

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ**

**ГОСУДАРСТВЕННАЯ ОРГАНИЗАЦИЯ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ДОНЕЦКИЙ НАЦИОНАЛЬНЫЙ УНИВЕРСИТЕТ ЭКОНОМИКИ И ТОРГОВЛИ
ИМЕНИ МИХАИЛА ТУГАН-БАРАНОВСКОГО»**

КАФЕДРА ЭКСПЕРТИЗЫ В ТАМОЖЕННОМ ДЕЛЕ



УТВЕРЖДАЮ

Первый проректор

Л. А. Омелянович

08 2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ПРОМЫШЛЕННЫЙ ШПИОНАЖ»

Укрупненная группа специальностей **38.00.00 Экономика и управление**

Специальность **38.05.02 Таможенное дело**

Факультет маркетинга, торговли и таможенного дела

4-й курс очной формы обучения

6-й курс заочной формы обучения

Учебный год: **2021-2022**
2023-2024

Донецк
2018

Рабочая программа по учебной дисциплине «Промышленный шпионаж» для студентов специальности 38.05.02 Таможенное дело. – 13 с.

Разработчик:

ст. преподаватель кафедры

экспертизы в таможенном деле Шульц А.С.



Рабочая программа утверждена на заседании кафедры экспертизы в таможенном деле

Протокол от «03» июля 2018 года № 17

Заведующая кафедрой



(подпись)

Н.И. Осипенко

СОГЛАСОВАНО

Декан факультета маркетинга, торговли и таможенного дела



(подпись)

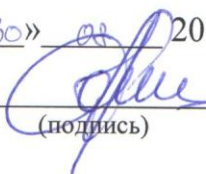
Д.В. Махносов

Дата «03» 07 2018 года

Одобрено Учебно-методическим советом Университета

Протокол от «30» 07 2018 года № рабочий

Председатель



(подпись)

Л.А. Омелянович

©А.С. Шульц, 2018 год

© ГО ВПО «Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского», 2018 год

1. ОПИСАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Наименование показателей	Укрупненная группа, специальности, специальность, образовательная программа	Характеристика учебной дисциплины	
		очная форма обучения	заочная форма обучения
Количество зачетных единиц – 2	38.00.00 Экономика и управление 38.05.02 Таможенное дело	вариативная	
Модулей – 1	специалитет	Год подготовки:	
Смысловых модулей – 2		4-й	6-й
Индивидуальные научно-исследовательские задания: не предусмотрено		Семестр	
Общее количество часов – 72		8-й	11-й
Количество часов в неделю для очной формы обучения: аудиторных – 2,0 самостоятельной работы студента – 2,0		Лекции	
		18 час.	8 час.
		Практические, семинарские занятия	
		18 час.	10 час.
		Лабораторные работы	
		час.	час.
	Самостоятельная работа		
	36 час.	54 час.	
Индивидуальные задания: не предусмотрено			
Вид контроля:			
зачет	зачет		

Соотношение количества часов аудиторных занятий и самостоятельной работы составляет:

для очной формы обучения – 36 : 36

для заочной формы обучения – 18 : 54

2. ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель: освоить знания, приобрести умения и сформировать компетенций в области обеспечения промышленной безопасности коммерческой деятельности предприятия.

Задачи:

- усвоить основные понятия в области обеспечения безопасности организации;
- изучить основные способы ведения промышленного шпионажа и каналы утечки информации;
- ознакомиться со способами перехвата информации;
- овладеть умениями проведения коммерческой разведки и защиты информации от промышленного шпионажа.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина С.1.В.27 «Промышленный шпионаж» относится к вариативной части профессионального цикла. Данная дисциплина является основополагающей для приобретения обучающимися навыков работы со способами ведения промышленного шпионажа, добычи и перехвата конфиденциальной информации, а также с техническими средствами защиты информации и обеспечивает их фундаментальными знаниями, необходимыми для изучения таких дисциплин, как: «Управление таможенным делом», «Интеллектуальная собственность», «Организация борьбы с таможенными правонарушениями» и др.

Изучение дисциплины «Промышленный шпионаж» базируется на знаниях, полученных обучающимися при изучении дисциплин «Информационные таможенные технологии» и «Экономическая безопасность».

4. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате освоения дисциплины студент должен обладать следующими профессиональными компетенциями (ПК):

- умением выявлять и анализировать угрозы экономической безопасности страны при осуществлении профессиональной деятельности (ПК-17);
- способностью противодействовать злоупотреблениям в профессиональной деятельности (ПК-22).

