

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Запорізький національний технічний університет

Методичні вказівки

до практичних занять з дисципліни "Правові основи захисту інформації" для студентів спеціальностей: 6.170102 "Системи технічного захисту інформації", 6.170101 "Безпека інформаційних та комунікаційних систем" всіх форм навчання

2009

Методичні вказівки до практичних занять з дисципліни "Правові основи захисту інформації" для студентів спеціальностей: 6.170102 "Системи технічного захисту інформації ", 6.170101 "Безпека інформаційних та комунікаційних систем" всіх форм навчання. / В.І. Слепцов - Запоріжжя: ЗНТУ, 2009. - 28 с.

Укладач: ст. викладач В.І. Слепцов

Рецензент: д.ф.м.н., проф. Л.М. Карпуков

Відповідальний за випуск: ст. викладач В.І. Слепцов

Затверджено
на засіданні кафедри
захисту інформації
Протокол № 8
від 18.03. 2009 р.

ПРАКТИЧНЕ ЗАНЯТТЯ № 1

ТЕМА : "ІНФОРМАЦІЙНЕ ПРАВО ТА ІНФОРМАЦІЙНІ СТОСУНКИ"

Дані питання

1. Поняття інформаційного права.
2. Інформаційне право в широкому і вузькому сенсі.
3. Джерела інформаційного права.
4. Інформаційні стосунки, види суб'єктів інформаційних стосунків.
5. Особливості та юридичні властивості інформації.
6. Законодавчий рівень забезпечення інформаційної безпеки.
7. Конституція України - як основне джерело права в області забезпечення інформаційної безпеки.
8. Застосування норм права у сфері захисту інформації.
9. Завдання та функції Державної служби спеціального зв'язку та захисту інформації України.
10. Види відповідальності за здійснення правопорушень в інформаційній сфері.

Контрольні питання

1. Визначите поняття інформаційного права та його місце в системі правового регулювання суспільних стосунків в Україні.
2. Назвіть та охарактеризуйте з погляду їх значущості джерела інформаційного права.
3. Поясніть необхідність правової регуляції суспільних стосунків в інформаційній сфері.
4. Що таке інформаційні стосунки? Чи завжди їх слід регулювати на основі права?
5. Що служить основою правового регулювання інформаційних стосунків?
6. Назвіть види реальних суб'єктів інформаційних стосунків.
7. Чому необхідно захищати інформацію?

8. Приведіть основні положення Конституції України, що стосуються інформаційних стосунків. Охарактеризуйте роль Конституції в правовому регулюванні суспільних стосунків у сфері захисту інтересів суб'єктів інформаційних стосунків.
9. З чого складається система нормативних правових актів України в області захисту інформації? Назвіть основні законодавчі акти в цій сфері.
10. Які завдання вирішує Державна служба спеціального зв'язку та захисту інформації?
11. Як диференціюється відповідальність за здійснення правопорушень в інформаційній сфері відповідно до законодавства України?

Практичне завдання

Складіть перелік видів інформаційних стосунків, що регульовані на основі використання норм інформаційного права.

Література, що рекомендується

1. Конституція України
2. Про інформацію: Закон України від 02.10.92 № 2658-12-ВР // ВВР, 1992, № 48, ст.650.
3. Указ Президента України № 836 від 18.09.2002 року "Про заходи щодо забезпечення інформаційної безпеки держави".
4. Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін. Основи інформаційного права України.: Навч. посіб./ О-72. - К.: Знання, 2004. - 274 с.
5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-Москва * Санкт-Петербург * Киев: ООО "ТИД "ДС", 2002.- 688 с.
6. Кримінальний кодекс України.
7. Кодекс України про адміністративні правопорушення.

ПРАКТИЧНЕ ЗАНЯТТЯ № 2

ТЕМА: "ВИДИ ТА ВЛАСТИВОСТІ ІНФОРМАЦІЙНИХ РЕСУРСІВ"

Дані питання

1. Поняття документа та інформаційних ресурсів.
2. Право власності на інформаційні ресурси.
3. Класифікація інформаційних ресурсів.
4. Режим доступу до інформації, класифікація інформації за режимом доступу.
5. Режим доступу до інформації, що належить державі.
6. Умови віднесення інформації, що належить державі, до категорії конфіденційної.
7. Поняття персональних даних, правова основа їх захисту.
8. Відповідальність за здійснення посягань на недоторканність приватного життя.

