МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Л.В. Перевалова, І.В. Лисенко, Г. М. Гаряєва

МЕТОДИЧНІ ВКАЗІВКИ

до практичних занять з навчального курсу
«Нормативно-правове забезпечення інформаційної безпеки
у національному та міжнародному співробітництві»
для студентів денної форми навчання, які навчаються за спеціальністю
035.10 «Філологія (прикладна та комп'ютерна лінгвістика)»

Затверджено
редакційно-видавничою
радою НТУ «ХПІ»,
протокол № 2 від 28.06. 2023 р.

Харків
НТУ «ХПІ»
2023

Методичні вказівки до практичних занять з навчального курсу «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» / уклад.: Л. В. Перевалова, І. В. Лисенко, Г. М. Гаряєва. – Харків: НТУ «ХПІ», 2023. – 48 с.

Укладачі: Л. В. Перевалова, І. В. Лисенко, Г. М. Гаряєва

Рецензент Н. В. Бабкова, кандидат технічних наук, доцент кафедри інтелектуальних комп’ютерних систем Національний технічний університет «Харківський політехнічний інститут»

Кафедра права

ВСТУП

На сучасному етапі розвитку людської цивілізації інформація стає стратегічно важливим ресурсом, від ефективного використання якого залежить безпека держави й перспективи формування та подальшого розвитку демократичного суспільства. Одночасно зі зростанням ролі інформації підвищується й важливість її захисту, яка забезпечується шляхом застосування інструментів інформаційної безпеки, що набуває особливої актуальності в умовах війни. Захист інформації є надзвичайно важливою складовою національної безпеки держави. Інформаційна безпека є складним, системним, багаторівневим явищем, на стан і перспективи розвитку якого мають безпосередній вплив зовнішні та внутрішні чинники, такі як політична обстановка у світі та внутрішньополітична обстановка в державі; наявність потенційних зовнішніх і внутрішніх загроз; стан і рівень інформаційно-комунікаційного розвитку країни.

Забезпечення інформаційної безпеки сприяє забезпеченню досягнення успіху при вирішенні завдань у політичній, військово-політичній, військовій, соціальній, економічній та інших сферах державної діяльності. Інформаційна безпека становить на меті забезпечення безпеки особистості, держави і суспільства в цілому.

Метою вивчення дисципліни «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» є:

• сприяння засвоєнню правових знань, формування вмінь і навичок застосовувати здобуті знання у професійної діяльності;

• формування у майбутніх фахівців розуміння сутності явища інформаційна безпека;

• ознайомлення з основними загрозами інформаційній безпеці та вироблення уявлення про ефективність інструментів забезпечення інформаційної безпеки особистості, держави, суспільства.

У результаті вивчення навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки у національному та міжнародному співробітництві» студенти повинні знати та аналізувати:

• міжнародні нормативно-правові документи щодо забезпечення інформаційної безпеки;

• чинне законодавство України в сфері інформаційної безпеки.

Уміти:

• орієнтуватись у системі джерел законодавства України та міжнародно-правового регулювання;

• аналізувати, узагальнювати та застосовувати норми права України у практичній діяльності, роз'яснювати їх зміст;

• складати та оформлювати документи юридичного характеру;

• добирати літературу з теми заняття, складати конспекти і тези виступів, знаходити правову інформацію;

• керуватись у практичній діяльності та поведінці правовими знаннями і переконаннями.

Плани практичних занять містять питання до занять та практичні завдання: складання термінологічного словника, тестові завдання, тематику рефератів, задачі та питання для самоконтролю.

При підготовці до практичних занять студент повинен ознайомитися з лекційним матеріалом, законодавчими актами, рекомендованою літературою.

Складання словника повинно слугувати засвоєнню понятійного апарату навчального курсу «Правове регулювання професійної діяльності психолога». 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. Залежно від складності та обсягу роботи над конкретним завданням пропонується одна або декілька задач кожному студентові, або групі студентів (2-5 осіб). 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 навчально-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.

У результаті вивчення рекомендованої, а також іншої літератури студент повинен підготувати вичерпні відповіді на всі питання практичного заняття.