-

В результате изучения учебной дисциплины студент должен

знать:

- факторы, определяющие информационную безопасность предприятия;
- порядок осуществления деловой разведки на предприятии;
- политико-правовое обеспечение безопасности на предприятии;
- функционирование риск-менеджмента;
- порядок защиты коммерческой тайны.

уметь:

- определять меры по предотвращению уровня краж на предприятиях торговли;
- разрабатывать и проводить мероприятия коммерческой разведки;
- осуществлять поиск и анализировать информацию из открытых источников.

владеть:

- навыками составления документов о неразглашении конфиденциальной информации работниками предприятий;
- методами оценки внешних и внутренних угроз организации;

- навыками ведения коммерческой разведки и защиты информации от промышленного шпионажа.

5. ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Смысловой модуль 1. Промышленный шпионаж и средства получения коммерческой информации

Тема 1. Основные способы ведения промышленного шпионажа и каналы утечки информации

1. Общие сведения о промышленном шпионаже
2. Способы ведения промышленного шпионажа
3. Каналы утечки информации

Тема 2. Анализ угроз информационной безопасности

1. Основные понятия информационной безопасности
2. Реальные и мнимые угрозы на предприятии, связанные с информацией

Тема 3. Средства перехвата аудиоинформации

1. Закладные устройства с передачей информации по радиоканалу
2. Закладные устройства с передачей информации по проводным каналам
3. Диктофоны и направленные микрофоны
4. Устройства, реализующие методы высокочастотного навязывания

Тема 4. Оптические средства добычи конфиденциальной информации

1. Оптико-механические приборы
2. Приборы ночного видения
3. Средства для проведения скрытой фотосъемки
4. Технические средства получения видеоинформации

Тема 5. Перехват информации в линиях связи.

1. Методы и средства несанкционированного получения информации в телефонных и проводных линиях связи
2. Методы и средства несанкционированного получения информации в каналах сотовой связи
3. Получение информации, обрабатываемой в компьютерных сетях

Смысловой модуль 2. Защита от промышленного шпионажа

Тема 6. Организация защиты информации

1. Основные понятия информационной безопасности
2. Организационные мероприятия по защите информации
3. Добровольная аттестация объектов информатизации по требованиям безопасности информации

Тема 7. Методы и средства выявления закладных устройств

1. Общие принципы выявления
2. Индикаторы поля и специальные радиоприемные устройства
3. Программно-аппаратные комплексы
4. Рекомендации по поиску устройств негласного «съема информации»

Тема 8. Технические средства защиты информации в помещениях и сетях связи

1. Общие принципы защиты
2. Средства защиты линий связи
3. Криптографические методы и средства защиты
4. Защита от пиратских подключений

Тема 9. Защита информации в компьютерных сетях

1. Виды потенциально опасных воздействий
2. Защита от ошибок обслуживающего персонала
3. Защита от заражения компьютерными вирусами
4. Программно-аппаратные средства защиты информации от несанкционированного доступа

6. СТРУКТУРА УЧЕБНОЙ ДИСЦИПЛИНЫ

Название смысловых модулей и тем	Количество часов											
	очная форма						заочная форма					
	всего	в том числе					всего	в том числе				
		л	п	лаб	инд.	с.р.с.		л	п	лаб	инд.	с.р.с.
Смысловой модуль 1. Промышленный шпионаж и средства получения коммерческой информации												
Тема 1. Основные способы ведения промышленного шпионажа и каналы утечки информации	8	2	2			4	8	1	1			6
Тема 2. Анализ угроз информационной безопасности	8	2	2			4	8	1	1			6
Тема 3. Средства перехвата аудиоинформации	8	2	2			4	8	1	1			6
Тема 4. Оптические средства добычи конфиденциальной информации	8	2	2			4	8	1	1			6
Тема 5. Перехват информации в линиях связи. Информация, обрабатываемая в компьютерных сетях	8	2	2			4	8		2			6
Итого по смысловому модулю 1	40	10	10			20	40	4	6			30
Смысловой модуль 2. Защита от промышленного шпионажа												
Тема 6. Организация защиты информации	8	2	2			4	8	1	1			6
Тема 7. Методы и средства выявления закладных устройств	8	2	2			4	8	1	1			6
Тема 8. Технические средства защиты информации в помещениях и сетях связи	8	2	2			4	8	1	1			6
Тема 9. Защита информации в компьютерных сетях	8	2	2			4	8	1	1			6
Итого по смысловому модулю 2	32	8	8			16	32	4	4			24
Всего часов	72	18	18			36	72	8	10			54
ИНИР	-	-	-			-	-	-	-			-
Всего часов	72	18	18			36	72	8	10			54

