**Методичні вказівки до проведення семінарських занять**

**З навчальної дисципліни**

**Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві**

**Курс «Нормативно-правове забезпечення інформаційної безпеки в національному та міжнародному співробітництві» має за мету** надати студентам знання та основні поняття з основ нормативно-правового забезпечення інформаційної безпеки держави, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство, ознайомити з законодавчими актами України та міжнародними документами, які регулюють інформаційну безпеку.

**Завдання методичних вказівок** – оволодіння поняттями забезпечення інформаційної безпеки, як однієї з найважливіших сфер діяльності в умовах входження держави в інформаційне суспільство, опанування основними термінами та категоріями інформаційної безпеки на рівні їх тлумачення та відтворення для практичного застосування та втілення у процесі фахової діяльності майбутнього спеціаліста з інформаційної безпеки. Студенти повинні навчитися вільно визначати роль і місце інформаційної безпеки в загальній системі національної безпеки; проводити аналіз моделі загроз інформаційним ресурсам; самостійно здійснювати аналіз протидії загрозам інформаційних ресурсів; здійснювати оцінку застосування чинних законодавчих та інших нормативних правових актів України та міжнародних документів в інформаційній сфері; обирати необхідний метод захисту інформаційних ресурсів; проводити дослідження та формувати пропозиції із вдосконалення системи захисту інформаційних ресурсів.

**Тема 1. Поняття інформаційної безпеки держави, суспільства та особи (2год.)**

***Мета:*** вивчення основних видів та властивостей інформації.

***Основні завдання:*** розуміння поняття інформації та видів інформації; визначення форм адекватності інформації; проведення класифікації інформації; характеристика якості інформації; дослідження основних властивостей інформації; поняття інформаційної безпеки та її сутності; визначення інтересів особи, держави та суспільства в інформаційній сфері.

**План**

1. Правове забезпечення інформації та інформаційної безпеки.

2. Інформація та види інформації. Інформаційні відносини.

3. Інформаційний суверенітет.

4. Сутність інформаційної безпеки. Види інформаційної безпеки.

5. Інформаційна сфера та інтереси особи, держави та суспільства.

**Задача 1.** На хімічному підприємстві, яке розташоване в межах міста, в 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 в приватне акціонерне товариство «Вест», де на нього покладалися 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 призвело до отримання значного прибутку. На зборах засновників ПАТ «Вест» було запропоновано преміювати Чернова, а його розробку використовувати в 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 цей спір 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 і точки зору норм міжнародного інформаційного права?

***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 й свободи;

б) суспільство - його духовні та матеріальні цінності;

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

***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?

***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. 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>

4. 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>

5. 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>

6. 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>

7. 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>

8. 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>

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

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

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

**Тема 2. Проблеми забезпечення інформаційної безпеки та кібербезпеки в Україні (2 год.)**

***Мета:*** вивчення основних понять та основних категорій інформаційної безпеки та кіберпезпеки.

***Основні завдання:*** вивчення основних категорій національної безпеки та кібербезпеки; визначення кіберпростору та його співвідношення з інформаційною безпекою в цілому; з’ясування факторів та засобів забезпечення національної безпеки; дослідження основних видів національної безпеки та системи забезпечення національної безпеки; визначення стратегії національної безпеки України, її основних напрямів.

**План**

1.Кіберпростір та його співвідношення з інформаційною безпекою.

2. Кібербезпека: склад та сутність.

3. Стратегія забезпечення національної безпеки.

4. Фундаментальні національні інтереси України.

***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 в 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 «Патрия» 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 ?*

***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 |

***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 національної безпеки України.

4. Пріоритети державної політики в інформаційній сфері.

5. Механізми реалізації інформаційній 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»

**Питання для самоконтролю.**

1. Що таке кіберборотьба?

2. Які основні особливості їй притаманні?

3. Дайте визначення поняття «кібернетична безпека».

4. Назвіть істотні ознаки, які його характеризують.

5. Причини головних проблем забезпечення кібернетичної безпеки.

6. Які стратегії затверджені в Законі України «Про національну безпеку України»?

7. Стратегія воєнної безпеки України.

8. Стратегія кібербезпеки України.

9. Стратегія громадської безпеки та цивільного захисту України.

***Рекомендована література:***

1. 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>

2. 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>

3. 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>

4. 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>

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

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

7. Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки [Текст] : словник / [уклад.: В. І. Єсін, С. Г. Рассомахін] ; Харківський національний університет імені В. Н. Каразіна. - Харків : ХНУ ім. В. Н. Каразіна, 2018. - 64 с.