Виступаючи на занятті, студент має чітко характеризувати обговорюване питання теми, прагнути стислості і логічності викладу. При цьому він може користуватися своїм конспектом, але не зачитувати його замість свого усного виступу, а використовувати лише як план підготовки до семінару.

Практичне заняття закінчується висновком викладача, який підводить підсумки, аналізує виступи, доповіді студентів.

ПРОГРАММА НАВЧАЛЬНОГО КУРСУ

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

Тема 1. Поняття інформаційної безпеки держави, суспільства та особи

Інформаційна безпека (поняття і визначення). Правове забезпечення інформації та інформаційної безпеки. Інформація та види інформації. Інформаційні відносини. Інформаційний суверенітет. Інформаційна безпека, її сутність. Види інформаційної безпеки. Інтереси особи, суспільства та держави в інформаційній сфері. Інформаційна сфера та інтереси особи, держави та суспільства.

Тема 2. Інформаційна безпека та кібербезпека

Кіберпростір: поняття та склад. Проблеми забезпечення інформаційної та кібербезпеки. Стратегії забезпечення національної безпеки держави. Закон України «Про національну безпеку». Кіберпростір та його співвідношення з інформаційною безпекою. Кібербезпека склад та сутність. Стратегія забезпечення національної безпеки. Фундаментальні національні інтереси України.

Тема 3. Загрози для інформаційної безпеки держави, суспільства, людини

Інформаційна безпека держави та життєво важливі інтереси особистості, суспільства та держави. Об'єкти та суб'єкти інформаційної безпеки. Концепція інформаційної безпеки. Поняття загроз інформаційній безпеці. Види загроз інформаційній безпеці та їх джерела. Фактори загроз інформаційній безпеці. Класифікація видів загроз інформаційній безпеці України. Внутрішні та зовнішні джерела загроз інформаційній безпеці України. Принципи забезпечення інформаційної безпеки. Система забезпечення інформаційної безпеки держави. Основні форми і способи забезпечення інформаційної безпеки держави.

Тема 4. Принципи, форми та методи забезпечення інформаційної безпеки держави

Основні та специфічні принципи забезпечення інформаційної безпеки держави. Основні форми забезпечення інформаційної безпеки держави: інформаційний патронат, інформаційна кооперація, інформаційне протиборство. Методи забезпечення інформаційної безпеки.

Тема 5. Інформаційне протиборство між країнами. Інформаційна війна

Інформаційне протиборство та його види. Об'єкти впливу інформаційного протиборства. Концепція інформаційного протиборства. Ступені інформаційного протиборства. Основні форми інформаційного протиборства. Інформаційна війна та її завдання. Особливості інформаційної війни. Концепція інформаційної війни. Органи інформаційної війни. Основні форми та рівні інформаційної війни. Засоби інформаційної війни. Інформаційні переваги у сфері інформаційного протиборства.

Тема 6. Інформаційна зброя в інформаційні війні

Інформаційна зброя та сфера її застосування. Основні об'єкти застосування інформаційної зброї. Види інформаційної зброї. Інформаційна зброя воєнного та невоєнного застосування. Особливості застосування інформаційної зброї. Засоби ураження комп'ютерних інформаційних систем. Програми з потенційно небезпечними наслідками.

Тема 7. Основи теорії інформаційної боротьби

Поняття теорії інформаційної боротьби та її мета. Зміст теорії інформаційної боротьби. Загальні основи теорії інформаційної боротьби та її структура. Теорія сил та засобів ураження інформації. Теорія захисту інформації. Фактори впливу: економічний, воєнний та інформаційний. Закони та закономірності інформаційної боротьби. Принципи інформаційної боротьби. Заходи інформаційної боротьби: інформаційне

забезпечення, інформаційний захист, інформаційна протидія. Способи та форми інформаційної боротьби.

Тема 8. Основи безпеки інформаційних ресурсів

Поняття та загальні властивості інформації. Одержувачі інформації. Поняття загроз. Загрози безпеки інформації та інформаційних ресурсів. Джерела загроз безпеці інформації. Класифікація вразливостей безпеки. Моделі порушень інформаційних ресурсів. Порушники, цілі та мета їх дій.

