**МЕТОДИЧНІ МАТЕРІАЛИ**

**що забезпечують самостійну роботу студентів**

**з навчального курсу**

 **«Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві»**

Методичні матеріали, що забезпечують самостійну роботу студентів з навчального курсу «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» містять питання та практичні завдання: складання термінологічного словника, тестові завдання, тематику рефератів, задачі та питання для самоконтролю.

Студент повинен ознайомитися з лекційним матеріалом, законодавчими актами, рекомендованою літературою.

Складання словника повинно слугувати засвоєнню понятійного апарату навчального курсу «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві». Термінологічний словник має містити терміни, яких студент не знає. Найважливіші та найскладніші терміни можна знайти в законодавчих актах, текстах лекцій, у підручниках та посібниках.

Тестові завдання дозволяють студентам досить швидко проконтролювати власний рівень засвоєння теоретичних знань. Можна виділити такі рекомендації у вирішенні тестових завдань: треба уважно прочитати запитання; перечитати варіанти відповідей; виключити ті варіанти відповідей, які точно є невірними; та вибрати ті, які є відповіддю на поставлене запитання.

Розв’язування практичних задач передбачає, що викладач пропонує студентам їх вирішити за допомогою діючого законодавства. Звітувати про вирішення студенти повинні на практичному занятті перед загальною групою студентів. Однак студенти можуть самостійно обрати проблемну ситуацію, яку вони мають описати, мотивувати її вибір та запропонувати варіанти вирішення.

Реферат або презентація готується по одній з запропонованих тем або на вибір студента. У рефераті необхідно обґрунтувати актуальність проблеми, яка розглядається; надати опис нормативно-правових актів, що регулюють відносини, які виникають у даній сфері; надати короткий огляд літературних джерел та поглядів різних науковців на суть проблеми; зміст реферату має бути логічним, послідовним, аргументованим та пов'язаний з сучасними українськими реаліями; студент повинен надати висновки та посилання на джерела, які використовувалися. Не зараховуються реферати, які є плагіатом, або передруком текстів з підручника чи Інтернету.

Невиконання завдань тягне за собою незадовільну оцінку!!!

У методичних матеріалах подана рекомендована література, яка складається з міжнародних документів, національних законодавчих актів, підручників, посібників, спрямованих на поглиблене вивчення окремих питань з навчального курсу «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві».

Водночас з рекомендованою літературою можна використати також інші доступні джерела.

***Тема 1. Поняття інформаційної безпеки держави, суспільства та особи***

**Завдання до практичного заняття:**

**1. Скласти термінологічний словник до теми 1.**

**2. Задачі:**

**Задача 1.** На хімічному підприємстві, яке розташоване в межах міста, у результаті аварії стався викид шкідливих речовин в атмосферу. Міська адміністрація разом з керівництвом підприємством вжила необхідних заходів для подолання цієї аварії, але ЗМІ було заборонено надавати інформацію щодо аварії та її наслідків.

Чи правомірні дії міської адміністрації з точки зору норм інформаційного права?

**Задача 2**. Інженер-програміст Чернов був прийнятий на роботу у приватне акціонерне товариство «Вест», де на нього покладено функції оператора ЕОМ щодо введення норм чинного законодавства в інформаційні бази, які «Вест» продавав на комерційній основі підприємствам легкої промисловості. У вільний від введення інформації час Чернову вдалося розробити і впровадити більш досконалий алгоритм обробки правової інформації в інформаційній базі, що помітно підвищило її цінність і дало можливість отримання значного прибутку. На зборах засновників ПАТ «Вест» було запропоновано преміювати Чернова, а його розробку використовувати у ході реалізації модернізованої програми на вигідних комерційних умовах. Однак Чернов заявив керівництву товариства, що воно порушує його авторські права, і зажадав, щоб йому відраховували весь прибуток за використання його програмного продукту.

Як вирішити цю суперечку з позиції норм інформаційного права?

