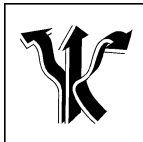


МІЖРЕГІОНАЛЬНА  
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ



МАУП



**НАВЧАЛЬНА ПРОГРАМА**  
дисципліни  
**“ЗАХИСТ ПІДПРИЄМНИЦЬКОЇ ІНФОРМАЦІЇ”**  
(для бакалаврів)

Київ 2006

Підготовлено директором УВКІ ім. Великого Князя Святослава  
*В. П. Каленяком* і викладачем кафедри безпеки і військово-козацьких  
дисциплін *А. М. Гривою*

Затверджено на засідання кафедри безпеки і військово-козацьких  
дисциплін УВКІ (протокол № 11 від 11.08.06)

*Схвалено Вченою радою Міжрегіональної Академії управління персоналом*

**Каленяк В. П., Грива А. М.** Навчальна програма дисципліни “Захист підприємницької інформації” (для бакалаврів). — К.: МАУП, 2006. — 18 с.

Навчальна програма містить пояснювальну записку, тематичний план, зміст дисципліни “Захист підприємницької інформації”, теми контрольних робіт, вказівки до виконання контрольної роботи, питання для самоконтролю, а також список літератури.

## ПОЯСНЮВАЛЬНА ЗАПИСКА

“Захист підприємницької інформації” — одна з основних дисциплін, яка забезпечує студентам здобуття комплексу теоретичних знань і практичних навичок щодо експлуатації технічних засобів охорони підприємств.

Програма дисципліни містить теоретичний матеріал і практичні рекомендації щодо розробки, впровадження та забезпечення функціонування системи захисту підприємницької інформації.

У теоретичному розділі висвітлюються правові основи інформаційної діяльності підприємств; загальна характеристика і можливості методів і засобів забезпечення безпеки підприємств, основні організаційно-правові заходи щодо охорони державної та комерційної таємниць, технічного захисту інформації з обмеженим доступом на підприємстві.

У практичній частині міститься навчальний матеріал, вивчення якого дає змогу студентам самостійно виконувати тактико-технічне обґрунтування вибору методів і засобів захисту інформації; здійснювати їх добір, установку та експлуатацію.

### ТЕМАТИЧНИЙ ПЛАН дисципліни “ЗАХИСТ ПІДПРИЄМНИЦЬКОЇ ІНФОРМАЦІЇ”

№ пор.	Назва змістового модуля і теми
1	2
	<b>Змістовий модуль I. Правові основи інформаційної діяльності підприємств</b>
1	Основні поняття і визначення інформаційної діяльності
2	Режим доступу до інформації
3	Міжнародна інформаційна діяльність
	<b>Змістовий модуль II. Охорона державної таємниці</b>
4	Охорона інформації
5	Основні організаційно-правові заходи щодо охорони державної таємниці
6	Режимно-секретні органи підприємств

1	2
7	<b>Змістовий модуль III. Захист інформації в автоматизованих системах</b> Державна політика в галузі технічного захисту інформації з обмеженим доступом
8	Класифікація автоматизованих систем і стандартні функціональні профілі захищеності інформації, що обробляється, від несанкціонованого доступу
9	Служба захисту інформації в автоматизованих системах, її права і завдання
10	Організаційний захист інформації
11	Захист інформації від витоку з технічних каналів
12	<b>Змістовий модуль IV. Захист комерційної інформації</b> Система правового захисту комерційної таємниці підприємства, її елементи та складові
13	Організація допуску та доступу до комерційної інформації
14	<b>Змістовий модуль V. Контроль за забезпеченням охорони підприємницької інформації</b> Відповідальність за порушення законодавства про державну та комерційну таємницю
15	Контроль за додержанням законодавства про державну (комерційну) таємницю та захисту інформації в АС на підприємстві
Разом годин: 81	

**ЗМІСТ**  
*дисципліни*  
**“ЗАХИСТ ПІДПРИЄМНИЦЬКОЇ ІНФОРМАЦІЇ”**

**Змістовий модуль I. Правові основи інформаційної діяльності підприємств**

**Тема 1. Основні поняття і визначення інформаційної діяльності**

Визначення інформації, її види та галузі. Державна інформаційна політика та головні напрями її реалізації. Основні принципи інфор-

маційних відносин. Права та обов'язки учасників інформаційних відносин. Суб'єкти та об'єкти інформаційних відносин. Інформаційна діяльність, її види та напрями.