Тема 9. Забезпечення безпеки інформації та інформаційних ресурсів

Напрями захисту інформації. Правовий захист: конституційне законодавство, загальні та спеціальні закони, підзаконні акти. Спеціальне законодавство та його значення для забезпечення інформаційної безпеки. Страхове забезпечення та його мета. Ліцензія як засіб забезпечення безпеки інформації. Комерційна таємниця. Забезпечення захисту та безпеки інформації на підприємстві. Особливості захисту комп'ютерних систем. Служба захисту інформації. Організаційний захист та його заходи. Інженерно-технічний захист та його засоби.

Тема 10. Захист інформаційних систем

Джерела інформації. Люди як джерела інформації. Конфіденційна інформація: поняття та джерела. Інформаційна система як об'єкт захисту. Структура інформаційної системи. Рівні захисту інформаційних систем: локальний, мережевий, на рівні користувачів. Основні принципи захисту інформаційних систем. Інформаційні ресурси та їх властивості. Корпоративні інформаційні системи (КІС).

Тема 11. Інформаційна безпека України

Національна безпека та її структура. Принципи забезпечення національної безпеки. Інформаційна безпека та її місце в національній безпеці України. Сутність інформаційної безпеки. Мета та завдання забезпечення інформаційної безпеки України. Основні реальні та потенційні загрози інформаційній безпеці України. Загрози інформаційної

безпеки: зовнішні та внутрішні загрози. Стан та перспективи розвитку інформаційної безпеки. Система та політика забезпечення інформаційної безпеки.

ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

Тема 1. Поняття інформаційної безпеки держави, суспільства та особи

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.

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

Мета: визначення основних понять загроза та небезпека інформаційної системи.

Основні завдання: визначення основних життєво важливих інтересів держави у 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. Інформаційна безпека 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.

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

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.

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

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.

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

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.

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 IT-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

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

Основні завдання: формування знань щодо національної безпеки країни; розуміння 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.

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?

ВАРІАНТИ КОНТРОЛЬНИХ РОБІТ

та вимоги до їх виконання

для студентів заочної форми навчання

Навчальний процес для студентів заочної форми навчання в НТУ «ХПІ» організовано відповідно до діючого законодавства і здійснюється як під час сесій, так і в міжсесійний період. Сесії для студентів заочної форми

навчання проходять двічі у навчальному році, протягом яких проводяться лекції, практичні заняття, консультації, іспити та заліки.

Лекції, які проводяться викладачами кафедри права, мають концептуальний, узагальнюючий та оглядовий характер. Практичні заняття проводяться за основними темами курсу, які виносяться на самостійне вивчення студентами.

У період між сесіями студенти працюють над засвоєнням навчального матеріалу як самостійно, так і під керівництвом викладача.

Основною формою роботи студента-заочника над засвоєнням навчального матеріалу є виконання ним індивідуальних завдань. Кожний навчальний курс, що викладається кафедрою права, містить тематику контрольних робіт, які студент виконує самостійно під керівництвом викладача.

Контрольна робота займає важливе місце у навчальному процесі, її основна мета – з'ясування студентами теоретичних положень, надбання ними навичок самостійної роботи із законодавчими актами, навчальною і науковою літературою, уміння застосовувати отримані знання для вирішення конкретних практичних ситуацій.

Контрольна робота складається з декількох завдань, які мають теоретичний та практичних характер. Кожне теоретичне завдання вимагає всебічної відповіді, що досягається за допомогою ретельного вивчення рекомендованих законодавчих актів, наукової та навчальної літератури. Практичне завдання складається з юридичної ситуації, яка повинна бути розв'язана за допомогою нормативно-правових актів, з обов'язковим посиланням на конкретні статті.

Завершується контрольна робота списком джерел, які використовувались при написанні роботи. Нормативні документи, навчально-методичні матеріали та інші джерела, які використовуються у контрольній роботі, повинні бути зазначені відповідно до загальних вимог.

Контрольна робота перевіряється викладачем і зараховується за результатами співбесіди викладача зі студентом.