7. ТЕМЫ СЕМИНАРСКИХ ЗАНЯТИЙ

Номер п/п	Название темы	Количество часов	
		очная форма	заочная форма
1	не предусмотрено		
Всего:			

8. ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Номер п/п	Название темы	Количество часов	
		очная форма	заочная форма
1	Нормативно-правовая база, регулирующая промышленный шпионаж	2	1
2	Уровни промышленного шпионажа, его объекты и субъекты, средства, формы и методы деятельности.	2	1
3	Источники получения информации в интересах деловой разведки	2	1
4	Методы работы со средствами перехвата аудио информации	2	1
5	Порядок использования оптических средств добычи конфиденциальной информации	2	2
6	Мониторинг защищенности предприятия от промышленного шпионажа	2	1
7	Применение закладных устройств для получения информации	2	1
8	Принцип работы технических средств защиты информации в помещениях и сетях связи	2	1
9	Защита от несанкционированной аудиозаписи	2	1
Всего:		18	10

9. ТЕМЫ ЛАБОРАТОРНЫХ РАБОТ

Номер п/п	Название темы	Количество часов	
		очная форма	заочная форма
1	не предусмотрено		
Всего:			

10. САМОСТОЯТЕЛЬНАЯ РАБОТА

Номер п/п	Название темы	Количество часов	
		очная форма	заочная форма
1	Понятие информационной безопасности. Генезис функции безопасности в истории общества	4	6
2	Объекты и субъекты информационной безопасности	4	6
3	Основные подходы к обеспечению безопасности личности, общества и государства	4	6
4	Основные задачи и направления разведывательной активности предприятия	4	6
5	Понятие конфиденциальной информации,	4	6
6	Информация, содержащая коммерческую тайну	4	6
7	Защита персональных данных физических лиц	4	6
8	Правила защиты информации на предприятии и кодекс поведения сотрудников, обладающих закрытой информацией	4	6
9	Пути совершенствования защиты информации на предприятии	4	6
Итого		36	54

11. ИНДИВИДУАЛЬНЫЕ ЗАДАНИЯ

Не предусмотрено

12. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1. Шульц А. С., Промышленный шпионаж: конспект лекций (эл. ресурс, рукопись). – ДонНУЭТ, 2016. – 95 с.
2. Шульц А. С., Промышленный шпионаж: Методические указания для подготовки к практическим занятиям для студентов специальности 38.05.02 «Таможенное дело» (рукопись), 2016.

13. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ ЗНАНИЙ СТУДЕНТОВ И ПРОМЕЖУТОЧНОЙ ИТОГОВОЙ АТТЕСТАЦИИ

13.1. Перечень вопросов для подготовки студентов к зачету:

1. Общие сведения о промышленном шпионаже.
2. Способы ведения промышленного шпионажа.
3. Каналы утечки информации.
4. Хозяйственный риск и его функции.
5. Классификация видов хозяйственных рисков.
6. Реальные и мнимые угрозы на предприятии, связанные с информацией.
7. Закладные устройства с передачей информации по радиоканалу.
8. Закладные устройства с передачей информации по проводным каналам.
9. Диктофоны и направленные микрофоны.
10. Устройства, реализующие методы высокочастотного навязывания.
11. Оптико-механические приборы.
12. Приборы ночного видения.
13. Средства для проведения скрытой фотосъемки.