*Література [1]*

### ***Тема 2. Режим доступу до інформації***

Режим доступу до інформації та його види. Державний контроль за додержанням встановленого режиму доступу до інформації. Доступ до відкритої інформації. Інформація з обмеженим доступом. Конфіденціальна інформація. Інформація комерційного та банківського характеру. Таємна інформація. Інформаційний запит щодо доступу до офіційних документів і запит щодо надання письмової або усної інформації. Право власності на інформацію.

*Література [1; 5]*

### ***Тема 3. Міжнародна інформаційна діяльність***

Зміст міжнародної інформаційної діяльності. Порядок міжнародного співробітництва в галузі інформації. Експорт та імпорт інформаційної продукції (послуг). Інформаційний суверенітет.

*Література [1]*

## **Змістовий модуль II. Охорона державної таємниці**

### ***Тема 4. Охорона інформації***

Охорона права на інформацію. Відповідальність за порушення законодавства про інформацію. Порядок оскарження протиправних дійнь.

*Література [1; 14]*

### ***Тема 5. Основні організаційно-правові заходи щодо охорони державної таємниці***

Державна політика щодо державної таємниці. Основні організаційно-правові заходи щодо охорони державної таємниці. Компетенція органів державної влади, органів місцевого самоврядування та їхніх посадових осіб у сфері охорони державної таємниці. Засекречування та розсекречування матеріальних носіїв інформації. Дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим. Допуск громадян до державної таємниці. Доступ громадян до державної таємниці. Обов'язки громадянина щодо збереження дер-

жавної таємниці. Обмеження прав у зв'язку з допуском та доступом до державної таємниці.

*Література* [2; 6; 14; 15; 17; 21]

### ***Тема 6. Режимно-секретні органи підприємств***

Порядок створення режимно-секретних органів, їх склад і мета діяльності. Порядок комплектування режимно-секретних органів спеціалістами. Основні завдання і права режимно-секретних органів.

*Література* [2; 6]

### **Змістовий модуль III. Захист інформації в автоматизованих системах**

#### ***Тема 7. Державна політика в галузі технічного захисту інформації з обмеженим доступом***

Шляхи забезпечення захисту інформації в АС. Вимоги і правила щодо захисту інформації, яка є власністю держави. Державне управління захистом інформації в АС.

*Література* [3; 16; 18–22; 25]

#### ***Тема 8. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності інформації, яка обробляється, від несанкціонованого доступу***

Визначення автоматизованої системи, вимоги до її функціонального складу. Класи та підкласи автоматизованих систем. Стандартні функціональні профілі захищеності, порядок їх визначення і застосування.

*Література* [31; 32]

#### ***Тема 9. Служба захисту інформації в автоматизованих системах, її права і завдання***

Призначення служби захисту інформації в АС. Завдання, функції, штатна структура служби захисту інформації, повноваження та відповідальність працівників служби, взаємодія з іншими підрозділами підприємства та зовнішніми організаціями. Організація служби захисту інформації.

*Література* [3; 6; 16; 19; 20]

### ***Тема 10. Організаційний захист інформації***

Комплексна система захисту інформації підприємства, порядок створення та основні вимоги до її функціонування. План захисту інформації в автоматизованій системі підприємства, його зміст і порядок розробки. Основні напрями організаційного захисту інформації. Аналіз внутрішніх і зовнішніх загроз для конфіденційної інформації. Організація роботи з співпрацівниками підприємства. Організація роботи з документами. Організація використання технічних засобів.

