трьох років близько 65 % збуту зубної пасти припадає на частку однієї з арабських країн Персидської затоки, де ця фірма контролює ринок аналогічної продукції, забезпечуючи собі стійке зростання прибутку за рахунок постійного збільшення збуту зубної пасти.

Інші іноземні виробники зубних паст не виявляють поки що зацікавленості щодо розповсюдження своєї продукції в даній країні, оскільки для цього необхідно пройти певну процедуру реєстрації, а також виконати всі написи на тюбику та упаковці арабською мовою з урахуванням місцевого діалекту. Конкуренція з боку місцевих виробників мінімальна через нерозвинутість їх виробничої бази та більш низьку якість продукції.

Однак тиждень тому в місцевих засобах масової інформації, включаючи радіо та телебачення, розпочалась кампанія з дискредитації продукції фірми на підґрунті помилкового твердження щодо наявності в складі зубних паст, які випускаються, домішок свинячого жиру. В результаті цього збут фірми зменшився на 70 %.

Обґрунтуйте стратегію й тактику виходу підприємства з кризового стану й збільшення його економічної безпеки.

ЗАВДАННЯ 4

Компанія, що спеціалізується на розробці й виготовленні електричних приладів, відмінила привілеї для керівних працівників – усі без виключення співробітники фірми користуються загальною їдальнею, стоянкою автомашин, літають на звичайних пасажирських літаках. Для керівників немає окремих кабінетів. Усі робочі місця – кімнатки, розділені звуконепроникними перегородками заввишки півтора метри, однакові для всіх – від президента компанії до низових працівників.

Дайте відповіді на такі питання:

1. Чи згодні ви з практикою компанії, чи ні?
2. Що в ній позитивного і що негативного?

ЗАВДАННЯ 5

“Розвиток успішної ІТ-компанії “Квазар-мікро”.

В середині листопада 2021 р. корпорація “Квазар-Мікро” відмітила 22-річчя роботи на українському ринку високих технологій. За оцінками аналітиків, загальна ємність українського ринку інформаційних і комунікаційних технологій у 2021 році становила близько750 млн. дол. Як бізнес-структура, корпорація об’єднує декілька юридичних осіб. В Україні “Квазар-Мікро” — головна компанія. Її заснував Євген Уткін — нині президент, потім з’явилися інші партнери. Нині у неї близько 30 акціонерів, більшість з них — працівники цієї компанії. Є дочірня компанія “Квазар-Мікро-Техніко”, що здійснює системну інтеграцію та

виробництво комп'ютерів. Крім того, ще одна дочірня компанія займається розробкою і виробництвом інтегральних схем та виробів електроніки. Функціонують декілька компаній у Чехії, Угорщині, країнах Балтії. При цьому є фінансовий партнер, який надає можливість компанії розвиватися в росії і Східній Європі. Обсяг продаж у минулому році становив 250 млн. грн. Тепер головний напрям — системна інтеграція, тобто бізнес-консалтинг, IT-консалтинг, бізнес-додатки, система управління підприємством, комп'ютерні мережі. Значні кошти інвестуються у виробництво комп'ютерів. 19 листопада 2021 року ЄБРР виділив корпорації кредит в сумі 8 млн. дол. на добудову нового заводу з виробництва комп'ютерів, потужністю 200 тис. комп'ютерів за рік. За словами президента корпорації Євгена Уткіна, в найближчі декілька років персонал буде використовувати нагромаджений досвід для повномасштабної експансії на ринки росії та країн Східної Європи. До того ж корпорація намагається виступати не як виробник комп'ютерів або дистриб'ютор, а як сервісна консалтингова компанія.

Питання до ситуації:

1. Які загрози можуть виникнути для компанії на іноземних ринках?
2. Проаналізуйте сильні та слабкі сторони компанії, загрози та можливості (SWOT аналіз) в контексті захисту від промислового шпигунства.
3. Перерахуйте законодавчі акти, котрими повинна керуватися компанія при виході на ринок Східної Європи та росії.

ЗАВДАННЯ 6

"Таємниця успіху IBM".

Успіх IBM часто забезпечували не технологічні нововведення. Нажаль, у багатьох випадках вони були не серед перших при їх втіленні, і технологія стала менш важливою, ніж методи збуту та продажу. IBM систематично продавали більше, ніж ті, хто мав кращу технологію, оскільки знали, як і що пояснити клієнту, як допомогти у впровадженні машини і як прив'язати його до себе після її придбання. Вдалий підхід до збуту — системне знання. Водночас слід нагадати, що у виробництві персональних комп'ютерів гігант IBM спочатку відставав від своїх конкурентів, піддавався фірмам-піонерам, але вже через три роки існування втричі перевищила їх. Цьому сприяло використання внутрішньо фірмових стандартів і збереження сумісності з машинами більш високого класу, що дало можливість споживачам використовувати накопичений за

десятиріччя банк програм. Отже, сьогодні перевага ветерана комп'ютеро будування перед новачками незаперечна.