Контрольні питання

1. Чому необхідною умовою включення інформації в інформаційні ресурси є її документування?
2. Як може формуватися право власності на інформаційні ресурси? Кому можуть належати інформаційні ресурси?
3. По яких ознаках можна класифікувати інформаційні ресурси?
4. Що таке режим доступу до інформації?
5. У чому корінна відмінність конфіденційної інформації від таємниці?
6. Поясніть роль держави в забезпеченні режиму доступу до інформації.
7. Що є підставою для віднесення інформації, що належить фізичним і юридичним особам, до категорії конфіденційної?
8. Яким ознакам повинна відповідати конфіденційна інформація, що належить державі?

9. Які правові основи захисту персональних даних? У чому полягає особливість застосування норм законодавства в цій сфері?

Практичне завдання

Складіть перелік видів інформації, що іменується як "таємниця", і визначите її приналежність до конфіденційної або таємної інформації.

Література, що рекомендується

1. Конституція України
2. Про інформацію: Закон України від 02.10.92 № 2658-12-ВР // ВВР, 1992, № 48, ст.650.
3. Укази Президента України:
№ 836 від 18.09.2002 року "Про заходи щодо забезпечення інформаційної безпеки держави"
№582 від 10.04 2000 року "Про заходи щодо захисту інформаційних ресурсів держави"
4. Цимбалюк В.С., Гавловський В.Д., Гриценко В.В. та ін. Основи інформаційного права України.: Навч. посіб./ О-72. - К.: Знання, 2004. - 274 с.
5. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-Москва * Санкт-Петербург * Киев: ООО "ТИД "ДС", 2002.- 688 с.
6. Кримінальний кодекс України.
7. Кодекс України про адміністративні правопорушення.

ПРАКТИЧНЕ ЗАНЯТТЯ № 3

ТЕМА: "ПРАВОВА ОХОРОНА ДЕРЖАВНИХ СЕКРЕТІВ, КОМЕРЦІЙНОЇ ТА БАНКІВСЬКОЇ ТАЄМНИЦІ"

Дані питання

1. Правові основи захисту державної таємниці в Україні.
2. Поняття грифа секретності, засекречування носіїв інформації, що складає державну таємницю, системи захисту державної таємниці.
3. Порядок віднесення інформації до державної таємниці.
4. Порядок засекречування та розсекречення відомостей, що складають державну таємницю, та їх носіїв.
5. Заходи до охорони державної таємниці.
6. Порядок надання допуску та доступу до відомостей, що становить державну таємницю.
7. Види відповідальності за здійснення правопорушень, пов'язаних з державною таємницею.
8. Загальна характеристика правопорушень, пов'язаних з державною таємницею, передбачених кримінальним кодексом України.
9. Критерії віднесення інформації до категорій "комерційна таємниця" та "банківська таємниця".
10. Правова охорона комерційної та банківської таємниці.
11. Відповідальність за здійснення правопорушень, пов'язаних з комерційною та банківською таємницею.

Контрольні питання

1. Назвіть критерії віднесення інформації до державної таємниці.
2. У яких областях діяльності держави можливе віднесення інформації до державної таємниці?
3. Що може бути носієм відомостей, що складають державну таємницю.
4. Що означає гриф секретності?
5. Які наслідки засекречування відомостей та їх носіїв?
6. З яких елементів складається система захисту державної таємниці?
7. Що означає режим секретності?

8. Що означає процес розсекречування відомостей та їх носіїв?
9. На кого покладається відповідальність за забезпечення режиму секретності?
10. У чому полягає відмінність Зводу відомостей, що складають державну таємницю, від Переліку таких відомостей?
11. Що є підставою для засекречування відомостей, отриманих в результаті практичної діяльності?
12. Які організаційно-правові заходи здійснюються в цілях охорони державної таємниці?
13. Яким вимогам повинен задовольняти суб'єкт господарської діяльності для отримання права здійснювати роботи, що пов'язані з державною таємницею?
14. Яким вимогам повинен задовольняти громадянин для отримання допуску до відомостей, що складають державну таємницю?
15. Які види відповідальності передбачені законодавством за здійснення правопорушень, пов'язаних з державною таємницею?
16. Які дії правопорушників, що пов'язані з державною таємницею, вважаються за злочинні?
17. Дайте визначення комерційної та банківської таємниці.
18. У чому полягає відмінність режимів доступу до відомостей, що складають комерційну та банківську таємницю?
19. Які відомості не можна відносити до комерційної таємниці?
20. Які дії правопорушників, що пов'язані з комерційною таємницею, вважаються за злочинні?