*Література* [3; 6; 16; 19; 20; 26]

### ***Тема 11. Захист інформації від витоку з технічних каналів***

Основні канали витоку інформації, їх групи та характеристики. Головна умова забезпечення безпеки інформації в АС. Зміст захисту інформації від витоку з технічних каналів. Основні завдання захисту. Захист інформації від витоку з візуально-оптичного каналу. Захист інформації від витоку з акустичного каналу. Захист інформації від витоку з електромагнітних каналів. Захищені електронно-обчислювальні машини. Захист від витоку за рахунок паразитної генерації. Захист від витоку за рахунок взаємного впливу проводів і ліній зв'язку. Захист від витоку з матеріально-речовинних каналів.

*Література* [3; 6; 16; 19; 20; 23; 24; 27–30]

## **Змістовий модуль IV. Захист комерційної інформації**

### ***Тема 12. Система правового захисту комерційної таємниці підприємства, її елементи та складові***

Концептуальні основи та принципи захисту комерційної таємниці. Поняття та ознаки комерційної таємниці. Об'єкти та суб'єкти права власності на комерційну таємницю. Юридичне закріплення права підприємства на комерційну таємницю. Організація роботи служби безпеки підприємства щодо захисту комерційної інформації. Визначення відомостей, що становлять комерційну таємницю підприємства.

*Література* [1; 7]

### ***Тема 13. Організація допуску та доступу до комерційної інформації***

Поняття допуску до комерційної таємниці. Перевірка осіб, які оформлюються до комерційної таємниці. Добір, виховання і навчан-

ня кадрів для роботи з комерційною таємницею. Порядок доступу до комерційної таємниці. Дозвільна система доступу до комерційної таємниці. Правове регулювання порядку збереження комерційної таємниці при укладенні господарських та інших підприємницьких договорів, веденні ділових переговорів.

*Література [1; 7]*

## **Змістовий модуль V. Контроль за забезпеченням охорони підприємницької інформації**

### ***Тема 14. Відповідальність за порушення законодавства про державну та комерційну таємницю***

Види порушень законодавства про державну таємницю, за здійснення яких передбачено дисциплінарну, адміністративну та кримінальну відповідальність. Кримінальна відповідальність за державну зраду, шпигунство, розголошення державної таємниці, втрату документів, що містять державну таємницю. Відповідальність за передачу або збирання відомостей, що становлять конфіденційну інформацію, яка є власністю держави. Незаконне використання спеціальних технічних засобів негласного отримання інформації. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем. Порушення правил експлуатації автоматизованих електронно-обчислювальних систем.

Кримінальна, цивільно-правова, адміністративна та дисциплінарна відповідальність за порушення законодавства про комерційну таємницю. Відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю. Відповідальність за розголошення комерційної таємниці.

*Література [2; 3; 7; 16; 19; 20]*

### ***Тема 15. Контроль за додержанням законодавства про державну (комерційну) таємницю та захисту інформації в АС на підприємстві***

Державні органи влади уповноважені здійснювати контроль за забезпеченням охорони державної таємниці, функціонуванням системи технічного захисту інформації. Види перевірок та їх зміст. Категорії порушень встановлених норм і вимог з технічного захисту



інформації. Порядок проведення атестації повноти та якості робіт з технічного захисту інформації на підприємстві. Методика контролю за додержанням законодавства про державну (комерційну) таємницю та захисту інформації в АС на підприємстві.