8. Інформаційна безпека [Текст] : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник [та ін] ; за заг. ред. Ю. Я. Бобала, І. В. Горбатого ; Національний університет "Львівська політехніка". - Львів : Львівська політехніка, 2019. - 580 с.

9.Інформаційна безпека держави [Текст] : навч. посіб. / В. М. Рудницький. С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкаський державний технологічний університет. - Харків : [ДІСА ПЛЮС], 2018. - 359 с.

**Тема 3. Інформаційна безпека та існуючі загрози (2 год.)**

***Мета:*** визначення основних понять загроза та небезпека інформаційної системи.

***Основні завдання:*** визначення основних життєво важливих інтересів держави в сфері інформаційної безпеки; визначення об’єктів та суб’єктів інформаційної безпеки; розкриття концепції інформаційної безпеки; розуміння існуючих внутрішніх та зовнішніх загроз інформаційної безпеки; розкриття основних форм та способів забезпечення інформаційної безпеки.

**План**

1. Інформаційної безпеки держави та життєво важливі інтереси особистості, суспільства та держави. Об’єкти та суб’єкти інформаційної безпеки.

2. Концепція інформаційної безпеки.

3. Класифікація видів загроз інформаційній безпеці України. Внутрішні та зовнішні джерела загроз інформаційній безпеці України.

4. Система забезпечення інформаційної безпеки держави. Основні форми і способи забезпечення інформаційної безпеки держави.

**Тестові завдання:**

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

а) особистості, суспільства і держави

б) інформації і 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 і 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

***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?

***Рекомендована література:***

1. 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>

2. 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>

3. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ ―ОЮА, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.

4. Інформаційна безпека держави : підручник / [ В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін. ] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.

5. Інформаційна безпека [Текст] : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник [та ін] ; за заг. ред. Ю. Я. Бобала, І. В. Горбатого ; Національний університет "Львівська політехніка". - Львів : Львівська політехніка, 2019. - 580 с.

6.Інформаційна безпека держави [Текст] : навч. посіб. / В. М. Рудницький. С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкаський державний технологічний університет. - Харків : [ДІСА ПЛЮС], 2018. - 359 с.

**Тема 4. Основні принципи, форми та методи забезпечення інформаційної безпеки (4год.)**

***Мета:*** визначення основних принципів та форм забезпечення інформаційної безпеки

***Основні завдання:*** визначення основних та специфічних принципів інформаційної безпеки; розуміти, в яких формах здійснюється забезпечення інформаційної безпеки; з’ясувати особливості інформаційного патронату, інформаційної кооперації та інформаційного протиборства.

**План**

1.Основні та специфічні принципи інформаційної безпеки.

2. Основні форми забезпечення інформаційної безпеки.

3. Інформаційний патронат.

4. Інформаційна кооперація.

5. Інформаційне протиборство.

***Практичні завдання:***

**Задача 1.**

Керівник служби безпеки фірми «Феміда» склав для персоналу фірми інструкцію по роботі з документами, що становлять комерційну таємницю. Відповідно до цієї інструкції працівники фірми повинні були давати відповідну підписку про її нерозголошення, або це зобов'язання мало включатися в якості окремого пункту в трудову угоду того чи іншого працівника. Якщо відомості, що становлять комерційну таємницю, доводилося розголошувати своїм діловим партнерам або клієнтам фірми, то положення про нерозголошення таємниці обов'язково повинні були включатися у відповідні договори з учасниками правовідносин.

Однак деякі працівники фірми були проти застосування до них таких мір, вони вважали, що ш так не розголошують комерційні таємниці.

*Дайте правову оцінку положень цієї інструкції з точки зору законодавства про інформаційну безпеку та вимоги працівників фірми.*

**Задача 2.**

Публіцист Волков надрукував у газеті «Вести» цікаву статтю під назвою «Скарби України», в якій привів отримані від експерта Служби Безпеки України Нестерова загальні відомості про державні запаси дорогоцінних металів і каменів, а також назвав розміри золотого запасу та валютних резервів України. Керівник відділу Служби Безпеки України Романов, прочитавши в газеті статтю Волкова і з'ясувавши, звідки він отримав інформацію, поставив перед своїм керівництвом питання про притягнення до відповідальності Нестерова за розголошення відомостей, які відносяться до державної таємниці.

*Проаналізуйте цю ситуацію з точки зору законодавства про інформаційну безпеку.*

**Задача 3.**

Депутати Шевченківської районної ради в місті Харків звернулися до Міністерства освіти і науки України з проханням направити до районного архіву копії 20 документів жителів Шевченківського району, які захистили кандидатські і докторські дисертації за останні десять років з тим, щоб сформувати власний масив інформації про науковий потенціал району. У цьому проханні було відмовлено на тій підставі, що всі масиви документів, що зберігаються в базах даних Міносвіти України, є виключно державними інформаційними ресурсами і відносяться до інформації з обмеженим доступом.