Контрольна робота має бути здана на рецензію викладачеві не пізніше ніж за місяць до початку сесії. Після перевірки викладачем контрольна робота зараховується або повертається студенту з зауваженнями. Студент повинен усунути усі зауваження до іспиту або заліку, обговорити з рецензентом дискусійні питання.

Студенти, що несвоєчасно здали контрольні роботи, до сесії не допускають; незараховані роботи є підставою для недопущення до іспиту, заліку.

Для студентів, що навчаються за заочною формою, у міжсесійний період викладачами кафедри проводяться консультації, графік проведення яких розміщується на сайті кафедри.

Студенти заочної форми навчання допускаються до участі у сесії, якщо вони не мають заборгованості за попередній курс (семестр) і до початку сесії виконали всі контрольні роботи та індивідуальні завдання з дисциплін, що виносяться на сесію.

ВИМОГИ ДО ЗМІСТУ КОНТРОЛЬНОЇ РОБОТИ

Контрольна робота повинна містити наступні складові частини:

Титульна сторінка. Лист повинен містити: назву міністерства, назву університету, назву кафедри; назву навчальної дисципліни; варіант, прізвище та ініціали студента, курс, номер академічної групи; посаду, прізвище та ініціали викладача (додаток А).

Зміст повинен відтворювати питання варіанту контрольної роботи, практичну ситуацію (якщо вона передбачається), із обов’язковим зазначенням номерів сторінок, на яких вони розміщені (додаток Б).

Вступ. У «Вступі» студент розкриває сутність і стан наукової проблеми, її актуальність, обґрунтовує необхідність проведення дослідження, мету написання роботи та завдання щодо її досягнення.

Теоретична частина містить відповіді на перше та друге питання та включає характеристику сучасного стану проблеми (відповідає обраній темі), опис нормативної бази, погляди різних авторів на проблему, визначає її позитивні і негативні наслідки. Також під час обґрунтування необхідно застосувати інформацію щодо конкретних нормативних актів (юридичні довідники, періодичні видання). Результати вивчення літературних джерел повинні бути представлені, як правило, не в формі механічного копіювання вибраних текстів, а у вигляді узагальнення та аналізу різних точок зору (якщо такі є) і підходів до досліджуваного питання. При цитуванні обов'язковим є посилання на джерело, яке оформлюється квадратними дужками, наприклад [1, с. 13], де 1 – це номер джерела у списку літератури, с. 13 – сторінка, де взята цитата або матеріал.

Практична частина – це конкретна практична ситуація, яку необхідно розв'язати з обов'язковим посиланням на законодавчі акти, вказати статті, за допомогою яких можливо розв'язати практичне завдання, надати пояснення до них.

Висновки. У висновках викладаються обґрунтовані результати, отримані студентом у процесі досягнення мети роботи, можливо, перелік пропозицій та рекомендацій.

Список літератури. Джерела розміщують у списку в алфавітному порядку прізвищ перших авторів або заголовків. Відомості про джерела, включені до списку, необхідно надавати відповідно до вимог державного стандарту з обов'язковими посиланнями на них у роботі.

Обсяг контрольної роботи повинен становити в друкованому варіанті 20–25 сторінок.

ОФОРМЛЕННЯ КОНТРОЛЬНОЇ РОБОТИ

Номер варіанту контрольної роботи студент вибирає за останнім номером залікової книжки або за номером прізвища у журналі групи.

Текст контрольної роботи викладається державною мовою. Приступаючи до виконання контрольної роботи, слід підібрати матеріал, який буде покладено в її основу.

Контрольна робота повинна складатися зі вступу, двох теоретичних питань, практичної частини, висновків, списку використаної літератури.

Кожне питання контрольної роботи оформляється з нової сторінки. Назви питань друкуються великими літерами по центру сторінки. Кожне питання повинне бути обсягом близько 5–10 аркушів комп'ютерного набору, повно висвітлювати тему, з обов'язковим залученням діючого законодавства України, навчальної та наукової літератури.