Питання до ситуації:

1. Які загрози можуть виникнути для компанії на іноземних ринках?

2. Проаналізуйте сильні та слабкі сторони компанії, загрози та можливості (SWOT аналіз) в контексті захисту від промислового шпигунства.

3. Зробіть висновки та запропонуйте шляхи удосконалення системи захисту від промислового шпигунства для підприємства.

ЗАВДАННЯ 7

"Mc Donald's вперше став збитковим".

Найкрупніша у світі мережа швидкого харчування McDonald's вперше завершила перший квартал 2022 року зі збитком. Основною причиною є масштабна програма реструктуризації бізнесу, в ході якої компанія змушена була закрити сотні закусочних по всьому світу і звільнити тисячі працівників. В період з квітня по грудень 2021 р. збитки становили 343,8 млн. дол., що еквівалентно середньому зниженню вартості акцій на 27%. Тобто збитки IV кварталу значно перевищили загальний прибуток 2020 року, який становив 271,9 млн. У 2021 році компанія зазнала збитків, пов'язаних з втратою трьох прибуткових ринків в Латинській Америці, а також від закриття закусочних в Японії та США. При цьому глава McDonald's Джим Кантклупо заявив, що його компанія має намір і в поточному році закривати закусочні в цих країнах. Мережа, що включає 30 тис. ресторанів по всьому світу, не змогла зупинити істотне падіння темпів зростання продажів на найбільшому з її ринків — у США, де цей показник знизився на 1,3%, а поза межами Штатів — на 1,6%. На думку аналітиків, основною причиною є недобросовісна конкуренція на американському ринку швидкого харчування, яка останнім часом дуже загострилася: все більшої ваги набирають конкуренти McDonald's — Burger King, Wendy's і Taco Bell. У закінченому кварталі 2021 року акції McDonald's втратили в ціні майже 14% при загальному зростанні на американському фондовому ринку. І навіть останні заходи — новий рівень "цінової війни", масові звільнення персоналу та залишення малоприбуткових ринків — не допомогли. Не дивлячись на зниження популярності фаст-фудів, закриваючи ресторани в одних країнах, McDonald's не відмовляється

Питання до ситуації:

1. Дайте визначення ситуаційної стратегії та тактики і наведіть приклад відповідно до запропонованої ситуації.

2. Оцініть, наскільки правильне рішення прийняло керівництво McDonald's. Обгрунтуйте відповідь.

3. Які фактори промислового шпигунства можна відслідкувати в ситуації?

4. Які загрози можуть виникнути для компанії на іноземних ринках?

5. Проаналізуйте сильні та слабкі сторони компанії, загрози та можливості (SWOT аналіз) в контексті захисту від промислового шпигунства.

6. Зробіть висновки та запропонуйте шляхи удосконалення системи захисту від промислового шпигунства для підприємства.

ЗАВДАННЯ 8

Товариство "Весна"

Спільне українсько-швейцарське товариство "ВЕСНА" є фіналістом 4-го Українського національного конкурсу з якості у номінації "Великі підприємства", член Клубу лідерів якості України з 1998 року. Рік заснування — 1945. З 29 листопада 1983 року — продовжило свою діяльність як СУШАТ "Весна". Кількість працюючих — 803 особи.

Основні види діяльності: розробка та виробництво жіночого та чоловічого одягу."Весна" є одним із провідний підприємств легкої промисловості України. Це стабільна, надійна та перспективна фірма, яка володіє значним виробничим, інтелектуальним та фінансовим потенціалом. Діяльність її спрямована на розробку, виробництво, реалізацію та експорт широкого асортименту швейних виробів. "Весна" щорічно виготовляє понад 400 нових моделей високоякісного сучасного одягу. Тільки за рахунок впровадження нової технології та освоєння складної високомодної продукції у 2021 році підприємство отримало 722,4 тис. грн. прибутку. Активна суспільна і підприємницька діяльність президента. В складних умовах функціонування економіки країни "Весна" не скоротило виробництво і не тільки зберегло робочі місця, а й збільшило їх кількість, налагодивши ділові зв'язки з фірмами Німеччини, США, Франції тощо. Було відкрито два високомеханізовані цехи та створено додаткові робочі місця. Девіз колективу — "Ми одна сім'я, наше підприємство — наш дім, всі наші досягнення та проблеми є спільними". З метою вивчення передових технологій та сучасного рівня технологічного устаткування щорічно групи спеціалістів відвідують швейні та машинобудівні фірми Німеччини й Іспанії. Це дає можливість вивчати досвід роботи зарубіжних підприємств та вносити пропозиції щодо

