Міністерство освіти і науки України

Львівський національний університет імені Івана Франка

Кафедра міжнародного права

*Серія міжнародне право*

**ІНФОРМАЦІЙНА БЕЗПЕКА**

Програма навчальної дисципліни та плани семінарських занять для студентів факультету міжнародних відносин

**Львів 2017**

Грабинський М.І. Інформаційна безпека. Програма навчальної дисципліни та плани семінарських занять для студентів факультету міжнародних відносин. – Львів.: факультет міжнародних відносин Львівського національного університету імені Івана Франка. – 2017. – \_\_ с.

Вивчення інформаційної безпеки дозволить студентам ознайомитися з основами захисту інформації: визначити зміст інформації, встановити суть та першоджерела інформації, опанувати навики літературного та правового аналізу, визначити джерела та способи загроз, що заподіюються інформації, виявити особливості застосування законодавства про захист персональних даних, з’ясувати правовий аспект здійснення документообігу підприємства, основні положення інформаційної безпеки людини, громади, компаній, держави та суб’єктів міжнародних відносин.

**І. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Тема 1.**

**Загальні положення про інформаційну безпеку (ІБ)**

Інформація як об’єкт ІБ: поняття, ознаки та види. Поняття та критерії оцінки ІБ. Сфери впливу на ІБ. ІБ як навчальна дисципліна.

**Тема 2.**

**ІБ у сучасному науковому просторі**

Доктрина інформаційної безпеки України. Поняття «Безпека інформації» та «Інформаційна безпека» в сучасному науковому просторі (за Волошиною Н.М.). Інформаційна безпека (за Кісілевич-Чорнойван О.М.). Міжнародна інформаційна безпека (за Кісілевич-Чорнойван О.М.). .

**Тема 3.**

**Зовнішні форми впливу на ІБ. Частина 1**

Технологічно-математична ІБ.. Міжнародна ІБ.. Загрози інформаційній безпеці. .

**Тема 4.**

**Внутрішні форми впливу на ІБ. Частина 2**

Юридична ІБ. . Внутрішньо-державна ІБ..

**Тема 5.**

**Забезпечення ІБ**

Аналіз інформації у ЗМІ. Правила цитування та перекладу. Достовірність, правдивість, правильність. Притча про Сократа і три сита . Інформація, що міститься в установчих документах суб’єктів господарювання та режим їх використання . Правове забезпечення захисту інсайдерської інформації суб’єктів господарювання. Зміст адміністративно-правового захисту інформації у суб’єктах господарювання

**Тема 6.**

**Правове забезпечення ІБ**

6. Закон України «Про інформацію». . Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» . Закон України «Про державну таємницю» . Закон України «Про захист персональних даних» . Основні положення постанов КМУ, що стосуються ІБ. Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) щодо ІБ. Галузеві стандарти ІБ

**Тема 7.**

**Аналіз інформаційних систем на предмет ІБ**

Аналіз сайтів. Види атак на сайти.. Кіберпростір, кібербезпека та кібертероризм . Захищеність офісних комп’ютерів. Захищеність електронних та фізичних документів. Канали витоку інформації . Методика розробки ІБ . Методи оцінки втрат . Методи оцінки ризиків . Захищеність криптовалют та систем блокчейн

**Тема 8.**

**ІБ людини**

Відбитки пальців рук. Інші біометричні дані людини. Рівні персональних даних. Методи та засоби соціального інжинирінгу . Захист інформації від соціотехнічних атак . Омбудсмен України про «Трискладовий тест»

**Тема 9.**

**ІБ підприємств, установ, організацій**

Теоретичні аспекти функціонування ІБ корпорацій . Особливості реалізації адміністративно-правових форм та методів у сфері забезпечення інформаційної безпеки корпорацій . Організації ІБ на підприємстві . Економічна безпека підприємства в умовах сучасного ринку . Служба інформаційної та економічної безпеки (СІЕБ) . Кадровий аспект СІЕБ. Підпис: захист та підробка. Печатка: захист та підробка. Види підробки документів

**Тема 10.**

**ІБ держави**

Основи національної безпеки держави – організаційно-правові аспекти . Інформаційні війни як джерело загроз національній безпеці держави . Інформаційна безпека України в сучасних умовах. ІБ у випадку надзвичайних ситуацій. Dark Net. Deep Web.