*Література* [2; 3; 7; 16; 19; 20]

### **ТЕМИ КОНТРОЛЬНИХ РОБІТ**

1. Порядок отримання підприємством спеціального дозволу на провадження діяльності, пов'язаної з державною таємницею.
2. Порядок розсекречування таємних документів.
3. Порядок продовження терміну дії рішення про віднесення інформації до державної таємниці.
4. Поняття інформаційного суверенітету України, шляхи та способи його забезпечення.
5. Правові норми допуску громадян України до державної таємниці.
6. Порядок комплектування спеціалістами режимно-секретних органів підприємств.
7. Порядок та обґрунтування вибору функціонального профілю захищеності автоматизованої система класу "1".
8. Порядок та обґрунтування вибору функціонального профілю захищеності автоматизованої система класу "2".
9. Порядок та обґрунтування вибору функціонального профілю захищеності автоматизованої система класу "3".
10. Порядок створення та організації роботи служби захисту інформації в автоматизованих системах підприємства.
11. Зміст етапів створення комплексної системи захисту інформації підприємства.
12. Сучасні методи та засоби захисту електронно-обчислювальних машин.
13. Спостереження як спосіб ведення економічної розвідки, його основні методи та засоби.
14. Сучасні методи та засоби захисту підприємницької інформації від витоку з візуально-оптичного каналу.
15. Сучасні методи та засоби захисту підприємницької інформації від витоку з акустичного каналу.
16. Загальні і специфічні методи захисту підприємницької інформації від витоку з електромагнітних каналів.

17. Сучасні проблеми організації захисту комерційної таємниці на підприємствах.
18. Передові досягнення в галузі захисту комерційних секретів іноземними компаніями.
19. Перевірка та вивчення ділових партнерів з метою збереження комерційної таємниці підприємства.
20. Ознаки інформації, що становить комерційну таємницю підприємства та організація спеціального режиму її використання.
21. Основні етапи створення системи захисту комерційної таємниці підприємства та їх зміст.
22. Складові системи захисту комерційної таємниці підприємства та їх характеристика.
23. Визначення відомостей, що становить комерційну таємницю підприємства.
24. Порядок надання допуску до комерційної таємниці підприємства та причини його позбавлення.
25. Порядок збереження комерційної таємниці підприємства після звільнення працівників, які були допущені до цих відомостей.
26. Порядок доступу до комерційної таємниці підприємства представників органів державної влади та управління.
27. Порядок доступу до комерційної таємниці підприємства представників суб'єктів підприємницької діяльності.
28. Призначення і зміст угоди між суб'єктами господарювання в межах України щодо нерозголошення комерційної таємниці.
29. Засоби несанкціонованого запису переговорів.
30. Засоби протидії несанкціонованому запису переговорів.

### ***ВКАЗІВКИ ДО ВИКОНАННЯ КОНТРОЛЬНОЇ РОБОТИ***

Виконання контрольної роботи передбачає розвиток навичок самостійного пошуку необхідної інформації, опрацювання та осмислення теоретичного і практичного матеріалу. Вибір теми — довільний.

Контрольна робота виконується на зброшурованих аркушах (формат А4). На титульній сторінці зазначаються: назва дисципліни (“Захист підприємницької інформації”); прізвище, ім'я, по батькові студента; домашня адреса; номер групи. Контрольна робота повинна містити план і список літератури.

На останній сторінці ставляться дата виконання роботи та підпис студента. Роботу необхідно здати в наукову частину в установлений термін.

### ***ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ***

1. Державна інформаційна політика та головні напрями її реалізації.
2. Основні принципи інформаційних відносин.
3. Права та обов'язки учасників інформаційних відносин.
4. Суб'єкти та об'єкти інформаційних відносин.
5. Види та напрями інформаційної діяльності.
6. Режим доступу до інформації та його види.
7. Державний контроль за додержанням встановленого режиму доступу до інформації.
8. Доступ до відкритої інформації.
9. Право власності на інформацію.
10. Інформаційний запит щодо доступу до офіційних документів і запит щодо надання письмової або усної інформації.
11. Порядок доступу до інформації з обмеженим доступом.
12. Порядок доступу до конфіденційної інформації.
13. Порядок доступу до інформації комерційного та банківського характеру.
14. Порядок доступу до таємної інформації.
15. Порядок міжнародного співробітництва у галузі інформації.
16. Експорт та імпорт інформаційної продукції (послуг).
17. Основні організаційно-правові заходи щодо охорони державної таємниці.
18. Компетенція органів державної влади, органів місцевого самоврядування та їхніх посадових осіб у сфері охорони державної таємниці.
19. Засекречування та розсекречування матеріальних носіїв інформації.
20. Допуск громадян до державної таємниці.
21. Доступ громадян до державної таємниці.
22. Обов'язки громадянина щодо збереження державної таємниці. Обмеження прав у зв'язку з допуском і доступом до державної таємниці.