вдосконалення роботи власних. Нестабільність економічних законів України, інфляційні процеси, падіння купівельної спроможності населення спонукають розробляти стратегічну політику не більше як на п’ять років, а плани – на один рік. З 2020 року практикується прийом на роботу на конкурсній основі згідно наступних критеріїв відбору: освіта, ділові якості, навики та стаж роботи за фахом, перспектива росту, перевірка за критерієм надійності персоналу. Така система значно знизила плинність кадрів та підняла рівень кваліфікації працюючих. Зросла активність персоналу. Так, якщо у 2019 році надходило 1–2 пропозиції щодо покращання роботи та умов праці, то у 2020 — 10, у 2021 — 21 пропозиція. На підприємстві функціонують продуктовий магазин, медпункт (стоматологічний, терапевтичний, гінекологічний кабінети, офтальмолог, масажист), працює тренувальний зал. Один раз в два роки проводиться комплексний медогляд працівників. Надається житло працівникам (у 2021 р — 27 квартир). Виплачуються дивіденди, 13-та та 14-та зарплати. Стратегія підприємства розрахована на публічність звітності та відкритість даних, яка Для оцінювання рівня задоволення потреб споживачів проводиться щорічне анкетування, яке дозволяє вивчати споживчий попит, задоволеність якістю та дизайном продукції. Підприємство веде постійне спостереження за дотриманням конфіденційності секретів виробництва, ноу-хау та раціоналізаторських пропозицій. Наявна висококваліфікована системи відеоспостереження. Згідно з відгуками постійних споживачів з Німеччини, продукція користується значним попитом. Відповідно збільшилися обсяги реалізації продукції “Весна” поза межами держави. Щорічно товариство збільшує кількість робочих місць, забезпечуючи молодь та інвалідів робочими місцями (з 2009 року — 190 робочих місць). Виділяються кошти для надання допомоги більш ніж 15 товариствам, інвалідам, дитячим будинкам та будинкам для престарілих. У 2021 році отримано прибутку на 3,2 тис. грн. більше запланованого рівня. Середня зарплата одного працюючого складає вдвічі вища, ніж по галузі.

Питання до ситуації:

1. Які загрози можуть виникнути для безпеки компанії на іноземних ринках?

2. Які види стратегічних альтернатив захисту від промислового шпигунства використовує підприємство?

3. Яку конкурентну стратегію реалізує компанія?

4. Проаналізуйте сильні та слабкі сторони компанії, загрози та можливості (SWOT аналіз) в контексті захисту від промислового шпигунства.

5. Зробіть висновки та запропонуйте шляхи удосконалення системи захисту від промислового шпигунства для підприємства.

СЛОВНИК ТЕРМІНІВ ТА ПОНЯТЬ

Безпека – такий стан суб’єкта, при якому ймовірність зміни властивих цьому суб’єкту якостей та параметрів його зовнішнього середовища незначна, менше певного інтервалу.

Джерела інформації – носії інформації у вигляді документів та інших матеріальних об'єктів, що зберігають інформацію, а також повідомлення засобів масової інформації, публічні виступи.

Економічна безпека – це універсальна категорія, яка відбиває захищеність суб'єктів соціально-економічних відносин на всіх рівнях, починаючи з держави і закінчуючи кожним її громадянином. Категорія економічної безпеки характеризує динамічну рівновагу економічної системи в часі, яка досягається в процесі її розвитку і адаптації до дій внутрішніх і зовнішніх чинників.

Інноваційна продукція — нові конкурентоздатні товари чи послуги, що відповідають вимогам до інноваційної діяльності.

Інноваційний продукт - результат науково-дослідної і/або дослідно-конструкторської розробки, що відповідає вимогам до інноваційної діяльності.

Інтегральна мікросхема (ІМС) - мікроелектронний виріб кінцевої або проміжної форми, призначений для виконання функцій електронної схеми, елементи і з'єднання якого неподільно сформовані в об'ємі і/або на поверхні матеріалу, що становить основу такого виробу, незалежно від способу його виготовлення.

Інтелектуальна власність - формалізований результат творчої інтелектуальної діяльності, що надає його автору або особі, визначеній чинним законодавством, право власності на цей результат, яке набувають, здійснюють та захищають відповідно до законодавче встановлених норм і правил.

