

МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ



**МЕТОДИЧНІ МАТЕРІАЛИ
ЩОДО ЗАБЕЗПЕЧЕННЯ
САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ
з дисципліни
“ПРАВОВІ ОСНОВИ ЗАХИСТУ
КОМЕРЦІЙНОЇ ТАЄМНИЦІ”
(для бакалаврів)**

Київ
ДП «Видавничий дім «Персонал»
2010

ПОЯСНЮВАЛЬНА ЗАПИСКА

Самостійна робота студентів є складовою навчального процесу, основним засобом опанування навчального матеріалу в час, вільний від обов'язкових навчальних занять.

Мета самостійної роботи студентів з дисципліни “Правові основи захисту комерційної таємниці” полягає у вивченні та конструктивно-критичному осмисленні чинної нормативно-правової бази, яка регулює діяльність з організаційно-правового забезпечення захисту інформації з обмеженим доступом.

Завдання самостійної роботи — засвоєння студентами теоретико-правових знань стосовно захисту комерційної таємниці в Україні, підготовки до поточних аудиторних занять.

Зміст самостійної роботи визначається навчальною програмою, а також цими методичними матеріалами.

У ході самостійної підготовки до практичних занять студенти повинні опрацювати прослуханий лекційний матеріал, всебічно розглянути зміст питань, що виносяться на заняття, опрацювати навчальну літературу, відповідні нормативно-правові акти.

Критерії оцінювання самостійної роботи студентів:

- оцінка “відмінно” — студент повно і всебічно розкриває питання теми, винесені на самостійне опрацювання, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, має власну точку зору стосовно відповідної теми і може аргументовано її доводити;
- оцінка “добре” — загалом рівень знань студентів відповідає вкладаєному вище, але мають місце деякі упущення при виконанні завдань, винесених на самостійне опрацювання, обґрунтування неточні, не підтверджуються достатньо обґрунтованими доказами;
- оцінка “задовільно” — студент розкрив питання, винесені на самостійне опрацювання, в загальних рисах, розуміє їх суть, намагається робити висновки, але при цьому припускається грубих помилок, матеріал викладає нелогічно і несамостійно;
- оцінка “незадовільно” — студент не в змозі дати відповідь на поставлене запитання або відповідь неправильна, не розуміє суті питання, не може зробити висновки.

Підготовлено професором кафедри правоохоронної діяльності *Е. І. Низенком*

Затверджено на засіданні кафедри правоохоронної діяльності (протокол № 10 від 27.06.08)

Схвалено *Вченою радою Міжрегіональної Академії управління персоналом*

Низенко Е. І. Методичні матеріали щодо забезпечення самостійної роботи студентів з дисципліни “Правові основи захисту комерційної таємниці” (для бакалаврів). — К.: ДП «Вид. дім «Персонал», 2010. — 48 с.

Методичні матеріали містять пояснювальну записку, тематичний план, зміст дисципліни “Правові основи захисту комерційної таємниці”, питання для самоконтролю, практичні і тестові завдання, а також список літератури.

- © Міжрегіональна Академія управління персоналом (МАУП), 2010
- © ДП «Видавничий дім «Персонал», 2010

ТЕМАТИЧНИЙ ПЛАН
дисципліни

“ПРАВОВІ ОСНОВИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ”

№ пор.	Назва змістового модуля і теми	Лекції	ПЗ	Сам. роб.
1	2	3	4	5
	Змістовий модуль I. Концептуальні засади та загальнооречені характеристики окремих напрямів захисту комерційної таємниці			
1	Охорона права на інформацію	2	2	9
2	Комерційна таємниця: основні поняття, загальні характеристики	2	2	9
3	Комерційна таємниця як об'єкт правової охорони інтелектуальної власності			
4	Концептуальні положення щодо комерційної таємниці			
5	Банківська таємниця, правове регулювання відносин у сфері її захисту			
	Змістовий модуль II. Система та форми захисту комерційної і банківської таємниці			
6	Заходи власника комерційної інформації з охорони її конфіденційності	2		9
7	Досвід захисту комерційних секретів західними фірмами			
8	Юридичне закріплення права підприємства на використання комерційної таємниці	2	2	9
9	Права та обов'язки власника прав на комерційну таємницю			
10	Допуск до комерційної таємниці співробітників підприємства	2	2	9
11	Обов'язкові умови, пов'язані із забезпеченням захисту комерційної таємниці підприємства			
12	Особливості правової охорони конфіденційної інформації при укладенні угоди з іноземною фірмою	2	2	
	Змістовий модуль III. Правові основи захисту комерційної таємниці та організаційне забезпечення діяльності з охорони інформації з обмеженим доступом			
13	Правове регулювання питань збереження комерційної таємниці при укладенні підприємницьких договорів та веденні ділових переговорів	2	2	

1	2	3	4	5
14	Технічний захист інформації, що містить комерційну таємницю			
15	Попередження правопорушень у сфері використання інформаційних технологій	2		9
16	Формування підрозділу інформаційної безпеки СБ підприємства та заходи, щодо захисту комерційної таємниці	2		9
17	Механізм реалізації прав особи на комерційну таємницю	2	2	7
18	Правові відносини підприємства з контролюючими органами з питань, пов'язаних із захистом комерційної таємниці та конфіденційних відомостей			
19	Правова характеристика уніфікованих основ захисту комерційної таємниці в міжнародному праві	2	2	
	Змістовий модуль IV. Локальні акти підприємства із захисту комерційної таємниці			
20	Конструювання типової моделі корпоративної норми “Положення про комерційну таємницю підприємства та правила її збереження”			
21	Типова модель методики визначення відомостей, що мають комерційну таємницю підприємства			
22	Типова модель корпоративної норми “Положення про дозвільну систему доступу співробітників підприємства та представників сторонніх організацій до відомостей, що мають комерційну таємницю підприємства”			
23	Типова модель організаційно-методичного документа з організації і ведення на підприємстві спеціального діловодства з носіями комерційної таємниці			
24	Типова модель корпоративної норми “Положення про підрозділ інформаційної безпеки СБ підприємства”			
	Разом годин: 108	22	16	70

ЗМІСТ **дисципліни** **“ПРАВОВІ ОСНОВИ ЗАХИСТУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ”**

Змістовий модуль І. Концептуальні засади та загальнотеоретичні характеристики окремих напрямів захисту комерційної таємниці

Тема 1. Охорона права на інформацію

Питання для самоконтролю

1. Визначення поняття “інформація”.
2. Охарактеризуйте правові ознаки інформації.
3. Визначити джерела інформації.
4. Які є основні види інформації?
5. Види інформації за суб'єктами права власності.
6. Види інформації за режимом доступу до неї.
7. Як співвідносяться поняття: первинний документ, вторинний документ?
8. Дати перелік засобів охорони персональних даних в Україні.
9. Процедура захисту прав громадян щодо обмеження поширення персональних даних.
10. Відповідальність за порушення порядку обігу персональних даних.

Практичні завдання

1. Складіть порівняльну таблицю визначення поняття “інформація”, закріплене законами України “Про інформацію”, “Про захист економічної конкуренції” та у ст. 200 Цивільного кодексу України.
2. Підготуйте письмові відповіді на запитання:
 - 1) Які відомості не можна вважати до комерційною таємницею в Україні?
 - 2) Об'єктом яких правовідносин може бути інформація?
 - 3) Які загальні рекомендації можна виокремити, аналізуючи теорію та практику захисту важливої інформації та будь-яких видів її носіїв, що безпосередньо належать концернам, корпораціям, компаніям США, Німеччини, Франції та інших країн?
 - 4) Чи можливо забезпечити надійне збереження комерційних секретів, керуючись лише національним законодавством України?

- 5) У чому полягає суть концепції захисту фірмових секретів, розробленої відомим спеціалістом із США в галузі захисту інформації А. Патоксом?

6) Етапи в організації інформації за методом “орсес”?

- 7) Які додаткові критерії застосовують для класифікації інформації?
- 8) Які правові гарантії захисту інформації з обмеженим доступом, що не становить державної таємниці, передбачено чинним законодавством України?

3. Підготуйте реферат на тему: “Формування національної системи захисту інформації в період відродження української національної державності (1917–1921 рр.)”.

4. Підготуйте реферат на тему: “Захист інформації в Запорозькій Січі та державі Богдана Хмельницького”.

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь.

1. **Визначити предмет навчального курсу “Правові основи захисту комерційної таємниці”:**

- а) це перелік тем, що розглядаються;
 - б) це вихідні знання про захист комерційної таємниці;
 - в) це право власності на комерційну таємницю. Концептуальні основи та принципи захисту комерційної таємниці, визначення, відповідно до законодавства, інформації, що має державну таємницю;
 - г) це створення системи захисту комерційної таємниці;
 - д) це механізм захисту інформації, яка має комерційну таємницю;
 - е) це відомості про конфіденційні ділові переговори, огляди ринку, маркетингові дослідження, плани розвитку підприємств, інші відомості, що мають підприємницький інтерес, порушення якого може завдати збитків її власникові;
 - є) наукова діяльність держави в галузі захисту комерційної таємниці;
 - ж) система правового захисту комерційної таємниці, правові джерела дисципліни;
 - з) поняття комерційної таємниці та її ознаки.
2. **Система дисципліни “Правові основи захисту комерційної таємниці”:**
- а) правовий зміст “інформація”;
 - б) поняття та види інформації з обмеженим доступом;

- в) правові та організаційні засади захисту комерційної таємниці в Україні;
- г) чинний правовий механізм охорони персональної інформації з обмеженим доступом;
- д) правове регулювання захисту інформації в автоматизованих системах;
- е) усі відповіді правильні;
- є) усі відповіді неправильні;
- ж) не усі відповіді правильні.

3. З перелічених видів інформації основними є такі:

- а) статистична інформація;
- б) адміністративна інформація (дані);
- в) масова інформація;
- г) інформація про діяльність державних органів влади та органів місцевого і регіонального самоврядування;
- д) правова інформація;
- е) інформація про особу;
- є) інформація довідково-енциклопедичного характеру;
- ж) соціологічна інформація;
- з) дані про ринки збуту, плани розвитку підприємств, інвестиції та інші відомості, що мають підприємницький інтерес.