**Задача 3.** Видавнича група «Пам’ять» видала книгу з секретною медичною історією колишнього Президента Франції Міттерана (зокрема, те, що він був хворий на рак і приховував це близько 10 років, перебуваючи на посаді президента). Книга вийшла через 9 днів після смерті президента. Сім'я Міттерана подала позов до суду на видавничу групу «Пам’ять».

Яке рішення повинен винести суд з точки зору норм міжнародного інформаційного права?

 **3. Тестові завдання:**

***1. Національна безпека - це стан:***

а) коли існує захист від небезпеки;

б) захищеності нації;

в) захищеності держави.

***2. Головними об'єктами національної безпеки є:***

а) громадянин - його права та свободи;

б) суспільство - його духовні та матеріальні цінності;

в) держава - її конституційний лад, суверенітет, територіальна цілісність і недоторканність кордонів.

***3. Чи відноситься підтримка оптимальних умов існування особистості та суспільства до основних принципів забезпечення національної безпеки?***

а) так;

б) ні.

***4. Чи відноситься пріоритет прав людини та верховенство права до основних принципів забезпечення національної безпеки?***

а) так;

б) ні.

***5. Яким засобам щодо забезпечення національної безпеки надається пріоритет у вирішенні конфліктів:***

а) договірним (мирним);

б) військовим.

***6. Національна безпека досягається:***

а) шляхом проведення виваженої державної політики у основних сферах діяльності держави;

б) шляхом дотримання балансу інтересів особистості, суспільства та держави;

в) чітким розмежуванням повноважень органів державної влади.

***7. Національні інтереси держави відображають:***

а) фундаментальні цінності та прагнення народу;

б) потреби народу в гідних умовах життєдіяльності;

в) цивілізовані шляхи створення й способи задоволення гідних умов життєдіяльності;

г) верховенство права.

***8. Національні інтереси держави та їх пріоритетність обумовлюються конкретною ситуацією, що складається:***

а) в країні;

б) за її межами:

в) в країні та за її межами.

**4. Практичне завдання:**

***Завдання 1.*** Віднайдіть у практиці Європейського суду з прав людини прецеденти, що стосуються прав особи в інформаційно-правовій сфері, проаналізуйте їх та складіть по них коротке резюме.

 **Питання для самоконтролю.**

1. Які основні підходи до визначення поняття «інформаційна безпека» Ви знаєте?

2. Назвіть основні ознаки інформаційної безпеки.

3. Назвіть основні визначення поняття «інформаційна безпека».

4. У чому полягають інтереси особи, суспільства та держави в інформаційній сфері?

5. Назвіть об’єкти, суб’єкти та види інформаційної безпеки.

6. Що таке інформація?

7. Що таке джерело інформації?

8. Які є носії інформації?

9. Що розуміють під інформаційними ресурсами?

10. Що таке загроза інформаційній безпеці?

***Тема 2. Інформаційна безпека та існуючі загрози***

**Завдання до практичного заняття:**

**1. Скласти термінологічний словник до теми 2.**

**2. Тестові завдання:**

***1. Інформаційна безпека - це забезпечення стану захищеності:***

а) особистості, суспільства і держави

б) інформації та інформаційних ресурсів

в) інформаційних прав і свобод людини і громадянина

г) демократії і соціального спокою

***2. Що відноситься до об'єктів інформаційної безпеки :***

а) держава

б) громадяни

в) суспільні організації та об'єднання

г) інформаційні системи

***3. Концепція інформаційної безпеки – це:***

а) офіційний документ

б) проект

в) систематизована сукупність відомостей про інформаційну безпеку держави і шляхи її забезпечення

***4. Концепція інформаційної безпеки визначає:***

а) класифікацію дестабілізуючих факторів та інформаційних загроз

б) способи і засоби захисту для конкретної особистості

в) способи і форми забезпечення інформаційної безпеки

г) основні положення по організації національної безпеки

***5. До дестабілізуючих факторів інформаційної безпеки відносяться:***

а) явища та процеси штучного походження

б) явища та процеси природного походження

в) явища та процеси, що породжують інформаційні загрози

***6. Загрози інформаційній безпеці – це:***

а) сукупність умов і факторів, що створюють небезпеку в інформаційній сфері

б) сукупність умов і факторів, що створюють небезпеку особистості, держави і суспільства

