МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра права та публічного адміністрування

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НДПП 1.2.8 «Нормативно-правове забезпечення інформаційної безпеки»

(шифр і назва навчальної дисципліни)

Освітньо-професійна програма _____Кібербезпека_____
(назва)

Спеціальність _____125 Кібербезпека_____
(код та найменування спеціальності)

Спеціалізація _____
(назва спеціалізації)

Факультет _____економіко-правовий_____
(назва факультету)

2020–2021 рік

Робоча програма «**Нормативно-правове забезпечення інформаційної безпеки**» для студентів ОПП Кібербезпека спеціальності 125 Кібербезпека

Розробник: старший викладач кафедри права та публічного адміністрування Темирова-Хмикіна В. І.

Робоча програма затверджена на засіданні кафедри права та публічного адміністрування

Протокол від «28» серпня 2020 року, № 1

В.о. завідувача кафедри права та публічного адміністрування

 Черних Є. М.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 5</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2" rowspan="2">Нормативна
(професійна та практична підготовка)</td></tr>
<tr><td>Напрям підготовки</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність
«Кібербезпека»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>2-й</td><td>2-й</td></tr>
<tr><td>Індивідуальне науково-дослідне завдання: реферат</td><td colspan="2">Семестр</td></tr>
<tr><td rowspan="2">Загальна кількість годин – 150</td><td>4-й</td><td>4-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="8">Тижневих годин для денної форми навчання:
аудиторних –
самостійної роботи студента –</td><td rowspan="8">Освітній ступінь:
«Бакалавр»</td><td>16 год.</td><td>10 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>10 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>98 год.</td><td>118 год.</td></tr>
<tr><td colspan="2">Індивідуальні завдання: 4 год.</td></tr>
<tr><td colspan="2" rowspan="2">Вид контролю:
екзамен</td></tr>
<tr></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної і індивідуальної роботи становить (%):
для денної Форми
здобуття вищої освіти – 40% /60%
для заочної Форми
здобуття вищої освіти – 34% / 66%

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є: є отримання студентами необхідних знань та навиків для застосування їх з питань механізму правового врегулювання відносин, пов'язаних з використанням інформації і захистом останньої від неправомірного використання. А також в подальшому використанню отриманих знань стосовно розробки методів і засобів криптографічного, технічного захисту інформації та при проектування систем захисту інформації. Особлива увага в курсі приділяється вивченню законів, Указів президента і постанов КМУ, нормативних документів, вітчизняних та міжнародних стандартів в галузі захисту та безпеки інформації. Здатність аналізувати сучасні стандарти та формувати загальні вимоги до інформаційної безпеки комп'ютерних систем і мереж.

Завдання: Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

- основні поняття у сфері інформації, захисту інформації та інформаційної безпеки;
- поняття і сутність інформаційної безпеки;
- поняття та види сучасних загроз інформаційній безпеці;
- нормативно-правові джерела регулювання у сфері інформації та інформаційної безпеки;
- поняття інформації та її види;
- підстави обмеження доступу до інформації;
- державна таємниця та її захист;
- нормативне регулювання сфери захисту державної таємниці;
- нормативне регулювання сфери обробки персональних даних;
- нормативне регулювання доступу до публічної інформації;

вміти:

- оперувати поняттями у сфері інформаційній безпеці;
- визначати загрози інформаційній безпеці;
- застосовувати норми, які регулюють відносини у сфері інформаційної безпеки, з метою забезпечення прав і обов'язків у сфері інформації.

Місце навчальної дисципліни в освітній програмі: навчальна дисципліна «**Нормативно-правове забезпечення інформаційної безпеки**» належить до навчальних дисциплін професійної підготовки освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека освітнього рівня «Бакалавр».

Передумови для вивчення дисципліни: вивчення дисципліни базується на знаннях одержаних у результаті вивчення таких навчальних дисциплін, як «Інформаційне право» та «Основи правознавства».