Практичне завдання

Перерахуйте заходи до забезпечення режиму секретності і режиму охорони комерційної таємниці з вказівкою їх відмінностей та збігів.

Література, що рекомендується

1. Закон України "Про державну таємницю".
2. Кримінальний кодекс України.
3. Кодекс України про адміністративні правопорушення.
4. Закон України "Про Службу безпеки України".

5. Постанова КМ України , від 16.02.1997, №180 "Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах"
6. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-Москва * Санкт-Петербург * Киев: ООО "ТИД "ДС", 2002.- 688 с.

ПРАКТИЧНЕ ЗАНЯТТЯ № 4

ТЕМА: "ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ (ІТС)"

Дані питання

1. Захист інформації в ІТС як підінститут інформаційного права, його системообразуючий законодавчий акт.
2. Основні категорії захисту інформації в ІТС, що визначені в законодавстві.
3. Об'єкти захисту в ІТС.
4. Визначення права власності на інформацію, що обробляється в ІТС, з урахуванням вимог законодавства.
5. Право суб'єктів права власності на юридичний захист із застосуванням норм цивільного, адміністративного, трудового та кримінального законодавства.
6. Доступ до інформації в ІТС.
7. Регулювання стосунків між суб'єктами в ІТС.
8. Особливості захисту інформації в ІТС, що є власністю держави, чи інформації обмеженого доступу, вимоги до захисту якої встановлені законодавством, або інформації, що відноситься до державної таємниці.
9. Методи та засоби захисту інформації в ІТС, що визначені законодавством.
10. Загальна характеристика правопорушень, пов'язаних з ІТС, які передбачені кримінальним кодексом України.
11. Нормативно-правова база електронного документообігу.
12. Забезпечення юридичної сили електронних документів.
13. Призначення електронного цифрового підпису (ЕЦП).
14. Правова відмінність ЕЦП від власноручного підпису.
15. Поняття та види сертифікату відкритого ключа ЕЦП.
16. Державна система сертифікації відкритих ключів ЕЦП.

Контрольні питання

1. Визначите місце правового регулювання захисту інформації в ІТС в системі інформаційного права України.
2. Що служить об'єктом регуляції Закону України "Про захист інформації в ІТС"? Дайте поняття захисту інформації згідно цьому законодавчому акту та прокоментуйте його.
3. Дайте визначення основних категорій Закону України "Про захист інформації в ІТС", які розглядаються як об'єкти суспільних інформаційних стосунків. У чому Ви бачите їх недоліки?
4. Приведіть перелік погроз інформаційній безпеці ІТС, виходячи із змісту Закону України "Про захист інформації в ІТС".
5. Що є об'єктом захисту в ІТС згідно законодавству України?
6. У якому порядку здійснюється юридичний захист інтересів суб'єктів права власності на інформацію, що обробляється в ІТС?
7. Охарактеризуйте порядок доступу до інформації в ІТС згідно вимогам законодавства.
8. У чому полягає суть правових стосунків між власником інформації і власником ІТС; між власником інформації та її користувачем?
9. Які вимоги до захисту інформації в ІТС встановлюються законодавцем?
10. Які особливості захисту інформації в ІТС, що є власністю держави, інформації обмеженого доступу, вимоги до захисту якої встановлені законодавством, або інформації, що відноситься до державної таємниці?
11. Які дії правопорушників, що зв'язані з використанням ІТС, вважаються за злочини?
12. Що таке електронний документ і його реквізити?
13. У яких випадках електронний документ не може бути використаний як оригінал?
14. Які можливості надає ЕЦП особі, що одержує електронні повідомлення?
15. У чому полягають системні відмінності ЕЦП від власноручного підпису?
16. Хто відноситься до суб'єктів правових стосунків у сфері використання ЕЦП?
17. У яких випадках засіб ЕЦП відноситься до категорії надійних?