23. Порядок створення режимно-секретних органів, їх склад і мета діяльності.
24. Основні завдання та права режимно-секретних органів.
25. Шляхи забезпечення захисту інформації в АС.
26. Вимоги і правила щодо захисту інформації, яка є власністю держави.
27. Державне управління захистом інформації в АС.
28. Визначення автоматизованої системи, вимоги до її функціонального складу.
29. Класи та підкласи автоматизованих систем. Стандартні функціональні профілі захищеності, порядок їх визначення і застосування.
30. Служба захисту інформації в автоматизованих системах підприємства, її призначення, права і завдання.
31. Організація робіт служби захисту інформації в автоматизованих системах підприємства.
32. Комплексна система захисту інформації підприємства, порядок створення та основні вимоги до її функціонування.
33. План захисту інформації в автоматизованій системі підприємства, його зміст і порядок розробки.
34. Основні напрями організаційного захисту інформації в автоматизованих системах підприємства.
35. Організація роботи з працівниками підприємства щодо захисту інформації в автоматизованих системах.
36. Організація виконання спеціальних правил використання технічних засобів підприємства для захисту інформації в автоматизованих системах.
37. Основні канали витоку інформації, їх групи та характеристики.
38. Зміст захисту інформації від витоку з технічних каналів.
39. Головна умова та основні завдання забезпечення безпеки інформації в автоматизованих системах підприємства.
40. Захист інформації від витоку з візуально-оптичного каналу.
41. Захист інформації від витоку з акустичного каналу.
42. Захист інформації від витоку з електромагнітних каналів.
43. Захист від витоку за рахунок паразитної генерації.
44. Захист від витоку за рахунок взаємного впливу проводів і ліній зв'язку.
45. Захист від витоку з матеріально-речовинних каналів.
46. Поняття та ознаки комерційної таємниці.

47. Об'єкти і суб'єкти права власності на комерційну таємницю.
48. Юридичне закріплення права підприємства на комерційну таємницю.
49. Організація роботи служби безпеки підприємства щодо захисту комерційної інформації.
50. Визначення відомостей, що становлять комерційну таємницю підприємства.
51. Поняття допуску до комерційної таємниці.
52. Добір, виховання і навчання кадрів для роботи з комерційною таємницею.
53. Порядок доступу до комерційної таємниці.
54. Дозвільна система доступу до комерційної таємниці.
55. Правове регулювання порядку збереження комерційної таємниці при укладенні господарських та інших підприємницьких договорів, веденні ділових переговорів.
56. Види порушень законодавства про державну таємницю, за здійснення яких передбачено дисциплінарну, адміністративну та кримінальну відповідальність.
57. Кримінальна відповідальність за державну зраду, шпигунство, розголошення державної таємниці, втрату документів, що містять державну таємницю.
58. Кримінальна, цивільно-правова, адміністративна та дисциплінарна відповідальність за порушення законодавства про комерційну таємницю.
59. Категорії порушень встановлених норм і вимог з технічного захисту інформації, їх характеристика та порядок дії при виявленні порушень.
60. Методика контролю за додержанням законодавства про державну (комерційну) таємницю та захисту інформації в АС на підприємстві.

## ***СПИСОК ЛІТЕРАТУРИ***

### *Основна*

1. Закон України “Про інформацію” від 02.10.92 № 2657-ХІІ.
2. Закон України “Про державну таємницю” від 21.09.99.
3. Закон України “Про захист інформації в автоматизованих системах” від 05.07.94.