**Тема 11.**

**ІБ суб’єктів міжнародних відносин**

Екологічна ІБ у міжнародних відносинах. Економічна ІБ у міжнародних відносинах. Гуманітарна ІБ у міжнародних відносинах. Правова ІБ у міжнародних відносинах. Соціотехнічний аспект ІБ.

**Тема 12.**

**ІБ як мультидисципліна**

ІБ як правова дисципліна. ІБ як технічна дисципліна. ІБ як політична дисципліна. **ІІ. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

|  |  |  |
| --- | --- | --- |
| №п/п | ТЕМА | Кількість годин |
| Лекції | Семінарські заняття | Самостійна робота | Індивідуальна робота |
| **Змістовий модуль 1** |
| 1 | Загальні положення про інформаційну безпеку | 2 | 2 |  |  |
| 2 | Інформаційна безпека у сучасному науковому просторі | 2 | 2 | \* |
| 3 | Зовнішні форми впливу на інформаційну безпеку | 2 | 2 |  |
| 4 | Внутрішні форми впливу на інформаційну безпеку | 2 |  |
| 5 | Забезпечення інформаційної безпеки | 2 | 2 |  |
| 6 | Правове забезпечення інформаційної безпеки | 2 |  |
| 7 | Аналіз інформаційних систем на предмет інформаційної безпеки | 2 |  |
| 8 | Аналіз публікацій ЗМІ на предмет інформаційної безпеки | 2 | \* |
| 9 | Аналіз нормативно-правових актів на предмет інформаційної безпеки | 2 | \* |
| **Змістовий модуль 2** |
| 10 | Інформаційна безпека людини | 2 | 2 |  |  |
| 11 | Інформаційна безпека підприємств, установ, організацій | 2 | 2 |  |  |
| 12 | Інформаційна безпека транснаціональних компаній |  | \* |
| 13 | Інформаційна безпека громадянського суспільства | 2 | 2 |  |
| 14 | Інформаційна безпека держави | 2 |  |
| 15 | Екологічна інформаційна безпека |  | \* |
| 16 | Інформаційна безпека суб’єктів міжнародних відносин | 2 | 2 |  |
| 17 | Інформаційна безпека як мультидисципліна | 4 |  |  |  |
|  | **Всього:** | **32** | 16 |  |  |

**ІІІ. ПЛАНИ СЕМІНАРСЬКИХ ЗАНЯТЬ**

**Практичне 1:**

**Загальні положення про інформаційну безпеку (ІБ)**

1. Інформація як об’єкт ІБ: поняття, ознаки та види

2. Поняття та критерії оцінки ІБ

3. Сфери впливу на ІБ

4. ІБ як навчальна дисципліна

**Семінар 2:**

**ІБ у сучасному науковому просторі**

1. Доктрина інформаційної безпеки України

2. Інформаційна безпека та Міжнародна інформаційна безпека (за Кісілевич-Чорнойван О. М.)

3. Інші наукові положення про Інформаційну безпеку

- підручники та навчальні посібники;

- монографії;

- наукові статті.

*У межах* ***третього*** *питання слід підготувати рецензію на джерело, яке Ви знайдете:*

* бібліографічне посилання
* коротка довідка про автора (за можливістю: вчене звання, науковий ступінь, місце праці)
* авторське визначення поняття «Інформаційна безпека» (якщо у джерелі таке міститься)
* основні положення:
	+ *щодо статей*: основні положення, які висвітлені автором
	+ *щодо монографій*: основні положення висновків, висвітлених автором
	+ *щодо підручників та посібників*: короткий аналіз структури (розділи і підрозділи), а також основні положення загальнотеоретичного розділу (зазвичай першого, де висвітлюється визначення ІБ)
* Ваш висновок

Рецензія має бути виконана на аркушах А4, шрифт Times New Roman, 14, одинарний міжрядковий інтервал, обсяг 2-3 сторінки.

Кожен студент – унікальне джерело.

**Практичне 3:**

**Форми впливу на ІБ**

1. Технологічно-математична ІБ

2. Юридична ІБ.

3. Внутрішньо-державна ІБ.

4. Міжнародна ІБ.