18. У яких випадках можливе використання тільки надійних засобів ЕЦП?
19. У чому полягають основні відмінності у функціях та об'ємі повноважень різних видів центрів сертифікації відкритих ключів?
20. Який орган державної виконавчої влади здійснює контрольні функції у сфері використання ЕЦП?

Практичне завдання

Складіть зразкову схему обробки інформації в локальній ІТС, зіставивши її режим правової охорони окремих процесів обробки.

Література, що рекомендується

1. Закон України "Про захист інформації в ІТС".
2. Закон України "Про державну таємницю".
3. Кримінальний кодекс України.
4. Кодекс України про адміністративні правопорушення.
5. Постанова КМ України, від 16.02.1997, №180 "Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах"
6. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа.
7. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа.
8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-Москва * Санкт-Петербург * Киев: ООО "ТИД "ДС", 2002.- 688 с.
9. Теоретические основы компьютерной безопасности / Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. : Учеб. пособие. -М.: Радио и связь, 2000. - 192 с.
10. Голубев В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / Навчальний посібник. -Запоріжжя: ГУ "ЗІДМУ", 2002. - 297 с.

ПРАКТИЧНЕ ЗАНЯТТЯ № 5

ТЕМА: "ЛІЦЕНЗУВАННЯ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ"

Дані питання

- а) основні положення Закону України "Про ліцензування певних видів господарської діяльності":
- поняття та види господарської діяльності, що підлягають ліцензуванню;
 - юридична значущість наявності ліцензії;
 - повноваження та обов'язки органів ліцензування;
 - розробка, затвердження та обнародування ліцензійних умов;
 - поняття ліцензії, порядок подачі та прийому заяви про видачу ліцензії, її зміст і форма;
 - порядок ухвалення рішення за прийнятою заявою, види рішень;
 - підстави для ухвалення рішення про відмову у видачі ліцензії;
 - здійснення державного нагляду за дотриманням ліцензіатами вимог законодавства.
- б) особливості ліцензування діяльності у сфері захисту інформації:
- правова основа для здійснення господарської діяльності у сфері технічного та криптографічного захисту інформації;
 - система державного ліцензування господарської діяльності у сфері захисту інформації;
 - види робіт у сфері ТЗІ і КЗІ, що підлягають ліцензуванню;
 - характеристика ліцензійних умов;
 - вимоги до суб'єкта господарювання при наділі його правом технічного та криптографічного захисту всіх видів інформації.

Контрольні питання

1. Що розуміється під господарською діяльністю, що підлягає ліцензуванню?
2. Як підрозділяються ліцензійовані види діяльності згідно законодавству?

3. Назвіть органи ліцензування, перерахуйте їх основні права та обов'язки.
4. Що розуміється під ліцензійними умовами і в чому їх значення?
5. Опишіть порядок подачі заяви про видачу ліцензії. Які документи представляє заявник в орган ліцензування?
6. Які існують форми ухвалення рішення органом ліцензування після розгляду заяви претендента?
7. Назвіть терміни дії ліцензій. Який порядок продовження цих термінів?
8. Яким чином і ким здійснюється контроль за дотриманням ліцензіатами ліцензійних умов?
9. Назвіть види відповідальності ліцензіата і відповідні права органу ліцензування.
10. На яких підставах може бути здійснено анулювання ліцензії? Назвіть терміни ухвалення такого рішення і вступу його в законну силу.
11. Які види відповідальності передбачені законодавством України за здійснення господарської діяльності без ліцензії?
12. Охарактеризуйте систему державного ліцензування господарської діяльності у сфері захисту інформації в Україні.
13. Які види робіт у сфері технічного та криптографічного захисту інформації підлягають ліцензуванню? Якими нормативними документами визначений цей перелік?
14. Яким вимогам повинен задовольняти претендент на отримання ліцензії для здійснення господарської діяльності у сфері технічного або криптографічного захисту інформації.
15. Які особливості ліцензійних умов для здійснення господарської діяльності у сфері захисту всіх видів інформації?

Практичне завдання

Складіть схему, що ілюструє порядок отримання ліцензії на право здійснення господарської діяльності у сфері технічного захисту інформації.