Інформація - відомості в будь-якій формі та вигляді, на будь-яких носіях (у тому числі листування, книги, помітки, ілюстрації (карти, діаграми, органіграми, малюнки, схеми тощо), фотографії, голограми, кіно, відеофільми, мікрофільми, звукові записи, бази даних комп'ютерних систем або повне чи часткове відтворення їх елементів), пояснення осіб та будь-які інші публічно оголошені чи документовані відомості.

Конфіденційна інформація:
- відомості, якими володіють, користуються або розпоряджаються окремі фізичні чи юридичні особи і які поширюються за їх бажанням відповідно до передбачених ними умов;
- є власністю держави і перебуває в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ до неї.

Криміналізація діяльності – явище, яке в цілому здійснює негативну дію на економічну безпеку як держави, так і на окремо взяті підприємства.

Контрафактні товари – товари, що містять об'єкти права інтелектуальної власності, ввезення яких на митну територію України або вивезення з цієї території призводить до порушення прав власника, що охороняються відповідно до чинного законодавства України та міжнародних договорів України, укладених в установленому законом порядку.

Копірайт (COPYRIGHT) - авторське право.

Корисна модель - нове й промислове придатне конструктивне виконання пристрою.

Кримінально-правовий спосіб захисту - кримінальна відповідальність за порушення прав інтелектуальної власності наступає, якщо власнику прав завдана матеріальна шкода у великому розмірі або у особливо великому розмірі.

Ліцензіар - особа, яка має виключне право дозволяти використання об'єкта права інтелектуальної власності.

Лщензіат - особа, яка отримує дозвіл від ліцензіара на використання об'єкта права інтелектуальної власності.

Ліцензія (ліцензія на використання об'єкта права інтелектуальної власності) -дозвіл особи, яка має виключне право дозволяти використання об'єкта права інтелектуальної власності (ліцензіара), що видається іншій особі (ліцензіату) на використання об'єкта права Інтелектуальної власності на певних умовах.

Недержавні організації, агентства, установи – різні приватні охоронні і детективні організації, аналітичні центри, інформаційні служби, учбові, наукові і консультаційні організації і т.д. Вони, як правило, за плату

надають послуги з охорони об'єктів, забезпечують захист інформації, комерційної таємниці, накопичують і уявляють інформацію про конкурентів, ненадійних партнерів і т.д.

Промисло́ве шпигу́нство стосовно бізнесу — це різновид економічного шпигунства, якому властиве звуження масштабів завдань з одержання інформації, що цікавить, від державного — до масштабу однієї або декількох фірм-конкурентів. Промислове шпигунство — вид недобросовісної конкуренції, діяльність із незаконного добування відомостей, що становлять комерційну цінність.

Промисловий зразок — результат творчої діяльності людини у галузі художнього конструювання.

Раціоналізаторська пропозиція - технічне вирішення, яке є новим і корисним підприємств, для якого воно призначено.

Рівень техніки - сучасна ступінь розвитку конкретної області техніки, з якою порівнюють нові винаходи. Домагання на визнання винаходу чи корисної моделі патентоспроможності повинні представити новий аспект, що виводить їх за межі відомих на даний момент науково-технічних знань.

Роялті - виплата ліцензійної винагороди шляхом періодичних відрахувань, які встановлюють у вигляді фіксованих ставок на базі розрахунку фактичного економічного результату від використання ліцензії (база роялті) і виплачуються ліцензіатом через певні проміжки часу.

Секретний винахід (секретна корисна модель) - винахід (корисна модель), що містить інформацію, віднесену до державної таємниці.

Службовий винахід (корисна модель) - винахід (корисна модель), створений працівником:

- з використанням досвіду, виробничих знань, секретів виробництва і обладнання роботодавця;
- у зв'язку з виконанням службових обов'язків чи дорученням роботодавця за умови, що трудовим договором (контрактом) не передбачене інше.

Технічні засоби захисту - технічні пристрої і/або технологічні розробки, призначені для створення технологічної перешкоди порушенню авторського права і/або суміжних прав при сприйнятті і/або копіюванні захищених (закодованих) записів у фонограмах (відеограмах) і передачах організацій мовлення чи для контролю доступу до використання об'єктів авторського права і суміжних прав.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ:

1. Муравська (Якубівська) Ю.Є. Тенденції розвитку промислового шпигунства у світі / Ю. Є. Муравська (Якубівська) // Ефективна економіка [Електронне наукове фахове видання]. - № 1. – Дніпропетровськ : ДДАТУ, 2017. Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5383

DSPACE: http://dspace.tneu.edu.ua/handle/316497/19379

2. Виштикалюк М. П. Методи промислового шпигунства в сучасних умовах технологічного розвитку [Текст] / М. П. Виштикалюк // «Перспективи розвитку сучасної науки» (м. Львів, 02-03 грудня 2016 р.). — Херсон : Видавничий дім "Гельветика", 2016. – С. 54-58.