4. *Закон України “Про науково-технічну інформацію”* від 25.06.93.
5. *Закон України “Про власність”* від 07.02.91.
6. *Закон України “Про підприємництво в Україні”* від 27.03.91.
7. *Закон України “Про захист від недобросовісної конкуренції”* від 07.06.96.
8. *Закон України “Про науково-технічну інформацію”* від 25.06.93.
9. *Закон України “Про зовнішньоекономічну діяльність”* від 16.04.91.
10. *Закон України “Про господарські товариства”* від 19.09.91.
11. *Закон України “Про Службу безпеки України”* від 25.03.92.
12. *Закон України “Про охорону прав на промислові зразки”* від 15.12.93.
13. *Закон України “Про наукову і науково-технічну діяльність”* від 01.12.98.
14. *Постанова Верховної Ради України “Про Концепцію (основу державної політики) національної безпеки України”* від 16.01.97 № 3/97-ВР.
15. *Постанова Кабінету Міністрів України “Про Положення про порядок видачі суб’єктам підприємницької діяльності спеціальних дозволів /ліцензій на здійснення окремих видів діяльності”* від 17 травня 1994 р. № 316.
16. *Постанова Кабінету Міністрів України “Концепція технічного захисту інформації в Україні”* від 8 жовтня 1997 р. № 1126.
17. *Постанова Кабінету Міністрів України “Про затвердження “Порядку організації та забезпечення режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях”* від 02.10.03 № 1561–12.
18. *Постанова Кабінету Міністрів України “Про заборону використання бюджетних коштів для закупівлі імпортованих товарів”* від 04.06.96 № 611.
19. *Указ Президента України “Положення про технічний захист інформації в Україні”* від 27.09.99 № 1229/99.
20. *Постанова Кабінету Міністрів України “Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах”* від 16.02.98 № 180.
21. *Звід відомостей, що становлять державну таємницю України (ЗВДТ-2000): Затв. наказом голови СБУ від 01.03.01*

№ 52, зареєстровано в Міністерстві юстиції України 22.03.01 № 264/545511.

22. *Інструкція* щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за їх дотриманням: Наказ Державної служби України з питань технічного захисту інформації від 23 травня 1994 р. № 46.
23. *Тимчасові* рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань та наводок (ТР ТЗІ – ПЕМВН-95): Наказ державної служби України з питань технічного захисту інформації від 9 червня 1995 р. № 25.
24. *Тимчасові* рекомендації у засобах ОТ від витоку каналами ПЕМВ (ТР ЕОТ-95): Наказ Державної служби України з питань технічного захисту інформації від 9 червня 1995 р. № 25.
25. *Тимчасове* положення про категорювання об'єктів (ТПКО-95): Наказ державної служби України з питань технічного захисту інформації від 1995 р. № 35.
26. *Тимчасові* рекомендації щодо розроблення розділу із захисту інформації в технічному завданні на створення автоматизованої системи (ТР АС – 96): Наказ державної служби України з питань технічного захисту інформації від 3 липня 1996 р. № 47.
27. *Державний* стандарт України ДСТУ 3396.0–96. Захист інформації. Технічний захист інформації. Основні положення.
28. *Державний* стандарт України ДСТУ 3396.1–96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
29. *Державний* стандарт України ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни та визначення.
30. *Державний* стандарт України ДСТУ 3859–99. Засоби інженерно-технічного укріплення та захисту об'єктів. Терміни та визначення.
31. *НД ТЗІ 2.5–004–99* “Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу”.
32. *НД ТЗІ 2.5–005–99* “Класифікація автоматизованих систем і стандартні функціональні класи захищеності оброблюваної інформації від несанкціонованого доступу”.