Література, що рекомендується

1. Закон України від 01.06.2000 р. № 1775 - 111 "Про ліцензування певних видів господарської діяльності".
2. Наказ ДССЗІ від 12.12.2001 р. № 151/72 "Про затвердження Порядку контролю за додержанням ліцензійних розумів провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації; розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг в галузі технічного захисту інформації".
3. "Ліцензійні умови здійснення господарської діяльності, пов'язаної з розробкою, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації (далі - Ліцензійні умови у галузі ТЗІ)", затверджені наказом Державного комітету України по питаннях регуляторної політики і підприємництва, Департаменту спеціальних телекомунікаційних систем і захисту інформації СБ України від 29.12.2000 N 89/67.
4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-Москва * Санкт-Петербург * Киев: ООО "ТИД "ДС", 2002.- 688 с.

ПРАКТИЧНЕ ЗАНЯТТЯ № 6

ТЕМА: "ПРАВОВІ ОСНОВИ СЕРТИФІКАЦІЇ ЗАСОБІВ ТЕХНІЧНОГО ТА КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ"

Дані питання

1. Поняття процесу і мети сертифікації.
2. Нормативно-правова база сертифікації засобів технічного та криптографічного захисту інформації.
3. Принципи проведення сертифікації.
4. Організаційна структура системи сертифікації засобів ТЗІ і КЗІ;
5. Об'єкти підтвердження відповідності.
6. Розподіл відповідальності в системі УкрСЕПРО.
7. Порядок проведення робіт із сертифікації засобів забезпечення ТЗІ загального призначення.
8. Поняття та види схем сертифікації.
9. Технічний нагляд за стабільністю показників, підтверджених сертифікатом відповідності.
10. Сертифікація імпортованих засобів забезпечення ТЗІ.

Контрольні питання

1. Назвіть державні стандарти, що є основними у сфері технічного та криптографічного захисту інформації. На підставі вимог яких законодавчих актів України засоби ТЗІ є об'єктами стандартизації та сертифікації?
2. Назвіть принципи проведення сертифікації засобів захисту інформації.
3. Охарактеризуйте поняття: "сертифікація", "сертифікат відповідності", "декларація про відповідність" відповідно до Закону України "Про підтвердження відповідності".
4. Назвіть основні повноваження органів виконавчої влади України у сфері підтвердження відповідності засобів ТЗІ і КЗІ.

5. Перерахуйте обов'язки виробників і постачальників продукції, що потребує сертифікації?
6. Опишіть порядок проведення робіт із сертифікації засобів забезпечення ТЗІ загального призначення.
7. Хто і з яких міркувань визначає схему сертифікації?
8. З якою метою і ким проводиться технічний нагляд за стабільністю показників, підтверджених сертифікатом відповідності.
9. Як здійснюється сертифікація продукції, що імпортується?

Практичне завдання

Складіть схему, що ілюструє процес сертифікації засобів забезпечення ТЗІ загального призначення з наступним технічним наглядом.

Література, що рекомендується

1. Закон України "Про стандартизацію".
2. Закон України "Про підтвердження відповідності".
3. Закон України "Про метрологію та метрологічну діяльність".
4. Декрет Кабінету Міністрів України № 46-93 від 10.05 1993 р. "Про стандартизацію і сертифікацію".
5. Державні стандарти України:
 - Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96;
 - Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96;
 - Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97.
 - Сертифікація. Основні терміни і визначення. ДСТУ 2462-94;
 - Система сертифікації УкрСЕПРО. Основні положення. ДСТУ 3410-96;
 - Система сертифікації УкрСЕПРО. Порядок проведення сертифікації продукції. ДСТУ 3413-96.
 - ГОСТ 34.310-95
 - ГОСТ 34.311-95.

- ДЕРЖАВНІ БУДІВЕЛЬНІ НОРМИ УКРАЇНИ.
Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва ДБН А.2.2-2-96 .

6. "Порядок проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення", затверджений сумісним наказом Держстандарту України і ДСТСЗІ СБУ 09.07.2001 р.

7. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты.-Москва * Санкт-Петербург * Киев: ООО "ТИД "ДС", 2002.- 688 с.