4. Для публічного поширення масової інформації використовуються такі засоби:

- а) періодичні друковані видання (преса) — газети, журнали, бюлетені;
- б) бюлетені;
- в) разові видання з визначеним тиражем;
- г) радіомовлення;
- д) телебачення;
- е) кіно;
- є) оголошення через засоби звукозапису під час публічних виступів;
- ж) оголошення через засоби відеозапису під час публічних виступів;
- з) листування.

5. Серед джерел інформації довідково-енциклопедичного характеру основними є:

- а) енциклопедії;

- б) словники;
- в) довідники;
- г) рекламні повідомлення та оголошення;
- д) путівники;
- е) картографічні матеріали;
- є) довідки, що видаються уповноваженими на те державними органами місцевого і регіонального самоврядування, об'єднаннями громадян, організаціями;
- ж) довідки, що видаються автоматизованими інформаційними системами.

6. Персональними даними про особу є:

- а) національність;
- б) освіта;
- в) сімейний стан;
- г) релігійність;
- д) стан здоров'я;
- е) адреса;
- є) дата і місце народження;
- ж) місце роботи;
- з) розмір вкладу на банківському рахунку.

7. Джерелами правової інформації є:

- а) Конституція України;
- б) законодавчі і підзаконні нормативні акти;
- в) міжнародні договори і угоди;
- г) норми і принципи міжнародного права;
- д) ненормативні правові акти;
- е) повідомлення засобів масової інформації;
- є) публічні виступи;
- ж) інші джерела інформації з правових питань.

8. Поняття "інформація" властиві такі ознаки:

- а) відомості про події та явища, що відбуваються у суспільстві, у державі, у навколишньому природному середовищі;
- б) дані, що можуть зберігатися в будь-якій формі і вигляді;
- в) документовані або публічно оголошені відомості;
- г) інформація як об'єкт цивільних прав, що належить до категорії нематеріальних благ;
- д) джерелами інформації є передбачені або встановлені законом носії інформації;

- е) документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій і явищ, процесів, фактів;
- є) сукупність документованих або публічно оголошених відомостей про право, його систему, юридичні факти, правопорядок;
- ж) відомості, систематизовані, документовані про навколишнє природне середовище, про суспільне, державне життя.

9. Предметом захисту інформації у системі захисних режимних заходів є:

- а) річні та інші звіти, технологічні карти;
- б) результати маркетингових досліджень ринків збуту;
- в) відомості про партнерів, конкурентів;
- г) дослідні зразки виробів;
- д) унікальне обладнання, що використовується у виробничому процесі;
- е) нові технології, "ноу-хау";
- є) цінна інформація у формі теоретичної промісловості або комерційної ідеї, плану; списки представників або посередників, картотеки клієнтів;
- ж) комерційні задуми, комерційно-політичні цілі фірми, матеріали нарад і засідань органів управління фірм, розміри і умови банківського кредиту, розрахунок цін, комп'ютерні програми.

Література [23; 26; 49; 51; 54; 56]

Тема 2. Комерційна таємниця: основні поняття, загальні характеристики.

Питання для самоконтролю

1. Дати визначення поняття "інформація з обмеженим доступом".
2. У яких випадках інформація з обмеженим доступом може бути поширена без згоди її власника?
3. Назвіть види інформації з обмеженим доступом.
4. Що таке конфіденційна інформація?
5. Визначення поняття "таємна інформація".
6. Види конфіденційної інформації.
7. Які види таємної інформації передбачено чинним законодавством України?
8. Назвіть певні ознаки інформації, що має комерційну таємницю для підприємства.
9. На яких умовах комерційна таємниця може продаватися на догвірній основі іншому підприємству у відповідності із законодавством України?

10. Чи можуть класифікуватись як комерційна таємниця фундаментальні наукові дослідження, котрі не дають прибутку?

Практичні завдання

1. Підготуйте письмові відповіді на запитання.

- 1) Як на законодавчому рівні розглядають інформацію з обмеженим доступом за своїм правовим режимом?
 - 2) Що необхідно з'ясувати, коли визначається вартість інформації, що має комерційну таємницю, коли порушено умови угоди про її збереження?
 - 3) Що розуміють під "правом власності на комерційну таємницю"?
 - 4) В якому законодавчому порядку захищається право власності на комерційну таємницю?
 - 5) Коли виникає право власності на комерційну таємницю і до якого часу воно діє?
 - 6) В якому порядку здійснюється рішення, прийняте підприємством про відчуження права власності на комерційну таємницю?
 - 7) Як власник комерційної таємниці може використовувати її?
 - 8) Що може бути об'єктами права власності на інформацію, яка має комерційну таємницю?
 - 9) Хто є суб'єктом права власності на комерційну таємницю, відповідно до чинного законодавства України?
2. Підготуйте реферат на тему: "Поняття та ознаки комерційної таємниці".
3. Підготуйте реферат на тему: "Поняття та види інформації з обмеженим доступом".
4. Підготуйте реферат на тему: "Правові основи охорони комерційної таємниці".

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь.

1. Право на інформацію громадянами, юридичними особами і державою не повинно порушувати:

- а) громадянські права;
- б) політичні права;
- в) економічні права;
- г) соціальні права;
- д) духовні права;
- є) екологічні права;
- ж) права та інтереси юридичних осіб.

2. Приймати остаточне рішення стосовно співвідношення права громадянської свободи з правом її власника на захист такої інформації, якщо вона була поширена без його згоди, уповноважені лише:

- а) органи судової влади;
- б) центральні органи виконавчої влади;
- в) Рада міністрів Автономної Республіки Крим;
- г) Київська міська державна адміністрація;
- д) Севастопольська міська державна адміністрація;
- е) органи внутрішніх справ;
- є) Служба безпеки України;
- ж) органи прокуратури.

3. До видів таємної інформації, передбаченої чинним законодавством, належить:

- а) державна таємниця;
- б) комерційна таємниця;
- в) службова таємниця;
- г) професійна таємниця;
- д) військова таємниця;
- е) банківська таємниця;
- є) адвокатська таємниця;
- ж) лікарська таємниця;
- з) таємниця усинювання.

4. Державна таємниця стосовно правового статусу являє собою різновид таємної інформації, що охоплює відомості у сфері:

- а) оборони;
- б) економіки;
- в) науки;
- г) техніки;
- д) зовнішніх відносин;
- е) державної безпеки;
- є) охорони правопорядку;
- ж) ринкової стратегії підприємства.

5. До конфіденційної інформації належать такі свідчення про особу:

- а) освіта;
- б) сімейний стан;
- в) релігійність;
- г) стан здоров'я;

- д) дата і місце народження;
- е) майновий стан;
- є) неблаговидні вчинки;
- ж) заворювання;
- з) злочинна діяльність;
- и) інтимні сторони життя.

6. Види інформації, що становлять ішу, передбачену чинним законодавством України таємницею:

- а) банківська таємниця;
- б) комерційна таємниця;
- в) військова таємниця;
- г) таємниця голосування;
- д) таємниця усинювання;
- е) лікарська таємниця;
- є) таємниця страхування;
- ж) таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції;
- з) служба (професійна) таємниця;
- и) таємниця нотаріальних дій;
- і) конфіденційна інформація, що є власністю держави.

7. Банківською таємницею є:

- а) відомості про стан рахунків клієнта;
- б) відомості про стан кореспондентських рахунків банків у Національному банку України;
- в) операції, проведені на користь чи за дорученням клієнта, здійснені ним угоди;
- г) фінансово-економічний стан клієнтів;
- д) системи охорони банку та клієнтів;
- е) інформація про організаційно-правову структуру юридичної особи — клієнта, її керівників, напрямки діяльності;
- є) відомості стосовно комерційної діяльності клієнтів чи будь-якого проекту, винаходу, зразка продукції тощо;
- ж) коди, що використовуються банками для захисту інформації;
- з) інформація щодо звітності окремого банку, за винятком тієї, що підлягає опублікуванню.

8. Банки зобов'язані забезпечити збереження банківської таємниці шляхом:

- а) обмеження кола осіб, які мають доступ до інформації, що становить банківську таємницю;

- б) здійснення контролю за збереженням конфіденційних документів;
- в) здійснення закритого листування за допомогою криптографічного захисту інформації і шифрованого зв'язку;
- г) координації робіт щодо захисту інформації з обмеженим доступом на об'єкт інформаційної діяльності, а також впровадження системи технічного захисту інформації;
- д) перевірки достатності рівня захищеності інформації в інформаційній системі;
- е) створення спеціального діловодства для документів, що містять банківську таємницю;
- є) застосування технічних засобів для запобігання несанкціонованому доступу до електронних та інших носіїв інформації;
- ж) застосування застережень щодо збереження банківської таємниці та відповідальності за її розголошення у договорах і угодах між банком і клієнтом.
- 9. Комерційна таємниця повинна відповідати таким вимогам:**
- а) бути власністю підприємства;
- б) бути засекреченою власником підприємства в його інтересах на визначений термін, у визначеному обсязі;
- в) мати дійсну або потенційну вартість з комерційних міркувань;
- г) не бути загальновідомою чи загальнодоступною згідно із законодавством України;
- д) надійно захищатися її власником або уповноваженою ним особою через систему інформації, розробку внутрішніх правил застосування, схову, обігу, знищення та запобігання розголошенню, введення відповідного кодування носіїв інформації тощо;
- е) не захищатися авторським і патентним правом;
- є) не стосуватися негативної діяльності підприємства, здатної завдати шкоди суспільству (порушень законів, адміністративних помилок, забруднення навколишнього середовища тощо);
- ж) бути товаром, який може продаватися на договірній основі іншому підприємству за умови її нерозголошення.

Література [41–43; 49; 50; 56]

Тема 3. Комерційна таємниця як об'єкт правової охорони інтелектуальної власності

Тема 4. Концептуальні положення щодо комерційної таємниці.