5. Загрози інформаційній безпеці

**Практичне 4:**

**Забезпечення ІБ. Правове забезпечення ІБ.**

**Аналіз інформаційних систем на предмет ІБ**

Аналіз інформації у ЗМІ. Правила цитування та перекладу

Достовірність, правдивість, правильність. Притча про Сократа і три сита

Інформація, що міститься в установчих документах суб’єктів господарювання та режим їх використання

Правове забезпечення захисту інсайдерської інформації суб’єктів господарювання

Зміст адміністративно-правового захисту інформації у суб’єктах господарювання

Закон України «Про інформацію».

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

Закон України «Про державну таємницю»

Закон України «Про захист персональних даних»

Основні положення постанов КМУ, що стосуються ІБ

Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) щодо ІБ

Галузеві стандарти ІБ

Аналіз сайтів. Види атак на сайти.

Кіберпростір, кібербезпека та кібертероризм

Захищеність офісних комп’ютерів

Захищеність електронних та фізичних документів

Канали витоку інформації

Методика розробки ІБ

Методи оцінки втрат

Методи оцінки ризиків

Захищеність криптовалют та систем блокчейн

**Притча про Сократа і три сита**

*Один чоловік запитав у Сократа:
– Знаєш, що мені сказав про тебе твій друг?
– Зачекай, – зупинив його Сократ, – просій спочатку те, що збираєшся сказати, через три сита.
– Три сита?
– Перш, аніж що-небудь говорити, потрібно це тричі просіяти. Спочатку через сито правди. Ти впевнений, що це правда?
– Ні, я просто чув це.
– Значить, ти не знаєш, це правда чи ні. Тоді просій через друге сито – сито доброти. Ти хочеш сказати про мого друга щось хороше?
– Ні, навпаки.
– Виходить, – продовжував Сократ, – ти збираєшся сказати про нього щось погане, але навіть не впевнений в тому, що це правда. Спробуємо третє сито – сито користі. Чи так вже необхідно мені почути те, що ти хочеш розповісти?
– Ні, в цьому немає необхідності.
– Отже, – підсумував Сократ, – в тому, що ти хочеш сказати, немає ні правди, ні доброти, ані користі. Навіщо тоді говорити?*

**Тема 7. ІБ людини**

1. Відбитки пальців рук

2. Інші біометричні дані людини

3. Рівні персональних даних

4. Методи та засоби соціального інжинирінгу (Бурячок-3)

5. Захист інформації від соціотехнічних атак (Бурячок-4)

6. Омбудсмен України про «Трискладовий тест»

**Тема 8. ІБ підприємств, установ, організацій**

1. Теоретичні аспекти функціонування ІБ корпорацій (Нашинець 2.1)

2. Особливості реалізації адміністративно-правових форм та методів у сфері забезпечення інформаційної безпеки корпорацій (Нашинець 2.2)

3. Організації ІБ на підприємстві (Кавун 3.1, 3.2)

4. Економічна безпека підприємства в умовах сучасного ринку (Кавун 3.8)

5. Служба інформаційної та економічної безпеки (СІЕБ) (Кавун 3.6)

6. Кадровий аспект СІЕБ (Кавун 3.7)

7. Підпис: захист та підробка

8. Печатка: захист та підробка

9. Види підробки документів

**Тема 9. ІБ держави**

1. Основи національної безпеки держави – організаційно-правові аспекти (Жарков 1)

2. Інформаційні війни як джерело загроз національній безпеці держави (Жарков 2)

3. Інформаційна безпека України в сучасних умовах (М.М.Присяжнюк)