*Чи є в даній ситуації порушення інформаційного законодавства, що регулює безпеку інформаційних ресурсів в Україні ?*

***Тематика рефератів:***

1. Основні завдання системи забезпечення інформаційної безпеки.

2. Мета функціонування системи забезпечення інформаційної безпеки.

3. Основні способи та засоби забезпечення інформаційної безпеки людини.

4. Опис та класифікація як методи аналізу стану забезпечення інформаційної безпеки.

5. Загальні методи забезпечення інформаційної безпеки.

6. Метод розвитку та його значення для забезпечення інформаційної безпеки.

7. Країни Європи в світовому інформаційному просторі.

8. Світовий інформаційний простір і місце країн Європи в ньому.

9. Системи інформаційної безпеки в країнах Європи

10. Система інформаційної безпеки у США.

**Питання для самоконтролю.**

1. Поняття забезпечення інформаційної безпеки держави.

2. Основні принципи забезпечення інформаційної безпеки держави.

3. Що таке превентивність?

4. Як можна тлумачити поняття адекватної інформованості?

5. Що таке інформаційний патронат?

6. Що таке інформаційна кооперація?

7. Дати визначення інформаційного протиборства.

8. Способи забезпечення інформаційної безпеки для конкретної особи.

9. Методи забезпечення інформаційної безпеки.

10. Рівні сфери інформаційної безпеки.

11. Які є методи впливу на інформацію?

***Рекомендована література:***

1. 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>

2. 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>

3. Заплотинський Б.А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ ―ОЮА, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. – 128 с.

4. Інформаційна безпека держави : підручник / [ В.М. Петрик, М.М. Присяжнюк, Д.С. Мельник та ін. ] ; в 2 т. – Т.1. / за аг. ред.. В.В. Остроухова. – К. : ДНУ «Книжкова палата Україна», 2016. – 264 с.

5. Інформаційна безпека [Текст] : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник [та ін] ; за заг. ред. Ю. Я. Бобала, І. В. Горбатого ; Національний університет "Львівська політехніка". - Львів : Львівська політехніка, 2019. - 580 с.

6. Інформаційна безпека держави [Текст] : навч. посіб. / В. М. Рудницький. С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкаський державний технологічний університет. - Харків : [ДІСА ПЛЮС], 2018. - 359 с.

**Тема 5. Інформаційна війна як найвищий ступень інформаційного протиборства (4 год.)**

***Мета:*** засвоєння основних понять та положень інформаційного протиборства та інформаційної війни, як форм забезпечення інформаційної безпеки.

***Основні завдання:*** вивчення основних видів інформаційного протиборства; розуміння концепції інформаційного протиборства; дослідження особливостей та завдань інформаційної війни як у мирний та воєнний часи; розуміння засобів інформаційної війни.

**План**

1. Інформаційне протиборство та його види.

2. Об’єкти впливу інформаційного протиборства.

3. Концепція інформаційного протиборства. Ступені інформаційного протиборства.

4. Інформаційна війна та її особливості. Завдання інформаційної війни.

5. Основні форми та рівні інформаційної війни.

6. Засоби інформаційної війни.

7. Інформаційні переваги у сфері інформаційного протиборства.

***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) інформаційне 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) інформаційна 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) інформаційна вплив;

б) інформаційна війна;

в) інформаційна битва.

***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?

***Рекомендована література:***

1.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>

2.Конвенція про кіберзлочинність. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_575#Text>

3. 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.

4. Почепцов Г. Сучасні інформаційні війни [Текст] / Георгій Почепцов. Вид. 2-ге, допов. Київ : Києво-Могил. акад., 2016. 502 с.

5. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с.

6. Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки [Текст] : словник / [уклад.: В. І. Єсін, С. Г. Рассомахін] ; Харківський національний університет імені В. Н. Каразіна. - Харків : ХНУ ім. В. Н. Каразіна, 2018. - 64 с. - Бібліогр.: с. 59-63.

**Тема 6. Інформаційна зброя та її складові (2 год.)**

***Мета:*** засвоєння поняття інформаційна зброя, її складових.

***Основні завдання:*** формування розуміння інформаційної зброї; дослідження сфери застосування інформаційної зброї; виявлення програм з потенційно небезпечними наслідками; здобуття практичних навичок із захисту інформаційних систем від загроз.