Результати навчання: Знання теоретичних основ та вміння свідомого поводження з інформацією в умовах використання сучасних інформаційно-комунікаційних засобів та враховування отриманих знань у практичної діяльності за обраної спеціальності. Уміння застосувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації. Уміння усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод і громадянина в Україні.

Програма побудована за вимогами кредитно-трансферної системи організації навчального процесу у вищих навчальних закладах та узгоджена з примірною структурою змісту навчального курсу, рекомендованою Європейською Кредитно-Трансферною Системою (ECTS).

Програма складається з двох змістовних модулів.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВНИЙ МОДУЛЬ 1

ТЕМА 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері

Вивчається правова основа забезпечення технічного захисту інформації в Україні. Види правових актів, їх визначення. Статті кодексів України відповідно яких наступає відповідальність за правопорушення в інформаційній сфері.

ТЕМА 2. Системи захисту інформації в банківських установах

Розглядаються шляхи забезпечення збереження банківської таємниці. Вимоги щодо захисту інформації у платіжних системах та складові частини системи захисту інформації.

ЗМІСТОВНИЙ МОДУЛЬ 2

ТЕМА 3. Порядок створення, впровадження та супроводження засобів ТЗІ

Вивчається порядок створення, впровадження та супроводження засобів ТЗІ, нормативні документи які регламентують цю діяльність.

ТЕМА 4. Стандарти в сфері криптографічного захисту інформації

Проводиться ознайомлення з міжнародними стандартами в сфері криптографічного захисту інформації та порівняння їх з стандартами України.

ТЕМА 5. Державні стандарти та будівельні норми України. Захист інформації

Ознайомлення та вивчання Державних стандартів та будівельних норми України, які використовуються при розробці комплексів та систем засобів захисту інформаційної структури.

ТЕМА 6. Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами

Ознайомлення та вивчання нормативних документів ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами.

ТЕМА 7. Нормативні документи ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах

Ознайомлення та вивчання нормативних документів ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах.

ТЕМА 8. Нормативні документи ТЗІ щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу

Ознайомлення та вивчання нормативних документів ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступ.

4. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
МОДУЛЬ 1						
Змістовий модуль 1						
Тема 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері	23	2	2	-	-	19
Тема 2. Системи захисту інформації в банківських установах	26	4	2	-	1	19
Разом годин за змістовий модуль 1	**49**	**6**	**4**	**-**	**1**	**38**
Змістовий модуль 2						
Тема 3. Порядок створення, впровадження та супроводження засобів ТЗІ	26	4	2	-	-	20
Тема 4. Стандарти в сфері криптографічного захисту інформації	27	4	2	-	1	20
Тема 5. Державні стандарти та будівельні норми України. Захист інформації	24	2	2	-	-	20
Разом годин за змістовий модуль 2	**77**	**10**	**6**	**-**	**1**	**60**
Загальна кількість годин	**126**	**16**	**10**	**-**	**2**	**98**

Назви змістових модулів і тем	Кількість годин					
	заочна форма					
	усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
МОДУЛЬ 1						
Змістовий модуль 1						
Тема 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері	44	2	2	-	-	40
Тема 2. Системи захисту інформації в банківських установах	47	4	2	-	1	40
Разом годин за змістовий модуль 1	**91**	**6**	**4**	**-**	**1**	**80**
Змістовий модуль 2						
Тема 3. Порядок створення, впровадження та супроводження засобів ТЗІ	45	4	2	-	1	38

Разом годин за змістовий модуль 2	**45**	**4**	**2**	**-**	**1**	**38**
Загальна кількість годин	**136**	**10**	**6**	**-**	**2**	**118**

5. Теми семінарських занять

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1.	Тема 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері	2	1
2.	Тема 2. Системи захисту інформації в банківських установах	2	1
3.	Тема 3. Порядок створення, впровадження та супроводження засобів ТЗІ	2	1
4.	Тема 4. Стандарти в сфері криптографічного захисту інформації	2	2
5.	Тема 5. Державні стандарти та будівельні норми України. Захист інформації	2	1
Разом:		**10**	**6**

6.Теми практичних занять

Практичні заняття не передбачено

7. Теми лабораторних занять

Лабораторні заняття не передбачено

8. Самостійна робота

Самостійна робота передбачає необхідність самостійного опанування студентами основними теоретичними положеннями, категоріями, термінами, що використовуються даною навчальною дисципліною, а також самостійне оволодіння основними методами наукового дослідження та розвиток самостійного теоретичного правового мислення.