Тема 5. Банківська таємниця, правове регулювання відносин у сфері її захисту

Змістовий модуль II. Система та форми захисту комерційної і банківської таємниці

Тема 6. Заходи власника комерційної інформації з охорони її конфіденційності

Питання для самоконтролю

1. Дати визначення поняття “конфіденційна інформація, що є власністю держави”.
2. Дати визначення поняття “конфіденційна інформація, що не є власністю держави”.
3. Які відомості не можна вважати конфіденційною інформацією, що є власністю держави?
4. Порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, що містять конфіденційну інформацію і є власністю держави.
5. Яким вимогам повинна відповідати інформація з переліку відомостей про конфіденційну інформацію, що є власністю держави?
6. Хто відповідає за забезпечення правильного ведення обліку, зберігання та використання документів з грифом “ДСК”?
7. Основні правила обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, що містять конфіденційну інформацію і є власністю держави:
 - прийняття і облік документів;
 - розмноження і розсилання (відправлення) документів;
 - формування виконаних документів;
 - використання документів;
 - зняття грифа “ДСК”;
 - відбору документів для зберігання і знищення;
 - забезпечення схоронності документів та перевірка їх наявності;
 - облік, зберігання і використання печаток, штампів і бланків.

8. Ким розробляється і затверджується перелік відомостей, які містять конфіденційну інформацію, що є власністю держави і яким надається гриф обмеження доступу – “ДСК”?
9. Які правові шляхи існують для збереження платіжних умов, що мають конфіденційний характер, при укладенні зовнішньоекономічної угоди?
10. В який термін здійснюється перевірка наявності документів з грифом “ДСК” у бібліотеках та архівних підрозділах?

Практичні завдання

1. Охарактеризуйте діючий порядок проставлення грифа “ДСК” на документі і на виданні.
2. Підготуйте письмові відповіді на запитання:
- 1) Чи можуть керівники центральних органів виконавчої влади, місцевих органів виконавчої влади зняти гриф “ДСК” з документів, підготовлених їх структурними підрозділами?
 - 2) За яких умов документи з грифом “ДСК”, видані до 1992 р., можуть розглядатися як відкриті документи?
 - 3) Як розглядаються документи, тиражовані у 1991 р. та пізніше з грифом ДСК або з нумерацією кожного примірника, але не опубліковані в офіційних виданнях, з яких знято грифи секретності?
 - 4) На які підрозділи організацій та установ покладається обов’язок з ведення обліку, зберігання, розмноження та використання документів з грифом “ДСК”?
 - 5) На які підрозділи організації покладається завдання із запобігання розголошенню відомостей, що містяться в документах з грифом “ДСК”, та випадків втраг таких документів?
 - 6) Який діє порядок приймання і обліку документів з грифом “ДСК”?
 - 7) Що перевіряється співробітниками канцелярії під час прийняття і розкриття кореспонденції з грифом “ДСК”?
 - 8) Як фіксується факт відсутності вкладень у конвертах (пакетах) документів або додатків до них?
 - 9) Як потрібно діяти, коли в організацію помилково надійшли документи з грифом “ДСК”?
 - 10) Як обліковуються вхідні, вихідні та внутрішні документи і видання з грифом “ДСК”?
3. Підготуйте реферат на тему: “Правове регулювання захисту конфіденційної інформації, що є власністю держави”.

4. Підготуйте реферат на тему: “Оброблення, зберігання та друкування документів з грифом “ДСК” та конфіденційної інформації, що є власністю держави”.

Тестові завдання

Із запропонованих варіантів вкажіть правильну відповідь.

1. **Друкування документів з грифом “ДСК” здійснюється з додержанням вимог:**
- а) друкування здійснюється у друкарському бюро організації;
 - б) до реєстраційного номера документа додається позначка “ДСК”;
 - в) друкування таких документів допускається у структурних підрозділах під відповідальність їх керівників;
 - г) оброблення, зберігання та друкування документів з грифом “ДСК” і конфіденційної інформації, що є власністю держави, з використанням автоматизованих систем дозволяється тільки за наявності виданого Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ агента відповідної комплексної системи захисту інформації в цій АС (автоматизована система) вимогам щодо захисту інформації;
 - д) на звороті останньої сторінки кожного примірника документа слід зазначити кількість надрукованих примірників, прізвище виконавця, власне прізвище друкаря і дату друкування документа;
 - е) надруковані і підписані документи з грифом “ДСК” разом з їх чернетками та варіантами передаються для реєстрації співробітнику канцелярії, який здійснює їх облік;
 - є) чернетки і варіанти знищуються виконавцем та співробітником канцелярії, про що на копії вихідного документа робиться напис: “Чернетки і варіанти знищені. Дата. Підписи”.
2. **Розсилання (відправлення) тиражу документів з грифом “ДСК” здійснюється з дотриманням вимог:**
- а) на підставі розрядунок, підписаних керівником організації (його заступником) та керівником канцелярії, із зазначенням облікових номерів примірників, що розсилаються рекомендованими або цінними поштовими відправленнями, а також кур’єрами організації;
 - б) пересилання документів з грифом “ДСК” до інших організацій у межах України здійснюється рекомендованими або цінними поштовими відправленнями;

в) доставка документів з грифом “ДСК” до інших організацій здійснюється на підставі письмового доручення;

г) документи справи і видання з грифом “ДСК”, що розсилаються, мають бути вкладені у конверти або упаковані таким чином, щоб виключалася можливість доступу до них;

д) на упаковці або конверті зазначаються адреси і найменування одержувача та відправника, номери вкладених документів з поначкою “ДСК”;

е) на конвертах (упаковках) документів з грифом “ДСК” забороняється зазначати прізвища і посади керівників організацій і виконавців документів, а також найменування структурних підрозділів;

є) ознайомлення представників засобів масової інформації з документами з грифом “ДСК” та передавання їм таких матеріалів допускається за письмовим дозволом керівника організації, якому надано право затверджувати переліки відомостей, що містять конфіденційну інформацію і є власністю держави. Такі документи попередньо розглядаються експертними комісіями, які приймають рішення про доцільність їх передавання або можливість зняття грифа “ДСК”, якщо вони втратили первісне значення;

ж) якщо в документах з грифом “ДСК” містяться відомості, що належать до компетенції інших організацій, передавання їх за кордон або у засоби масової інформації може бути здійснене лише за письмовою згодою тих організацій.

3. У номенклатурі справ, якими передбачається порядок формування документів з грифом “ДСК”, в обов’язковому порядку включаются та дотримуються такі положення:

а) всі довідкові та реєстраційні картотеки;

б) реєстраційні журнали на документи з грифом “ДСК”;

в) дозволяється формувати в окремій справі документи з грифом “ДСК” залежно від виробничої та інформаційної потреби;

г) дозволяється формувати в окремій справі документи з грифом “ДСК” разом з іншими несекретними документами з одного й того ж питання;

д) якщо в організації створюється велика кількість однакових видів документів (наказів, інструкцій, планів тощо) з грифом “ДСК” та без цього грифа, їх формують в окремій справі. У но-

менклатурі справ в графі “індекс справи” до номера справи з документами з грифом “ДСК” додається позначка “ДСК”;

е) у разі долучення документа з грифом “ДСК” до справи з документами, що не мають такого грифа, на справі ставиться позначка “ДСК”, а до номенклатури справ вносяться відповідні зміни;

є) може бути передбачено запровадження однієї справи із заголовком “Документи з грифом “ДСК”, коли у діяльності окремої організації створюється незначна кількість документів з грифом “ДСК”;

ж) термін зберігання однієї справи із заголовком “Документи з грифом “ДСК” не встановлюється, а у відповідній графі номенклатури справ проставляється позначка “ЕК” (експертна комісія).

4. Після закінчення діловодного року справа “Документи з грифом “ДСК” переглядається:

а) посторінково членами експертної комісії організації;

б) посторінково керівником та його заступниками;

в) у разі потреби приймається рішення про переформування документів;

г) документи постійного зберігання, що містяться у справі “Документи з грифом “ДСК”, формуються в окрему справу, якій надається окремий заголовок і яка додатково включається до номенклатури справ;

д) якщо у справі “Документи з грифом “ДСК” містяться документи тимчасового і постійного зберігання, вона може не переформуватися;

е) якщо у справі “Документи з грифом “ДСК” містяться тільки документи тимчасового зберігання, вона може не переформуватися;

є) термін зберігання справи, у якій містяться тільки документи тимчасового зберігання, встановлюється відповідно до найбільшого терміну зберігання документів, що містяться в цій справі;

ж) термін зберігання справи, у якій містяться тільки документи тимчасового зберігання, встановлюється відповідно до найменшого терміну зберігання документів, що містяться в цій справі.

5. Справи з несекретними документами, в яких накопичуються окремі документи з грифом “ДСК”, повинні відповідати таким вимогам:

- а) мають бути віднесені до категорії обмеженого розповсюдження і використання;
- б) на обкладинках і титульних сторінках справ з грифом “ДСК” є проставлений гриф “ДСК”;
- в) справи з документами з грифом “ДСК” повинні мати внутрішні описи;
- г) в номенклатуру справ з несекретними документами, в яких на- копичуються окремі документи з грифом “ДСК”, повинні вно- ситися відповідні уточнення;
- д) до роботи із справами з грифом “ДСК” допускаються особи, які мають безпосереднє відношення до цих справ, згідно із списка- ми, погодженими з канцелярією;
- е) до роботи із справами з грифом “ДСК” допускаються особи, які не мають безпосереднього відношення до цих справ;
- є) до роботи з окремими документами, які накопичуються в спра- вах з грифом “ДСК”, допускаються особи згідно із вказівками, викладеними у резолюціях керівників організації (структур- них підрозділів);
- ж) допуск працівників до роботи з виданням з грифом “ДСК” ви- значається керівниками організації.