в) загрози впливу неякісної інформації

***7. За якими групами класифікуються загрози інформаційній безпеці:***

а) за загрозами щодо впливу неякісної інформації

б) за трьома групами відповідно до об’єктів та суб’єктів інформаційної безпеки

в) за загрозами щодо впливу на інформацію та інформаційні ресурси

г) за загрозами інформаційним правам і свободам особистості

***8. Забезпечення інформаційної безпеки – це:***

а) сукупність заходів для досягнення стану захищеності потреб суспільства в інформації

б) дотримання загальних і специфічних принципів забезпечення інформаційної безпеки.

**3. Практичне завдання:**

***Завдання 1***

Проаналізуйте Рішення Європейського суду з прав людини у справі «Pinto Coelho проти Португалії».

*Якими критеріями користувався суд для визначення правомірності розкриття інформації?*

***Завдання 2.*** Проаналізуйте Рішення Європейського суду з прав людини у справі «Aditions Plon проти Франції».

*Який підхід застосований судом для визначення правомірності обмеження поширення інформації. Чи може аналогічний підхід застосовуватися і до обмеження доступу до інформації?*

 **Питання для самоконтролю.**

1. Яким чином розрізняються групи загроз інформації?

2. Дайте визначення поняттям «загроза», «небезпека».

3. Визначте види загроз за ймовірністю реалізації.

4. Визначте види загроз за джерелами походження.

5. Визначте види загроз за значенням.

6. Визначте види загроз за структурою та об’єктом впливу.

7. Визначте види загроз за характером реалізації.

8. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?

9. Визначте політичні фактори загроз.

10. Визначте економічні фактори загроз.

11. Визначте організаційно-технічні фактори загроз.

12. Назвіть джерела загроз інформаційній безпеці особи.

13. Назвіть джерела загроз інформаційній безпеці суспільству.

14. Назвіть джерела загроз інформаційній безпеці держави.

15. Які існують етапи розвитку засобів інформаційних комунікацій?

***Тема 3. Інформаційна війна як найвищий ступінь інформаційного протиборства***

**Завдання до практичного заняття:**

**1. Скласти термінологічний словник до теми 3.**

**2. Тестові завдання**:

***1. Самостійним видом і складовим елементом будь-якого різновиду боротьби, що проводиться постійно як за мирного часу так і за воєнного часу - це:***

а) інформаційне протиборство;

б) інформаційна боротьба;

в) інформаційна війна.

***2. Які комплекси завдань представляє собою інформаційна боротьба:***

а) цілеспрямованого добування інформації;

б) цілеспрямованого й комплексного впливу на всі складові інформаційного середовища протидіючої сторони;

в) захисту власних інформаційних ресурсів та інших складових інформаційного середовища.

***3. За мирний час інформаційна боротьба, який має характер:***

а) таємний;

б) масовий вплив на інформаційні ресурси чужої сторони;

в) масовий вплив на зниження бойових можливостей чужої сторони.

***4. Назвати основні заходи інформаційної боротьби:***

а) інформаційне забезпечення;

б) інформаційна протидія;

в) інформаційний захист.

***5. Складові інформаційної боротьби:***

а) інформаційно-психологічна боротьба;

б) інформаційна протидія (введення противника в оману);

в) інформаційна безпека (забезпечення безпеки своїх інформаційних систем);

г) інформаційна розвідка;

д) радіоелектронна боротьба;

е) комп’ютерно-телекомунікаційна боротьба.

***6. Який комплекс заходів проводиться в умовах дезінформації протилежної сторони:***

а) інформаційна війна;

б) інформаційна протидія;

в) інформаційний захист.

***7. Основні форми ведення інформаційної боротьби:***

а) інформаційний вплив;

б) інформаційна атака;

в) інформаційна битва;

в) інформаційна операція.

***8. Як називається організоване застосування сил і засобів інформаційної боротьби для розв'язування завдань завоювання інформаційного противника:***

а) інформаційний вплив;

б) інформаційна війна;

в) інформаційна битва.