Опрацьовуючи самостійно матеріал, студенти зобов’язані використовувати джерела, що запропоновані в загальному списку рекомендованих джерел.

Формами контролю виконання студентами самостійної роботи є усне опитування та перевірка правильності виконання письмових навчальних завдань під час індивідуально-консультативної роботи викладача.

№ з/п	Назва теми	Кількість годин	
		денна / заочна форма	
1	Тема 1. Правове забезпечення та відповідальність за правопорушення в інформаційній сфері	12	14

2	Тема 2. Системи захисту інформації в банківських установах	12	14
3	Тема 3. Порядок створення, впровадження та супроводження засобів ТЗІ	12	14
4	Тема 4. Стандарти в сфері криптографічного захисту інформації	12	14
5	Тема 5. Державні стандарти та будівельні норми України. Захист інформації	12	14
6	Тема 6. Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами	12	14
7	Тема 7. Нормативні документи ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах	12	14
8	Тема 8. Нормативні документи ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу	14	20
Разом:		**98**	**118**

9. Індивідуальні завдання

Індивідуальна робота передбачає:

- написання самостійної (індивідуальної) наукової роботи з аналітичним оглядом наукових публікацій за визначеною тематикою,
- вивчення та захист глосарію,
- участь у науковому студентському гуртку, конференціях, круглих столах, тощо.

Мета наукової роботи з аналітичним оглядом наукових публікацій: напрацювання самостійних творчих навичок з підготовки письмової роботи, яка представляє собою загальний огляд (аналіз) наукових публікацій та розгорнуте і аргументоване викладення власного погляду студента, з можливістю критичного підходу до деяких наукових теоретичних підходів за визначеною темою наукового дослідження.

Вимоги до змісту самостійної (індивідуальної) наукової роботи:

- структура роботи складається з титульного аркушу (Додаток 1), плану, вступу, основної частини, загальних висновків, списку використаних наукових та нормативних джерел. Посилання на використані джерела є обов'язковими;
- вступ має містити: аналіз актуальності проблематики дослідження (висвітлення актуальності не повинно бути багатослівним, досить кількома реченнями висловити сутність проблеми наукового завдання), мету і завдання, об'єкт дослідження (це процес або явище, що породжує проблемну ситуацію й обране для вивчення), предмет дослідження (міститься в межах об'єкта);

- основний зміст роботи повинен містити детальний аналіз проблематики визначеної теми наукової роботи з оглядом наукових підходів та власних аргументованих ідей до вирішення проблеми, можливий аналіз нормативного матеріалу та матеріалів юридичної практики;
- загальні висновки по роботі – коротке викладення чітко сформульованих ідей і належно обґрунтованих пропозицій основної частини, які мають науково-практичне значення і є самостійним здобутком студента;
- список використаних джерел (не менш ніж 5 найменувань).

Оформлення роботи:

- загальний об'єм всієї роботи не має перевищувати 10–15 сторінок;
- поля: верхнє, нижнє – 2 см, зліва – 2,5 см, справа – 1,5 см;
- шрифт – 14 Times New Roman, інтервал – 1,5;
- нумерація сторінок.

Першою сторінкою є титульний аркуш, який включають до загальної нумерації сторінок, але на ньому номер сторінки не ставлять. На наступних сторінках номер проставляють у правому верхньому куті сторінки без крапки в кінці. Не припустимою є підготовка проекту в зошитах, або на листах формату А-4, що заповнені з обох сторінок.

Оцінювання: рівень аналізу наукових (нормативних) джерел, повнота розкриття теми, послідовність і правильність аргументації власних думок, якість оформлення та презентації, тощо.

Тематика самостійної (індивідуальної) наукової роботи затверджується викладачем.