14. Технические средства получения видеоинформации.
15. Методы и средства несанкционированного получения информации в телефонных и проводных линиях связи.
16. Методы и средства несанкционированного получения информации в каналах сотовой связи.
17. Получение информации, обрабатываемой в компьютерных сетях.
18. Основные понятия информационной безопасности.
19. Организационные мероприятия по защите информации.
20. Добровольная аттестация объектов информатизации по требованиям безопасности информации.
21. Общие принципы выявления закладных устройств.
22. Индикаторы поля и специальные радиоприемные устройства.
23. Программно-аппаратные комплексы.
24. Рекомендации по поиску устройств негласного «съема информации».
25. Общие принципы защиты.
26. Средства защиты линий связи.
27. Криптографические методы и средства защиты.
28. Защита от пиратских подключений.
29. Виды потенциально опасных воздействий.
30. Защита от ошибок обслуживающего персонала.
31. Защита от заражения компьютерными вирусами.
32. Программно-аппаратные средства защиты информации от несанкционированного доступа.
33. Нормативно-правовая база, регулирующая промышленный шпионаж.
34. Уровни промышленного шпионажа, его объекты и субъекты, средства, формы и методы деятельности.
35. Источники получения информации в интересах деловой разведки.
36. Методы работы со средствами перехвата аудио информации.
37. Порядок использования оптических средств добычи конфиденциальной информации.
38. Мониторинг защищенности предприятия от промышленного шпионажа.
39. Применение закладных устройств для получения информации.
40. Принцип работы технических средств защиты информации в помещениях и сетях связи.
41. Защита от несанкционированной аудиозаписи.
42. Основные задачи и направления разведывательной активности предприятия.
43. Защита персональных данных физических лиц.
44. Понятие конфиденциальной информации.
45. Информация, содержащая коммерческую тайну.
46. Понятие информационной безопасности.
47. Генезис функции безопасности в истории общества.
48. Объекты и субъекты информационной безопасности.
49. Основные подходы к обеспечению безопасности личности, общества и государства.
50. Правила защиты информации на предприятии.
51. Кодекс поведения сотрудников, обладающих закрытой информацией.

14. РАСПРЕДЕЛЕНИЕ БАЛЛОВ, КОТОРЫЕ ПОЛУЧАЮТ ОБУЧАЮЩИЕСЯ

Текущее тестирование и самостоятельная работа									Сумма в баллах
Смысловой модуль 1					Смысловой модуль 2				
T1	T2	T3	T4	T5	T6	T7	T8	T9	100
10	10	10	10	10	10	15	15	10	

Соответствие государственной шкалы оценивания академической успеваемости и шкалы ECTS

По шкале ECTS	Сумма баллов за все виды учебной деятельности	По государственной шкале	Определение
A	90-100	«Отлично» (5)	отличное выполнение с незначительным количеством неточностей
B	80-89	«Хорошо» (4)	в целом правильно выполненная работа с незначительным количеством ошибок (до 10 %)
C	75-79		в целом правильно выполненная работа с незначительным количеством ошибок (до 15 %)
D	70-74	«Удовлетворительно» (3)	неплохо, но со значительным количеством недостатков
E	60-69		выполнение удовлетворяет минимальные критерии
FX	35-59	«Неудовлетворительно» (2)	с возможностью повторной аттестации
F	0-34		с обязательным повторным изучением дисциплины (выставляется комиссией)

15. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

Основная:

1. Каторин Ю.Ф. Защита информации техническими средствами [Электронный ресурс]: учебное пособие / Ю.Ф. Каторин, А.В. Разумовский, А.И. Спивак. – Электрон. текстовые данные. – СПб.: Университет ИТМО, 2012. – 417 с. – Режим доступа: <http://www.iprbookshop.ru/66445.html>. – ЭБС «IPRbooks».

2. Сычев Ю.Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов [Электронный ресурс]: учебное пособие / Ю.Н. Сычев. – Электрон. текстовые данные. – Саратов: Вузовское образование, 2017. – 195 с. – Режим доступа: <http://www.iprbookshop.ru/72345.html>. – ЭБС «IPRbooks».

3. Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 702 с. – Режим доступа: <http://www.iprbookshop.ru/63594.html>. – ЭБС «IPRbooks».

Дополнительная:

1. Алексеев А.П. Многоуровневая защита информации [Электронный ресурс] / А.П. Алексеев. – Электрон. текстовые данные. – Самара: Поволжский государственный университет

телекоммуникаций и информатики, 2017. – 128 с. – Режим доступа: <http://www.iprbookshop.ru/75387.html>. – ЭБС «IPRbooks».

2. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс] / В.Ф. Шаньгин. – Электрон. текстовые данные. – Саратов: Профобразование, 2017. – 544 с. – Режим доступа: <http://www.iprbookshop.ru/63592.html>. – ЭБС «IPRbooks».

3. Беловицкий К.Б. Режим коммерческой тайны в системе обеспечения экономической безопасности хозяйствующего субъекта [Электронный ресурс]: учебное пособие / К.Б. Беловицкий. – Электрон. текстовые данные. – М.: Научный консультант, 2017. – 124 с.– Режим доступа: <http://www.iprbookshop.ru/75143.html>. – ЭБС «IPRbooks».