3. Муравська Ю. Є. Навчально-методичні матеріали з дисципліни «Аналітична розвідка» ; уклад. : Ю. Є. Муравська. – Тернопіль : ТНЕУ, 2018. – 46 с.

DSPACE: http://dspace.tneu.edu.ua/handle/316497/29079

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.Зянько В. В. Раціоналізація бізнесової поведінки підприємств України шляхом аналізу переваг та небезпек конкурентної розвідки та промислового шпигунства / В. В. Зянько, В. С. Ревенко // Причорноморські економічні студії. - 2016. - Вип. 6. - С. 187-191.

6. 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.

7.Якубівська Ю. Є. Промислове шпигунство з боку Китаю як загроза для економічної безпеки / Ю. Є. Якубівська // Збірник тез доповідей всеукраїнської науково-практичної конференції «Тактичні та стратегічні пріоритети зміцнення фінансово-економічної безпеки держави», м. Тернопіль, 8-9 квітня 2016 р., ТНЕУ. – Тернопіль, 2016. – С.152-154.

DSPACE: http://dspace.tneu.edu.ua/handle/316497/19381

8. 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

9. 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

10. 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.

DSPACE: http://dspace.tneu.edu.ua/handle/316497/19386

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

12. 2021 Special 301 Report. URL: https://ustr.gov/sites/default/files/files/reports/2021/2021%20Special%20301%20Report%20(final).pdf (дата звернення 03.01.2023)

13. Balanced International Trade in Services EBOPS (2005-2019). WTO STATS. 2020. URL: https://stats.wto.org/

14. Bodyanskiy Y., Pirus A., Deineko A. Multilayer radial-basis function network and its learning // Proceedings of the 15th International Conference on Computer Sciences and Information Technologies (CSIT). IEEE, 2020. P. 92-95.

15. Commission staff working document: Counterfeit and Piracy Watch List. European commission. Brussels, 1.12.2022 SWD(2022) 399 final. URL: https://circabc.europa.eu/ui/group/d0803128-7d62-40ee-8349-c43ee92745aa/library/b36f701d-2850-4768-9b3e-e487140e11e5/details?download=true

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

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

18. Martynyuk V., Muravska Y. Forming a foreign trade partnership strategy in the context of strengthening national economic security: A case study of Ukraine. Forum Scientiae Oeconomia.Warszawa, 2020. Vol 8 No 2 (2020). P. 5-24 (Scopus, у співавторстві).

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

20. 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.

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

22. 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.

23. Ludziejewski, Zdzisław. 2013. Bezpieczeństwo informacyjne w instytucjach gospodarczych. Zeszyty naukowe WSOWL, nr. 4 (170), s. 5-58.

24. 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.

25. 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.

26. Morris, Mel. 2010. Intelligence, knowledge and organised crime: Computer Fraud & Security: CEO, Prevx, p. 13-15.

27. CcCallion, Jane. 2013. New EU rules on industrial espionage issued: ITPro : http://www.itpro.co.uk/hacking/20163/new-eu-rules-industrial-espionage-issued

28. Rid, Thomas and McBurney, Peter. 2012. Cyber-Weapons:The RUSI Journal, p. 6-13.

29. 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

30. Turaliński, Kazimierz. 2018. Wywiad gospodarczy i polityczny. metodyka, taktyka i źródła pozyskiwania. Radom: "Media Polskie". (446 s.).

Навчально-методичне видання

Юлія МУРАВСЬКА

Навчально-методичні матеріали

з дисципліни

ПРОТИДІЯ ПРОМИСЛОВОМУ ШПИГУНСТВУ

Підписано до друку 18.04.2023 р.
Формат 60х84/16. Папір офсетний.
Друк офсетний. Зам. № 23-229
Умов.-друк. арк. 1,5. Обл.-вид. арк. 1,7.
Тираж 30 прим.

Віддруковано ФО-П Шпак В. Б.
Свідоцтво про державну реєстрацію В02 № 924434 від 11.12.2006 р.
м. Тернопіль, бульвар Просвіти, 6/4. тел. 097 299 38 99.
E-mail: tooums@ukr.net

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції ДК № 7599 від 10.02.2022 р.