Теми:

1. Міжнародні стандарти криптографічних методів захисту інформації.
2. Забезпечення захисту інформації в АС.
3. Захист інформації в банківських установах.
4. Захист інформації WEB-сторінки від несанкціонованого доступу.
5. Захист конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах.
6. Правова основа забезпечення технічного захисту інформації в Україні.
7. Комплекси засобів захисту комп'ютерної системи від несанкціонованого доступу.

Додаток 1
Зразок оформлення титульного аркушу індивідуальної роботи

Міністерство освіти і науки України
Маріупольський державний університет
Кафедра права та публічного адміністрування

ІНДИВІДУАЛЬНЕ НАУКОВО-ДОСЛІДНЕ ЗАВДАННЯ
з навчальної дисципліни «**Нормативно-правове забезпечення інформаційної безпеки**»
на тему: «**_____**»

Виконав:
студент (ка) ІІ курсу
ОС «Бакалавр»
спеціальності «Кібербезпека»,

_____
(П.І.Б.)

Науковий керівник:

_____
(посада, П.І.Б. викладача)

Маріуполь – 2021

10. Методи навчання

Проведення аудиторних лекцій, практичних занять, консультацій, а також самостійна робота студентів за відповідними матеріалами.

11. Критерії оцінювання

Систему контролю складають: усне опитування (співбесіда), реферати, електронні презентації, семінари та екзамен.

12. Засоби оцінювання

КОНТРОЛЬНІ ПИТАННЯ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Трансформаційні процеси в системах забезпечення національної та міжнародної безпеки.
2. Інформація як джерело небезпеки.
3. Інформаційна та кібернетична безпека.
4. Об’єкти та суб’єкти інформаційної небезпеки.
5. Інформаційна безпека як об’єкт правовідносин.
6. Національна та міжнародна безпека.
7. Правове забезпечення захисту інформації.
8. Правова відповідальність за правопорушення в інформаційній сфері.
9. Правові проблеми забезпечення інформаційної безпеки.
10. Поняття інформаційної безпеки держави та складових національних інтересів України в інформаційній сфері.
11. Основні положення інформаційної безпеки держави.
12. Загрози безпеці інформації.
13. Основи інформаційного протиборства.
14. Психологічна війна та інформаційно-психологічна безпека держави.
15. Основи державної інформаційної політики.
16. Види персональних даних у державі.
17. Принципи захисту персональних даних у державі.
18. Основи безпеки інформаційних ресурсів держави.
19. Основи управління інформаційною безпекою держави

13. Розподіл балів, які отримують студенти

Максимальна кількість балів за вивчення дисципліни складає 100 балів.

Рейтинг успішності студента за вивчення – це сума балів за змістовий практичний модуль (семінарські заняття), модуль самостійної роботи, тестовий модульний контроль.

Модуль 1 Поточне тестування та самостійна робота																		Модуль 2 ІНДЗ	Модуль 3 Підсумкова атестація	Сума
ЗМ 1		ЗМ 2																25	Екзамен – 50	100
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8													
3	3	3	3	3	3	3	4													

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсової роботи, практики	для заліку
90–100	**A**	відмінно	зараховано
82–89	**B**	добре	
74–81	**C**		
64–73	**D**	задовільно	
60–63	**E**		
35–59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0–34	**F**	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

14. Інструменти, обладнання та програмне забезпечення

1. Конспект лекцій, методичні рекомендації семінарських робіт;
2. Презентації лекцій з курсу – ел.вигляд;
3. Нормативні документи, навчальна та довідкова література.

15. Рекомендовані джерела інформації

Базові нормативно-правові акти

1. Конституція України.
2. Кримінальний кодекс України.
3. Цивільний кодекс України .
4. Кодекс України про адміністративні порушення.

1) Закон України

1. Закон України «Про державну таємницю».
2. Закон України « Про інформацію».
3. Закон України «Про захист інформації в автоматизованих системах».
4. Закон України «Про Державну службу спеціального зв’язку та захисту інформації України».

5. Закон України «Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання» .

6. Закон України «Про ліцензування певних видів господарської діяльності» .

7. Закон України «Про телекомунікації».

8. Закон України «Про електронні документи та електронний документообіг».

9. Закон України «Про електронний цифровий підпис».

10. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

11. Закон України «Про основи національної безпеки України».

12. Закон України «Про Національну систему конфіденційного зв'язку».

13. Закон України «Про наукову і науково-технічну експертизу».

14. Закон України «Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Республіки Білорусь про співробітництво в галузі технічного захисту інформації».

15. Закон України «Про електронні довірчі послуги».

2) Нормативні документи.

1. НД ТЗІ 2.7-008-08 «Вимоги та рекомендації із забезпечення захисту мовної інформації від витоку акустичним та вібро-акустичним каналами. Методичні вказівки».

2. НД ТЗІ 2.3-017-08 «Методика контролю захищеності мовної інформації від витоку акустичним та вібро-акустичним каналами».

3. НД ТЗІ 2.2-006-08 «Захист інформації на об'єкти інформаційної діяльності. Норми протидії технічній розвідці в акустичному і вібро-акустичному каналах витоку мовної інформації».

4. НД ТЗІ 2.2-003-06 «Протидія технічним розвідкам. Норми з протидії засобам радіолокаційної розвідки».

5. НД ТЗІ 2.3-010-06 «Протидія технічним розвідкам. Методика контролю ефективності протидії засобам радіолокаційної розвідки».

6. НД ТЗІ 2.4-003-06 «Протидія технічним розвідкам. Рекомендації щодо протидії засобам радіолокаційної розвідки».

7. НД ТЗІ 2.3-011-06 «Протидія технічним розвідкам. Методики контролю виконання норм з протидії засобам фотографічної та оптико-електронної розвідок».

8. НД ТЗІ 2.4-004-06 «Протидія технічним розвідкам. Рекомендації з протидії засобам фотографічної та оптико-електронної розвідок».

9. НД ТЗІ 1.6-002-03 «Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації».

10. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

11. НД ТЗІ 2.5-008-2002 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2».

12. НД ТЗІ 4.7-002-01 «Визначення захищеності мовної інформації від витоку акустичним і вібро-акустичним каналами. Методичні вказівки».

13. НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів тех.-нічного захисту інформації від несанкціонованого доступу».

14. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі».

15. НД ТЗІ Р-001-2000 «Засоби активного захисту мовної інформації з акустичними та вібро-акустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації».

16. НД ТЗІ 1.5-001-2000 «Радіовиявлювачі. Класифікація. Загальні технічні вимоги».

17. НД ТЗІ 2.5-006-99 «Класифікатор засобів копіювально-розмножувальної техніки».

18. НД ТЗІ 2.7-002-99 «Методичні вказівки з використання засобів копіювально-розмножувальної техніки».

19. НД ТЗІ 1.1-001–99 «Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення».

20. НД ТЗІ 2.5-001–99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту».

21. НД ТЗІ 2.5-002-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту».

22. НД ТЗІ 2.5-003-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту».

23. НД ТЗІ 2.7-001-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт».

24. НД ТЗІ 3.7-002-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)».

25. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

26. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ю-терних системах від несанкціонованого доступу».

27. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

28. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».

Інформаційні ресурси

1. Офіційний портал Верховної Ради України [Электрон. ресурс]. Режим доступа: http://www.rada.gov.ua

2. Вікіпедія — вільна енциклопедія [Электрон. ресурс]. Режим доступа: http://www. ru.wikipedia.org/

3. Википедия — свободная энциклопедия [Электрон. ресурс]. Режим доступа: http://www. ru.wikipedia.org/

4. Wikipedia [Электрон. ресурс]. Режим доступа: http://www. wikipedia.org/

5. Законодавство України [Электрон. ресурс]. Режим доступа: http://zakon3.rada.gov.ua/laws

6. Державна служба спеціального зв'язку та захисту інформації України [Электрон. ресурс]. Режим доступа: http://dstszi.kmu.gov.ua/dstszi/control/uk/index