Контрольна робота редагується і подається не пізніше залікового тижня в наступному вигляді:

– друкується з одного боку аркуша паперу. Папір формату А 4 (210х297 мм). Шрифт – Times New Roman, кг 14, міжрядковий інтервал 1; поля: ліве – 2,5 см, верхнє – 2,0 см, праве – 1,0 см, нижнє – 2,0 см;

– таблиці і малюнки необхідно розміщати після першого посилання на них у тексті, нумерувати згідно з питанням роботи подвійною нумерацією (наприклад – Таблиця 2.1). Слово «Таблиця» форматується по правій стороні напівжирним шрифтом. На рядок нижче по центру пишеться назва таблиці звичайним шрифтом. Слово «Мал.» форматується по центру напівжирним шрифтом. Відразу після нумерації малюнка з великої літери звичайним шрифтом пишеться його назва.

Послідовність розташування листів у контрольній роботі:

• Титульна сторінка;

• Зміст;

• Вступ;

• Питання роботи;

• Висновки;

• Список використаних джерел.

До загального обсягу роботи не входять додатки, список використаної літератури, таблиці та малюнки, які повністю займають площу сторінки. Але всі сторінки зазначених елементів підлягають суцільній нумерації. Робота має бути акуратно надрукована з дотриманням стилістичних і граматичних норм. У тексті обов'язково повинні бути посилання на літературу та інші джерела, що використовувалися при підготовці контрольної роботи.

Нумерація сторінок має бути наскрізною. Порядковий номер сторінки позначають арабською цифрою і проставляють у правому верхньому куті сторінки без крапки чи рисок. Титульний аркуш (додається) включається до загальної нумерації сторінок контрольної роботи, але номер сторінки на титульному аркуші, як правило, не проставляють.

Ілюстративний матеріал – малюнки, графіки, схеми тощо слід розміщувати безпосередньо після першого посилання на нього у тексті. Якщо графік, схема, таблиця не вміщується на сторінці, де є посилання, їх подають на наступній сторінці. На кожний ілюстративний матеріал мають бути посилання в тексті.

КРИТЕРІЇ ОЦІНЮВАННЯ КОНТРОЛЬНОЇ РОБОТИ

Кожна контрольна робота оцінюється, виходячи з аналізу сукупності таких критеріїв:

1. Актуальність матеріалу теми (питання).

2. Зміст питання має системно розкривати обрану тему.

ВАРІАНТИ КОНТРОЛЬНИХ РОБІТ

для студентів заочної форми навчання

з навчальної дисципліни

«Нормативно-правове забезпечення інформаційної безпеки

У національному та міжнародному співробітництві»

ВАРІАНТ 1

1. Визначте що розуміється під «інформаційною безпекою України»?

2. Надайте характеристику суб'єктів інформаційної безпеки.

3. Проаналізуйте форми та способи ведення інформаційної боротьби.

ВАРІАНТ 2

1. Визначте місце інформаційної безпеки в системі національної безпеки України.

2. Охарактеризуйте інформаційно-комунікаційну систему та її рівні.

3. Проаналізуйте сучасні рівні інформаційного протиборства.

ВАРІАНТ 3

1. Визначте основні напрями політики інформаційної безпеки України.

2. Охарактеризуйте основні завдання захисту інформації в мережі.

3. Надайте оцінку органам інформаційної війни.

ВАРІАНТ 4

1. Охарактеризуйте сфери прояву реальних та потенційних загроз безпеці України.

2. Проаналізуйте напрями захисту інформації.

3. Визначте основні форми інформаційної війни.

ВАРІАНТ 5

1. Проаналізуйте основні завдання України у сфері реалізації інформаційної політики з питань євроінтеграції.

2. Визначте, у чому полягає зміст інженерно-технічного захисту інформації та інформаційних ресурсів.

3. Розкрийте поняття та істотні ознаки кібернетичної безпеки.

ВАРІАНТ 6

1. Визначте ліцензію як засіб захисту інформації.

2. Проаналізуйте завдання України у сфері реалізації інформаційної політики з питань євроінтеграції.

3. Охарактеризуйте основні принципи забезпечення інформаційної безпеки.

ВАРІАНТ 7

1. Визначте критерії загроз інформації.