**План**

1. Інформаційна зброя воєнного та невоєнного застосування.

2. Засоби ураження комп’ютерних інформаційних систем.

3. Програми з потенційно небезпечними наслідками.

***Складіть таблицю:***

Види інформаційного протиборства

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

***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?

***Рекомендована література:***

1. 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>

2. 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>

3. Конвенція про кіберзлочинність. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_575#Text>

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

5. Заруба О.Г. Планування спеціальних інформаційних операцій. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С.140-154 110.

6. Золотухін Д. Ю. Біла книга спеціальних операцій проти України, 2014 – 2018. К., 2018. 384 c.

7. Почепцов Г. Сучасні інформаційні війни [Текст] / Георгій Почепцов. Вид. 2-ге, допов. Київ : Києво-Могил. акад., 2016. 502 с.

8. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с.

9. Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки [Текст] : словник / [уклад.: В. І. Єсін, С. Г. Рассомахін] ; Харківський національний університет імені В. Н. Каразіна. - Харків : ХНУ ім. В. Н. Каразіна, 2018. - 64 с. - Бібліогр.: с. 59-63.

**Тема 7. Теорія інформаційної боротьби та її сутність (4год.)**

***Мета:*** вивчення поняття та змісту теорії інформаційної війни.

***Основні завдання:***  формування розуміння, що таке теорія інформаційної війни, її структури; виявлення основних факторів впливу; дослідження основних заходів інформаційної боротьби.

**План**

1. Поняття теорії інформаційної боротьби та її мета.

2. Фактори впливу: економічний, воєнний та інформаційний.

3. Загальні основи теорії інформаційної боротьби та її структура. Теорія сил та засобів ураження інформації. Теорія захисту інформації.

4. Особливості законів та закономірностей інформаційної боротьби.

5. Заходи інформаційної боротьби: інформаційне забезпечення, інформаційний захист, інформаційна протидія.

6. Способи інформаційної боротьби та їх класифікація.

***Тестові завдання:***

***1.Інформаційна боротьбі ведеться тільки***

а) у воєнний час;

б) у мірний час;

в) завжди;

г) у воєнний та мірний час.

***2. До факторів впливу на інформаційну боротьбу відносяться:***

а) воєнний фактор;

б) суспільний фактор;

в) міжнародні фактори;

г) економічний фактор;

д) інформаційний фактор

***3. Політичний фактор інформаційної боротьби визначає:***

а) мету та завдання;

б) причини виникнення;

в) шляхи запобігання;

г) людські ресурси;

д) військову зброю.

***4. Які закони знаходять свій прояв у інформаційній боротьбі:***

а) економічні закони;

б) закони діалектики;

в) закони війни;

г) закони залежності ходу та кінця війни;

д) закони держави.

***5. До принципів інформаційної боротьби відносяться:***

а) принцип верховенства права;

б) принцип універсальності;

в) принцип високої активності й рішучості дій;

г) принцип дотримання прав людини;

д) принцип безперервності інформаційної боротьби.

***6. До заходів інформаційної боротьби відносяться:***

а) дезінформація;

б) інформування;

в) трансдезінформування;

г) обробка інформації.

***7. Способи інформаційної боротьби:***

а) силові способи;

б) інформаційні способи;

в) комбіновані;

г) способи відвернення уваги.

***8. До основних форм ведення інформаційної боротьби зазвичай відносять такі:***

а) інформаційна дія;

б) інформаційна битва;

в) інформаційний удар;

г) усі перелічені.

***Тематика рефератів:***

1.Інтелектуальні способи інформаційної боротьби.

2. Способи блокування інформації.

3.Мета та завдання інформаційної операції.

4. Інформаційне забезпечення в умовах інформаційної боротьби.

5. Загальна характеристика принципів інформаційної боротьби.

**Питання для самоконтролю.**

1. Дати визначення інформаційної боротьби.

2. Яка мета інформаційної боротьби?

3. Які фактори впливають на зміст інформаційної боротьби?

4. Які існують заходи інформаційної боротьби?

5. Охарактеризувати принципи інформаційної боротьби.

6. Дати визначення метода оцінки ефективності інформаційної боротьби.

7. Які існують форми ведення інформаційної боротьби?

8. Які існують способи інформаційної боротьби?

9. Що таке радіоелектронно-вогневий удар?

10.Формула для обчислення числового значення критерію ефективності інформаційної боротьби.

***Рекомендована література:***

1. 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>

2. 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>

3. Конвенція про кіберзлочинність. [Електронний ресурс]. Режим доступу: <https://zakon.rada.gov.ua/laws/show/994_575#Text>

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

5. Заруба О.Г. Планування спеціальних інформаційних операцій. Інформаційна безпека людини, суспільства, держави. 2017. № 1 (21). С.140-154 110.