ПРАКТИЧНЕ ЗАНЯТТЯ № 7

ТЕМА: "ПРАВОВЕ РЕГУЛЮВАННЯ СУСПІЛЬНИХ СТОСУНКІВ, ПОВ'ЯЗАНИХ З ТВОРЧОЮ ДІЯЛЬНІСТЮ"

Дані питання

1. Поняття творчої діяльності та її результату.
2. Правова база регулювання стосунків, пов'язаних з творчою діяльністю.
3. Винятковість авторського та патентного права, їх принципова відмінність.
4. Правова охорона відкриттів.
5. Стосунки, що регульовані авторським правом.
6. Визнання авторства; твори, які охороняються авторським правом.
7. Виникнення та здійснення авторського права.
8. Автор і співавтор, їх немайнові та майнові права.
9. Вільне використання твору.
10. Вільне відтворення твору.
11. Авторське право на твір, створений за договором з автором, що працює по найму.
12. Право спадкоємства.
13. Терміни охорони прав авторів.
14. Передача прав на володіння або використання творів.

Контрольні питання

1. Охарактеризуйте поняття "творча діяльність", "результат творчої діяльності". Які загальні риси творчій діяльності та її результатів в різних областях?
2. Назвіть функції цивільного права в регулюванні суспільних стосунків, пов'язаних з творчою діяльністю.
3. Які спеціальні інститути цивільного права регулюють стосунки, пов'язані з творчою діяльністю? У чому полягає специфіка цих інститутів права?
4. Які права називаються винятковими і чому?

5. У чому полягає відмінність авторського від винахідницького права?
6. Чи здійснюється в Україні правовий захист відкриттів? Якщо ні, то чому?
7. Які права авторів творів захищаються авторським правом?
8. Як можна формалізувати виникнення авторського права на твір?
9. Якими немайновими правами володіє автор твору?
10. Якими майновими правами володіє автор твору?
11. У яких випадках можливий перехід творів в суспільне надбання?

Практичне завдання

Виділіть ознаки, згідно яким авторське право, будучи одним з інститутів цивільного права, бере участь в регулюванні суспільних інформаційних стосунків.

Література, що рекомендується

1. Цивільний кодекс України.
2. Закон України "Про авторські права і суміжні права".
3. Закон України "Про охорону прав на винаходи і корисні моделі".

ПРАКТИЧНЕ ЗАНЯТТЯ № 8

Тема: "Патентне право"

Дані питання

1. Призначення патентного права.
2. Об'єкти винаходу і корисної моделі, умови надання правової охорони їх авторам.
3. Види патентів, терміни їх дії.
4. Умови патентопридатності винаходу, корисної моделі.
5. Права винахідника (ів) і працедавця на отримання та використання патенту.
6. Основні права, які витікають з патенту.
7. Передача прав на володіння або використання патентів.
8. Обмеження авторських прав на секретний винахід або корисну модель.
9. Примусове відчуження прав на винахід (корисну модель).
10. Дії, які не визнаються порушенням авторських прав винахідника.

Контрольні питання

1. Які об'єкти можуть бути представлені як винахід чи корисна модель?
2. Назвіть умови надання правового захисту авторам винаходів і корисних моделей.
3. Охарактеризуйте умови патентопридатності винаходу, корисної моделі.
4. У якому порядку реалізуються права винахідників на отримання патенту?
5. Перерахуйте основні права та обов'язки, які витікають з патенту.
6. У чому полягають особливості службового патенту?
7. Які обмеження авторських прав допускаються на секретний винахід або корисну модель?
8. У якому порядку здійснюється передача прав на володіння або використання патентів?

9. У яких випадках можливе примусове відчуження прав на винахід (корисну модель)?
10. Які дії не визнаються порушенням авторських прав винахідника?

Практичне завдання

Опишіть схематично процес отримання патенту на винахід з вказівкою суб'єктів, що беруть в нім участь.

Література, що рекомендується

1. Цивільний кодекс України.
2. Закон України "Про охорону прав на винаходи і корисні моделі".

Додаток

Нормативно-правова база для здійснення робіт у сфері захисту інформації в Україні

Закони України

1. Закон України "Про Службу безпеки України".
2. Закон України "Про державну таємницю".
3. Закон України "Про інформацію".
4. Закон України "Про ліцензування певних видів господарської діяльності".
5. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".
6. Закон України "Про авторські права і суміжні права".
7. Закон України "Про охорону прав на винаходи і корисні моделі".
8. Господарчий кодекс України.
9. Громадський кодекс України.
10. Закон України "Про Національну програму інформатизації".
11. Закон України "Про наукову і науково-технічну діяльність".
12. Закон України "Про наукову і науково-технічну експертизу".
13. Закон України "Про Національну систему конфіденційного зв'язку".
14. Закон України "Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання".
15. Закон України "Про електронні документи та електронний документообіг".
16. Закон України "Про електронний цифровий підпис".
17. Закон України "Про основи національної безпеки України".
18. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".