2. Охарактеризуйте способи та методи забезпечення інформаційної безпеки конкретної особи.

3. Визначте поняття комерційної таємниці та способи її захисту.

ВАРІАНТ 8

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

2. Обґрунтуйте завдання та функції служби безпеки підприємства.

3. Проаналізуйте основні організаційні заходи та дайте їх характеристики.

ВАРІАНТ 9

1. Охарактеризуйте види загроз інформаційної безпеки.

2. Визначте порядок визнання громадянина безвісно відсутнім.

3. Охарактеризуйте основні підходи до визначення дестабілізуючих факторів.

ВАРІАНТ 10

1. Проаналізуйте джерела загроз інформаційній безпеці особи та дайте їх характеристики.

2. Визначте завдання інженерно-технічного захисту інформації.

3. Розкрийте, в чому полягають основні особливості кіберборотьби.

ВАРІАНТ 11

1. Проаналізуйте джерела загроз інформаційній безпеці суспільству.

2. Дайте визначення кібернетичної безпеки та вкажіть її істотні ознаки.

3. Охарактеризуйте основні завдання правового захисту інформації.

ВАРІАНТ 12

1. Надайте характеристику Конституції України та конституційного законодавства щодо захисту інформації.

2. Визначте основні напрями забезпечення безпеки інформації.

3. Охарактеризуйте причини головних проблем забезпечення кібернетичної безпеки.

ВАРІАНТ 13

1. Визначте джерела загроз інформаційній безпеці держави.

2. Охарактеризуйте стратегії, які затверджені у Законі України «Про національну безпеку України».

3. Виділить фізичні засоби захисту та розкрийте їх завдання.

ВАРІАНТ 14

1. Дайте оцінку класифікації вразливостей безпеки інформації.

2. Визначте основні завдання захисту інформації в мережі.

3. Розкрийте способи та методи забезпечення інформаційної безпеки конкретної особи.

ВАРІАНТ 15

1. Проаналізуйте джерела та фактори загрози інформації.

2. Дайте визначення інформаційно-комунікаційної системи та охарактеризуйте її рівні.

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

ВАРІАНТ 16

1. Охарактеризуйте загрози інформаційній безпеці України у воєнній сфері.

2. Визначте джерела та носії інформації.

3. Проаналізуйте переваги цифрового шифрування.

ВАРІАНТ 17

1. Охарактеризуйте види загроз комп’ютерної інформації.

2. Надайте характеристику законодавству, яке забезпечує захист інформації та інформаційних ресурсів.

3. Розкрийте зміст моделі системи захисту інформації.

ВАРІАНТ 18

1. Дайте оцінку видам інформації.

2. Охарактеризуйте різновиди побудови комп'ютерних мереж.

3. Розкрийте поняття інформаційних ресурсів.

ВАРІАНТ 19

1. Проаналізуйте види інформаційних ресурсів.

2. Охарактеризуйте загрози інформаційній безпеці України в економічній сфері.

3. Визначте поняття інформації.

ВАРІАНТ 20

1. Проаналізуйте завдання України у сфері реалізації інформаційної політики з питань євроінтеграції.

2. Визначте організаційно-технічні фактори загроз.

3. Охарактеризуйте причини головних проблем забезпечення кібернетичної безпеки.

ВАРІАНТ 21

1. Охарактеризуйте засоби несанкціонованого доступу.

2. Розкрийте політичні фактори загроз.

3. Визначте групи загроз інформації та критерії їх виділення.

ВАРІАНТ 22

1. Охарактеризуйте загрози інформаційній безпеці України в екологічній сфері.

2. Визначте економічні фактори загроз.

3. У чому полягає мета та цілі порушників об'єктів інформаційної діяльності.

ВАРІАНТ 23

1. Визначте методи правового регулювання інформаційних відносин.

2. Дайте характеристику видам інформаційної зброї.

3. Проаналізуйте основні напрями політики інформаційної безпеки України.

ВАРІАНТ 24

1. Дайте характеристику підзаконним актам, які регулюють забезпечення інформаційної безпеки.

2. Визначте поняття "місце інформаційної безпеки" в системі національної безпеки України.