6. Золотухін Д. Ю. Біла книга спеціальних операцій проти України, 2014 – 2018. К., 2018. 384 c.

7. Почепцов Г. Сучасні інформаційні війни [Текст] / Георгій Почепцов. Вид. 2-ге, допов. Київ : Києво-Могил. акад., 2016. 502 с.

8. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с.

9. Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки [Текст] : словник / [уклад.: В. І. Єсін, С. Г. Рассомахін] ; Харківський національний університет імені В. Н. Каразіна. - Харків : ХНУ ім. В. Н. Каразіна, 2018. - 64 с. - Бібліогр.: с. 59-63.

**Тема 8. Основи безпеки інформаційних технологій (4 год.)**

***Мета:*** засвоєння понять інформація, безпека інформації, інформаційні ресурси.

***Основні завдання:*** визначення форм адекватності інформації; проведення класифікації мір інформації;характеристика якості інформації; дослідження основних властивостей інформації. визначення поняття інформаційні технології; визначення співвідношення понять інформаційні технології та інформаційні системи; проведення класифікації та видів інформаційних технологій; формування основних проблем безпеки інформаційних технологій.

**План**

1. Інформація та її зміст. Одержувачі інформації.

2. Загрози порушення конфіденційності, цілісностіта доступності інформації.

3. Загрози безпеки інформації та інформаційних ресурсів.

4. Порушення та їх види.

5. Джерела загроз безпеки інформації: антропогенні, техногенні та викликані стихійними джерелами.

6. Порушники,цілі та мета їх дій.

***Тестові завдання:***

***1. Інформація (законодавче визначення) – це***

а) відомості про оточуючий світ;

б) документовані відомості про події, що відбуваються у навколишньому середовищі;

в) будь-які дані чи відомості про події та явища, збережені на матеріальних носіях, у тому числі – в електронному вигляді;

г) відомості про що-небудь.

***2. Властивості інформації:***

а) системність, селективність, якість, універсальність, масовість, спадкоємність;

б) субстанціональна несамостійність, невичерпність, трансформуємість, масовість, здатність до обмеження, системність;

в) фізична невідчужуваність, відокремленість, двоєдність, тиражованість, організаційної форми, екземплярність;

г) відокремленість, двоєдність, тиражованість.

***3. Види інформації як об’єкта інформаційних відносин:***

а) статистична, масова, соціальна, законодавча, довідково-енциклопедична;

б) статистична, масова, документи, правова, інформація про діяльність державних органів влади;

в) правова, інформація про діяльність державних органів влади;

г) статистична, масова, інформація про діяльність державних органів влади, права, персональні дані, довідково-енциклопедична, соціологічна, адміністративна.

***4. Основні способи захисту інформації:***

а) організаційно-технічні;

б) технічні, програмні, криптографічні та правові;

в) організаційно-управлінські;

г) технічні, програмні та криптографічні.

***5. Ознаки інформації:***

а) фізична невідчужуваність, двоєдність, тиражованість, організаційна форма, відокремленість, екземплярність;

б) системність, селективність, субстанційна несамостійність, спадкоємність, невичерпність, масовість, трансформованість, універсальність, здатність до обмеження, якість;

в) невичерпність, двоєдність, якість, обмеженість, спадкоємність, організаційна форма;

г) якість, обмеженість, спадкоємність.

***6. Інформаційна сфера – це сфера***

а) обігу інформації;

б) створення інформації;

в) обіг інформації, під час якого суб’єкти реалізують свої потреби і можливості по відношенню до інформації;

г) отримання інформації.

***7. Об’єкти інформаційної сфери:***

а) інформація, інформаційні ресурси;

б) інформація, інформаційні ресурси, інформаційна інфраструктура;

в) інформація, інформаційні ресурси, інформаційні системи;

г) інформаційно-телекомунікаційні системи.

***8.Об’єктивні закони розвитку інформаційної сфери:***

а) закон неповного використання інформації, закон перекручування інформації;

б) закон організації і обмеження інформації;

в) закон організації і обмеження інформації, закон інформаційного випередження;

г) закон Мерфі.

***9. Інформаційні ресурси – це***

а) сукупність документів в інформаційних системах;

б) сукупність документів в інформаційній сфері;

в) сукупність документів в базах даних;

г) сукупність будь-яких документів.