**3. Тематика рефератів:**

1. Інформаційно-технічне протиборство.

2. Інформаційно-психологічне протиборство.

3. Інформаційна експансія.

4. Інформаційна агресія як ступень інформаційного протиборства.

5. Інформаційна війна та її завдання.

6. Історія інформаційних війн.

7. Концепція інформаційної війни.

8. Інформаційна війна на державному рівні.

9. Інформаційна війна у воєнні часи.

10. Умови для досягнення інформаційних переваг.

**Питання для самоконтролю.**

1. Дайте визначення поняття «інформаційне протиборство».

2. Назвіть рівні проведення інформаційного протиборства.

3. Назвіть основні ступені інформаційного протиборства.

4. Що відноситься до органів інформаційної війни?

5. Назвіть основні форми інформаційної війни.

6. Що являє собою оперативна безпека?

***Тема 4. Інформаційна зброя та її складові***

**Завдання до практичного заняття:**

**1. Скласти термінологічний словник до теми 4.**

**2. Заповніть таблицю**

Види інформаційного протиборства

|  |  |
| --- | --- |
| Інформаційно-технічне протиборство | Інформаційно-психологічне протиборство |
|   |   |

**3. Тематика рефератів:**

1. Програми з потенційно-небезпечними наслідками та їх функції.

2. Комп’ютерні віруси.

3. Засоби несанкціонованого доступу.

4. Програмні закладки.

5. Троянські програми.

6. Логічні бомби та люки.

7. Засоби ураження людей та їхньої психіки.

8. Особливості застосування інформаційної зброї.

***Підготувати презентації з запропонованих тем.***

 **Питання для самоконтролю.**

1.Яким чином відрізняється інформаційна зброя від звичайних засобів ураження?

2. Назвіть сферу застосування інформаційної зброї.

3. Назвіть основні об’єкти застосування інформаційної зброї.

4. Що таке комп’ютерні віруси?

5. Які існують види програмних закладок?

6. Назвіть та охарактеризуйте засоби несанкціонованого доступу.

7. Які існують особливості застосування інформаційної зброї?

***Тема 5. Проблеми забезпечення інформаційної безпеки та кібербезпеки в Україні***

**Завдання до практичного заняття:**

**1. Скласти термінологічний словник до теми 5.**

 **2. Практичні завдання**

**Задача 1.** Між ПАТ «Альфа банк» та Міжнародною юридичною фірмою «Gide Loyretee Nouel» підписана угода про надання останнім послуг. Керівник ПАТ «Альфа банк» Куріло відмовив у наданні копії договору Міжнародній юридичній фірмі «Gide Loyretee Nouel», надавши тільки інформацію, яка, на його думку, стосувалася умов отримання бюджетних коштів та надання відповідних послуг. При цьому як підставу для відмови в наданні копії самого договору Куріло послався на те, що договір може містити також комерційну таємницю та іншу конфіденційну інформацію.

*Чи слід вважати відмову Куріло в цій ситуації правомірною?*

**Задача 2.** Національне інформаційне агентство, використовуючи можливості контролю телефонних каналів зв'язку, перешкоджало недержавному підприємству «Поляр» в реалізації його функцій міжнародного інформаційного обміну та пропонувало йому укласти договір на надання послуг у галузі експлуатації каналів зв'язку. Однак умови, на яких пропонувалося укласти цей договір, були для підприємства «Поляр» невигідні: згідно з умовами договору, воно повинно було передати національному інформаційному агентству за послуги свої майнові права на 25 % акцій.

*Чи правомірні дії національного агентства з точки зору законодавства щодо міжнародного інформаційного обміну ?*

**Задача 3.** Комерційний банк «Укрсоцбанк» уклав договір з юридичною фірмою «Патрія» про впровадження в своєму юридичному відділі найсучасніших інформаційних систем «Банківське право» і «Правові основи роботи з цінними паперами». Юридична фірма встановила в банку названі системи, отримала обумовлену винагороду і, попередивши банк про конфіденційність отриманих ним відомостей про системи, приступила до виконання нового замовлення. Президент банку вирішив зробити приємне своєму колезі голові правління іншого банку, і одного разу передав його ІТ-спеціалістам всю інформацію про нові системи. Дізнавшись про це, генеральний директор юридичної фірми «Патрія» Горлов подав позов до суду на банк «Укрсоцбанк» і зажадав відшкодування фірмі заподіяної шкоди за розголошення конфіденційних відомостей.