4. ІБ у випадку надзвичайних ситуацій

5. Dark Net

6. Deep Web

**Тема 10. ІБ суб’єктів міжнародних відносин**

1. Екологічна ІБ у міжнародних відносинах

2. Економічна ІБ у міжнародних відносинах

3. Гуманітарна ІБ у міжнародних відносинах

4. Правова ІБ у міжнародних відносинах

5. Соціотехнічний аспект ІБ

**IV. ТЕМАТИКА ДЛЯ ІНДИВІДУАЛЬНОГО НАУКОВО-ДОСЛІДНОГО ЗАВДАННЯ**

1. Аналіз на предмет інформаційної безпеки інформації про екологічний стан Львівської області після «Ожидівської аварії»
2. Аналіз на предмет інформаційної безпеки інформації про екологічний стан Львівської області після «Сміттєвої кризи»
3. Аналіз на предмет інформаційної безпеки інформації про стан співпраці та характер наявних домовленостей між Україною та МВФ
4. Аналіз на предмет інформаційної безпеки інформації про стан співпраці та характер наявних домовленостей між Україною та групою Світового банку
5. Аналіз на предмет інформаційної безпеки інформації про стан співпраці та характер наявних домовленостей між Україною та ЄБРР
6. Аналіз на предмет інформаційної безпеки інформації про стан співпраці та характер наявних домовленостей між США та РФ
7. Аналіз на предмет інформаційної безпеки інформації про стан співпраці та характер наявних домовленостей між США та Північною Кореєю
8. Аналіз на предмет інформаційної безпеки інформації про глобальні економічні загрози
9. Аналіз на предмет інформаційної безпеки інформації про глобальні екологічні загрози
10. Аналіз на предмет інформаційної безпеки інформації про глобальні політичні загрози
11. Аналіз на предмет інформаційної безпеки інформації про загрози виникнення локальних конфліктів та сутичок у Європі
12. Аналіз на предмет інформаційної безпеки інформації про забезпечення прав та свобод корінного населення США
13. Аналіз на предмет інформаційної безпеки інформації про забезпечення прав та свобод кримських татар в окупованій Автономній Республіці Крим
14. Аналіз на предмет інформаційної безпеки інформації про забезпечення прав та свобод українців на території РФ
15. Аналіз на предмет інформаційної безпеки інформації про забезпечення прав та свобод росіян на території України
16. Аналіз на предмет інформаційної безпеки інформації про забезпечення прав та свобод угорців, молдаванів та румунів на території України
17. Аналіз на предмет інформаційної безпеки інформації про забезпечення прав та свобод євреїв, поляків та німців на території України
18. Аналіз на предмет інформаційної безпеки веб-сайтів органів державної влади України

**V. КОНТРОЛЬНІ ЗАПИТАННЯ З ДИСЦИПЛІНИ**

***Перший змістовий модуль***

1. Інформація як об’єкт інформаційної безпеки: поняття, ознаки та види.
2. Поняття та критерії інформаційної безпеки.
3. Надайте визначення наступним термінам:
	* Інформаційна безпека
	* Безпека інформації
	* Захищеність інформації

***Другий змістовий модуль***

1. Інформація як об’єкт інформаційної безпеки: поняття, ознаки та види.
2. Поняття та критерії інформаційної безпеки.
3. Надайте визначення наступним термінам:
	* Інформаційна безпека
	* Безпека інформації
	* Захищеність інформації

**VI. РЕКОМЕНДОВАНІ ДЖЕРЕЛА**

**НОРМАТИВНО-ПРАВОВІ АКТИ:**

Конституція України (статті 32, 34, 40 та 50)

Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», введено в дію Указом Президента України від 25 лютого 2017 року № 47/2017

1. Закон про основні засади забезпечення кібербезпеки України від 06.10.2017
2. Проект Закону про обіг криптовалюти в Україні - http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\_1?pf3511=62684
3. Проект - СТРАТЕГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ - http://www.niss.gov.ua/public/File/2013\_nauk\_an\_rozrobku/kiberstrateg.pdf