6. Порядок користування відомостями з документів, які ма- ють гриф “ДСК”, передбачає виконання таких положень організаційно-правового механізму захисту конфіденційної інформації:

- а) забороняється користуватися відомостями з документів з гри- фом “ДСК” для відкритих виступів або опублікування у засобах масової інформації;
- б) забороняється експонувати документи з грифом “ДСК” на від- критих виставках, на стендах, у вітринах або інших громадських місцях;
- в) опублікування або передавання для опублікування несекретних відомостей обмеженого поширення допускається у разі потреби з письмового дозволу керівника організації, якщо такі відомості не суперечать затвердженню в установі перелікам конфіденцій- ної інформації, що є власністю держави;
- г) передача конфіденційної інформації, що є власністю держави, каналами зв'язку здійснюється лише з використанням засобів технічного або криптографічного захисту інформації;

- д) представники інших організації допускаються до ознайомлен- ня і роботи з документами з грифом “ДСК” з дозволу керівників тих організації, структурних підрозділів у володінні та розпо- рядженні яких перебувають ці документи, за наявності письмо- вого захисту організації, в яких вони працюють, із зазначенням характеру завдання, що виконується;
- е) виписки з документів і видань з грифом “ДСК”, що містять відо- мості обмеженого поширення, робляться у зошитах, що мають аналогічний гриф, які після закінчення роботи надсилаються на адресу організації, яка дала дозвіл на ознайомлення і роботу з документами з грифом “ДСК”;

- є) справи та видання з грифом “ДСК” видаються виконавцям і приймаються від них під розписку в картці обліку справ і ви- дань, що видаються за встановленою формою;
- ж) копіювання для сторонніх організації документів з грифом “ДСК”, одержаних від інших організації, здійснюється з органі- заціями-авторами цих документів;
- з) зняття копій, а також здійснення виписок з документів з гри- фом “ДСК” співробітниками організації, де зберігаються доку- менти, проводиться без дозволу керівника організації.

7. Зняття грифа “ДСК” з документів, справ і видань повинно здійснюватися з врахуванням такого порядку:

- а) рішення про зняття грифа “ДСК” приймається експертною ко- місією організації-автора документа (видання) чи правонаступ- ника;
- б) до складу експертної комісії, яка повинна прийняти рішення щодо зняття грифа “ДСК” з документа, включаються працівни- ки канцелярії, режимно-секретного та інших структурних під- розділів організації;
- в) рішення комісії оформляється актом та затверджується керів- ником організації;
- г) один примірник акта експертної комісії разом із справами пере- дається до архівного підрозділу організації;
- д) справи постійного зберігання разом з примірником акта ек- пертної комісії передаються до відповідної державної архівної установи;
- е) про зняття грифа обмеження доступу повідомляються всі орга- нізації, яким надсилався цей документ (видання);

- є) на обкладинках справ гриф “ДСК” погашається штампом або записом від руки із зазначенням дати і номера акта, що став підставою для зняття грифа, аналогічні відмітки роблять на опису і на номенклатурі справ;
- ж) проведення експертизи наукової цінності документів і справ з грифом “ДСК”, затвердження її результатів здійснюється відповідно до Положення про принципи і критерії визначення цінності документів, затвердженого постановою Кабінету Міністрів України від 20 жовтня 1995 р. № 853.

8. Порядок передачі справ із структурних підрозділів до архівного підрозділу організації, а також відібрання для знищення передбачає здійснення таких дій:

- а) передача до архівного підрозділу справ з документами з грифом “ДСК” з терміном обмеження до 10 років включно здійснюється за номенклатурами справ, описи при цьому можуть не складатися;
- б) підготовка справ для архівного зберігання здійснюється згідно з правилами, встановленими Головархівом;
- в) справи з грифом “ДСК” постійного зберігання передаються до державних установ з обов’язковою посторінковою перевіркою документів, включених до них;
- г) відібрані для знищення справи з грифом “ДСК” можуть оформлятися окремим актом або включатися у загальний акт з іншими несекретними справами, відібраними до знищення, після номерів цих справ проставляється відмітка “ДСК”;
- д) відібрані для знищення документи, справи і видання з грифом “ДСК” перед здачею на переробку як макулатура повинні подрібнюватися до стану, що виключає можливість прочитати їх; після знищення матеріалів з грифом “ДСК” в облікових документах (картках, журналах, номенклатурах справ, описах справ тимчасового зберігання) робиться відповідна відмітка;
- є) інформаційні бюлетені, реферативні інформаційні видання, телефонні та адресні довідники, друкарський брак знищується без акта, але з відміткою в облікових формах і засвідчується підписами виконавця і працівника, відповідальних за їх облік і зберігання;
- ж) відібрані до знищення документи з грифом “ДСК” на переробку як макулатура можна не подрібнювати згідно з вказівками керівників організації, у володінні якої перебувають ці документи.

9. Видача громадянам України видань з грифом “ДСК” у бібліотеках здійснюється з дотриманням правил:

- а) забороняється включати видання з грифом “ДСК” у відкриті каталоги та бібліографічні покажчики;
- б) видання з грифом “ДСК” включаються тільки у службові каталоги;
- в) видача у масових бібліотеках громадянам України видань з грифом “ДСК” здійснюється за письмовими клопотаннями керівників організації, в яких працюють ці громадяни, із зазначенням теми роботи;
- г) дозволи на видачу громадянам України видань з грифом “ДСК” у масових бібліотеках дійсні протягом року;
- д) у відомчих бібліотеках закритого типу видання з грифом “ДСК” видаються співробітникам цієї організації за списками, затвердженими керівником організації;
- е) у відомчих бібліотеках закритого типу видання з грифом “ДСК” видаються співробітникам цієї організації за письмовим дозволом керівника організації, що зберігає ці видання;
- є) у відомчих бібліотеках закритого типу видання з грифом “ДСК” видаються співробітникам інших організацій за письмовим зверненням цих організацій та з письмового дозволу керівника організації, що зберігає ці видання;
- ж) видання з грифом “ДСК” можуть видаватися по міжбібліотечному абонементу на підставі письмових запитів керівників організації, яким ці видання потрібні, за письмовим дозволом керівника, що зберігає ці видання.

Література [8; 10; 23; 41; 43; 48]

Тема 7. Досвід захисту комерційних секретів західними фірмами

Тема 8. Юридичне закріплення права підприємства на використання комерційної таємниці

Питання для самоконтролю

1. Охарактеризуйте, для чого підприємству необхідно закріпити право на комерційну таємницю, визначення її складу, обсяг та можливість захистити.
2. Чи можливо підприємству на правовій основі відшкодувати завдану шкоду від порушення його комерційної таємниці?

3. Виконання яких умов є обов'язковим при роботі з комерційною таємницею та дозволяє підприємству створити правові гарантії його права на комерційну таємницю?
4. Назвіть внутрішні документи підприємства, в яких здійснюється закріплення його права на комерційну таємницю.
5. Аргументуйте, чому з погляду права комерційну таємницю пов'язують з засобами захисту від неякісної конкуренції в межах реалізації права на інтелектуальну власність.
6. Яке значення має в захисті комерційної таємниці розроблений і затверджений керівником підприємства і введений в дію "Перелік відомостей, що становлять комерційну таємницю підприємства"?
7. Який внутрішній документ підприємства передбачає створення на підприємстві системи допуску і доступу до його комерційної таємниці?
8. Назвіть види оформлення договірних зобов'язань про зберігання комерційної таємниці з тими працівниками, які мають до неї відношення як виконавці певної роботи або як посадові особи.
9. В якому розділі статуту необхідно зафіксувати положення про те, що підприємство має право класифікувати інформацію як комерційну таємницю та визначити порядок її захисту?
10. Ким визначається порядок захисту комерційної таємниці і хто має право вимагати від співробітників виконання встановленого на підприємстві порядку та правил збереження комерційної таємниці?

Практичні завдання

1. Доведіть, що підприємству слід зафіксувати в статуті право не виконувати вимоги органів державного управління, якщо вони виходять за межі їх повноважень, пов'язаних з доступом до комерційної таємниці.
2. Обґрунтуйте, чи записані в статуті положення дають підприємству право вимагати захисту своїх інтересів перед державними і судовими органами; включати вимоги щодо захисту конфіденційної інформації в усі види договорів підприємницького характеру; користуватися цією інформацією для отримання прибутків.
3. За якою схемою повинна бути зафіксована в Установчому договорі вимога до його учасників про необхідність дотримання правил щодо збереження комерційної таємниці.
4. Які необхідно передбачити у Колективному договорі обов'язки адміністрації та колективу працівників підприємства щодо забезпечення збереження комерційної таємниці.

5. Наведіть загальні правові підстави для внесення в статут положень, які дають підприємству право вимагати захисту своїх інтересів і комерційної таємниці.

6. Охарактеризуйте основні форми застосування активної охорони комерційної таємниці від несанкціонованого власником використання.

7. Проаналізуйте можливі етапи організації активної охорони комерційної таємниці на підприємстві, які повинні бути відображені в "Положенні про дозвільну систему доступу співробітників підприємства та представників сторонніх організацій до відомостей, які мають комерційну таємницю підприємства".

8. Охарактеризуйте об'єкти, що контролюють надійність прийнятих до реалізації заходів з охорони комерційної таємниці, оскільки система контролю є дієвим засобом щодо виявлення недоліків у забезпеченні збереження комерційної таємниці.

9. Наведіть правомірність певних вимог і нормативних положень, яких необхідно дотримуватись при розробці статутів і установчих договорів щодо закріплення права підприємства на комерційну таємницю.

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь.

1. **Нормативні положення, які слід внести до Установчого Договору, щоб закріпити право підприємства на організацію роботи з захисту комерційної таємниці:**

- а) склад засновників;
- б) розмір статутного фонду;
- в) порядок утворення статутного фонду;
- г) порядок оцінки нематеріальних внесків;
- д) порядок прийняття рішень з управління товариством;
- е) порядок захисту інтелектуальної власності, яка є внеском в статутний фонд і є комерційною таємницею одного чи кількох засновників;
- є) порядок входження в об'єднання будь-якого із його засновників (юрідичних осіб) з власною системою захисту комерційної таємниці;
- ж) прийняття рішень про спільну власність на комерційну таємницю всіх або частини засновників об'єднання на умовах, передбачених Установчим договором;

з) закріплення за підприємством права на володіння, користування та розпорядження інформацією, яка у відповідності з законодавством України може бути віднесеною до категорії “комерційно-таємниці”.

2. У Положенні про комерційну таємницю підприємства важливо зафіксувати певні дії з організації активної охорони комерційної таємниці та правила її збереження:

- а) визначити предмет охорони;
- б) встановити періоди існування конкретних відомостей як комерційної таємниці;
- в) виділити категорії носіїв комерційної таємниці;
- г) скласти схему роботи та переміщення конкретних відомостей;
- д) розробити дозвільну систему доступу до відомостей, що мають комерційну таємницю;
- е) визначити відповідальних осіб за охорону і використання комерційної таємниці;
- є) передбачити матеріальне заохочення осіб, які забезпечують охорону комерційної таємниці;
- ж) використання носіїв інформації, що роблять неможливим несанкціоноване її копіювання.