***10. До складу правового режиму інформаційних ресурсів входять норми, які визначають:***

а) порядок документування інформації та її захисту;

б) порядок документування інформації, її захист, право власності та документи, категорії інформації з точки зору доступу до неї;

в) право власності на документи, категорії інформації з точки зору доступу до неї;

г) порядок документування інформації та її захисту.

**Питання для самоконтролю.**

1. Що є джерелом та фактором загрози інформації?

2. Які є види загроз комп’ютерної інформації?

3. Які є групи джерел загроз безпеці інформації?

4. Наведіть класифікацію вразливостей безпеці інформації?

5. Які класи (види) загроз розрізняються в інформаційній сфері?

6. Які загрози відносяться до рівня порушення конфіденційності ?

7. Які загрози відносяться до рівня порушення цілісності ?

8. Які існують категорії джерел конфіденційної інформації?

9. Які є моделі порушень інформаційних ресурсів?

10. Яка мета та цілі порушника об’єктів інформаційної діяльності?

11. Наведіть класифікацію порушника за характером дій?

***Рекомендована література:***

1. 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>

2. 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>

3. 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>

4. 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>

5. 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>

6. 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>

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

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

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

**Тема 9. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів (4год.)**

***Мета:*** вивчення концептуальних положень захисту інформації та інформаційних ресурсів.

***Основні завдання:*** визначення базових загроз безпеці інформації та інформаційних ресурсів; розуміння важливості класифікації уразливостей безпеці інформації та інформаційних ресурсів; вивчення основних напрямів забезпечення безпеки; з’ясування загальних положень правого захисту; розуміння загальних положень організаційного захисту; виявлення загальних положень інженерно-технічного захисту; вивчення архітектури захисту інформації в інформаційних системах та мережах.

**План**

1. Правовий захист: конституційне законодавство, загальні та спеціальні закони, підзаконні акти. Спеціальне законодавство.

2. Страхове забезпечення та його мета.

3. Ліцензія як засіб забезпечення безпеки інформації.

4. Комерційна таємниця.

5. Забезпечення захисту та безпеки інформації на підприємстві.

6. Організаційний захист та його заходи.

7. Особливості захисту комп’ютерних систем. Служба захисту інформації. 8. Інженерно-технічний захист та його засоби.

***Тестові завдання:***

***1. Напрями захисту інформації:***

а) комп’ютерні засоби;

б) правовий захист;

в) державний захист;

г) служба захисту інформації.

***2. Засоби захисту інформації:***

а) попередження, виявлення загроз;

б) припинення загроз та відновлення збитків;

в) державні засоби;

г) індивідуальний захист.

***3. Правовий захист регулюється:***

а) міжнародними актами;

б) Конституцією України;

в) відомчими актами;

г) законодавством.

***4.Завдання страхування як засобу захисту інформації:***

а) забезпечення страхового захисту фізичних та юридичних осіб;

б) захист власної інформації;

в) державний захист;

г) захист засобів обробки інформації від внутрішніх та зовнішніх загроз.

***5. Форми захисту інформації:***

а) патентне право;

б) авторське право;

в) конституційне право;

г) визнання відомостей конфіденційними.

***6. Організаційний захист інформації забезпечує:***

а) надійний механізм захисту інформації;

б) організацію режиму охорони роботи з документами;

в) технічні засоби безпеки;

г) інформаційно-аналітичну діяльність.

***7. Засоби інженерно-технічного захисту поділяються на:***

а) службові;

б) фізичні;

в) технічні;

г) криптографічні.

***8. Програмні засоби захисту:***

а) реєстрація користувачів;

б) захист операційних систем;

в) технічні;

г) ідентифікація засобів та файлів.

***Тематика рефератів:***

1. Загальна характеристика міжнародних актів та національного законодавства, спрямованого на захист інформації та інформаційних ресурсів.

2. Конституційні права на інформацію та забезпечення її захисту.

3. Страхове забезпечення захисту інформації як напрям правового захисту.

4. Ліцензія як офіційний засіб захисту інформації.

5. Комерційна таємниця та способи її захисту.

6. Основні організаційні засоби захисту інформації та їх види.

7. Особливості організаційного захисту комп’ютерних інформаційних систем.

8. Правовий статус служби безпеки підприємства.

9. Особливості програмного захисту інформації.

10. Криптографічні засоби захисту інформації.

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

**Питання для самоконтролю.**

1. Які напрями захисту інформації існують?

2. Сформулюйте поняття права.

3. Яка структура правових актів, що орієнтовані на правовий захист інформації?

4. Дати визначення ліцензії.

5. Що таке комерційна таємниця?

6. Що забезпечує організаційний захист?

7. Назвіть основні організаційні заходи.

8. Функції служби безпеки підприємства (фірми, організації).

9. Завдання служби безпеки підприємства (фірми, організації).

10. Що таке інженерно-технічний захист? Його завдання.

11. Фізичні засоби захисту та їх завдання.

12. Які апаратні засоби захисту інформації Ви знаєте?

13. Що таке криптографія?

14. Назвіть переваги цифрового шифрування.

***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. 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>

3. 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>

4. 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>

4. 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>

5. 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>

6. 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>

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

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

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

**Тема 10. Захист інформаційних систем (2 год.)**

***Мета:*** вивчення основних критерій безпеки інформаційних технологій.

***Основні завдання:*** вивчення основних понять про стандарти інформаційної безпеки; розуміння основних засобів забезпечення безпеки комп’ютерних систем та інформаційних технологій; з’ясування основних положень загальних критеріїв безпеки інформаційних технологій; дослідження функціональних вимог до засобів захисту, вимог та рівнів гарантій засобів захисту.

**План**

1. Джерела інформації. Люди як джерела інформації.

2. Інформаційна система, її структура.

3. Інформаційні ресурси та їх властивості.

4. Рівні захисту інформації: локальний, мережевий, на рівні користувачів.

5. Корпоративні інформаційні системи (КІС).

***Складіть таблицю:***

|  |  |
| --- | --- |
| Джерела конфіденційної інформації | Характеристика джерел |
| 1. Люди |  |

***Тематика рефератів:***

1.Інформаційна система як об’єкт захисту.

2. Характерні ознаки інформаційних систем.

3. Рівні захисту інформаційних систем.

4. Основні види експлуатації інформаційних систем.

5. Європейські критерії безпеки інформаційних технологій.

6. Канадські критерії безпеки комп’ютерних систем.

7. Основні положення загальних критерії безпеки інформаційних технологій.

8. Функціональні вимоги до засобів захисту.

9. Загальні вимоги та структуру гарантій безпеки.

10. Загальні вразливості корпоративних інформаційних систем

**Питання для самоконтролю.**

1. Які існують категорії джерел конфіденційної інформації?

2. Які складові має інформаційна система?

3. Розкрийте поняття «цілісність».

4. Розкрийте поняття «доступність».

5. Розкрийте поняття конфіденційності інформації.

6. Назвіть основні напрями забезпечення безпеки інформації.

7. Розкрийте зміст моделі системи захисту інформації.

8. Якими показниками може бути оцінено якість розподілу доступу?

9. Назвіть основні принципи та рівні захисту інформаційних систем.

10. Розкрийте поняття інформаційно-комунікаційної системи.

11. Назвіть рівні інформаційно-комунікаційних мереж.

12. Сутність випадкового методу доступу до ресурсів системи.

13. Основні завдання захисту інформації в мережі?

14. Різновиди побудови комп’ютерних мереж?

15. Що повинні включати угоди обміну програмним забезпеченням?

16.Назвіть заходи управління обробкою й зберіганням інформації.

***Рекомендована література:***

1. 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>

2. 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>

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

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

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

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

**Тема 11. Забезпечення інформаційної безпеки України (2год.)**

***Мета:*** вивчення основних складових та політики забезпечення інформаційної безпеки України.

***Основні завдання:*** формування знань щодо національної безпеки країни; розумінні її сутності та структури; визначення основних принципів національної безпеки; дослідження зовнішніх та внутрішніх загроз інформаційної безпеки; розуміння мети та завдань інформаційної безпеки.

**План**

1. Національна безпека та її структура.

2. Принципи забезпечення національної безпеки.

3. Загрози інформаційної безпеки: зовнішні та внутрішні загрози.

4. Сутність інформаційної безпеки. Мета та завдання забезпечення інформаційної безпеки України.

***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 в 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

13. Дудикевич В. Б., Опірський І. Р., Гаранюк П. І., Зачепило В. С., Партика А. І. Забезпечення інформаційної безпеки держави: навч. посіб. Львів: Видавництво Львівської політехніки, 2017. 204 с.

14. Ємельянов В. М. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України / В. М. Ємельянов, Г. Л. Бондар // 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 «Книжкова палата України», 2016. 264 с.

16. Інформаційна безпека / За ред. Ю. Я. Бобала та 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) [Текст] : 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.

21. 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. – К., 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. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с.

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

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

***Питання до заліку:***

1. Що розуміється під «інформаційною безпекою України»?

2. Місце інформаційної безпеки в системі національної безпеки України.

3. Основні напрями політики інформаційної безпеки України.

4. Основні завдання у сфері інформаційної безпеки.

5. Сфери прояву реальних та потенційних загроз 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. Завдання України у сфері реалізації інформаційної політики з питань євроінтеграції.

10. Критерії загроз інформації

11. Дайте визначення поняттям «загроза» та «небезпека», їх особливості.

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. Основні підходи до визначення дестабілізуючих факторів.

18. Політичні фактори загроз.

19. Економічні фактори загроз.

20. Організаційно-технічні фактори загроз.

21. Джерела загроз інформаційній безпеці особи та їх характеристика.

22. Джерела загроз інформаційній безпеці суспільству.

23. Джерела загроз інформаційній безпеці держави.

24. Охарактеризуйте етапи розвитку засобів інформаційних комунікацій.

25. Джерела конфіденційної інформації та їх категорії.

26. Складові інформаційної системи.

27. Конфіденційність інформації:поняття та ознаки.

28. Основні напрями забезпечення безпеки інформації.

29. Розкрийте зміст моделі системи захисту інформації.

30. Основні принципи та рівні захисту інформаційних систем.

31. Інформаційно-комунікаційна система та її рівні.

32. Основні завдання захисту інформації в мережі.

33. Різновиди побудови комп’ютерних мереж.

34. Напрями захисту інформації.

35. Структура правових актів, що орієнтовані на правовий захист інформації.

36. Ліцензія як засіб захисту інформації

37. Комерційна таємниця та її захист.

38. Основні організаційні заходи та їх характеристика.

39. Функції служби безпеки підприємства (фірми, організації).

40. Завдання служби безпеки підприємства (фірми, організації).

41. Інженерно-технічний захист, його завдання.

42. Фізичні засоби захисту та їх завдання.

43. Апаратні засоби захисту інформації.

44. Криптографія, її сутність та завдання.

45. Переваги цифрового шифрування.

46. Джерела та фактори загрози інформації.

47. Види загроз комп’ютерної інформації.

48. Класифікація вразливостей безпеці інформації.

49. Класи (види) загроз в інформаційній сфері.

50. Мета та цілі порушників об’єктів інформаційної діяльності.

51. Класифікація порушників за характером дій.

52. Інформаційна боротьба та її мета.

53. Принципи інформаційної боротьби.

54. Заходи інформаційної боротьби.

55. Форми та способи ведення інформаційної боротьби.

56. Інформаційна зброя та сфера її застосування.

57. Основні об’єкти застосування інформаційної зброї.

58. Види інформаційної зброї.

59. Охарактеризуйте засоби несанкціонованого доступу.

60. Особливості застосування інформаційної зброї.

61. Інформаційне протиборство та рівні його проведення.

62. Основні ступені інформаційного протиборства.

63. Органи інформаційної війни.

64. Основні форми інформаційної війни.

65. Забезпечення інформаційної безпеки держави: поняття та принципи.

66. Адекватна інформованість, її значення.

67. Інформаційний патронат, сутність та значення.

68. Інформаційна кооперація: поняття та сутність.

69. Інформаційне протиборство.

70. Способи та методи забезпечення інформаційної безпеки конкретної особи.

71. Рівні сфери інформаційної безпеки.

72. Групи загроз інформації, критерії їх виділення.

73. Визначте види загроз за ймовірністю реалізації.

74. Визначте види загроз за джерелами походження.

75. Визначте види загроз за значенням.

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

77. Визначте види загроз за характером реалізації.

78. Основні підходи до визначення дестабілізуючих факторів.

79. Політичні фактори загроз.

80. Визначте економічні фактори загроз.

81. Визначте організаційно-технічні фактори загроз.

82. Джерела загроз інформаційній безпеці особи та їх характеристика.

83. Джерела загроз інформаційній безпеці суспільству.

84. Джерела загроз інформаційній безпеці держави.

85. Етапи розвитку засобів інформаційних комунікацій.

86. Кіберборотьба, її основні особливості.

87. Кібернетична безпека: поняття та істотні ознаки.

88. Охарактеризуйте причини головних проблем забезпечення кібернетичної безпеки.

89. Які стратегії затверджені в Законі України «Про національну безпеку України»? Надайте їх характеристику.

90. Охарактеризуйте стратегію воєнної безпеки України.

91. Охарактеризуйте стратегію кібербезпеки України.

92. Стратегія громадської безпеки та цивільного захисту України.

93. Інформаційна безпека та її ознаки.

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

95. Об’єкти, суб’єкти та види інформаційної безпеки.

96. Інформація: поняття та види.

97. Джерела та носії інформації.

98. Законодавче забезпечення захисту інформації та інформаційних ресурсів.

99. Інформаційні ресурси: поняття та види

100. Загрози інформаційній безпеці людині, державі, суспільству.