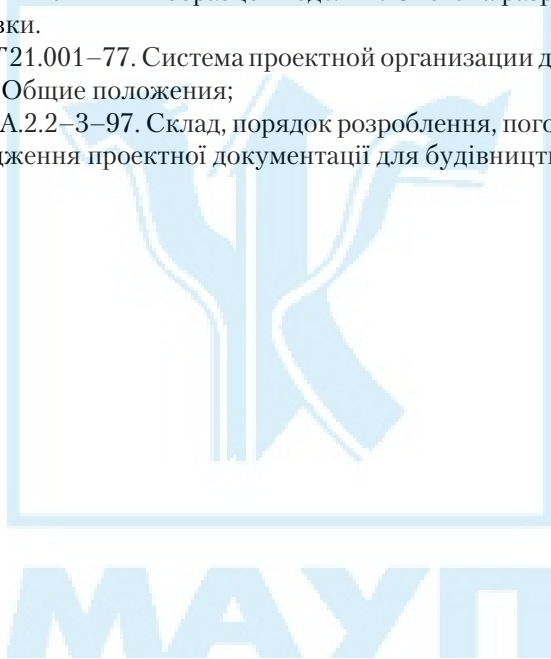
#### *Додаткова*

33. *ДСТУ 1.0–93*. Державна система стандартизації України. Основні положення.
34. *ДСТУ В 1.0–96*. Державна система стандартизації України. Стандартизація озброєння та військової техніки. Основні положення.

35. *ГОСТ В 2.902–68.* Система разработки и постановки на производство военной техники. Единая система конструкторской документации.
36. *ГОСТ В 15.201–83.* Система разработки и постановки на производство военной техники. Тактико-техническое (техническое) задание на выполнение опытно-конструкторской работы.
37. *ГОСТ В 15.203–79.* Система разработки и постановки на производство военной техники. Порядок выполнения опытно-конструкторских работ по созданию образцов. Основные положения.
38. *ГОСТ В 15.204–79.* Система разработки и постановки на производство военной техники. Порядок выполнения опытно-конструкторских работ по созданию составных частей образцов. Основные положения.
39. *ГОСТ В 15.206–84.* Система разработки и постановки на производство военной техники. Программы обеспечения надежности. Общие требования;
40. *ГОСТ В 15.208–82.* Система разработки и постановки на производство военной техники. Единый сквозной план создания образца (системы, комплекса) и его (их) составных частей. Основные положения.
41. *ГОСТ В 15.210–78.* Система разработки и постановки на производство военной техники. Испытания опытных образцов изделий. Основные положения.
42. *ГОСТ В 15.211–78.* Система разработки и постановки на производство военной техники. Порядок разработки программ и методик испытаний опытных образцов изделий. Основные положения.
43. *ГОСТ В 20.39.308–76.* Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний. Конструктивно-технические требования.
44. *ГОСТ В 20.57.304–76.* Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний. Методы оценки соответствия требованиям по надежности.




45. *ГОСТ В 20.57.306–76.* Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний.
46. *ГОСТ В 20.57.310–76.* Комплексная система общих технических требований. Аппаратура, приборы, устройства и оборудование военного назначения. Общие технические требования, методы контроля и испытаний.
47. *ГОСТ В 23226–78.* Порядок разработки программ и методик испытаний опытных образцов изделий. Система разработки и постановки.
48. *ГОСТ 21.001–77.* Система проектной организации для строительства. Общие положения;
49. *ДБН А.2.2–3–97.* Склад, порядок розроблення, погодження та затвердження проектної документації для будівництва.



## ***ЗМІСТ***

Пояснювальна записка.....	3
Тематичний план дисципліни “Захист підприємницької інформації” .....	3
Зміст дисципліни “Захист підприємницької інформації” .....	4
Теми контрольних робіт.....	9
Вказівки до виконання контрольної роботи .....	10
Питання для самоконтролю .....	11
Список літератури .....	13



Відповідальний за випуск	<i>А. Д. Вегеренко</i>
Редактор	<i>Т. М. Тележенко</i>
Комп’ютерне верстання	<i>М. М. Соколовська</i>

**МАУП**

Зам. № ВКЦ-2763

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