3. До Колективного договору необхідно внести нормативні положення з забезпечення збереження комерційної таємниці:

- а) взаємні обов'язки адміністрації та колективу співробітників підприємства з позиції правового захисту комерційної таємниці;
- б) порядок робіт з комерційною інформацією (документами, виробами, продукцією) співробітників;
- в) відповідальність за порушення порядку роботи з комерційною таємницею;
- г) для запобігання можливості завдати економічних збитків підприємству адміністрація зобов'язується організувати та забезпечити систему заходів з захисту комерційної таємниці;
- д) колектив зобов'язується дотримуватися встановлених на підприємстві порядку та правил збереження комерційної таємниці;
- е) адміністрація зобов'язується забезпечити працівників підприємства, які мають відношення до комерційної таємниці, необхідними методичними матеріалами і інструкціями, проводити навчання працівників з проблем захисту комерційної таємниці;

є) за порушення встановленого на підприємстві порядку роботи з конфіденційною, комерційною таємницею усувати від роботи з такою інформацією;

ж) притягати порушників порядку роботи з відомостями, що мають комерційну таємницю, до дисциплінарної та іншої відповідальності, передбаченої КЗПП України.

Література [41; 43; 49–51; 56; 57; 70]

Тема 9. Права та обов'язки власника прав на комерційну таємницю

Тема 10. Допуск до комерційної таємниці співробітників підприємства

Питання для самоконтролю

1. Право керівника підприємства, незалежно від форми власності, встановлювати спеціальні правила регулювання допуску до інформації категорії “комерційна таємниця”, забезпечуючи тим самим умови для її збереження.
2. Вимоги, які доцільно взяти за основу при організації роботи з допуску співробітників підприємства до комерційної таємниці.
3. Загальна характеристика змісту поняття “допуск до комерційної таємниці”.
4. Правові навантаження на поняття “допуск персоналу до комерційних секретів”.
5. Юридичні зобов'язання, що виникають у зв'язку з існуючим порядком допуску персоналу підприємства до комерційної таємниці.
6. Наслідки, які можуть виникнути у випадках, коли співробітник порушує вимоги, пов'язані з зобов'язанням про збереження довіреної йому комерційної таємниці.
7. Характеристика триступеневої системи важливості комерційної таємниці.
8. Особливості оформлення допуску конкретного співробітника до комерційної таємниці за ступенем важливості.
9. Коли допуск до комерційної таємниці співробітників підприємства вважається правомірним, тобто має юридичну силу?
10. Хто має право позбавляти співробітника допуску до комерційної таємниці?

Практичні завдання

1. Охарактеризуйте методологію вивчення та перевірки власного підприємства або уповноваженою ним особою кандидата для роботи з відомостями, що мають комерційну таємницю.
2. Підготуйте в довільній формі так зване попередження-зобов'язання про нерозголошення співробітником підприємства після звільнення комерційних секретів, до яких він мав доступ.
3. Підготуйте реферат на тему "Юридичне поняття допуску до комерційної таємниці".
4. Підготуйте реферат на тему "Перевірка осіб, що оформляються до комерційних секретів".
5. Охарактеризуйте дві різні юридичні категорії "допуск" і "доступ" до комерційної таємниці, чим вони відрізняються?
6. Розкрийте шляхи оформлення власником підприємства рішення про надання доступу до конкретної комерційної таємниці і її матеріальних носіїв представнику сторонньої організації і збереження цієї особою конфіденційної інформації, з якою він був ознайомлений.
7. Охарактеризуйте поняття "режим доступу до інформації" відповідно до ст. 28 Закону "Про інформацію".
8. Розкрийте особливості способів вирішення питання про юридичні гарантії збереження в таємниці конфіденційної інформації підприємства, до якої отримали доступ представники органів державного управління та ділових кіл.
9. Підготуйте в письмовому вигляді "Положення про дозвілну систему доступу співробітників підприємства і представників сторонніх організацій до відомостей, що мають комерційну таємницю підприємства".

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь.

1. **Допуск до комерційної таємниці надається дієздатним громадянам України віком від 18 років і передбачає враховувати такі фактори:**
 - а) перевірку співробітника в зв'язку з допуском до комерційної таємниці;
 - б) ознайомлення співробітника з ступенем відповідальності за порушення законодавства про розголошення комерційної таємниці;

- в) виявлення в оформлюваного підозрілих зв'язків з співробітниками конкуруючих фірм;
 - г) встановлення недостовірних відомостей під час підготовки матеріалів до оформлення допуску;
 - д) наявність судимості за тяжкі злочини, насамперед за протиправні дії, пов'язані з комерційним шпигунством, зловживаннями в сфері кредитно-фінансової і економічної діяльності;
 - е) відсутність у співробітника підприємства обгрунтованої необхідності в роботі з комерційною таємницею;
 - є) наявність у співробітника психічних захворювань, тяжіння до вживання наркотичних засобів;
 - ж) тяжіння до вживання алкоголю, внаслідок чого може статися витік інформації.
- ## 2. Причинами та підставами для позбавлення допуску можуть бути:
- а) розголошення співробітником довіреної йому конфіденційної таємниці;
 - б) невиконання вимог режиму, встановленого "Положенням про комерційну таємницю та правила її збереження";
 - в) сприяння вітчизняним і іноземним конкурентам у здійсненні діяльності, яка завдає шкоди інтересам підприємства;
 - г) грубе порушення співробітником "Положення про комерційну таємницю";
 - д) втрата співробітником документів та інших матеріальних носіїв, які містять комерційну таємницю;
 - е) виявлення щодо співробітника відомостей, які компрометують його і які він приховував, а тому вони не могли бути враховані при вирішенні питання про допуск;
 - є) переведення співробітника на іншу ділянку роботи або посаду, що не пов'язана з необхідністю доступу до відомостей, що складають комерційну таємницю;
 - ж) тяжіння до вживання алкоголю.

3. На Заході перевірка на благодійність громадян, які отримують допуск до фірмових і банківських секретів, включають такі дії:

- а) співбесіда в кадровому апараті, коли кандидат на роботу з комерційною таємницею заповнює необхідні документи;

- б) намагання отримати максимум відомостей, зокрема: як часто і чому кандидат змінює місце роботи, за якими адресами мешкав, де служив;
- в) перевірка за основними і додатковими картотеками МВС;
- г) встановлення за місцем проживання кандидатів контактів з дільничними інспекторами поліції з метою перевірки способу життя, поведінки, виявлення компрометуючих зв'язків;
- д) після всіх перевірок за спеціально розробленими методиками методист-психолог проводить тестування;
- е) з'ясування мети та обставин поїздки за кордон;
- є) перевірка біографічних даних кандидата за останні 10 років;
- ж) ґрунтовне вивчення досьє кандидата на роботу з комерційною таємницею.

4. Зобов'язання про нерозголошення комерційної таємниці має мати такі реквізити:

- а) прізвище, ім'я, по батькові співробітника;
- б) посада;
- в) зобов'язання не розголошувати відомості, що мають комерційну таємницю;
- г) попередження про те, що у випадку розголошення довірених секретів з ним може бути розірвано трудову угоду за ініціативою власника підприємства;
- д) попередження про те, що у випадку розголошення комерційної таємниці підприємства робітник може бути притягнутий до відповідальності в порядку, встановленому законодавством України;
- е) дата та особистий підпис співробітника, який дав зобов'язання;
- є) підпис представника служби безпеки, що проінструктував співробітника, який підписав зобов'язання;
- ж) попередження-зобов'язання про нерозголошення після звільнення комерційних секретів, до яких робітник мав доступ.

Література [56; 60; 63; 65; 70–71]

Тема 11. Обов'язкові умови, пов'язані із забезпеченням захисту комерційної таємниці підприємства

Тема 12. Особливості правової охорони конфіденційної інформації при укладенні угоди з іноземною фірмою

Змістовий модуль III. Правові основи захисту комерційної таємниці та організаційне забезпечення діяльності з охорони інформації з обмеженим доступом

Тема 13. Правове регулювання питань збереження комерційної таємниці при укладенні підприємницьких договорів та веденні ділових переговорів

Тема 14. Технічний захист інформації, що містить комерційну таємницю

Тема 15. Попередження правопорушень у сфері використання інформаційних технологій

Питання для самоконтролю

1. Регулювання правових відносин щодо захисту інформації в автоматизованих системах за умов дотримання права власності громадян України і юридичних осіб на інформацію, права власника інформації на її захист.
2. Загальна характеристика механізму управління захистом інформації в автоматизованих системах і здійснення постійного контролю за дотриманням інформаційної безпеки.
3. Значення і можливості забезпечення режиму секретності під час обробки інформації в автоматизованих системах.
4. Назвіть державні стандарти, що визначають особливості захисту інформації в автоматизованій системі.
5. Дайте визначення понять "автоматизована система", "інформаційно-телекомунікаційна система".
6. Охарактеризуйте групи відносин, що виникають між суб'єктами в процесі обробки інформації в автоматизованій системі.
7. Яким шляхом забезпечується захист інформації в АС?
8. Охарактеризуйте особливості відповідальності за порушення законодавства про захист інформації в автоматизованих системах.

9. Назвіть орган, уповноважений здійснювати управління захистом інформації в автоматизованих системах відповідно до Закону України “Про захист інформації в автоматизованих системах” від 5 липня 1994 р.

Практичні завдання

1. Підготуйте письмові відповіді на запитання:

- 1) Що необхідно зробити для забезпечення надійного захисту в разі застосування програмно-технічних обчислювальних засобів імпортного походження при приєднанні їх до Інтернету?
 - 2) Розкрийте специфіку відносин, що виникають між суб'єктами в процесі обробки інформації в автоматизованій системі.
 - 3) Систематизуйте підстави для виникнення відносин, що виникають між суб'єктами в процесі обробки інформації в автоматизованій системі.
 - 4) Хто повинен забезпечити захист інформації, якщо інформація є власністю держави або належить іншому власнику?
 - 5) Охарактеризуйте особливості відповідальності власника АС за шкоду, заподіяну власнику інформації.
 - 6) Охарактеризуйте відносини між власником інформації та користувачем, що виникають під час захисту інформації в автоматизованих системах.
- 2.** Підготуйте реферат на тему “Захист інформації в автоматизованих системах”.
- 3.** Підготуйте реферат на тему “Відповідальність за порушення законодавства про захист інформації в автоматизованих системах”.
- 4.** Підготуйте реферат на тему “Застосування заходів щодо захисту конфіденційної інформації, що циркулює в автоматизованій системі органів державної влади”.

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь.

1. Захист інформації в АС відповідно до ст. 10 Закону України “Про захист інформації в автоматизованих системах” забезпечується шляхом:

- а) дотримання суб'єктами правових відносин норм, вимог та правил організації інформації та технічного характеру щодо захисту оброблюваної інформації;
- б) дотримання суб'єктами правових відносин вимог та правил щодо захисту та доступу до інформації, яка є власністю держави;

ви, або інформації, захист якої гарантується державою, встановлюється державним органом (ДСТСЗІ);

- в) використання засобів обчислювальної техніки;
- г) застосування засобів зв'язку і АС в цілому, які мають відповідний сертифікат;
- д) використання;
- е) перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому встановленим вимогам щодо захисту інформації;
- є) сертифікація засобів обчислювальної техніки, засобів зв'язку і АС;
- ж) здійснення контролю щодо захисту інформації;
- з) здійснення перевірки, сертифікації у розроблених заново засобах захисту інформації.

2. Для розв'язання завдань зі сфери технічного захисту інформації на практиці найчастіше застосовують:

- а) спеціальні широкосмугові передавачі для створення загордженної активної прямо шумової перешкоди;
- б) прилади, що унеможливають застосування закладних прослуховуючих пристроїв;
- в) пристрої, що унеможливають перехоплення електромагнітних коливань, випромінюваних радіотехнічними засобами;
- г) екранування комп'ютера;
- д) металеві листи, які можна покласти на двері, стіни, підлогу, стелю для досягнення екранування приміщень;
- е) обов'язкове екранування тих кімнат і боксів, в яких розміщено сервери корпоративної мережі та Інтернет;
- є) підтвердження реальних наслідків (ефективності) застосовуваних методів активного або пасивного захисту інформації шляхом вимірювання рівня сигналів, випромінюваних комп'ютером;
- ж) проведення робіт з перевірки ефективності екранування по всьому периметру захищеної від випромінювання зони.

3. Найважливішими структурними елементами системи захисту інформації, пов'язаними взаємними відносинами, можна вважати такі засоби захисту:

- а) фізичні;
- б) адміністративні;
- в) апаратні;
- г) антивірусні програми;

- д) засоби, що мінімізують високочастотні випромінювання комп'ютера;
- е) криптографічні;
- є) атестація системи комп'ютерної безпеки;
- ж) технології, засновані на нашілені спеціальних матеріалів на внутрішню поверхню корпусу комп'ютера з метою знизити рівень сигналу, що випромінюється робочою станцією.

4. Технічні канали відтоку інформації створюються людиною штучно шляхом:

- а) встановлення в комп'ютері закладок;
- б) встановлення в мережі електроживлення радіотрансляторів;
- в) високочастотного навіязування (тобто контактним способом вводять струми високої частоти через мережу електроживлення на нелінійні елементи);
- г) прийняття контрольним приймачем електромагнітних коливань на комбінаційних частотах, які промодульовані інформаційними сигналами, опрацьованими в комп'ютері;
- д) формування таємного каналу передачі цифрової інформації у вигляді файлів (стегосистема);
- е) приховування таємних повідомлень за допомогою окремих спецпрограм, алгоритмів, способів, які дають можливість шукати потрібну інформацію у комп'ютері і передавати її шляхом модулювання зображення монітора;
- є) керованих електромагнітних паразитних випромінень за допомогою програмних засобів;
- ж) стандартної техніки застосування "вірусів".

Література [24; 45; 49; 52–54; 60; 65]

Тема 16. Формування підрозділу інформаційної безпеки СБ підприємства та заходи щодо захисту комерційної таємниці

Питання для самоконтролю

1. Охарактеризуйте законодавчу базу України, яка дозволяє створювати підрозділ інформаційної безпеки служби безпеки підприємства.
2. Система правового захисту комерційної таємниці має певні принципи побудови. Проаналізуйте їх.
3. Охарактеризуйте принцип комплексного системного підходу до вирішення проблем захисту комерційної таємниці, який знахо-

дить відображення в законах "Про банки і банківську діяльність", "Про захист на винаходи і корисні моделі" і включає комплекс певних заходів.

4. Хто відповідає за організацію і забезпечення захисту комерційної таємниці підприємства і який спеціальний підрозділ має певні права, пов'язані із захистом комерційної таємниці?
5. Керівник якого підрозділу підприємства може бути уповноваженою особою власника підприємства з питань захисту комерційної таємниці?
6. Охарактеризуйте основні вимоги щодо захисту комерційної таємниці, які повинні знати співробітники підприємства та ступінь їх особистої відповідальності за порушення встановлених правил захисту комерційної таємниці.
7. Яким вимогам повинні відповідати відомості, які виробляються підприємством та його працівниками, щоб бути скерованими в загальні внутрішні та зовнішні інформаційні потоки, що потребують захисту?
8. Назвіть застережні заходи в роботі з чернетками документів, що використовуються при підготовці документів обмеженого користування. Проаналізуйте їх.
9. Наведіть особливості попередження витоку конфіденційних відомостей, які підготовлені на підприємстві для засобів масової інформації і пов'язані з його діяльністю.
10. У чому полягає організація на підприємстві відповідного режиму поведінки з комерційною таємницею в місцях проведення виробничих нарад, ділових переговорів з питань, які мають комерційну таємницю, що передбачено Указом Президента України від 27 вересня 1999 р. "Про положення про технічний захист інформації"?

Практичні завдання

1. Підготуйте письмові відповіді на запитання.

1. Дайте перелік фахівців підрозділу інформаційної безпеки служби безпеки підприємства і охарактеризуйте їхні функціональні обов'язки.
2. Розкрийте головні завдання підрозділу інформаційної безпеки служби безпеки підприємства.
3. Яка роль підрозділу інформаційної безпеки СБ підприємства у організації і веденні належного обліку документів з грифом "комерційна таємниця"?

4. Яким чином здійснюється співробітниками підрозділу інформаційної безпеки СБ підприємства квартальна і річна перевірка наявності документів, що не потрібні в роботі?
5. Що розуміють під принципом, який на практиці часто називається "політикою частих столів"?
6. Охарактеризуйте заходи співробітників підрозділу інформаційної безпеки щодо запобігання розголошення і витоку комерційних секретів при веденні діловодства, а також за відкритого службового листування.
7. Яким чином органи судової влади та прокуратури забезпечують охорону права юридичних осіб на комерційну таємницю?
8. Назвіть нормативно-правові акти за ієрархією, що регулюють суспільні відносини в сфері охорони комерційної таємниці.
9. Розкрийте повноваження співробітників підрозділу інформаційної безпеки СБ підприємства у сфері забезпечення охорони комерційної таємниці.
10. Охарактеризуйте порядок обліку і зберігання співробітниками підрозділу інформаційної безпеки СБ підприємства конфіденційної інформації, що є власністю підприємств, які не підпадають під державне управління (комерційні банки, господарські товариства, асоціації, концерни і т. п.).

2. Підготуйте реферат на тему "Формування підрозділу інформаційної безпеки СБ підприємства з забезпечення захисту комерційної таємниці".

3. Підготуйте реферат на тему "Застосування підрозділом інформаційної безпеки СБ підприємства заходів захисту відомостей, що містяться в конкретних носіях комерційної інформації".

4. Підготуйте реферат на тему "Застосування підрозділом інформаційної безпеки СБ підприємства загальних засобів забезпечення захисту відомостей, що містять комерційну таємницю".

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь.

1. **У структуру підрозділу інформаційної безпеки СБ підприємства можуть входити:**
 - а) керівник підрозділу інформаційної безпеки (заступник начальника служби безпеки підприємства);
 - б) юрист;

- в) фахівці в галузі економічної розвідки, промислової контррозвідки;
- г) фахівці, які вміють застосовувати спеціальну техніку для захисту приміщень;
- д) системний адміністратор;
- е) системний програміст;
- є) криптограф;
- ж) аудитор;
- з) спеціаліст інформаційної системи.

2. Основні напрямки захисту комп'ютерної системи підприємства:

- а) захист апаратури та носіїв інформації від пошкодження, викрадення, знищення;
- б) захист інформації в мережах зв'язку та вузлах комутації;
- в) захист від витоку інформації через побічні канали електромагнітних випромінювань та наведень;
- г) захист інформаційних ресурсів від несанкціонованого доступу;
- д) захист юридичної значущості електронних документів (забезпечення доказу правдивості того, що документ був створений і відправлений справді автором);
- е) захист від незаконного проникнення в комп'ютерні системи і мережі, автоматизовані системи, здатного спричинити перекручення або знищення інформації чи то носіїв інформації;
- є) захист від втручання в роботу комп'ютерних мереж банків через мережу "Інтернет" для отримання доступу до конфіденційної інформації шляхом "зламу систем захисту";
- ж) оптимізація організаційних і організаційно-технічних заходів опрацювання конфіденційної інформації з метою попередження її викрадення, знищення.

3. Виходячи з вимог безпеки інформації, пошук радіоелектронних засобів несанкціонованого знімання інформації повинен, серед яких можна назвати такі:

- а) вивчення службою безпеки підприємства оперативної обстановки біля об'єкта інформації;
- б) перевірка радіоэфіру за межами приміщення;
- в) перевірка монітору радіоэфіру у приміщенні за допомогою нелінійних локаторів у діапазоні частот 0,1–2000 МГц;
- г) перевірка комп'ютерів, телефонних апаратів, електротехнічних засобів за допомогою скануючого приймача;

- д) перевірка стін приміщення за допомогою діапазонного скануючого приймача або індикаторів поля;
 - е) обстеження меблів та інших предметів у приміщенні за допомогою детектора випромінювання;
 - є) перевірка телефонної та електричної лінії за допомогою комп'юлексу "Scanner 99";
 - ж) технічний контроль за спеціальною апаратурою, що використовується для забезпечення безпеки і таємності інформації.
- 4. Роботи з захисту інформації, що обертається в комп'ютерах і комп'ютерних мережах, проходять у таких напрямках:**
- а) протидія несанкціонованому доступу до інформаційних потоків підприємства за допомогою програмного забезпечення і засобів інженерно-технічної розвідки;
 - б) блокування несанкціонованого доступу до зберігання і опрацювання інформації за допомогою засобів обчислювальної техніки, що передається через лінії зв'язку абонентів;
 - в) попередження несанкціонованої модифікації інформації;
 - г) обстеження підрозділом інформаційної безпеки підприємства об'єктів, на яких використовуються комп'ютерні технології;
 - д) атестування системи комп'ютерної безпеки з метою підтвердити відповідність вимогам стандарту безпеки інформації;
 - е) категорювання об'єктів, що мають комп'ютерні системи;
 - є) використання рубіжної системи захисту підприємницької інформації;
 - ж) шляхом тотального контролю об'єктів захисту з ЕОМ.

Література [42; 52; 57; 58; 63–65]

Тема 17. Механізм реалізації прав особи на комерційну таємницю

Питання для самоконтролю

1. Розкрийте зміст поняття "персональні дані".
2. Розкрийте зміст поняття "конфіденційна інформація".
3. Дайте перелік засобів охорони персональних даних в Україні.
4. Процедура захисту прав громадян щодо обмеження поширення персональних даних.
5. Інформація про стан здоров'я особи, як об'єкта правового захисту.
6. Розкрийте зміст механізму захисту конфіденційної інформації в інтересах її власника.

7. Відповідальність за порушення порядку обігу персональних даних.
8. Порядок використання засобами масової інформації персональних даних.
9. Яка роль Конституційного Суду України у формуванні засад захисту персональних даних?
10. Недоліки чинного законодавства у сфері судового захисту прав громадян щодо обмеження на поширення відомостей, які знаходяться у власності, користуванні чи розпорядженні окремих фізичних осіб і розголошуються за їх бажанням відповідно до передбачених ними умов.

Практичні завдання

Підготуйте письмові відповіді на запитання:

1. Що розуміють під головними засадами механізму захисту конфіденційної інформації, що знаходиться у власності, користуванні чи розпорядженні окремих фізичних осіб.
2. Як на законодавчому рівні розглядають конфіденційну інформацію про стан здоров'я особи?
3. Ваші погляди на обмеження журналістських розслідувань щодо збирання, зберігання, використання та поширення конфіденційної інформації про приватну особу без її згоди, з урахуванням, що вона не є публічною, а тому інформація не є суспільно необхідною.
4. Підготуйте реферат на тему "Предмет адвокатської таємниці".

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь.

1. **Медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про стан здоров'я особи, не мають права розголошувати інформацію, крім передбачених законодавчими актами випадків:**
 - а) факт звернення за медичною допомогою фізичної особи;
 - б) результати медичного обстеження, огляду;
 - в) інтимну і сімейну сторону життя громадянина;
 - г) діагноз;
 - д) методи лікування фізичної особи;
 - е) ким, коли і на яких підставах громадянина було поставлено на облік у психоневрологічному диспансері;
 - ж) ким, коли і на яких підставах громадянина було знято з обліку у психоневрологічного диспансері;

- з) інформацію з диспансерної картки.
- 2. Забороняється будь-яке втручання в адвокатську діяльність, вимагати відомості, що становлять адвокатську таємницю, зокрема:**
- а) адвокат, його помічник не можуть бути допитані з певних питань як свідки;
 - б) документи, пов'язані з виконанням адвокатам доручення, не підлягають оглядові;
 - в) без згоди адвоката документи, пов'язані з виконанням ним доручення, не підлягають вилученню;
 - г) без санкції Генерального прокурора України, його заступника, прокурорів Республіки Крим, області, міста Києва забороняється прослуховування телефонних розмов адвокатів у зв'язку з оперативно-розшуковою діяльністю;
 - д) забороняється чинити будь-які перешкоди здійсненню правомірної діяльності адвоката з надання правової допомоги або порушення встановлених законом гарантій їх діяльності та професійної таємниці;
 - е) при здійсненні професійних обов'язків адвокат зобов'язаний зберігати в таємниці питання, з яких громадянин звертався до нього, суть консультацій, порад, роз'яснень та інших відомостей;
 - ж) адвокату, помічнику адвоката забороняється використовувати відомості, що становлять предмет адвокатської таємниці у своїх інтересах або в інтересах третіх осіб;
 - з) документи, пов'язані з виконанням адвокатом доручення, не підлягають розголошенню.

3. Захист інформації про майновий стан особи забезпечено інститутом банківської таємниці, тому банки зобов'язані гарантувати таємницю:

- а) банківського рахунку;
- б) операцій за рахунком;
- в) відомостей про фінансово-економічний стан клієнтів;
- г) стану рахунків клієнтів;
- д) відомостей про клієнта;
- е) операцій, які було здійснено на користь чи за дорученням клієнта;
- є) здійснені клієнтом угоди;
- ж) кореспондентських рахунків банків у Національному банку України.

4. Права власника патенту:

- а) патент надає його власнику виключне право використовувати винахід (корисну модель) на свій розсуд;
- б) використання секретного винаходу власником патенту має здійснюватися з додержанням вимог Закону України "Про державну таємницю" та за погодженням із Державним експертом;
- в) власник деклараційного патенту на секретну корисну модель має право на одержання від державного органу, визначеного КМУ України, грошової компенсації на покриття витрат за сплату зборів, передбачених Законом України "Про охорону прав на винаходи і корисні моделі" від 15 грудня 1993 р. № 3687-XII.
- г) власник патенту може використовувати попереджувальне маркування із зазначенням номера патенту на продукті чи на упаковці продукту, виготовленого із застосуванням запатентованого винаходу;
- д) патент надає його власнику право забороняти іншим особам використовувати винахід (корисну модель) без його дозволу;
- е) власник патенту може передавати на підставі договору право власності на винахід (корисну модель) будь-якій особі, яка стає його правонаступником;
- ж) власник патенту надає будь-якій особі дозвіл (видає ліцензію) на використання винаходу (корисної моделі) на підставі ліцензійного договору;
- з) ліцензіар не має права надавати ліцензії на використання винаходу (корисної моделі) іншій особі на цій же території в об'єкті наданих ліцензійних прав;
- і) власник патенту може вимагати припинення дій, що порушують або створюють загрозу порушення його права і відновлення становища, що існувало до порушення права.

Література [3-6; 12-13; 19-20; 26; 41]

Тема 18. Правові відносини підприємства з контролюючими органами з питань, пов'язаних із захистом комерційної таємниці та конфіденційних відомостей

Тема 19. Правова характеристика уніфікованих основ захисту комерційної таємниці в міжнародному праві

Змістовий модуль IV. Локальні акти підприємства із захисту комерційної таємниці

Тема 20. Конструювання типової моделі корпоративної норми "Положення про комерційну таємницю підприємства та правила її збереження".

Тема 21. Типова модель методики визначення відомостей, що мають комерційну таємницю підприємства

Тема 22. Типова модель корпоративної норми "Положення про дозвілну систему доступу співробітників підприємства та представників сторонніх організацій до відомостей, що мають комерційну таємницю підприємства"

Тема 23. Типова модель організаційно-методичного документа з організації і ведення на підприємстві спеціального діловодства з носіями комерційної таємниці.

Тема 24. Типова модель корпоративної норми "Положення про підрозділ інформаційної безпеки СБ підприємства"

СПИСОК ЛІТЕРАТУРИ

Основна

1. Конституція України. — К., 1996.
2. Коментар до Конституції України. — К., 1996.
3. Цивільний кодекс України. — К., 2003.
4. Кодекс України про адміністративні правопорушення // Право України. — 1995. — № 3–4.

5. Кримінальний кодекс України від 5 квітня 2001 р. // ВВР України. — 2001. — № 25–26. — С. 131.
6. Господарський Кодекс України. — К., 2004.
7. Закон України "Про власність" (із змін та допов.) // ВВР України. — 1992. — № 30.
8. Про захист від недобросовісної конкуренції: Закон України від 7 червня 1996 р. № 236/96-ВР // "Голос України" від 02.07.96; ВВР України — 1996. — № 36. — С. 164. Вводиться в дію Постановою ВР від 7 черв. 1996 р. № 237/96-ВР з 1 січня 1997 р. (із змін. і допов., внесеними ЗУ від 18 листоп. 1997 р. № 642/97-ВР // "Голос України" від 17.12.97 р.; "Уряд. кур'єр" від 18.12.97 р.
9. Закон України "Про господарські товариства" // ВВР України. — 1991. — № 49 (із змін. і доп.).
10. Про захист економічної конкуренції: Закон України від 11 січня 2001 р. № 2210-Ш // ВВР України. — 2001. — № 12. — С. 64.
11. Закон України "Про внесення змін та доповнень до деяких законодавчих актів, що регулюють банківську діяльність" // Голос України. — 1994. — 1 квіт.
12. Закон України "Про патентування деяких видів підприємницької діяльності" // ВВР України. — 1996. — № 20. — С. 82.
13. Закон України "Про охорону прав на зазначення походження товарів" // ВВР України. — 1999. — № 32. — С. 267.
14. Закон України "Про Національний банк України" // ВВР України. — 1999. — № 29. — С. 238.
15. Закон України "Про усунення дискримінації в оподаткуванні суб'єктів підприємницької діяльності, створених з використанням майна та коштів вітчизняного походження" // ВВР України. — 2000 — № 12. — С. 97.
16. Закон України "Про природні монополії" // ВВР України. — 2000. — № 30. — С. 238.
17. Закон України "Про внесення змін та доповнень до деяких законодавчих актів України" // ВВР України. — 1993. — № 26.
18. Про основні напрями конкурентної політики на 2000–2002 роки та заходи щодо їх реалізації: указ Президента України від 26.02.2000 р.
19. Закон України "Про охорону прав на винаходи та корисні моделі" // Голос України. — 1994. — 3 берез.
20. Закон України "Про охорону прав на знаки для товарів та послуг" // Голос України. — 1994. — 17 лют.

21. Закон України “Про охорону прав на промислові зразки” // ВВР України. — 1994. — № 33.
22. Закон України “Про внесення змін і доповнень до Закону Української РСР “Про захист прав слюживачів” // Голос України. — 1994. — 15 січ.
23. Закон України “Про інформацію” // ВВР України. — 1992. — № 48. — Ст. 650.
24. Закон України “Про захист інформації в автоматизованих системах” // ВВР України. — 1994. — № 31. — Ст. 286.
25. Закон України “Про державну таємницю” // ВВР України. — 1994. — № 16. — Ст. 93. В ред. закону № 1079-XIV від 21.09.99 // ВВР України. — 1999. — № 49. — Ст. 428.
26. Закон України “Про науково-технічну інформацію” // ВВР України. — 1993. — № 33. — Ст. 345.
27. *Концепція* технічного захисту інформації в Україні: затв. постановою Кабінету Міністрів України від 8 жовт. 1997 р. № 1126.
28. “Положення про технічний захист інформації в Україні”: затв. указом Президента України від 27 верес. 1999 р. № 1229/99.
29. “Про затвердження Положення про контроль за функціонуванням системи технічного захисту інформації”: Департамент спеціальних телекомунікаційних систем та захисту інформації служби безпеки України: наказ № 61 від 22.12.99.
30. “Про затвердження Інструкції про порядок забезпечення режиму безпеки, що повинен бути створений на підприємствах, установах та організаціях, які здійснюють підприємницьку діяльність у галузі криптографічного захисту конфіденційної інформації, що є власністю держави”: Департамент спеціальних телекомунікаційних систем та захисту інформації служби безпеки України: наказ № 45 від 22.10.99.
31. “Про затвердження Положення про порядок розроблення, вивчення та експлуатації засобів криптографічного захисту конфіденційної інформації”: Департамент спеціальних телекомунікаційних систем та захисту інформації служби безпеки України: наказ № 53 від 30.11.99.
32. *Інструкція* про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави: затв. постановою Кабінету Міністрів України від 27.11.98 № 1893.
33. *Положення* про режимно-секретні органи в міністерствах, відомствах, уряді Автономної Республіки Крим, місцевих органах державної виконавчої влади, виконкомах Рад, на підприємствах,

- в установах і організаціях: затв. постановою Кабінету Міністрів України від 04.08.95 № 609.
 34. “Про затвердження Інструкції щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за їх дотриманням”: наказ № 46 Державної служби безпеки України з питань технічного захисту інформації від 23.05.94.
 35. *Інструкція* про умови і правила провадження підприємницької діяльності (ліцензійні умови), пов’язані з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, та контроль за їх дотриманням: затв. наказом Ліцензійної палати України та Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 17.11.98 №104/81.
 36. *Наказ Міністерства* України у справах науки і технологій, Міністерства економіки України, Міністерства фінансів України від 28.01.97 “Про затвердження Порядку комплексної перевірки діяльності науково-дослідних установ, які повністю або частково фінансуються за рахунок державного бюджету”.
 37. *Постанова* від 20 липня 1996 р. № 830 “Про затвердження Типового положення з планування, обліку і калькулювання собівартості науково-дослідних та дослідно-конструкторських робіт”.
 38. *Рішення Конституційного Суду* України від 30 жовтня 1997 р. у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України “Про інформацію” та статті 12 Закону України “Про прокуратуру” (справа К. Г. Устименка).
- Додаткова*
39. *Андрощук Г., Вороненке Л.* Методика виявлення свіденій, со- ставляючих комерческу тайну // Бизнесинформ. — 1999. — № 11–12. — С. 13–18.
 40. *Андрощук Г. А., Пахаренко А. П.* Право інтелектуальної соб- ственности в США // Бизнесинформ. — 1999. — № 16. — С. 12–15.
 41. *Андрощук Г., Вороненке Л.* Захист комерційної таємниці: економіко-правовий аспект // Інтелектуальна власність. — 1999. — № 9. — С. 7–15.
 42. *Андрощук Г., Вороненке Л.* Какіе свіденія могут составлять комерческу тайну // “Бизнесинформ.” — 1999. — № 9–10. — С. 12–18.

43. *Андрощук Г. О.* Правове регулювання захисту комерційної таємниці в Україні // "Адвокат". — 1997. — № 4 (7). — С. 49–53.
44. *Андрощук Г. А., Галак Н. М., Коваль А. А. и др.* Промышленная собственность: охрана и защита прав владельцев. — К., 1991. — 160 с.
45. *Андрощук Г. А., Давыдов И. Ю.* Предпринимательство и безопасность. — К.: Знания, 1993. — 27 с.
46. *Андрощук Г. А., Работягова Л. И.* Патентное право: правовая охрана изобретений: Учеб. пособие — К.: МАУП, 1999. — 216 с.
47. *Андрощук Г. О.* Пираты индустрии. — К.: Знания, 1991. — 48 с.
48. *Андрощук Г. О.* Правове регулювання ноу-хау // Проблеми науки. — 1999. — № 12. — С. 51–58.
49. *Андрощук Г. О.* Секретна інформація як об'єкт правової охорони // Інтелектуальна власність. — 1999. — № 3–4. — С. 29–34.
50. *Андрощук Г., Вороненко Л.* Коммерческая тайна и конкуренция // Проблемы науки. — 1999. — № 6. — С. 49–99.
51. *Андрощук Г., Вороненко Л.* Определение сведений, подлежащих защите при проведении опытно-конструкторских работ // Бизнесинформ — 1999. — № 13–14. — С. 9–11.
52. *Ержык Ж.* Промышленный шпионаж. — М.: Междунар. отношения, 1971. — 176 с.
53. *Гасанов Р. М.* Шпионаж и бизнес. — М., 1993. — 320 с.
54. *Громов Г. Р.* Очерки информационной технологии. — М.: Информарт, 1992. — 336 с.
55. *Гуров А. И.* Профессиональная преступность: прошлое и современность. — М.: Юрид. лит., 1990. — 304 с.
56. *Интеллектуальная собственность в Украине: правовые основы и практика:* Науч.-практ. изд.: В 4 т. / Под общ. ред. А. Д. Святоцкого. — К.: Ин Юре, 1999.
57. *Казакевич О. Ю., Кошчев Н. В., Максимешко В. Г., Пилия А. Г., Шиян Н. И.* Предприниматель в опасности: способы защиты: Практик. руководство для предпринимателей и бизнесменов. — М., 1992. — 72 с.
58. *Козлов С. Б., Иванов Е. В.* Предпринимательство и безопасность / Под общ. ред. Ю. Б. Долгополова. — М.: Агентство НТИ. — 1991. — Ч. 1, 2. — 507 с.
59. *Козлов С. Б., Иванов Е. В.* Предпринимательство и безопасность / Под общ. ред. Ю. Б. Долгополова. — М.: Агентство НТИ. — 1991. — Ч. 3. — 397 с.

60. *Коммерческая тайна* (поиск, суждения, размышления, предложения): Твор. коллектив "Секрет" объединения "Гал-приз". — Изд. 2-е, доп. — Львов, 1991. — 286 с.
61. *Корнеев Л. А.* Тайная война монополий. — К.: Политиздат Украины, 1978. — 126 с.
62. *Меньшиков А. А.* Правовые вопросы передачи ноу-хау в международной торговле: Автореф. дисс. на соискание ученой степени к. ю. н. — М.: ИГПАН СССР, 1983.
63. *Нелли О. Л., Низенко Е. Л., Панфилов В. М.* Роль негосударственных служб безопасности в защите экономических интересов предпринимательства. — К.: Поліграф-Сервіс, 2001.
64. *Низенко Е. Л.* Організаційно-правове забезпечення, формування та реалізація державної політики в сфері безпеки підприємництва // Зб. наук. пр. — Вип. 3. — К., 2003. — С. 79–84.
65. *Низенко Э. И.* Обеспечение безопасности предпринимательской деятельности: Учеб. пособие. — К.: МАУП, 2003. — 123 с.
66. *Никифоров Г. К., Азнакаев Г. Н.* Защита коммерческой тайны. — К.: Юринформ, 1994. — 88 с.
67. *Никифоров Г. К., Никифоров С. С.* Підприємництво та правовий захист комерційної таємниці: Навч.-практ. посіб. для вищ. навч. закл. — К.: Олан, 2001. — 208 с.
68. *Практика защиты коммерческой тайны в США:* Руководство по защите Вашей деловой информации. — М.: СП "Stokus Intel-nation", 1990. — 253 с.
69. *Свинсон Б.* Экономическая преступность: Пер. со швед.; Вступ. ст. М. А. Моргуновой и Ю. А. Решетова; Под ред. М. А. Моргуновой. — М.: Прогресс, 1987. — 160 с.
70. *Соловьев Э. Я.* Коммерческая тайна и её защита. — М., 1996. — 64 с.
71. *Чернявский А. А.* Безопасность предпринимательской деятельности: Конспект лекций. — К.: МАУП, 1998. — 124 с.
72. *Чернявский А. А.* Промышленный шпионаж и безопасность предпринимательства: Учеб.-метод. пособие. — К.: МЗУУП, 1994. — 64 с.
73. *Штумпф Г.* Договор о передаче ноу-хау. — М.: Прогресс, 1976. — С. 25.

ЗМІСТ

Пояснювальна записка.....	3
Тематичний план дисципліни	
“Правові основи захисту комерційної таємниці”	4
Зміст дисципліни	
“Правові основи захисту комерційної таємниці”	6
Список літератури.....	42

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *О. М. Коваленко*
Комп'ютерне верстання *І. О. Музика*

Зам. № ВКЦ-4303

Формат 60×84/16. Папір офсетний.
Друк ротативний трафаретний.

Наклад 30 пр.

Міжрегіональна Академія управління персоналом (МАУП)
03039 Київ-39, вул. Фрометівська, 2, МАУП

ДП «Видавничий дім «Персонал»

03039 Київ-39, просп. Червонозоряний, 119, літ. ХХ

*Свідчення про внесення до Державного реєстру
суб'єктів видавничої справи ДК № 3262 від 26.08.2008*