**ЛІТЕРАТУРА:**

1. Competitive intelligence. [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Competitive\_intelligence.
2. GAO-10-606. CYBERSPASE United States Faces Challenges in Addressing Global Cybersecurity and Governance, Washington, July 2010. [Електронний ресурс]. – Режим доступу: http://web.ebscohost.com.
3. GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently Addressed United States Government Accountability Office, Washington, July 2010. [Електронний ресурс]. – Режим доступу: http://web.ebscohost.com.
4. Peter Neumann, Donald Parker. A summary of computer misuse techniques. In 12th National Computer Security Conference, 1989.
5. Peter Neumann. Computer-Related Risk. ACM Press/Addison Wesley, 1995.
6. Аносов А.О. Моделювання DDos атак на комп’ютерні мережі для визначення ознак їх проведення / А.О. Аносов // Науково-технічний журнал «Сучасний захист інформації» – 2015. – № 3. –С. 13 – 17.
7. Богуш В.М. Основи інформаційної культури (електронний варіант). - К.: ДУІКТ, 2002. – 244 стор.
8. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.
9. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В. Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний Н.В. Лукова-Чуйко – К. : ДУТ - КНУ, 2016. – 178 с.
10. Бурячок В.Л. Варіант механізму злому інформаційно-телекомунікаційних систем та їх захисту від стороннього кібернетичного впливу. // Науково-технічний журнал «Сучасний захист інформації» ДУІКТ України, № 4, 2011, с. 76 – 84
11. Бурячок В.Л. Застосування бездротових мереж в ході організації та проведення розвідки систем телекомунікацій // Науково-технічний журнал «Сучасний захист інформації» Державного університету телекомунікацій. № 4, 2013, с. 57 – 67
12. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник] / В.Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. –К. : ПВП «Задруга», 2014. – 320 с.
13. Бурячок В.Л. Модель формування дерева атак для одержання інформації в інформаційно-телекомунікаційних системах і мережах при вилученому доступі. // Науковий журнал «Інформатика та математичні методи в моделюванні» Одеського національного політехнічного університету, № 2, 2013, с. 123 – 131
14. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К. : НАУ. – 2013. – 432 с.
15. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.
16. Бурячок В.Л. Оценка живучести систем защиты информационного пространства систем управления воздушным движением // В.Л. Бурячок, С.О. Гнатюк / Безпека інформації. – Том 19, №1. – 2013. –С. 40-45.
17. Бурячок В.Л. Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу / В.Л. Бурячок, О.А.Ільяшов, Г.М. Гулак // Актуальні питання підготовки фахівців із розслідування кіберзлочинів: круглий стіл НА СБ України, 25.11.2011 р.: доповіді та тези доповідей. –К.:, 2012. –С. 27–32.
18. Бурячок В.Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу. // В.Л.Бурячок, О.Г. Корченко, В.О., Хорошко, В.А. Кудінов / Науково-технічний журнал «Захист інформації» Національного авіаційного університету. Том 15, № 1, 2013, с. 5 – 14
19. Бурячок В.Л. Сучасні системи виявлення атак в інформаційно-телекомунікаційних системах і мережах. Модель вибору раціонального варіанта реагування на прояви стороннього кібернетичного впливу. // Науковий журнал «Інформаційна безпека»
20. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
21. БурячокВ.Л. Практичні аспекти методології сучасного інформаційного пошуку //Інформаційна безпека. – 2011. – №2(6). –С. 149–154.
22. БурячокВ.Л. Технологія використання уразливостей Web ресурсів у процесі організації та проведення мережевої розвідки інформаційно-телекомунікаційних систем // Науковий журнал "Безпека інформації" Національного авіаційного університету. Том 19#2, 2013. с. 83 – 87
23. БурячокВ.Л., Гулак Г.М., ХорошкоВ.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // Наука і оборона. – 2011. –№ 3. –С. 35–42.
24. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк // Безпека інформації. - 2013. - Т. 19, № 2. - С. 118-129. - Режим доступу: http://nbuv.gov.ua/UJRN/bezin\_2013\_19\_2\_8.
25. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. // Безпека інформації. – 2013. – Том19, № 2 (2013) –С. 118-129.
26. Гриняев С. Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. – Мн.: Харвест, 2004. – 448 с.
27. Гриняев С.Н. Интеллектуальнoe противодействие информационному оружию. – M.: СИНТЕГ, 1999. – 232 с.
28. Грязнов Е.С., Панасенко С.А. Безопасность локальных сетей. – М.: Вузовский учебник, 2006.- 525 с.
29. Економічна енциклопедія: У трьох томах. Т. 2. / Редкол.: …С. В. Мочерний (відп. ред.) та ін. – К.: Видавничий центр “Академія”, 2000. – 864 с.
30. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2008. — 352 с.
31. Карпов Г. Атака на DNS или ночной кошмар сетевого администратора [Електронний ресурс] / Геннадий Карпов. – Режим доступу: http://www.hackzone.ru/articles/dns-poison.html, 02.06.2007.

Кісілевич-Чорнойван О. М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять / О. М. Кісілевич-Чорнойван // Юриспруденція: теорія і практика. - 2009. - № 8. - С. 11-18. - Режим доступу: http://nbuv.gov.ua/UJRN/utp\_2009\_8\_2

Кісілевич-Чорнойван О. М. Міжнародне інформаційне право: навч. посіб. / О. М. Кісілевич-Чорнойван. — К. : ДП «Вид. дім «Персонал», 2011. – 160 с.

1. Козлачков П.С. Основные направления развития систем информационной безопасности. – М.: финансы и статистика, 2004. – 736 с.
2. Конкурентная разведка в Internet / В.В.Дудихин, О.В.Дудихина. 2-е изд. испр. и доп. – М.: ООО “Издательство АСТ”, 2004. – 229 с.

Корченко О. Кібернетична безпека держави: характерні ознаки та проблемні аспекти [Електронний ресурс] / О. Корченко, В. Бурячок, С. Гнатюк // Безпека інформації. - 2013. - Т. 19, № 1. - С. 40-44. - Режим доступу: http://nbuv.gov.ua/UJRN/bezin\_2013\_19\_1\_9

1. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти // О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк / Безпека інформації. – Том 19, №1. – 2013. –С. 40-45.
2. Ландэ Д.В. Конкурентная разведка в WEB. [Електронний ресурс] / Д.В.Ландэ, В.В.Прищепа. –Режим доступу: http://z-filez.info/story/konkurentnaya-razvedka-v-web.
3. Леваков Г.Н. Анатомия информационной безопасности. – М.: ТК Велби, издательство Проспект, 2004. – 256 с.
4. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. — К.: КНТ, 2006. – 280 с.
5. М.Левин. E-mail “безопасная”: взлом, “спам” и “хакерские” атаки на системы электронной почты Internet. – М.: Бук-пресс, 2006. – 192 с.
6. МакнамараД. Секреты компьютерного шпионажа. Тактика и контрмеры / Д. Макнамара; пер.с англ.; под ред. С.М. Молявко. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.
7. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. –К. : ВІКНУ, 2011. – Вип. 30. –С. 159-165.
8. Меньшаков Ю.К. Теоретические основы технических разведок: Учебное пособие / Ю.К. Меньшаков; под ред.Ю.Н.Лаврухина. – М.: Узд-во МГТУ им. Н.Э. Баумана, 2008. – 524 с.
9. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2017. – 168 с.
10. Пашнев Д.В. Виды и классификация преступлений, совершаемых с помощью компьютерных технологий / Д.В. Пашнев // Компьютерная преступность и кибертерроризм : Сборник научных статей ; под ред. В.А. Голубева, Н.Н. Ахтырской. – Запорожье : Центр исследования компьютерной преступности, 2004. –Вып. 2. –С. 42–46.
11. Почепцов Г. Г. Інформаційна політика / Г.Г.Почепцов. С.А.Чукут. - К.: Знання. 2008. – 663 с.
12. Почепцов Г.Г. Информационные войны.- М.: Рефл-бук, К.: Ваклер, 2001.- 576 с.
13. Практика ИБ \ SANS - Топ 20 наиболее критичных защитных мер и средств. https://www.sugarsync.com/pf/D6870693\_7400982\_60553
14. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности. [Електронний ресурс]. – Режим доступу: http://book.itep.ru/10/2012.htm
15. Силаенков А.Н. Проектирование системы информационной безопасности: учеб.пособие – Омск: Изд-во ОмГТУ, 2009. – 128 с.
16. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. –К. : ВБ «Аванпост-Прим». – 2012. – 214 c.
17. Соколов Д.Н., Степанюк А.Д. Защита от компьютерного терроризма. – М.: БХВ-Петербург, Арлит, 2002. – 456 с.
18. Східноукраїнського національного університету ім.В.Даля, № 1(9), 2013, с. 33 – 40
19. Сыч О.С. Комплексная антивирусная защита локальной сети. – М.: финансы и статистика, 2006. – 736 с.
20. Торокин А.А. Инженерно-техническая защита информации: учеб. пособие для студентов, обучающихся по специальностям в области информационной безопасности. / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.
21. Черняк В.З. Тайны промышленногошпионажа. / В.З.Черняк. – М.: Вече, 2002. – 512 с.
22. Шеломенцев Володимир Петрович Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення - Боротьба з організованою злочинністю і корупцією (теорія і практика) - 2012 – с.312-320
23. Шестак Н.В. География Интернета. Основные факторы и показатели развития Интернета, виды интернет-услуг: материалы межрегиональной научно-практической конференции «Профессиональное образование в условиях дистанционного обучения. Достижения, проблемы, перспективы» [Электронный ресурс] / Шестак Н.В.-М.,СГА, 2004. - Режим доступа: http://www.muh.ni/arcli/konf\_mSliestak.htm?user=bef81c55bc3cb65d2076769b3ba3e52
24. Ярочкин В.И. Технические каналы утечки информации. / В.И. Ярочкин. – М.: ИПКИР, 1994. – 112 с.