3. Охарактеризуйте основні об'єкти застосування інформаційної зброї.

ВАРІАНТ 25

1. Надайте класифікацію порушників за характером їх дій.

2. Розкрийте сутність та значення інформаційного патронату.

3. Охарактеризуйте основні підходи до визначення дестабілізуючих факторів.

ВАРІАНТ 26

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

2. Розкрийте сутність та значення адекватної інформованості.

3. Охарактеризуйте основні особливості кіберборотьби.

ВАРІАНТ 27

1. Які види адміністративних стягнень встановлені законодавством за порушення права на інформацію.

2. Проаналізуйте сутність інформаційної кооперації.

3. Дайте визначення кіберборотьби та розкрийте її сутність.

ВАРІАНТ 28

1. Дайте визначення поняття та ознаки кримінального злочину в сфері інформаційної безпеки.

2. Охарактеризуйте апаратні засоби захисту інформації.

3. Розкрийте принципи інформаційної боротьби.

ВАРІАНТ 29

1. Проаналізуйте об’єкти інформаційної безпеки.

2. Які види кримінальної відповідальності встановлені ККУ за порушення інформаційної безпеки.

3. Охарактеризуйте заходи інформаційної боротьби.

ВАРІАНТ 30

1. Надайте характеристику суб’єктам інформаційної безпеки.

2. Проаналізуйте фізичні засоби захисту інформації та їх завдання.

3. Охарактеризуйте стратегію кібербезпеки України.

ДОДАТОК А

Зразок титульного аркуша

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра права

Контрольна робота

з дисципліни «----------»

Варіант__

Виконав (-ла) студент (-ка)
__курсу, групи -____за
Прізвище, ім'я, по батькові
Перевірив: доцент, ПІП

Харків 2023

ДОДАТОК Б

ЗМІСТ

ДОДАТОК В

Приклади бібліографічного опису джерел інформації

В.1. Опис джерел інформації складається з елементів, що становлять відомості про нього.

В.1.1. Відомості про книги повинні включати: прізвище (у називному відмінку) і ініціали автора; заголовок книги; призначення книги; найменування установи, що опублікувала книгу; місце видання; видавництво; рік видання; загальний обсяг у сторінках.

В.1.2. Відомості про частину добутку (наприклад, стаття в збірнику) повинні включати прізвище, ініціали автора та заголовок складової частини. Далі йдуть відомості про добуток: ініціали та прізвище автора; заголовок добутку, у якому поміщена складова частина; місце видання; видавництво; рік видання; сторінки, на яких поміщена складова частина.

Питання до заліку

з навчальної дисципліни

«Нормативно-правове забезпечення інформаційної безпеки

в національному та міжнародному співробітництві»

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 безпеки 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.

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-IV. [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. С. 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 «Книжкова 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. Почепцов, Г. Виртуальные войны. Фейки. Харьков : Фолио, 2019. 506 с.

29. Почепцов Г. Сучасні інформаційні війни. Київ : 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.

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.

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

ЗМІСТ

Навчальне видання

Методичні вказівки

до практичних занять з навчального курсу
«Нормативно-правове забезпечення інформаційної безпеки
у національному та міжнародному співробітництві»
для студентів денної форми навчання,

які навчаються за спеціальністю 035.10
«Філологія (прикладна та комп'ютерна лінгвістика)»

Укладачі:

ПЕРЕВАЛОВА Людмила Вікторівна

ЛИСЕНКО Ірина В'ячеславівна

ГАРЯЄВА Ганна Михайлівна

Роботу рекомендував до друку А. В. Кипенський

В авторській редакції

План 2023 р., поз. 598

Підп. до друку 21.11.2023. Формат 60x84 1/16.
Папір офсетний. Друк цифровий. Гарнітура Times New Roman.
Ум. друк. арк. 2,79. Наклад 150 прим. Зам. № 2/11/23.
Ціна договірна

Видавець Видавничий центр НТУ «ХПІ».

Свідоцтво про державну реєстрацію ДК № 5478 від 21.08.2017 р.

61002, Харків, вул. Кирпичова, 2