Державні стандарти України

1. ДСТУ 3396.0-96. «Захист інформації. Технічний захист інформації. Основні положення».
2. ДСТУ 3396.1-96. «Захист інформації. Технічний захист інформації. Порядок проведення робіт».
3. ДСТУ 3396.2-97. "Захист інформації. Технічний захист інформації. Терміни та визначення".
4. ДБН А.2.2-2-96. "Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва".
5. ДСТУ 3410-96, ДСТУ 3420-96, ДСТУ 3498-96. Система сертифікації УкрСЕПРО. Державна система сертифікації УкрСЕПРО.

Укази Президента України

1. № 836 від 18.09.2002 року "Про заходи щодо забезпечення інформаційної безпеки держави".
2. № 614 від 04.07.2002 року "Питання забезпечення діяльності Національної системи конфіденційного зв'язку".
3. № 891 від 24.09.2001 року "Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних".
4. №582 від 10.04 2000 року "Про заходи щодо захисту інформаційних ресурсів держави".
5. № 1229 від 27.09.1999 року "Про Положення про технічний захист інформації в Україні".
6. № 505 від 22.05. 1998 року "Про Положення про порядок здійснення криптографічного захисту інформації в Україні".

Постанови КМ України

1. Постанова КМ від 27.12.2002 р. N 2036 "Про утворення Міжвідомчої координаційної ради з питань створення, розвитку та функціонування Національної системи конфіденційного зв'язку".
2. Постанова КМ від 16.11.2002 р. N 1772 "Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту

державних інформаційних ресурсів в інформаційних та телекомунікаційних системах".

3. Постанова КМ від 11.10.2002 р. N 1520 "Про затвердження Державної програми створення, розвитку та забезпечення функціонування Національної системи конфіденційного зв'язку".
4. Постанова КМ від 11.10.2002 р. N 1519 "Про затвердження Порядку надання послуг конфіденційного зв'язку органам державної влади та органам місцевого самоврядування, державним підприємствам, установам та організаціям".
5. Постанова КМ від 13.03.2002 р. № 288 "Про затвердження переліків центральних органів виконавчої влади, на які покладаються функції технічного регулювання у визначених сферах діяльності та розроблення технічних регламентів".
6. Постанова КМ від 13.03.2002 р. № 281 "Про деякі питання захисту інформації, охорона якої забезпечується державою".
7. Постанова КМ від 4.01. 2002 р. № 3 "Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади".
8. Постанова КМ від 4.07. 2001 р. № 756 "Про затвердження переліку документів, які додаються до заяви про видачу ліцензії для окремого виду господарської діяльності".
9. Постанова КМ від 14.11. 2000, N 1698 "Про затвердження переліку органів ліцензування".
10. Постанова КМ від 09.12. 1999, N 2238 "Про Концепцію розвитку зв'язку України до 2010 року".
11. Постанова КМ від 04.02. 1998, N 121 "Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних".
12. Постанова КМ, від 08.10.1997, № 1126 "Про затвердження Концепції технічного захисту інформації в Україні".
13. Постанова КМ від 16.02.1997, №180 "Про затвердження Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах".