*Які норми інформаційного законодавства були порушені і яке рішення мас прийняти суд?*

**3. Заповніть таблицю за такою схемою:**

|  |  |
| --- | --- |
|  Вид інформації | Відомості, що відносяться до виду інформації |
| 1. Інформація про фізичну особу | Відомості чи сукупність відомостей про фізичну особу |

**4. Тематика рефератів:**

1. Загальний аналіз Доктрини національної безпеки України, яка введена в дію Указом Президента від 25.02.2017 р.

2. Національні інтереси України в інформаційній сфері (з використанням положень Доктрини та іншого матеріалу).

3. Загрози національним інтересам та національній безпеці України.

4. Пріоритети державної політики в інформаційній сфері.

5. Механізми реалізації інформаційної безпеки в Україні.

6. Стратегія національної безпеки України.

7. Стратегія кібербезпеки України.

8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (загальний аналіз).

9. Загальний аналіз Закону України «Про захист персональних даних».

10. Загальний аналіз Закону України «Про державну таємницю».

11. Загальний аналіз Постанов КМУ «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», «Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію».

***Тема 6. Забезпечення інформаційної безпеки України***

**Завдання до практичного заняття:**

**1. Скласти термінологічний словник до теми 6.**

 **2. Тематика рефератів:**

1. Закон України «Про національну безпеку України».

2. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення.

3. Особливості забезпечення інформаційної безпеки у різних сферах суспільного життя.

4. Перспективи міжнародного співробітництва України у галузі забезпечення інформаційної безпеки.

5. Заходи щодо реалізації політики забезпечення інформаційної безпеки України.

**Питання для самоконтролю.**

1. Що розуміється під «інформаційною безпекою України»?

2. Яке її місце в системі національної безпеки України?

3. Основні напрями політики інформаційної безпеки України?

4. Найважливіші завдання у сфері інформаційної безпеки?

5. В яких сферах проявляються реальні та потенційні загрози безпеці України?

6. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.

7. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.

8. Охарактеризуйте загрози інформаційній безпеці України в екологічній сфері.

9. Які завдання реалізації інформаційної політики з питань євроінтеграції?

10. Яким чином розрізняються групи загроз інформації?

11. Дайте визначення поняттям «загроза», «небезпека».

12. Визначте види загроз за ймовірністю реалізації.

13. Визначте види загроз за джерелами походження.

14. Визначте види загроз за значенням.

15. Визначте види загроз за структурою та об’єктом впливу.

16. Визначте види загроз за характером реалізації.

17. Які основні підходи до визначення дестабілізуючих факторів ви знаєте?

18. Визначте політичні фактори загроз.

19. Визначте економічні фактори загроз.

20. Визначте організаційно-технічні фактори загроз.

21. Назвіть джерела загроз інформаційній безпеці особи.

22. Назвіть джерела загроз інформаційній безпеці суспільству.

23. Назвіть джерела загроз інформаційній безпеці держави.

24. Які існують етапи розвитку засобів інформаційних комунікацій?

**РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

 1. Конституція України // Відомості ВРУ, 1996, №30, ст..141, [Електронний ресурс]. Режим доступу:

<https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

2. Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-ІV. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_575#Text>

3. Про інформацію: Закон України // Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

4. Про національну безпеку України: Закон України// Відомості Верховної Ради (ВВР), 2018, № 31, ст.241. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

5. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України// Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>

6. Про доступ до публічної інформації: Закон України // Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

7. Про Державну службу спеціального зв’язку та захисту інформації України: Закон України// Відомості Верховної Ради України (ВВР), 2006, № 30, ст.258. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/3475-15#Text>

8. Резолюция 60/45, принятая Генеральной Ассамблеей ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». [Електронний ресурс]. Режим доступу:

<https://zakon.rada.gov.ua/laws/show/995_e45#Text>

9. Директива 97/66/ЄС Європейського Парламенту і Ради «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі». [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_243#Text>

10. Решение № 1106 «Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий» от 03.12.2013. [Електронний ресурс]. Режим доступу: <https://www.osce.org/files/f/documents/0/a/109648.pdf>

11. Конвенція про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію. [Електронний ресурс]. Режим доступу:<https://zakon.rada.gov.ua/laws/show/995_266#Text>

12. Верголяс О. О. Міжнародно-правове регулювання інформаційного протиборства: реалії та перспективи. Visegrad Journalon Human Rights. 2019. №3. C. 58-63

14. Ємельянов В. М., Бондар Г. Л. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. Публічне управління та регіональний розвиток. 2019. № 5. С. 493-523.

15. Інформаційна безпека держави: підручник: в 2 т. Т. 1. / В.М. Петрик та ін.; за заг. ред. В.В. Остроухова. Київ:ДНУ «Книжк. палата України», 2016. 264 с.

16. Інформаційна безпека / За ред. Ю. Я. Бобала, І. В. Горбатого. Львів: Вид-во Львівської політехніки. 2019. 580 с.

17. Історія інформаційно-психологічного протиборства: підруч./ [Я.М.Жарков, Л. Ф. Компанцева, В. В. Остроухов В. М. Петрик, М. М. Присяжнюк, Є. Д. Скулиш]; за заг. ред. д.ю.н., проф., засл. юриста України Є. Д. Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.

18. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посіб. / А. В. Боровик, І. М. Копотун. Луцьк : Волинь Поліграф, 2019. 304 с.

19. Корпоративна безпека: практичний посібник. Консалтингова компанія Сідкон. 2018. 276 с.

20. Когут Ю.І. Кібербезпека та ризики цифрової трансформації компаній. Вид-во SIDCON. 2021, 372 с.

21. Лісовська Ю. П. Інформаційна безпека України: навч. посіб. Київ: Кондор, 2018. 172 с.

22. Лизанчук В. Інформаційна безпека України: теорія і практика. Львів. Вид-во ЛНУ ім. Івана Франка. 2017. 728 с.

23. Мехед Д., Ткач Ю., Базилевич В., Гур’єв В., Усов Я. Аналіз вразливостей корпоративних інформаційних систем. Захист інформації. 2018. № 1. С. 61 – 66.

24. Могильний С. Б. Інформаційна безпека при роботі в Інтернеті: навч.-метод. посібник / за ред. О. В. Лісового та ін. Київ, 2018. 105 с.

25. Нашинець-Наумова А. Ю. Інформаційна безпека суб’єктів господарювання: проблеми теорії та практики правозастосування: Монографія. Видав. Дім «Гельветика». 2017. 386 с.

26. Петрик В., Присяжнюк М. Інформаційна безпека держави. Підручник у 2-х томах. Київ. Вид-во «Книжкова палата України». 2016. 264 с.

27. Почепцов Г. Сучасні інформаційні війни / Г. Почепцов. К. : Вид.дім «Києво-Могилянська академія», 2015. 497 с.

28. Харитонов Є. О., Давидова І. В. Інформаційна безпека: проблеми приватного права. Навч.- методичний посібник. Вид-во Фенікс, 2020. 194 с.

**ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ**

1. Верховна Рада України: офіційний веб-портал парламенту України. Законодавство України. – Режим доступу:<https://zakon.rada.gov.ua/laws>

2. Кабінет міністрів України. Урядовий портал. Єдиний веб-портал органів виконавчої влади України. – Режим доступу : <https://www.kmu.gov.ua/>

3. Офіційний вісник України. – Режим доступу : [www.gdo.kiev.ua](http://www.gdo.kiev.ua/).

4. Статистика України: науковий журнал [Електронний ресурс]. – Режим доступу : [www.ukrstat.gov.ua](http://www.ukrstat.gov.ua/).