4. Десятов М.С. Делопроизводство и режим секретности в органах внутренних дел [Электронный ресурс]: учебное пособие / М.С. Десятов [и др.]. – Электрон. текстовые данные. – Омск: Омская академия МВД России, 2017. – 68 с. – Режим доступа: <http://www.iprbookshop.ru/72851.html>. – ЭБС «IPRbooks».

16. ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1. IPRbooks: Электронно-библиотечная система [Электронный ресурс]: [«АЙ Пи Эр Медиа»] / [ООО «АЙ Пи Эр Медиа»]. – Электрон. текстовые, табл. и граф. дан. – Саратов, [2018]. – Режим доступа: <https://http://www.iprbookshop.ru>.

2. Электронно-библиотечная система «КнигаФонд»: учебная и научная литература. Специальные условия сотрудничества для вузов и ссузов [Электронный ресурс] / ООО «Центр цифровой дистрибуции». – Электрон. текстовые, табл. и граф. дан. – [Москва], сор. 2008-2018. – Режим доступа: <http://www.knigafund.ru/>.

3. Znanium.com: электронно-библиотечная система [Электронный ресурс] / «Научно-издательский центр Инфра-М». – Электрон. текстовые, табл. и граф. дан. – [Москва], сор. 2012-2018. – Режим доступа: <http://znanium.com/>.

4. Elibrary.ru [Электронный ресурс]: науч. электрон. б-ка / ООО Науч. электрон. б-ка. – Электрон. текстовые. и табл. дан. – [Москва]: ООО Науч. электрон. б-ка., 2000.– Режим доступа: <https://elibrary.ru>.

5. Научная электронная библиотека «КиберЛенинка» [Электронный ресурс] / [ООО «Итеос»; Е. Кисляк, Д. Семячкин, М. Сергеев]. – Электрон. текстовые дан. – [Москва: ООО «Итеос», 2012-]. – Режим доступа : <http://cyberleninka.ru>.

6. Grebennikon [Электронный ресурс]: электрон. б-ка / [Издат. дом «Гребенников»]. – Электрон. текстовые дан. – [Москва: Издат. дом «Гребенников», 2005]. – Режим доступа: <https://grebennikon.ru>.

17. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Учебные занятия по дисциплине проводятся в лекционных аудиториях и специализированных компьютерных лабораториях с точками доступа в сеть Интернет, которые предназначены для проведения практических занятий, выполнения курсовых и дипломных работ, магистерских диссертаций, с возможностями доступа к современным информационным технологиям, демонстрационные программы на цифровых носителях, которые содержат аудио- и видеоинформацию, касающуюся отдельных тем учебной дисциплины «Промышленный шпионаж».

Номер п/п	Наименование лабораторий и специализированных кабинетов	Перечень оборудования, количество
1	Учебная аудитория № 4233 для проведения лекций	учебная мебель, доска, мультимедийный проектор, экран
2	Компьютерные классы №№ 4413, 4415, 4238 для проведения практических занятий	учебная мебель, доска, компьютеры с соответствующим программным обеспечением
3	Читальный зал библиотеки № 4129 для проведения самостоятельной работы	компьютеры с выходом в сеть Интернет, доступ к электронно-библиотечной системе

18. КАДРОВОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Фамилия, имя, отчество	Должность (для совместителей место основной работы, должность)	Наименование учебного заведения, которое окончил (год окончания, специальность, квалификация по диплому)	Ученая степень, шифр и наименование научной специальности, ученое звание, какой кафедрой присвоено, тема диссертации	Повышение квалификации (наименование организации, вид документа, тема, дата выдачи)
Шульц Анна Сергеевна	старший преподаватель кафедры экспертизы в таможенном деле	Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского, 2009 г., «Товароведение и экспертиза в таможенном деле», магистр.	–	Аспирантура по специальности 05.18.08 – товароведение непродовольственных товаров; ГО ВПО «Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского», сертификат о повышении педагогического мастерства № 0105 от 22.09.2016 г., «Учебная программа Школы педагогического мастерства по 4-м направлениям» (72 ч); Донецкий национальный университет экономики и торговли имени Михаила Туган-Барановского, свидетельство № 12 СПК 997476 от 02.06.2015 г., «Разработка и внедрение дистанционного курса на базе платформы Moodle по дисциплине «Инструментальные методы исследований в таможенном деле»».