НД ТЗІ

1. Наказ ДСТСЗІ СБ України від 14.07.04 № 56 "Про затвердження Граничних тарифів на послуги конфіденційного зв'язку".
2. Наказ ДСТСЗІ СБ України від 08.07.04 №52 "Про затвердження Порядку формування реєстру організаторів державної експертизи та Порядку формування реєстру експертів з питань технічного захисту інформації".
3. Наказ ДСТСЗІ СБ України від 24.04.2003 р. № 41 про введення в дію нормативного документу "НД ТЗІ 1.6-002-03 Правила побудови, викладення, оформлення та позначення нормативних документів системи технічного захисту інформації".
4. Наказ ДСТСЗІ СБ України від 02.04.2003 р. № 33 про введення в дію нормативного документу "НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу".
5. Наказ ДСТСЗІ СБ України від 28.04.1999 р. № 22 про введення в дію нормативного документу " НД ТЗІ 1.1-002-99 Загальні положення що до захисту інформації у комп'ютерних системах від несанкціонованого доступу".
6. Наказ ДСТСЗІ СБ України від 28.04.1999 р. № 22 про введення в дію нормативного документу " НД ТЗІ 1.1-003-99 Трємінєлогія в області захисту інформації у комп'ютерних системах від несанкціонованого доступу".
7. Наказ ДСТСЗІ СБ України від 28.04.1999 р. № 22 про введення в дію нормативного документу " НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації у комп'ютерних системах від несанкціонованого доступу".
8. Наказ ДСТСЗІ СБ України від 28.04.1999 р. № 22 про введення в дію нормативного документу " НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем та стандартні функціональні профілі захищеності оброблюваної інформації у комп'ютерних системах від несанкціонованого доступу".
9. Наказ ДСТСЗІ СБ України від 13.12.2002 р. № 84 про введення в дію нормативного документу "НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2".

10. Наказ ДСТСЗІ СБ України від 07.06.2002 р. № 35 "Про затвердження Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації".
11. Наказ ДСТСЗІ СБ України від 23.02.2002 р. № 9 "Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб".
12. Наказ ДСТСЗІ СБ України від 24.12.2001 р. № 76 "Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах."
13. Наказ ДСТСЗІ СБ України від 12.12.2001 р. № 151/72 "Про затвердження Порядку контролю за додержанням ліцензійних умов провадження господарської діяльності з розроблення, виробництва, використання, експлуатації, сертифікаційних випробувань, тематичних досліджень, експертизи, ввезення, вивезення криптосистем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівлі криптосистемами і засобами криптографічного захисту інформації; розроблення, виробництва, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг в галузі технічного захисту інформації".
14. Наказ ДСТСЗІ СБ України від 06.11.2001 р. № 64 про введення в дію нормативного документу "НД ТЗІ 2.3-006-2001 Радіовиявлювачі аналізуювальні. Методи та засоби випробувань".
15. Наказ ДСТСЗІ СБ України від 11.09.2001 р. № 54 про введення в дію нормативного документу "НД ТЗІ 2.3-005-2001 Радіовиявлювачі панорамні. Методи та засоби випробувань."
16. Наказ ДСТСЗІ СБ України від 09.07.2001 р. № 329/32 про введення в дію нормативного документу "Порядок проведення робіт із сертифікації засобів - забезпечення технічного захисту інформації загального призначення".
17. Наказ ДСТСЗІ СБ України від 09.04.2001 р. № 12 про введення в дію нормативного документу "НД ТЗІ 2.3-004-2001 Радіовиявлювачі індикаторні. Методи та засоби випробувань".
18. Наказ ДСТСЗІ СБ України від 06.04.2001 р. № 11 про введення в дію нормативного документу "НД ТЗІ 2.3-003-2001 Технічний захист інформації мовної інформації в симетричних абонентських

аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань".

19. Наказ ДСТСЗІ СБ України від 06.04.2001 р. № 11 про введення в дію нормативного документу "НД ТЗІ 2.3-002-2001 Технічний захист інформації мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби пасивного приховування мовної інформації. Нелінійні атенуатори та загороджувальні фільтри. Методика випробувань".
20. Наказ ДСТСЗІ СБ України від 06.04.2001 р. № 11 про введення в дію нормативного документу "НД ТЗІ 4.7-001-2001 Технічний захист інформації мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби визначення наявності та віддаленості місця контактного підключення засобів технічної розвідки. Рекомендації щодо розроблення методів випробувань".
21. Наказ ДСТСЗІ СБ України від 1.03.2001 р. № 52 про введення в дію нормативного документу "Звід відомостей, що становлять державну таємницю".
22. Наказ ДСТСЗІ СБ України від 27.02.2001 р. № 5 про введення в дію нормативного документу "НД ТЗІ 2.3-001-2001 Радіовиявлювачі вимірювальні. Методи та засоби випробувань".
23. Наказ ДСТСЗІ СБ України від 09.02.2001 р. № 2 про введення в дію нормативного документу "НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення".