МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

з дисципліни

“УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ ОРГАНІЗАЦІЙ ТА УСТАНОВ”

(для бакалаврів, спеціалістів)

Київ
ДП «Видавничий дім «Персонал»
2012

ЗМІСТ

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

Затверджено на засіданні кафедри правоохоронної діяльності (протокол № 7 від 27.02.09)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *В. Д. Бондар*
Комп’ютерне верстання *А. М. Голянда, О. М. Бабаєва*

Низенко Е. І. Методичні рекомендації щодо забезпечення самостійної роботи студентів з дисципліни “Управління системою безпеки організацій та установ” (для бакалаврів, спеціалістів). — К.: ДП «Вид. дім «Персонал», 2012. — 91 с.

Методичні рекомендації містять пояснювальну записку, тематичний план, зміст дисципліни “Управління системою безпеки організацій та установ”, теми самостійної роботи студентів, методичні вказівки до написання самостійної роботи, питання для самоконтролю, задачі, практичні і тестові завдання, а також список літератури.

Зам. № ВКЦ-4753

Формат 60×84/16 . Папір офсетний.
Друк ротаційний трафаретний.
Ум. друк. арк. 5,35. Обл.-вид. арк. 3,43. Наклад 50 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

Свідоцтво про внесення до Державного реєстру суб’єктів видавничої справи ДК № 3262 від 26.08.2008

Надруковано в друкарні ДП «Видавничий дім «Персонал»

68. *Шеннон К.* Работы по теории информации и кибернетике. — М.: Иностр. лит., 1963.
69. *Ярочкин В. И., Халупин Д. В.* Основы защиты информации. Служба безопасности предприятия: Учеб. пособие. — М., 1993.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Самостійна робота студентів є складовою навчального процесу, основним засобом опанування навчального матеріалу в позаурочний час.

Мета самостійної роботи студентів — сприяти засвоєнню у повному обсязі навчальної програми та формуванню самостійності як особистісної риси та важливої професійної якості, сутність якої полягає в умінні систематизувати, планувати та контролювати власну діяльність.

Самостійна робота повинна сприяти розвитку творчого потенціалу студента та реалізації професійних навичок.

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

Зміст самостійної роботи студентів визначається навчальною програмою дисципліни "Управління системою безпеки організацій та установ", а також цими методичними матеріалами.

У процесі самостійної підготовки до практичних занять студенти повинні опрацювати 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 викладеному вище, але мають місце деякі упущення при виконанні завдань, винесених на самостійне опрацювання, обґрунтування неточні, не підтверджуються достатньо аргументованими доказами;
- оцінка **"задовільно"** — студент розкрив питання, винесені на самостійне опрацювання, в загальних рисах, розуміє їх сутність, намагається робити висновки, але при цьому припускається помилок, матеріал викладає нелогічно;

• оцінка **“незадовільно”** — студент не в змозі дати відповідь на поставлене запитання або відповідь неправильна, не розуміє сутності питання, не може зробити висновки.

ТЕМАТИЧНИЙ ПЛАН
дисципліни
“УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ ОРГАНІЗАЦІЙ ТА УСТАНОВ”

№ пор.	Назва змістового модуля і теми	Лекції	ПЗ	Самостійна робота
1	2	3	4	5
	Змістовий модуль І. Загальні положення забезпечення безпеки в організаціях та установах			
1	Науково-пізнавальні засади вчення про безпеку	2	2	
2	Правове забезпечення безпеки організацій та установ	2		4
3	Управління системою безпеки банку	2		4
4	Механізм захисту банківської таємниці	2		4
	Змістовий модуль ІІ. Створення системи захисту організацій та установ від зовнішніх та внутрішніх загроз			
5	Діагностування загроз безпеки	2		6
6	Система охорони організацій та установ	2		6
7	Група режиму в забезпеченні безпеки організацій та установ	2	2	
8	Детективна група у формуванні умов, які забезпечують стабільний розвиток та функціонування об’єкта і захист від внутрішніх та зовнішніх загроз	2		4

50. *Криминология*: Учебник (для учебных заведений МВД Украины) / Под ред. В. Г. Лихолоба, В. П. Силонова. — К., 1997.
51. *Крысин А. В.* Безопасность предпринимательской деятельности. — М.: Финансы и статистика, 1996.
52. *Методика* работы в кризисных ситуациях (Обзор конкретных методических ситуаций): Метод. разработка. — М.: Арсин ЛТД, 1996.
53. *Низенко Е. І., Каленяк В. П.* Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К.: МАУП, 2006. — 134 с.
54. *Рекомендации* по повышению безопасности объектов. — М., 1995.
55. *Рубанов В., Дмитриев Ю.* К вопросу о защите промышленных секретов совместных предприятий // Хозяйство и право. — 1989. — № 1.
56. *Самотуга В., Андреев С.* Коммерческая тайна и ее защита. — М.: Внешторгиздат, 1992.
57. *Спесивцев А. В., Вегнер В. А., Крутиков А. Ю.* Защита информации и персональных ЭВМ. — М.: Радио и связь, 1992.
58. *Стенг Д., Мун С.* Секреты безопасности сетей. — К.: Диалектика, 1995.
59. *Учебник* телохранителя. Базовый курс. — М.: Мир безопасности, 1996.
60. *Федоткин С., Гураев Ю.* Сборник материалов по основам организации охранной деятельности. — М., 1996.
61. *Фролов Г.* Тайны тайнописи. — М., 1992.
62. *Хуберт Г.* Искусственный интеллект как средство обеспечения безопасности. — М., 1999.
63. *Цивилюк Г. Е.* Школа безопасности. Пособие по выживанию. — М.: ЭКСМО, 1995.
64. *Чернявский А. Д.* Безопасность предпринимательской деятельности. — К.: МАУП, 1998.
65. *Чернявский А.* Краткая история развития промышленного шпионажа // Деловая Украина. — 1993. — № 67. — С. 69–71.
66. *Чернявский А.* Методы коммерческой и экономической разведки // Деловая Украина. — 1993. — № 74.
67. *Чигринов В. В.* Концепция безопасности коммерческого банка. — К.: Оптима, 2001.

38. *Нелін О. І., Низенко Е. І., Панфілов В. М.* Роль недержавних служб безпеки в захисті економічних інтересів підприємництва. — К.: Поліграф-Сервіс, 2001.
39. *Низенко Е. І.* Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К.: МАУП, 2006.
40. *Низенко Е. І.* Організаційно-правове забезпечення, формування та реалізація державної політики в сфері безпеки підприємництва // Зб. наук. праць. — К.: Приватне право і підприємництво. — 2003. — Вип. 3 — С. 79–84.
41. *Низенко Э. И.* Обеспечение безопасности предпринимательской деятельности: Учеб. пособие. — К.: МАУП, 2003.
42. *Організаційно-правові* основи захисту інформації з обмеженим доступом: Навч. посіб. / А. Б. Соцький, О. Г. Тимошенко, А. М. Гуз та ін., За заг. ред. В. С. Сідака. — К.: Вид-во Європ. ун-ту, 2006.
43. *Павловський В. Д.* Загальна теорія організації інформаційної безпеки щодо захисту інформації в автоматизованих системах від злочинних посягань // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2001. — № 3. — С. 185–193.
44. *Пожарная* безопасность. — М.: Недра, 1980.
45. *Потєхіна В.* Правильний вибір стратегії охорони комерційної таємниці та винаходу як передумова успішного підприємництва та суспільного розвитку // Підприємництво, господарство і право. — 2005. — № 9. — С. 118–120.
46. *Топалова Л. Д.* Засоби захисту комерційної таємниці // Регіональні проблеми боротьби з економічною злочинністю: Матеріали наук. практ. конф., 16 травня 2003 р. — Донецьк, 2003. — С. 185–189.
47. *Хавронюк М.* Підприємницьке шпигунство і розголошення комерційної таємниці: Юридичний аналіз складів злочинів, питання удосконалення відповідальності // Підприємництво, господарство і право. — 1999. — № 9. — С. 14–21.
48. *Хорошко В. А., Чекатков А. А.* Методи і засоби захисту інформації. — К.: Юніор, 2003.

Додаткова

49. *Ханит Ч., Зартрьян В.* Разведка на службе вашего предприятия: Пер. с фр. — К., 1992.

1	2	3	4	5
	Змістовий модуль III. Тактика попереджувальної діяльності служби безпеки суб'єктів господарювання щодо загроз цілісності та функціональності організацій та установ			
9	Тактика дій служби безпеки організацій та установ у нестабільних умовах внутрішнього та зовнішнього середовища	2		6
10	Тактичні особливості розвідувальної діяльності служби безпеки організацій та установ	2	2	
11	Економічний шпіонаж як сфера таємної діяльності конкурентів і протидія йому	2		4
12	Характеристика зовнішнього середовища розвідувальної діяльності підприємства	2	2	
13	Програма комплексних заходів забезпечення безпеки організацій та установ	2	2	
14	Організаційні засади діяльності суб'єкта господарювання зі збереження комерційної таємниці	2		4
15	Комерційна таємниця як об'єкт правової охорони	2	2	
	Змістовий модуль IV. Економічна безпека організацій та установ та її співвідношення з економічною безпекою держави			
16	Концепція про місце і роль недержавних організацій та установ у системі захисту економічної безпеки України	2	2	

1	2	3	4	5
17	Тенденції формування та реалізації державної політики в галузі безпеки організацій та установ приватної форми власності	2		4
18	Послуги суб'єктів недержавної системи безпеки із захисту і просування інтересів окремих громадян, організацій та установ	2		4
19	Канали витоку інформації з обмеженим доступом з організацій та установ	2	2	
20	Напрями контролю систем безпеки різних типів і рівнів			
21	Економічна безпека в умовах конкурентної боротьби	2		4
22	Конфлікт інтересів між власником інформації з обмеженим доступом і державними органами, організаціями, яким вона може бути передана	2		4
	Змістовий модуль V. Забезпечення безпеки у сфері комп'ютерних технологій			
23	Особливості злочинної діяльності у сфері використання комп'ютерних технологій	2		4
24	Методи приховування факту передавання повідомлення не викликаючи підозри	2		4
Разом годин: 108		24	16	68

26. *Безопасность* бизнеса: Справ. пособие / Под ред. Ю. И. Когута. — К., 1993.
27. *Беляков К. І.* Протидія правопорушенням, що вчиняються з використанням інформаційних технологій — проблеми науково-методологічного та навчально-методичного забезпечення // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2003. — № 7. — С. 95–104.
28. *Боттом Н., Галатти Р.* Экономическая разведка и контрразведка: Практ. пособие: Пер. с англ. — Новосибирск, 1994.
29. *Бутузов В. М., Шеломенцев В. П.* Застосування високих технологій при технічному документуванні злочинної діяльності // Боротьба з організованою злочинністю і корупцією (теорія і практика). — 2004. — № 8. — С. 118–124.
30. *Виявлення* та розслідування злочинів, що вчиняються у сфері інформаційних технологій: Наук.-практ. посібник / Б. В. Романюк, В. Д. Гавловський, М. В. Гуцалюк, В. М. Бутузов; За заг. ред. проф. Я. Ю. Кондратьєва. — К.: Вид. Паливода А. В., 2004.
31. *Гасанов Э.* Энциклопедия личной безопасности. — М.: Аквариум, 1994.
32. *Голубєв В. О., Павловський В. Д., Цимбалюк В. С.* Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / Гуманітарний ун-т "Запорізький ін-т держ. та муніципального управління" / За заг. ред. Р. А. Калюжного. — Запоріжжя: Просвіта, 2001.
33. *Заплатинський В. М.* Основи кримінологічної безпеки сучасного бізнесу: Навч. посіб. — К.: Вид-во КДТЕУ, 2000.
34. *Зубок М. І.* Інформаційно-аналітичне забезпечення діяльності комерційного підприємництва, банку // Бізнес і безпека. — 2003. — № 1.
35. *Зубок М. І., Зубок Р. М.* Безпека підприємницької діяльності. — К.: Істина, 2004.
36. *Криміналістична* тактика і методика розслідування окремих видів злочинів: Навч. посіб. для вищ. навч. закл. / П. Д. Біленчук, А. П Гель, Г. С. Семаков. — К.: МАУП, 2007.
37. *Ліпкан В. А.* Безпекознавство: Навч. посіб. — К.: Вид-во Європ. ун-ту, 2003.

16. *Наказ* Ліцензійної палати України і СБУ “Про умови і правила провадження підприємницької діяльності (ліцензійні умови) з розроблення, виготовлення і реалізації спеціальних технічних засобів (в тому числі іноземного виробництва) для зняття інформації з каналів зв’язку, інших засобів негласного отримання інформації та контроль за їх дотриманням” від 07.04.99. № 30/76.
17. *Положення* про Державний комітет України з питань регуляторної політики та підприємництва: Затв. Указом Президента України від 25 травня 2000 р. № 721/2000.
18. *Положення* про порядок ліцензування підприємницької діяльності: Затв. постановою Кабінету Міністрів України від 3 липня 1998 р. № 1020 // Офіц. вісн. України. — 1998. — № 27. — Ст. 1004.
19. *Постанова* Верховної Ради України “Про Державну програму боротьби зі злочинністю” від 25 червня 1993 р. № 3225-XII // ВВР України. — 1993.
20. *Постанова* Верховної Ради України “Про концепцію (основи державної політики) національної безпеки України” // Голос України. — 1997. — 4 лют.
21. *Постанова* Кабінету Міністрів України “Про перелік відомостей, що не становлять комерційної таємниці” від 9 серпня 1993 р. № 611 // З. П. — 1993. — № 12. — Ст. 269.
22. *Наказ* Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України “Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації” від 30.11.99 № 53.
23. *Указ* Президента України “Про заходи щодо забезпечення підтримки та подальшого розвитку підприємницької діяльності в Україні” від 15 липня 2000 р. № 906/2000 // Офіц. вісн. України. — 2000. — № 13.
24. *Бандурка А. М., Горбачев А. В.* Оперативно-розыскная деятельность: правовой анализ: Науч.-практ. пособие. — К., 1994.
25. *Батурин Ю. М., Жодзинский А. М.* Компьютерная преступность и компьютерная безопасность. — М.: Юрид. лит., 1991.

ЗМІСТ
дисципліни
“УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ ОРГАНІЗАЦІЙ ТА УСТАНОВ”

Змістовий модуль І. Загальні положення забезпечення безпеки в організаціях та установах

Тема 1. Науково-пізнавальні засади вчення про безпеку

Питання для самоконтролю

1. Національна безпека України як полісистемне утворення.
2. Схарактеризуйте об’єкт захисту.
3. Схарактеризуйте види надзвичайних ситуацій за характером виникнення, що можуть дестабілізувати функціонування об’єкта.
4. Назвіть основні види навмисних дій.
5. Назвіть найбільш поширені способи вчинення актів кримінального тероризму.
6. Визначте напрями захисту об’єкта від кримінального тероризму.
7. Вкажіть, з яких блоків інформації може складатися концепція захисту об’єкта.
8. Дайте характеристику організованої злочинності як “особливого феномену”.
9. Як злочинці використовують банки у своїх корисливих цілях?

Практичні завдання

1. Розробіть концепцію захисту підприємства.
2. Складіть письмовий план заходів організаційно-правового характеру щодо нейтралізації дестабілізуючих факторів, які мають потенційну можливість порушити систему функціонування об’єкта підприємницької діяльності.
3. Підготуйте реферат на тему: “Боротьба кримінальних структур за переділ власності та її вплив на підприємницьку діяльність”.

4. Підготуйте реферат на тему: “Кримінальний тероризм і система безпеки підприємництва”.
5. Схарактеризуйте компетенцію суб’єктів управління недержавного сектора відносно виконання ними свого функціонального призначення в якості члена загальної соціальної системи.
6. Схарактеризуйте концептуальні підходи до моніторингу формування економічної безпеки підприємництва.
7. Схарактеризуйте правову основу діяльності недержавних охоронно-детективних організацій у розвинених країнах світу.
8. Підготуйте реферат на тему: “Безпекознавча парадигма”.
9. Підготуйте реферат на тему: “Наука безпекознавство”.
10. Підготуйте реферат на тему: “Методологія безпекознавства”.

Тестові завдання

Зазначте правильну відповідь.

***1. Методичні поради щодо запобігання вчиненню злочинів, пов’язаних із захопленням заручників, можуть бути такими*:**

а) посилена охорона особи чи об’єкта посягання;
б) при наявності інформації у служби безпеки комерційного підприємства щодо захоплення заручників відповідні заходи повинні проводитися при керівній ролі та у взаємодії з оперативними службами органів внутрішніх справ;
в) відміна рейсу транспортного засобу при загрозі його захоплення;
г) проведення ретельніших оглядів багажу, що транспортують із собою пасажири, для запобігання проникнення крізь контрольні пункти недозволених речей, які можуть бути використані для здійснення злочинного наміру;
д) присутність серед пасажирів працівників оперативних підрозділів;
е) нейтралізація основних організаторів злочину;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

СПИСОК ЛІТЕРАТУРИ

Основна

1. *Конституція* України // ВВР України. — 1996. — № 30 зі змін. від 8 грудня 2004 р.
2. *Кримінальний* кодекс України від 5 квітня 2001 р. // ВВР України. — 2001. — № 25–26. — Ст. 131.
3. *Кодекс* України про адміністративні правопорушення // Кодекси України. — 1998. — Кн. 1.
4. *Закон* України “Про захист інформації в автоматизованих системах” // ВВР України. — 1994. — № 31. — Ст. 286.
5. *Закон* України “Про пожежну безпеку” від 17.12.93 № 3745-XII зі змін. від 12.03.11.
6. *Закон* України “Про захист економічної конкуренції” від 11.01.01 № 2210-III // ВВР України. — 2001. — № 12. — Ст. 64.
7. *Закон* України “Про телекомунікації” від 18.11.03 № 1280-IV-ВР.
8. *Закон* України “Про рекламу” від 03.07.96 № 270/96-ВР.
9. *Закон* України “Про ліцензування певних видів господарської діяльності” від 01.06.2000 № 1775-III // Урядовий кур’єр. — 2000. — 2 серп. — № 139.
10. *Закон* України “Про господарські товариства” від 19.09.91 // ВВР України. — 1991. — № 49 (із змін. та допов).
11. *Закон* України “Про власність” (із змін. та допов.) // ВВР України. — 1992. — № 30.
12. *Закон* України “Про банки і банківську діяльність” від 07.12.2000 № 21231-III // ВВР України. — 2000. — № 42.
13. *Закон* України “Про Службу безпеки України” від 25.03.92 № 2229-XII // ВВР України. — 1992. — № 27. — Ст. 382.
14. *Закон* України “Про оперативно-розшукову діяльність” від 18.02.92 № 2135-XII (із змін. та допов.) // ВВР України. — 1992. — № 22. — Ст. 303.
15. *Наказ* Міністра внутрішніх справ України “Про затвердження інструкції про порядок видачі суб’єктам підприємницької діяльності ліцензій на надання послуг по охороні колективної і приватної власності, а також охороні громадян, монтажу, ремонту і профілактичному обслуговуванню засобів охоронної сигналізації” від 28.02.94 № 112.

е) зміна режимів роботи пристроїв або програм;
ж) незаконне отримання паролів та інших реквізитів розмежування поступу з подальшим маскуванням злочинця підзаконного користувача;
з) впровадження злочинними угрупованнями апаратних і програмних закладок, вірусів, що дають змогу долати систему захисту та здійснювати доступ до системних ресурсів (інформаційної системи);
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

***3. Основні шляхи умисної дезорганізації роботи, виведення системи з ладу, проникнення в інформаційну систему і несанкціонованого доступу до інформації такі*:**
а) фізичне руйнування комп'ютерної системи або вивід з ладу її найбільш важливих комп'ютерів;
б) відключення або вивід з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолоджування, вентиляції, ліній зв'язку тощо);
в) дії з дезорганізації функціонування комп'ютерної системи, у тому числі зміна режимів роботи пристроїв або програм, саботаж персоналу, постановка могутніх активних радіоперешкод на частотах пристроїв системи тощо;
г) впровадження агентів конкуруючих фірм складу персоналу (адміністрацію, службу безпеки підприємства);
д) вербування, підкуп, шантаж персоналу або окремих працівників, що мають певні повноваження;
е) застосування підслуховуючих пристроїв, дистанційної фото- і відеозйомки тощо;
ж) розкрадання носіїв інформації;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [25; 30; 34; 55; 63]

***2. При проведенні операцій по затриманню злочинців, які вчиняють замах на захоплення заручників, плануються заходи щодо*:**
а) недопущення закінчення злочину-захоплення заручників;
б) затримання всіх співучасників замаху;
в) забезпечення особистої безпеки осіб, щодо яких вчинюється замах;
г) взаємодія працівників оперативних підрозділів з працівниками служби безпеки комерційного підприємства;
д) розробка заходів щодо забезпечення безпеки членів групи захоплення з фіксацією показового матеріалу;
е) аналіз версій;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

***3. Умовами, які сприяють вчиненню злочинів, пов'язаних із захопленням заручників, можуть бути*:**
а) порушення вимог нормативних актів, що регламентують діяльність комерційних структур;
б) відсутність або незалежна охорона об'єкта та керівників комерційних структур;
в) відсутність інформації у службі безпеки комерційних структур щодо підготовки злочинів такого характеру;
г) недооцінка суспільної небезпеки захоплення заручників з боку керівників комерційних структур;
д) виявлення та усунення причин, що породжують такі злочини та умов, що сприяють їх вчиненню;
е) виявлення осіб, які задумують, готують чи виконують ці злочини;
ж) попередження задуманих злочинів і запобігання тих, що вчиняються;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [1–5; 19; 24; 31; 36–38; 56]

Тема 2. Правове забезпечення безпеки організацій та установ

Питання для самоконтролю

1. Формування бази правового забезпечення національної безпеки.
2. Стан національної безпеки України та основні завдання недержавних суб'єктів щодо її забезпечення.
3. Першочергові заходи по реалізації недержавними суб'єктами державної політики забезпечення національної безпеки України.
4. Основні функції недержавної системи забезпечення національної безпеки України.
5. Основні елементи організації основи недержавної системи забезпечення національної безпеки України.
6. Стан правового захисту підприємництва та вироблення заходів безпеки.
7. Види та напрями правового захисту підприємництва.
8. Правова допомога — інтегральна частина захисту прав та інтересів підприємців.
9. Правовий захист інформації у сфері підприємництва.
10. Захист прав власника у сфері підприємницької діяльності.

Практичні завдання

1. Проведіть письмовий аналіз Указу Президента України "Питання Державного комітету України з питань регуляторної політики та підприємництва" від 25.05.2000 р.
2. Схарактеризуйте нормативно-правове забезпечення недержавної системи безпеки підприємництва (у письмовій формі).
3. Схарактеризуйте структуру законопроекту "Про забезпечення безпеки особистості і підприємницької діяльності" (у письмовій формі).
4. Схарактеризуйте у письмовій формі структуру законопроекту "Про охоронну діяльність".
5. Схарактеризуйте у письмовій формі структуру законопроекту "Про недержавну детективну діяльність".

1. Просочування інформації по каналах ПЕМВН може формуватись за рахунок:

а) побічних електронних і магнітних полів, що створюються інформативними сигналами ЕОМ, а також технічних засобів обробки інформації і допоміжних технічних засобів та систем, на які можуть впливати ці небезпечні сигнали;
б) електротехнічних і магнітних полів, що створюються гармоніками змінного струму електроживлення ЕОМ, модульованих складовими інформаційного сигналу;
в) інформативного сигналу в лініях і каналах систем передачі даних і допоміжних системах, в ланцюзі електроживлення, заземлення й інших провідних комунікаціях, що мають вихід за межі зони безпеки інформації;
г) радіовипромінювання генераторів, що входять до складу ЕОМ й інших технічних засобів, а також випромінювань паразитної генерації, що виникає при нестійкій роботі лінійних елементів, підсилювачів сигналів, що моделюються сигналами інформаційних систем;
д) нерівномірності споживаного струму ЕОМ по мережі електроживлення;
е) дії звукових коливань на технічні засоби обробки інформації;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

2. Умисні загрози інформації:

а) використання відомого способу доступу до системи або її частини з метою нав'язування заборонених дій, звернення до файлів, що містять інформацію, яка цікавить конкурентів;
б) маскування під дійсного користувача шляхом нав'язування характеристик авторизації такого користувача;
в) маскування під дійсного користувача після отримання характеристик (авторизації) доступу;
г) використання службового положення, тобто незапланованого перегляду (ревізії) інформації файлів співробітниками обчислюваного центру;
д) відключення або вивід з ладу підсистем забезпечення безпеки ІС;

9. SOFTTEMPESS-технології таємного передавання даних керованим каналом паразитних електромагнітних випромінювань і наводок.
10. Передавання розвіданої інформації через випромінювання монітора.

Практичні завдання

1. Які тимчасові умови необхідні для утримання каналу просочування інформації?
2. Схарактеризуйте фізичні процеси, що відбуваються в конструктивних елементах ПК та створюють об'єктивні передумови для появи так званих паразитних інформаційних сигналів, в ланцюги і середовищах, не призначених для передачі цього сигналу.
3. Схарактеризуйте існуючі класифікації потенційних загроз інформації за природою їх виникнення.
4. Поясніть власне бачення обставин, що впливають на можливість отримати інформацію шляхом перехоплення випромінювань комунікаційних каналів, центрального процесора, принтера, дисплея.
5. Назвіть сукупність дій з окремих напрямів захисту даних в комп'ютерних системах або мережі від незаконного перехоплювання і несанкціонованого зняття інформації, що зберігається на НЖМД (накопичувач з жорсткими магнітними дисками).
6. Який фізичний процес є основоположним для витоку мовної інформації з приміщення, в якому працює комп'ютер?
7. Як проходить процес маскування використання телефонних ліній для дистанційного збору аудіоінформації з контрольованих приміщень (на прикладі пристрою "телефонне вухо"), тобто йдеться про прослуховування кімнат.
8. Як маскують телефонні "закладки" і де найчастіше намагаються їх встановлювати?
9. Як маскують застосування так званих мереживних "закладок", що живляться від мережі 220 v?
10. Підготуйте реферат на тему: "Можливі канали просочування інформації".

Тестові завдання

Зазначте правильну відповідь.

6. Схарактеризуйте у письмовій формі структуру законопроекту "Про застосування сили при виконанні службових обов'язків працівниками комерційної служби безпеки".
7. Підготуйте реферат на тему: "Залучення громадських об'єднань, підприємств з безпеки різних форм власності до забезпечення безпеки України".
8. Підготуйте реферат на тему: "Деякі актуальні аспекти стану правового захисту у сфері підприємництва".
9. Підготуйте реферат на тему: "Нормативно-правове забезпечення захисту конфіденційної інформації суб'єктів господарювання".

Тестові завдання

Зазначте правильну відповідь.

1. Умовно структура нормативно-правового забезпечення захисту інформації з обмеженим доступом складається з трьох рівнів (загальнодержавний, галузевий та рівень підприємства), які включають:

а) підзаконні нормативно-правові акти (постанови, укази, розпорядження, а також акти уповноваженого органу у сфері захисту інформації, що пройшли державну реєстрацію);

б) нормативні документи з питань ТЗІ (технічний захист інформації) (державні стандарти і прирівняні до них державні будівельні норми);

в) нормативні документи системи ТЗІ, які видаються Державною службою спеціального зв'язку та захисту інформації (для Держспецзв'язку);

г) відомчі нормативні документи з питань створення ІТС (інформаційно-технічні системи), які мають погоджуватися у встановленому порядку з Держспецзв'язку і дія яких поширюється тільки на ІТС сфери управління органу державного управління;

д) нормативні документи, які мають чинність в межах підприємства, установи, організації або конкретної ІТС; Наказ Держстандарту України та ДСТСЗІ СБ України від 09.07.01 № 329/32, зареєстрованим в Мін-ві юстиції України 26.07.01 № 640/5831;

е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не всі відповіді правильні.

2. Адміністративні засоби захисту є заходами організаційного характеру, що регламентують процеси функціонування інформаційних банківських систем. Основні з них:

а) розробка чіткої технології обробки інформації в інформаційних банківських системах;
б) контроль за дотриманням чіткої технології обробки інформації;
в) організація захисту від встановлення прослуховуючої апаратури;
г) ретельний добір персоналу;
д) законодавчо-нормативна база, яка регламентує права і обов'язки користувачів автоматизованої інформаційної системи;
е) внутрішні документи сформовані у вигляді наказів, розпоряджень, інструкцій тощо;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

3. До переліку відомостей, що містять комерційну таємницю, можуть бути віднесені:

а) технологія виробництва;
б) технологія обладнання;
в) модифікація раніше відомих технологій і процесів;
г) результати і програми НДДКР (науково-дослідних і конструкторських розробок);
д) перспективні методи управління;
е) виробничі, комерційні та фінансово-кредитні відносини з партнерами;
ж) плани щодо збільшення (зменшення) виробництва;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [1–5; 19; 24; 31; 36–38; 56]

б) читання інформації з екрану відеомонітора сторонньою особою під час відсутності законного користувача на робочому місці;
в) читання інформації із залишених програмістами без нагляду друкованих програм, чорнових записів;
г) підключення до пристроїв ПК спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
д) використання спеціальних технічних засобів для перехоплення паразитного випромінювання монітора;
е) перехоплення інформації за допомогою каналів побічного електромагнітного випромінювання і наведень (ПЕМВН) елементів локальної мережі ПК;
ж) введення таємних шляхів у комп'ютерну систему програм-закладок з вірусами "Троянський кінь", "Черв'яки", тощо;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [10; 12; 15; 20; 23; 36; 37; 45; 54; 60]

Тема 24. Методи приховування факту передавання повідомлення не викликаючи підозри

Питання для самоконтролю

1. Поняття та методи приховування інформації-криптографії і стегонографії.
2. Зміст поняття "стегосистеми", "контейнер", "приховуване (вбудоване) повідомлення", "стегоключ".
3. Формула загального процесу стегонографії.
4. Основні вимоги, яких необхідно дотримуватися для того, щоб сформований таємний канал передавання інформації не викликав підозри.
5. Поняття "файл-контейнер" і "файл-повідомлення".
6. Комп'ютерні стегосистеми, застосовувані зловмисниками.
7. Уявлення про те, як встановити в комп'ютерму систему "програму-закладку".
8. Технологія маскування процесу встановлення програми-закладки в комп'ютер.

д) кількісний та якісний аналіз даних для побудови моделі загроз і оптимізації заходів по зниженню ризику, що пов'язаний з виявленими "вузькими" місцями;
е) опис загроз і схематичне подання шляхів їх реалізації;
ж) організаційні заходи, що регламентують порядок інформаційної діяльності з урахуванням норм і вимог ТЗІ;
з) первинні механічні заходи захисту інформації з обмеженим доступом;
и) основні технічні заходи, що передбачають захист інформації з використанням засобів забезпечення ТЗІ;
к) усі відповіді правильні;
л) усі відповіді неправильні;
м) не всі відповіді правильні.

***2. Способи шахрайства, засновані на використанні підроблених пластикових кредитних карток частіше за все ґрунтуються*:**
а) на викраденні інформації у вигляді пари чисел — номера кредитної картки та її пін-коду;
б) на викраденні, яке може відбуватися на етапі розсилання кредитної картки споживачеві;
в) на викраденні інформації, яке може відбуватися в момент введення пін-коду в торговий термінал чи банкомат;
г) на викраденні інформації про номер кредитної картки, її пін-коду, яке може відбуватися в момент передачі інформації з каналів зв'язку в режимі роботи "on-line";
д) на тому, що номер кредитної картки і пін-код можуть бути викрадені з банку або обслуговуючої організації;
е) на даних про номер кредитної картки і пін-код, які добувають хакери шляхом незаконного доступу до комп'ютерних систем у фінансово-кредитних організаціях;
ж) на здійсненні зняття грошей з рахунку за допомогою фальшивої копії кредитної картки;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

***3. Стосовно користувачів ПК можливі такі канали витоку*:**
а) розкрадання носіїв інформації;

Тема 3. Управління системою безпеки банку

Питання для самоконтролю

1. Основні напрями діяльності служби безпеки комерційного банку, що випливають з концепції безпеки цього підприємства.
2. Поняття, суть і зміст безпеки комерційного банку.
3. Засоби управління, від яких значною мірою залежить ефективність процесу досягнення мети безпеки банку (пізнавально-програмуючі і організаційно-регулюючі).
4. Об'єкти системи безпеки банку.
5. Суб'єкти правовідносин у сфері забезпечення безпеки банку.
6. Яку роль відіграє безпека банку для їх керівників і служб безпеки при визначенні політики у сфері банківської безпеки?
7. Соціальний зміст цілей і завдань системи безпеки банку (стратегічні, тактичні, оперативні).
8. Чому без засобів групи управління у сфері безпеки неможливий належний взаємозв'язок і взаємообумовленість між елементами всієї системи безпеки банку (структурні підрозділи і окремі співробітники)?
9. З чим пов'язане поняття "механізм" (технологія) управління і поняття "зміст управління"?
10. Групи чинників, що загрожують нормальному функціонуванню банку, їх характеристика (небезпека, ризик, загроза).

Практичні завдання

1. Підготуйте письмово комплексний план забезпечення безпеки банку, який охоплює усі сфери діяльності служби безпеки та може включати такі розділи, як організаційні питання, робота з кадрами, ресурсне забезпечення, контроль тощо.
2. Схарактеризуйте основні методи керування службою безпеки банку (економічні, розпорядницькі і соціально-психологічні).
3. Ваша думка щодо структури процесу керування діяльності служби безпеки банку, яка складається з трьох стадій, кож-

на з яких містить у собі послідовно здійснювані етапи або операції.

4. Зазначте, за якою схемою здійснюється оцінка обстановки з урахуванням відносин, які складаються у галузі банківської діяльності і мають владно-організаційний характер.
5. Визначте конкретні заходи і засоби, які повинна передбачити система забезпечення безпеки інформаційних ресурсів банку.
6. Схарактеризуйте методологію дослідження процесів формування, функціонування, розвитку системи забезпечення інформаційної безпеки банку.
7. Поясніть власне бачення обставин, що впливають на можливість отримати інформацію шляхом перехоплення випромінювань комунікаційних каналів, центрального процесора, принтера, дисплея на об'єктах ЕОМ.
8. Яка роль використання інформаційних технологій у сфері банківської діяльності?
9. Розкрийте ваше бачення щодо нормативно-правової основи формування і функціонування системи забезпечення інформаційної безпеки банку.
10. Розкрийте власну модель системи інформаційної безпеки банку.

Тестові завдання

Зазначте правильну відповідь.

***1. Система регулювання доступу на об'єкти комерційного банку має передбачати*:**

а) об'єктивне визначення "надійності" осіб, які допускаються до банківської діяльності;
б) максимальне обмеження кількості осіб, які допускаються на об'єкти комерційного банку;
в) установлення для кожного працівника (або відповідача) певного по часу, місцю і виду діяльності права доступу на об'єкт;
г) чітке визначення порядку видачі дозволу і оформлення документів для входу на об'єкт банківської системи;
д) усі відповіді правильні;
е) усі відповіді неправильні;
ж) не всі відповіді правильні;

2. Як злочинці використовують глобальну мережу Інтернет "для відмивання" своїх прибутків та відкривають рахунки, не зустрічаючись з банківськими працівниками?
3. Схарактеризуйте спосіб неправильного доступу до комп'ютерної інформації, який полягає в таємному підключенні комп'ютера злочинця до комп'ютерної системи чи мережі законних користувачів по телефонних каналах або радіозв'язку.
4. Схарактеризуйте спосіб проникнення до чужих інформаційних мереж шляхом електронного "злому".
5. Схарактеризуйте спосіб несанкціонованого доступу до чужих інформаційних мереж, які здійснюються шляхом використання чужих паролів, коли незаконний користувач видає себе за законного користувача.
6. Схарактеризуйте спосіб неправомірного доступу до баз і банків даних, який полягає у прихованій заміні чи доповненні до комп'ютерних програм, що функціонують у комп'ютерній системі.
7. Схарактеризуйте спосіб неправомірного доступу до комп'ютерної інформації, який здійснюється шляхом незаконного використання універсальних програм, застосованих в аварійних системах (у разі виникнення збоїв та інших відхилень у роботі комп'ютерів).
8. Схарактеризуйте метод "Логічна бомба", який застосовують для того, щоб ухилитись від оплати за використання послуги, наприклад, щодо автоматичних розрахунків по виплаті заробітної плати.
9. Схарактеризуйте фізичну сутність комп'ютерного віруса.

Тестові завдання

Зазначте правильну відповідь.

***1. Для досягнення мети щодо технічного захисту інформації у сфері комп'ютерних технологій здійснюється*:**

а) аналіз об'єктів ТЗІ;
б) аналіз умов функціонування підприємства;
в) оцінка ймовірності прояву загроз інформаційної безпеки;
г) оцінка очікуваної шкоди від реалізації загрози, яка стосується інформаційної безпеки;

е) неможливість використання машинних програм у зв'язку з відсутністю розроблених алгоритмів вирішення завдань, побудованих на типових слідчих ситуаціях;
ж) подання перекрученої статистичної звітності;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [10; 15; 17; 20; 23; 26; 37; 39; 40; 63]

Змістовий модуль V. Забезпечення безпеки у сфері комп'ютерних технологій

Тема 23. Особливості злочинної діяльності у сфері використання комп'ютерних технологій

Питання для самоконтролю

1. Класифікація способів скоєння злочинів залежно від об'єкта злочину з використанням інформаційних технологій.
2. Кібер-тероризм.
3. Незаконний доступ до комп'ютерних систем у фінансово-кредитних організаціях за допомогою хакерів.
4. Шахрайство з пластиковими картками, пов'язане з використанням фантомної картки.
5. Для чого зроблена комп'ютерна програма (логічний спосіб), яка має назву "Черв'яки"?
6. Поняття комп'ютерного саботажу, його види. Втручання у комп'ютерну систему.
7. Механічні методи знищення інформації на НЖМД (накопичувач на жорсткому магнітному диску).
8. Перехоплення інформації за рахунок випромінювання принтерів, клавіатури.
9. Комп'ютер — джерело відтоку мовної інформації, фізика цього явища.
10. Поняття "графіка локальної мережі" (локальне випромінювання).

Практичні завдання

1. Схарактеризуйте способи використання членами злочинних угруповань фальшивих банкоматів.

2. Управлінський вплив, спрямований на забезпечення банківської безпеки, залежить від засобів управління, основними з яких є такі, що:

а) забезпечують злагодженість, органічне поєднання індивідуальних, колективних і суспільних інтересів;
б) демонструють зв'язок суб'єкта управління з об'єктами, що є прийомом здійснення керуючого впливу суб'єкта управління на об'єкт банківської діяльності;
в) є найбільш активними і рухомими елементами в системи управління;
г) мають альтернативний характер;
д) усі відповіді правильні;
е) усі відповіді неправильні;
ж) не всі відповіді правильні;

3. Головне призначення системи забезпечення безпеки банку полягає у досягненні цілей безпеки, а основною функцію цієї системи є забезпечення інтересів об'єкта через:

а) моніторингування загроз;
б) діагностування загроз;
в) виявлення та ідентифікацію дії внутрішніх і зовнішніх загроз;
г) запобігання та припинення дії внутрішніх і зовнішніх загроз;
д) мінімізація та нейтралізація дії загроз;
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не всі відповіді правильні.

Література [1–5; 19; 24; 31; 36–38; 56]

Тема 4. Механізм захисту банківської таємниці

Питання для самоконтролю

1. Поняття банківських правовідносин.
2. Банківські правовідносини, які виникають у процесі систематичної діяльності спеціальних суб'єктів — Національного банку України, інших банків та фінансових установ з приводу інформації, яка підпадає під режим банківської таємниці.
3. Визначення поняття банківської таємниці.

4. Коло суб'єктів, які мають здійснювати безпосереднє зберігання відомостей про операції, рахунки та вклади клієнтів банку та інших кредитних установ.
5. Механізм встановлення відомостей, які повинні охоплювати режим банківської таємниці, оскільки стали відомі кредитні організації в процесі обслуговування клієнта.
6. Дайте правову характеристику терміна "службовці банку", який не є визначеним законодавчо, а тому потребує подальшої деталізації в розумінні ст. 364 Кримінального Кодексу України.
7. Розкрийте особливості використання та відповідного захисту відомостей про клієнтів, що містяться в Єдиній інформаційній системі "Реєстр позичальників", становлять банківську таємницю та є власністю переліченої інформації.
8. Наведіть загальні правові засади щодо захисту при проведенні валютних аукціонів Національного банку, оскільки учасники Аукціону забов'язані подавати Аукціонному Комітету на його вимогу відомості про обсяг угод купівлі іноземної валюти за рахунок клієнтів та за свій рахунок.
9. Схарактеризуйте вимоги, яких необхідно дотримуватися Національному банку України при здійсненні своїх функцій з використанням при цьому отриманої від банків інформації, що містять банківську таємницю.

Практичні завдання

1. Дайте правову оцінку звуження кола суб'єктів, які мають право на гарантований захист інформації про себе, котра була свого часу передана банку, у випадку коли будь-яка фізична особа припинила користуватись його послугами.
2. Дайте правову оцінку виведення законодавством з-під правової охорони режиму банківської таємниці та відомостей про діяльність та стан рахунків кореспондентів банку.
3. Схарактеризуйте дії, які зобов'язаний здійснити банк з метою забезпечення режиму банківської таємниці при роботі з відповідними відомостями працівників банку.
4. Схарактеризуйте коло осіб, які повинні підписувати зобов'язання щодо збереження банківської таємниці при вступі на посаду.

г) державної контрольно-ревізійної служби;
д) спеціально уповноважений орган виконавчої влади з питань фінансового моніторингу;
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не всі відповіді правильні.

2. Служба безпеки банку має спеціальні відділи, які виконують такі дії:

а) режимно-секретний відділ забезпечує охорону державної таємниці;
б) відділ фінансової безпеки забезпечує розроблення та своєчасне здійснення заходів щодо запобігання фінансової шкоди банку;
в) відділ внутрішніх ревізій забезпечує контроль за додержанням чинного законодавства і нормативних актів Національного банку України, внутрішніх банківських положень;
г) відділ по роботі з персоналом забезпечує банк потрібними фахівцями;
д) відділ охорони;
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не всі відповіді правильні.

3. Вчиненню правопорушень в банківській сфері сприяють різні причини суб'єктивного і об'єктивного характеру. Найбільш суттєвими з них є:

а) відсутність чіткого уявлення про кредитну систему;
б) відсутність уявлення про форми і методи кредитування, їх економічну і правову систему;
в) важливий доступ до банківської документації та іншої інформації;
г) недостатнє знання цивільно-правової та адміністративно-законодавчої бази, що регулює компетенцію різних суб'єктів юридичних і фізичних осіб;
д) відсутність методу розслідування окремих видів злочинів у сфері кредитної діяльності;

Практичні завдання

1. Зазначте, в яких випадках видаються правоохоронним органам довідки про рахунки та вклади громадян?
2. За яких умов банком може бути надана інформація правоохоронним органам, що становить банківську таємницю і охороняється державою?
3. Правове регулювання відносин підприємства з правоохоронними органами у випадках, коли останнім необхідно отримати від учасників фінансово-господарських відносин інформацію, що має комерційну або банківську таємницю.
4. Чим обмежена можливість контролюючих органів виконавчої влади ознайомлюватися з конфіденційними відомостями або з комерційною таємницею підприємства?
5. Які правові особливості мають дії правоохоронних органів щодо виїмки у підприємства документів, що мають комерційну або банківську таємницю, оскільки саме до таких носіїв секретів встановлено спеціальний порядок отримання відомостей?
6. Чи можуть видаватися довідки державним податковим інспекціям про рахунки та вклади окремих громадян стосовно діючого законодавства України?
7. Шляхи покращення законодавства в банківській сфері.
8. Підготуйте реферат на тему: "Правові основи банківської системи та їх захист від злочинних посягань".
9. Підготуйте реферат на тему: "Економічна безпека банку".
10. Підготуйте реферат на тему: "Обставини, які сприяють скоєнню злочинів у фінансово-кредитній сфері".

Тестові завдання

Зазначте правильну відповідь.

1. Указом Президента України "Про деякі заходи з регулювання підприємницької діяльності" від 23.07.98 № 817/08 (ст. 5) встановлено, що контролюючими органами, які мають право здійснювати планові виїзди, перевірки фінансово-господарської діяльності суб'єктів підприємницької діяльності, є:

а) органи Державної податкової служби;

б) митні органи;

в) органи державного казначейства;

5. Схарактеризуйте обсяг загальної інформації, що становить банківську таємницю, яку має право надати банк іншим банкам при наданні кредитів, банківських гарантій, що фактично законом не визначено.
6. На інформаційну систему "Реєстр позичальників" обліку позичальників (боржників), які мають прострочену заборгованість за кредитами, наданими комерційними банками.
7. Уповноважені особи, що мають доступ до Єдиної інформаційної системи "Реєстр позичальників".
8. Зазначте, за якою схемою і які структурні підрозділи Національного банку України забезпечують функціонування Єдиної інформаційної системи "Реєстр позичальників".
9. Схарактеризуйте, що має заноситись від комерційного банку до даних ЄІС "Реєстр позичальників", які саме відомості вона повинна містити.
10. Схарактеризуйте порядок використання комерційним банком інформації з бази даних ЄІС "Реєстр позичальників".
11. До кого може подати позов клієнт комерційного банку про відшкодування збитків, завданих незаконним використанням інформації з "Реєстру позичальників", яку надав до Єдиної інформаційної системи про свого клієнта банк, що уклав договір з Національним банком про надання послуг через цю систему?
12. Підготуйте реферат на тему: "Забезпечення режиму банківської таємниці".

Тестові завдання

Зазначте правильну відповідь.

1. З метою приведення у відповідність до Закону України "Про банки і банківську діяльність" № 2121-III від 07.12.2000 р. Положення про єдину інформаційну систему "Реєстр позичальників", затверджене Постановою Національного банку України № 245 від 27.06.2001 р. "Про створення єдиної інформаційної системи обліку позичальників (боржників)", необхідно внести до його чинної редакції такі зміни:

а) виключити положення щодо колективної власності банків-учасників Єдиної інформаційної системи "Реєстр позичальників" на інформацію, що становить банківську таємницю та знаходиться в ЄІС;

б) визначити обсяг інформації, що надається банком про свого клієнта до ЄІС "Реєстр позичальників" та становить банківську таємницю;
в) визначити обсяг інформації, що банк може отримати з єдиної інформаційної системи "Реєстр позичальників";
г) визначити напрями використання інформації, що містить банківську таємницю, яку банк отримав з єдиної інформаційної системи "Реєстр позичальників";
д) визначити порядок збереження банками інформації, яку вони одержали з ЄІС "Реєстр позичальників";
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не всі відповіді правильні.

2. До суб'єктів, які мають право знайомитись з певним обсягом інформації, що становить банківську таємницю, можна віднести:

а) власників інформації, яка належить до банківської таємниці, та треті особи з письмового дозволу власника названої інформації;
б) суди;
в) органи прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України;
г) органи Державної податкової служби України;
д) органи, якими розкривається банківська таємниця у порядку, передбаченому законодавством, що стосується боротьби з легалізацією грошей, здобутих злочинним шляхом;
е) службовців Національного банку України або уповноважених ними осіб, які в межах повноважень, наданих Законом України "Про Національний банк України", здійснюють функції банківського нагляду або валютного контролю;
ж) державні нотаріальні контори або приватні нотаріуси, іноземні консульські установи по справах спадщини за рахунками померлих власників рахунків (вкладів);
з) органи Державної податкової служби України;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

к) усі відповіді неправильні;
л) не всі відповіді правильні.

Література [25; 30; 45; 47; 50; 63]

Тема 22. Конфлікт інтересів між власником інформації з обмеженим доступом і державними органами, організаціями, яким вона може бути передана

Питання для самоконтролю

1. Суперечності в нормах Закону України "Про банки і банківську діяльність" щодо правового регулювання режиму використання організаціями банківської таємниці та конфіденційної інформації.
2. Розбіжності у правових актах, що регулюють надання відомостей кредитними, митними та іншими установами, контролюючими органами, які становлять конфіденційну інформацію та комерційну таємницю.
3. Підстави, які породжують зазначені правила витребування зазначеними органами закритої інформації з обмеженим доступом у суб'єктів підприємницької діяльності.
4. Нормативне регулювання інформаційних відносин банків з органами Служби безпеки України, прокуратури і судами.
5. Створення єдиного банку даних про імідж, платоспроможність і надійність суб'єктів підприємницької діяльності.
6. Взаємозв'язок між зміною правил фінансово-господарської діяльності і виникаючими у зв'язку з цим протиріччями у нормативній базі.
7. Яку роль в економічній безпеці банку відіграє забезпеченість конфіденційності банківської інформації?
8. Як здійснюється нормативне закріплення Положення про інформацію банку?
9. Назвіть, кому банк зобов'язаний розкрити інформацію, що має правовий статус банківської таємниці відповідно ст. 62 Закону України "Про банки і банківську діяльність" від 07.12.2000 № 2121-III.
10. Чому згідно зі ст. 13 ЗУ "Про Національний банк України" членам Ради Національного банку забороняється розголошувати інформацію, яка отримана ними від банків у зв'язку з виконанням службових обов'язків?

е) слабкий режим збереження відомостей, які є комерційною таємницею, відсутність повної гарантії збереження фірмових секретів;
ж) наявність вузьких точок у захисті комп'ютерної мережі та каналів зв'язку;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

***2. У роботі структурних підрозділів підприємства можна виділити такі недоліки*:**
а) завищена кількість управлінського персоналу;
б) не виконуються повною мірою функції підрозділів;
в) слабка матеріальна зацікавленість у результаті праці;
г) багатоступінчастість доходження завдань до виконавців;
д) велике запізнення при реагуванні на виробничі зміни;
е) відсутність критеріїв управлінських рішень;
ж) недостатня інформованість управлінських служб;
з) недостатня структуризація завдань;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

***3. Ранніми ознаками або симптомами кризи підприємства можуть бути*:**
а) негативна реакція партнерів по бізнесу, постачальників, кредиторів на ті чи інші заходи, що проводить організація;
б) затримки з представниками бухгалтерії звітності та її якість, що може свідчити про низький рівень кваліфікації персоналу;
в) збільшення заборгованості з боку організації постачальникам і кредиторам;
г) зменшення доходів організації, зниження рівня прибутку;
д) позачергові перевірки організації;
е) обмеження діяльності підприємства з боку органів влади;
ж) відміна або припинення дії ліцензії;
з) необґрунтоване злиття дочірніх фірм;
и) усі відповіді правильні;

***3. Відповідно до ст. 62 Закону України "Про банки і банківську діяльність" № 2121-III від 07.12.2000 р., крім власника інформації, що містить банківську таємницю, банк зобов'язаний розкрити таку інформацію*:**
а) на письмову вимогу суду або за рішенням суду;
б) спеціально уповноваженому органу виконавчої влади з питань фінансового моніторингу на його письмову вимогу щодо здійснення фінансових операцій, які підлягають фінансовому моніторингу згідно з законодавством про запобігання та протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом;
в) органам державної податкової служби України на їх письмову вимогу з питань оподаткування або валютного контролю стосовно операцій за рахунками конкретної юридичної особи або фізичної особи — суб'єкта підприємницької діяльності за конкретний проміжок часу;
г) органам прокуратури України, Служби безпеки України, Міністерства внутрішніх справ України — на їх письмову вимогу стосовно операцій за рахунками конкретної юридичної особи або фізичної особи — суб'єкта підприємницької діяльності;
д) органам державної виконавчої служби на їх письмову вимогу з питань виконання рішень судів стосовно стану рахунків конкретної юридичної особи або фізичної особи — суб'єкта підприємницької діяльності;
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не всі відповіді правильні.

Література [1–5; 12; 24; 31; 36–38]

Змістовий модуль ІІ. Створення системи захисту організацій та установ від зовнішніх та внутрішніх загроз

Тема 5. Діагностування загроз безпеки

Питання для самоконтролю

1. Поняття загрози безпеці (у широкому значенні) та чинників, що загрожують нормальному функціонуванню об'єкта і

об'єднані відповідно у такі групи, як небезпеки, ризик, загрози.
2. Поняття виклику як одного з елементів системи небезпек.
3. Значення факторного аналізу чинників дестабілізуючого і стабілізуючого характеру для відпрацювання і реалізації конкретних заходів у системі забезпечення безпеки, спрямованих на нейтралізацію та придушення дестабілізаційних чинників.
4. Природа небезпеки (загроз), виявлення її джерел та детермінант, які створюють потенційну можливість порушення функціонування та розвитку системи безпеки.
5. Чому безпека завжди має розглядатися у парі з небезпекою?
6. Класифікація загроз системі безпеки за ймовірністю реалізації.
7. Класифікація загроз системі безпеки за ступенем небезпеки ставлення до них.
8. Необхідність у розробленні чітких критеріїв, показників, параметрів безпеки.
9. Поняття, критерії безпеки, ознаки, показник, індикатор безпеки.
10. Сутність критеріальної оцінки стану безпеки з позиції найважливіших процесів, що відображають суть безпеки.

Практичні завдання

1. До чого зводиться практичне визначення "діагнозу" стану безпеки, методика його проведення?
2. З яких двох найважливіших елементів складається концепція ризику у стратегії безпеки?
3. Наведіть вашу точку зору, чому оцінка рівня безпеки організації та установ поряд з аналізом фактів ризику передбачає також використання категорій збитків: фактичних, очікуваних, потенційних, тих, що компенсуються і не компенсуються.
4. Зазначте, на яких рівнях можуть відбуватися негативні наслідки критичних соціально-економічних ситуацій у вигляді збитків, що виникають при цьому.
5. Схарактеризуйте основні стадії виникнення небезпек: зародження, розвиток, безпосередньо їх актуалізація.

4. Обґрунтуйте, чому економічну безпеку підприємства розглядають в наукових працях як економіко-правову забезпечувальну підсистему.
5. Наведіть переваги розробки адекватної організаційної структури підприємства, яка може бути створена для вироблення ефективних управлінських рішень в рамках екосесента.
6. Чому орган економічної безпеки підприємства є радчим органом, який може лише розробляти пропозиції щодо реалізації господарських інтересів?
7. Від чого залежить економічна стабільність та розвиток економіки країни в розвиненому ринковому середовищі?
8. Підготуйте реферат на тему: "Підходи щодо становлення системи безпеки підприємництва як складової національної безпеки держави".
9. Підготуйте реферат на тему: "Економічна безпека суб'єкта підприємництва".
10. Підготуйте реферат на тему: "Економічна безпека та ризики підприємництва в контексті проектного підходу".

Тестові завдання

Зазначте правильну відповідь.

1. Українські підприємства опинилися серед бурхливих змін зовнішнього ринкового оточення та зіткнулися із загрозами внутрішнього характеру, серед яких можна зазначити такі:

а) управлінські та виробничі помилки;
б) прорахунки в кадровій політиці через наявність непрофесіоналів та небажаних осіб;
в) невідповідність у визначенні цілей та завдань окремих підрозділів суб'єктів підприємництва, наявності в них власних відмінних інтересів у рамках підприємства, що може призвести до серйозних конфліктів;
г) таємне співробітництво персоналу з представниками структур, що являють небезпеку для підприємства;
д) порушення порядку та правил дотримання на об'єкті режиму безпеки, що створює передумови для реалізації злочинними елементами своєї мети та виникнення надзвичайних ситуацій;

л) усі відповіді правильні;
м) усі відповіді неправильні;
н) не всі відповіді правильні.

Література [25; 30; 34; 55; 62]

Тема 21. Економічна безпека в умовах конкурентної боротьби

Питання для самоконтролю

1. Конкурентне середовище і економічна безпека.
2. Економічне суперництво.
3. Недобросовісна конкуренція, її зміст.
4. Основні напрями конкурентної боротьби підприємств у галузі економіки і технології.
5. Захист службою безпеки господарюючого суб'єкта життєздатності підприємства від ворожих дій конкурентів і негативного впливу дестабілізуючих соціально-економічних факторів.
6. Фактори, на які слід зважати при вирішенні питання про вибір службою безпеки організації, установи стратегії і тактики запобігання правопорушень в умовах ринкової економіки.
7. Поняття політики безпеки підприємства.
8. Поняття стратегії системи підприємства.
9. Поняття екосесентно-економічної безпеки підприємства.
10. Наведіть класифікацію різноманітних типів та видів ризиків підприємства.

Практичні завдання

1. У чому полягає висока актуальність теоретичних досліджень проблем економічної безпеки підприємств — екосесент (economic security of enterprise)?
2. Чому ідентифікація та аналіз ризиків та антикризових заходів є обов'язковою складовою проектного підходу (мислення) до постійного забезпечення високої конкурентоспроможності суб'єкта підприємства?
3. Назвіть основні переваги проектного підходу сучасного управління підприємством і підприємництвом порівняно з традиційною орієнтацією на бачення проблеми та розробки шляхів її вирішення.

6. Обґрунтуйте завдання діагностики небезпек, яке постає у виявленні тих ознак, які б вказували на зародження та формування небезпек; проведення аналізу та прогнозування розвитку небезпек, термінів створювання загрози, а також можливої шкоди, що супроводжують її виникнення.
7. У чому полягає вирішення завдання діагностики небезпек щодо ідентифікації на ранніх стадіях тих ознак і того середовища, яке продукує і сприяє розвитку небезпек?
8. Визначте ваше ставлення щодо існування своєрідних передвісників загроз та небезпек.
9. Суб'єктивні і об'єктивні показники безпеки, завдяки яким можна вирішувати завдання щодо ідентифікації ознак, які б вказували на формування і розвиток небезпек, можуть знаходитись у взаємній суперечці. Внаслідок чого це трапляється?
10. Поясніть, чому у випадку "конфлікту аксіологій" (аксіологія — від грецьк. *axsa* — цінність, *logos* — вчення, "вчення про цінність") постає необхідність у виробленні поміркованого управлінського рішення, яке має ґрунтуватися на оцінюванні загроз не лише об'єкта, а й конкретної особи.

Тестові завдання

Зазначте правильну відповідь.

***1. Особливості, які характеризують процес діагностування небезпек та загроз, можна окреслити, переважно враховуючи різні чинники, а саме*:**

а) дані про ті чи інші небезпечні чинники часто не викликають певної уваги, проте не сприймаються належним чином;
б) суб'єктивні показники залежать не лише від фізичного, а й від інтелектуального розвитку людини, які зумовлюють критеріальну шкалу оцінок тих чи інших чинників у якості загрозливих або небезпечних;
в) кожна небезпека і загроза є оригінальною і характеризується специфічними і притаманними лише їй, лише в даний час і у конкретному місці ексклюзивними ознаками;

г) вважаючи небезпеку та загрозу природною складовою будь-якої системи безпеки, а отже, наголошуючи на їх суті, слід зважати на той факт, що вони характеризуються відсутністю просторово-часової інваріантності під час їх еволюції аж до практичного виявлення і актуалізації;
д) аналіз і порівняння небезпек і загроз, що дають можливість спостерігати динаміку їх розвитку, демонструючи відтворення їх у вигляді графіків, таблиць;
е) різноманітні засоби технічної безпеки можуть бути технічними індикаторами, а таблиці і графіки можуть бути застосовані для порівняння бажаного та реального стану безпеки через аналіз змін у середовищі функціонування об'єкта;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

***2. До принципів побудови показників безпеки належать*:**
а) об'єктивність;
б) системність;
в) необхідність;
г) достатність;
д) утилітарність (прикладний характер);
е) відповідність нормам права;
ж) критерії, за допомогою яких обираються ті чи інші стратегії забезпечення безпеки організацій та установ.
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

***3. Небезпеки та загрози вимірюють за такими ознаками*:**
а) за кількістю загиблих людей і тих, які зазнали ушкоджень;
б) за розмірами шкоди;
в) за розмірами матеріальних втрат у процентах від загального доходу обєкта;
г) за щорічним зростанням шкоди у процентах із прогнозом подальшого розвитку;

д) активний вплив самої системи на інші, які діють також у середовищі функціонування об'єкта;
е) самоорганізація, коли зовнішні впорядковуючі впливи відсутні.
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

***2. У результаті погоджувальної взаємодії, характерної для системи різних типів, відбуваються процеси, для яких характерно*:**
а) упорядкування;
б) виникнення з хаосу певних структур;
в) перетворення та ускладнення цих структур;
г) нелінійність;
д) наявність зворотних зв'язків;
е) можливість робити управляючий вплив на систему;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

***3. Основні етапи, з яких може складатися процедура аналізу конкретної системи*:**
а) формування цілей і основних ідей дослідження;
б) визначення меж системи-основи для відділення об'єкта від зовнішнього середовища, розмежування його внутрішніх і зовнішніх зв'язків;
в) виявлення суті цілісності, що передбачає охоплення всієї типологічної сукупності зв'язків об'єкта;
г) визначення побудови системи — поелементного складу;
д) аналіз взаємозв'язків елементів системи;
е) побудова структури й організації системи, через які виражено зумовлену стійкими зв'язками впорядкованість системи та спрямованість цієї впорядкованості;
ж) виявлення функції системи та її підсистем;
з) аналіз функціонування, що забезпечує реальну життєдіяльність (роботу) системи;
и) виявлення керованості системи і механізми взаємозв'язку в ієрархічній побудові системи, прямі та зворотні зв'язки функціонування, що роблять об'єкт керованим;
к) конструювання системної моделі;

5. Рівні, типи, моделі в загальному контексті теорії самоорганізації, положення якої необхідно враховувати при системі безпеки.
6. Система безпеки як спосіб самоорганізації.
7. Необхідність існування системи безпеки.
8. Суть системи безпеки.
9. Принципи функціонування системи безпеки.
10. Загальна модель системи безпеки.

Практичні завдання

1. Безпекотворчий процес з вашого погляду.
2. Зазначте відмінності поняття "інтенсифікація системи безпеки" і "екстенсифікація системи безпеки".
3. Що розуміють під поняттям "рівень" самоорганізації?
4. Що розуміють під поняттям "моделі" самоорганізації?
5. Що розуміють під поняттям "тип" самоорганізації?
6. Дія якої системи забезпечує ефективне функціонування та розвиток об'єкта?
7. Які функції виконує система безпеки, являючись одним із ефективних засобів реалізації інтересів об'єкта?
8. Схарактеризуйте зміст "статусної" функції щодо системи безпеки об'єкта.
9. Схарактеризуйте зміст "захисної" функції щодо системи безпеки об'єкта.
10. Схарактеризуйте зміст "стратегічної" функції щодо системи безпеки об'єкта.

Тестові завдання

Зазначте правильну відповідь.

***1. Неодмінним атрибутом всіх систем безпеки є*:**

а) їх прагнення до самозбереження в тій якості, в якій вони знаходяться;
б) адаптація системи безпеки до системосередовища, яке включає сукупність внутрішніх і зовнішніх впливів;
в) самозбереження, яке відбувається через "підбір" і виживання в системі безпеки тих структур, які вигідні для її функціонування;
г) заміна непридатних структур на такі, що сприяють ефективності у досягненні мети;

д) за кількісним порівнянням втрат від небезпек у конкретному підприємстві з втратами в інших підприємствах;
е) рівнем економічного розвитку організації, установ;
ж) рівнем заробітної плати;
з) максимально можливим зниженням сумарного ризику;
и) дослідженням небезпек за моделями об'єктів, що вивчають за певними критеріями з наступним розповсюдженням результатів на оригінал;
к) усі відповіді правильні;
л) усі відповіді неправильні;
м) не всі відповіді правильні.

Література [25; 30; 34; 55]

Тема 6. Система охорони організацій та установ

Питання для самоконтролю

1. Законодавчі засади ліцензування надання охоронних послуг.
2. Система периферійного захисту будинків.
3. Правове регулювання охорони послуг, які надають підприємницькі структури.
4. Контрольно-наглядова діяльність ДСО при МВС України за суб'єктами підприємницької діяльності з надання охоронних послуг.
5. Юридична відповідальність працівників недержавних охоронних структур.
6. Службові розслідування за фактами порушення організації охорони організацій та установ.
7. Майнова відповідальність за шкоду, заподіяну при використанні договірних робіт з охорони власності юридичних осіб.
8. Фактори, що визначають параметри технічних засобів охорони для оснащення зон і рубежів безпеки організацій та установ.
9. Мета побудови системи охорони організацій та установ.
10. Зовнішні та внутрішні загрози захисту комерційного об'єкта.

Практичні завдання

1. Підготуйте письмову відповіді на такі питання:
- Визначте ваше ставлення стосовно того, що до складу підприємництва недержавної охорони вводяться: посади керівного персоналу, чергові частини, групи контролю за несенням служби, групи реагування підприємства недержавної охорони, структурні підрозділи по організації об'єктової охорони, супроводженню вантажів, охорони пунктів обміну валюти.
- Поясніть, для чого підрозділ охорони іноді створюється як структурний елемент у складі служби безпеки підприємства, організації, установи, а іноді як самостійне підприємство недержавної охорони.
- Зазначте, як здійснюється управління нарядами недержавної охорони у разі відсутності чергової частини цього підрозділу недержавної охорони.
- В якому випадку об'єкт вважається прийнятим під охорону і яким документом оформляється його прийняття?
- Куди передається для проведення розрахунків копія наказу підприємства недержавної охорони (юридичною особою) про прийняття об'єкта під охорону?
- Для чого одночасно з укладенням договору на охорону сам факт приймання об'єкта під охорону оформлюється також договором між підприємством недержавної охорони та власником повноважень на володіння (користування) об'єктом?
- В якому порядку проводиться інструктаж нарядів недержавної охорони щодо несення служби відповідальними за його підготовку і куди заносяться щодобово результати інструктажу?
- В якому порядку проводиться практичне відпрацювання тактики дій щодо виконання завдань, поставлених перед персоналом недержавної охорони по охороні об'єктів.
- Організація дозорів і секретів для охорони об'єкта, огляду його території і затримання осіб.

2. Розкрийте особливості організації охорони об'єктів підрозділом недержавної охорони.

3. Підготуйте реферат на тему: "Права, обов'язки та відповідальність персоналу недержавної охорони".

е) атестація системи комп'ютерної безпеки;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

***3. Засоби захисту широко використовуються для таких цілей*:**

а) протидія незаконному заволодінню конфіденційної інформації через візуально-оптичні, акустичні канали;
б) протидії вивідуванню відомостей у співробітників, яким інформація була довірена;
в) протидії незаконному заволодінню конфіденційною інформацією через матеріальні речові канали (викладання зразків, виробів, копіювання, фотографування документів, креслень);
г) запобігання знищенню інформації або несанкціонованої її модифікації;
д) усунення несанкціонованого доступу до документів і комп'ютерної інформації через технічні канали;
е) програмне забезпечення;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

Література [2; 7; 10; 15; 18; 25; 27]

Тема 20. Напрями контролю систем безпеки різних типів і рівнів

Питання для самоконтролю

1. Характеристика інтенсивного та експертного видів розвитку систем безпеки організацій та установ.
2. Самоорганізаційні засади систем безпеки об'єкта змішаного типу розвитку.
3. Формування адекватної загрозам і небезпекам системи внутрішньої безпеки організацій та установ.
4. Аналіз сучасного стану напрямів діяльності самоорганізаційних систем у сфері надання послуг з безпеки фірмам-клієнтам.

багато в чому залежить від правильного вибору адекватних приборів, пристроїв, апаратури.

8. Зазначте вимоги до екранування приміщень, в яких встановлена обчислювальна техніка, яку застосовують банківські установи.
9. Зазначте, які методи і заходи входять до системи захисту інформаційних ресурсів підприємства.
10. Схарактеризуйте фізичні засоби захисту інформаційних систем.

Тестові завдання

Зазначте правильну відповідь.

***1. Пошук радіоелектронних засобів несанкціонованого знімання інформації поетапний*:**

а) вивчення службою безпеки підприємства оперативної обстановки біля об'єкта інформації;
б) перевірка радіоефіру за межами приміщення;
в) перевірка моніторингу радіоефіру у приміщенні за допомогою нелінійних локаторів у діапазоні частоти 0,1 — 2000 МГц;
г) перевірка комп'ютерів, телефонних апаратів, електротехнічних засобів за допомогою скануючого приймача;
д) перевірка стін приміщення за допомогою скануючого діапазонного приймача або індикаторів поля;
е) обстеження меблів та інших предметів у приміщенні за допомогою детектора випромінювання;
ж) перевірка телефонної та електронної лінії за допомогою комплексу "Scanner 99";
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

***2. Найважливішими структурними елементами системи захисту інформації можна вважати такі заходи*:**

а) фізичні;
б) адміністративні;
в) апаратні;
г) програмні;
д) криптографічні;

4. Підготуйте реферат на тему: "Забезпечення умов особистої безпеки працівників недержавної охорони під час здійснення заходів охорони і безпеки".

Тестові завдання

Зазначте правильну відповідь.

***1. Контроль за несенням служби під час виконання заходів охорони має такі особливості*:**

а) здійснюється шляхом проведення гласних і негласних фізичних перевірок організації та несення служби нарядами недержавної охорони на маршрутах і постах під час виконання ними охоронних функцій;
б) перевірки проводяться цілодобово за розробленими графіками;
в) графіки негласних перевірок складаються окремо;
г) перевірки плануються (проводяться) у кількості та періодичності, що забезпечує на високому професійному рівні здійснення нарядами недержавної охорони завдань з надання охоронних послуг;
д) фізичні перевірки мають бути раптовими та ефективними, без стереотипу їх проведення;
е) відповідальність за організацію служби та її кінцеві результати покладається на керівника підрозділу охорони;
ж) разом із фізичним контролем несення служби нарядами охорони проводиться контроль з використанням засобів телефонного та радіозв'язку;
з) застосовують для контролю несення служби нарядами охорони різноманітні засоби технічного контролю несення служби (системи визначення і фіксації місцезнаходження нарядів охорони, напрямку їх руху, жетонного методу контролю);
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

***2. При перевірках організації та несення служби вивчаються*:**

а) правові підстави здійснення охоронних заходів на посту (маршруті);

б) наявність договору про приймання об'єкта під охорону між підприємством недержавної охорони та власником повноважень на володіння об'єктом;
в) використання сил та засобів підрозділу охорони;
г) підготовка, порядок допуску до служби працівників недержавної охорони, якість проведення їх інструктажів;
д) управління нарядами недержавної охорони, своєчасність доведення інформації про зміни в оперативній обстановці;
е) порядок взаємодії з нарядами міськрайорганів внутрішніх справ та міліції охорони;
ж) дотримання системи контролю та її ефективність;
з) наявність наряду на маршруті (посту), його екіпірування;
и) забезпечення пропускного режиму на об'єкті;
к) збереження службової документації, засобів зв'язку, спеціальних засобів, майна;
л) усі відповіді правильні;
м) усі відповіді неправильні;
н) не всі відповіді правильні.

***3. Персонал недержавної охорони зобов'язаний*:**
а) пильно охороняти доручені йому матеріальні цінності від протиправних посягань;
б) не допускати на об'єкти, що охороняються, сторонніх осіб;
в) постійно підвищувати свою професійну майстерність;
г) виявляти ініціативу і наполегливість при виконанні покладених на них завдань;
д) забезпечувати неухильне дотримання встановленого на об'єкті пропускного та внутрішньооб'єктового режиму;
е) бути непримиренним до розкрадачів матеріальних цінностей, будь-яких проявів безгосподарності, які можуть призвести до їх крадіжки, знищення або псування майна, що охороняється;
ж) своєчасно інформувати безпосередніх керівників про осіб, що підозрюються у протиправній діяльності щодо майна;
з) добре знати об'єкти, що охороняються, їх особливості і вразливі місця, установлені технічні засоби охорони, протипожежного захисту;

6. Придбання на підприємстві конкурента джерела постачання конфіденційної інформації, яке таємно за винагороду передає комерційні секрети.
7. Таємне дослідження окремих екземплярів продукції конкурентів у лабораторії вивсекції для виявлення їх технологічних характеристик.
8. Електромагнітне перехоплення через зовнішні комунікаційні канали комп'ютерної системи або шляхом відімкнення до ліній периферійних пристроїв.
9. Виток інформації в каналах зв'язку.
10. Перехоплення інформації з комп'ютерних систем без дозволу компетентних органів за допомогою технічних засобів, за рахунок випромінювань центрального процесора, дисплея, комунікаційних каналів, принтера.

Практичні завдання

1. Схарактеризуйте метод перехоплення конкуруючими комерційними фірмами цінної інформації шляхом введення спеціальної програми-закладки в комп'ютерну систему.
2. Схарактеризуйте засоби та методи таємного спостереження за екраном відеомонітора шляхом перехоплення композитного сигналу, що виникає під час оброблення інформації в комп'ютері.
3. У чому полягає зміст ідеї вчених, які діють в галузі оптико-електронної розвідки щодо зараження потрібного комп'ютера спеціальною програмою-закладкою "Троянський кінь"?
4. Зазначте, як здійснюється зміст інформаційних ресурсів внутрішньої мережі підприємства від кваліфікованого проникнення з глобальної мережі до корпоративної мережі установи, де зосереджені узагальнені дані.
5. Поясніть, чому виникає можливість прослуховування розмови поруч з комп'ютером.
6. Зазначте, як здійснюються на практиці два основні методи — активний і пасивний, які застосовують для розв'язання завдань зі сфери технічного захисту інформації.
7. Визначте ваше ставлення щодо того, що успішне застосування методів і засобів захисту від загроз відтоку інформації

б) місцеві державні адміністрації;
в) органи місцевого самоврядування;
г) органи ліцензування;
д) Міністерство внутрішніх справ України;
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не усі відповіді правильні.

3. Побудова недержавної системи безпеки особи та підприємництва повинна здійснюватися на основі дотримання таких принципів, як:
а) законність;
б) дотримання прав і свобод громадян;
в) централізоване управління;
г) комплекс використання сил і засобів;
д) корпоративна етика;
е) конфіденційність;
ж) компетентність;
з) прогресуюче стимулювання суб'єктів системи;
и) координація і взаємодія з правоохоронними органами;
к) усі відповіді правильні;
л) усі відповіді неправильні;
м) не усі відповіді правильні.

Література [15; 17; 19; 20; 25; 26; 29; 30; 37]

Тема 19. Канали витоку інформації з обмеженим доступом з організацій та установ

Питання для самоконтролю

1. Класифікація методів збирання інформації залежно від вирішуваних завдань розвідки.
2. Засадничі положення загальних, особливих та приватних методів економічної розвідки на рівні підприємства.
3. Джерела інформації про конкурентів.
4. Застосування методів незаконного заволодіння (збирання, відбору і передавання) інформації користувачу-конкуренту.
5. Методи проникнення на об'єкт що охороняється.

и) не розголошувати відомості про стан і чисельність охорони об'єктів, їх оснащеність охоронною і охоронно-пожежною сигналізацією;
к) усі відповіді правильні;
л) усі відповіді неправильні;
м) не всі відповіді правильні.

Література [2; 3; 15–34]

Тема 7. Група режиму в забезпеченні безпеки організацій та установ

Питання для самоконтролю

1. Головні функції групи режиму.
2. На кого покладається здійснення пропускного режиму?
3. Хто встановлює пропускний режим на об'єкті, що охороняється?
4. Обов'язкове чи ні виконання встановлених вимог пропускного режиму для всіх осіб, що тимчасово чи постійно знаходяться на підохоронному об'єкті?
5. Хто здійснює контроль за дотриманням пропускного режиму?
6. Які документи дають право на вхід (вихід) робітників, службовців та інших осіб на територію (з території) об'єкта, що охороняється?
7. На які види поділяються перепустки за строком дії і хто встановлює строк дії постійних перепусток?
8. Строк дії тимчасових перепусток.
9. Вилучення тимчасових перепусток з простроченим терміном дії і тимчасових перепусток осіб, які вибувають з об'єкта, що охороняється, у зв'язку із закінченням терміну перебування на об'єкті.
10. Умови, за яких разова перепустка для одноразового відвідування об'єкта, що охороняється, дійсна.
11. Особливості оформлення разової перепустки при груповому відвідуванні об'єкта.

Практичні завдання

1. Зазначте, коли відносно дня відвідування подаються до бюро перепусток письмові заявки на видачу разових перепусток.
2. Визначте, супроводжує відповідача від КПП і назад чи ні уповноважений працівник підохоронного об'єкта, що його приймає.
3. Визначте особливості допуску у неробочі дні осіб на територію об'єкта, що охороняється.
4. Забороняється або можна пропустити на територію об'єкта, що охороняється, осіб у нетверезому стані зі спиртними напоями, господарськими сумками, а також транспортні засоби особистого користування?
5. Забороняється чи ні співробітникам об'єктів, що охороняються, і відвідувачам вносити (ввозити) на об'єкт вибухові речовини, горючі і легкозаймисті рідини і матеріали, зброю, боєприпаси і спецзасоби?
6. Визначте порядок допуску на об'єкт осіб, що прибули на наради й інші подібні заходи, а також особливості дій постів недержавної охорони, що здійснюють пропускний режим.
7. Порядок вивозу вантажів, виносу матеріальних цінностей з об'єктів, заміни меблів, устаткування, проводки електромережі, а також дій працівників, які здійснюють охорону підприємства.
8. Визначте порядок допуску водія, експедитора або іншої особи, якій доручено супроводження вантажу на територію об'єкта, що охороняється.
9. Підготуйте реферат на тему: "Планування і здійснення режимних заходів при виконанні всіх видів робіт, де використовується закрита інформація".
10. Підготуйте реферат на тему: "Порядок доступу представників сторонніх організацій до документів і відомостей, що містять комерційну таємницю".

Тестові завдання

Зазначте правильну відповідь.

1. Контрольно-пропускний пункт КПП для транспортних засобів обладнується:

а) типовими розсувними чи двостулковими воротами з електропроводами та дистанційним управлінням;

6. У чому полягає контроль за здійсненням господарської діяльності з надання на договірній основі послуг, пов'язаних з охороною державної та іншої власності, охорони громадян?
7. Зазначте, як регулюються відносини, що пов'язані приватною професійною діяльністю по здісненню заходів охорони та безпеки під час перевезення вантажів.
8. Зазначте перелік видів технічних засобів, які можуть використовуватись при недержавному забезпеченні безпеки особи та підприємницької діяльності.
9. Відносно кого забороняється застосовувати спеціальні засоби і в яких випадках?
10. Обґрунтуйте, чому при забезпеченні безпеки підприємницької діяльності забороняється проведення оперативно-розшукових заходів, а також використання спеціальних технічних засобів, що призначені для негласного отримання інформації.

Тестові завдання

Зазначте правильну відповідь.

1. До послуг, що надаються при здійсненні охоронної діяльності, належать:

а) охорона об'єктів;
б) охорона нерухомого і рухомого майна;
в) охорона фізичних осіб;
г) провадження робіт по проектуванню, монтажу, ремонту та експлуатаційному обслуговуванню систем та засобів охоронної та тривожної сигналізації;
д) провадження робіт з технічного захисту об'єктів;
е) здійснення централізованої охорони та спостереження;
ж) надання консультацій з питань правомірного захисту від протиправних посягань;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

2. Контроль за охоронною діяльністю у межах своєї компетенції здійснюють:

а) центральні органи виконавчої влади;

2. Послуги суб'єктів недержавної системи безпеки, що надаються згідно з чинним законодавством України окремим громадянам, організаціям і установам.
3. Умови, за яких може здійснюватися відповідна діяльність суб'єктів недержавної підсистеми безпеки у формі взаємодопомоги правоохоронним органам.
4. Збирання відомостей у цивільних справах на договірній основі з учасниками процесу.
5. Зміст письмового повідомлення суб'єкта недержавної безпеки у правоохоронний орган про дані з виявленого злочину проти підприємства, яке направляють, не очікуючи порушень кримінальної справи.
6. Пошук втраченого майна підприємства.
7. Охорона майна підприємства.
8. Документування фактів неправомірного використання товарних (фірмових) знаків підприємства.
9. Захист життя і здоров'я персоналу підприємства від протиправних зазіхань.
10. Забезпечення порядку в місцях здійснення підприємством представницьких, конфіденційних і масових заходів.

Практичні завдання

1. Визначте ваше ставлення стосовно забезпечення особистої безпеки засновників підприємств усіх форм власності та службових осіб шляхом їх охорони.
2. Схарактеризуйте організаційні засади здійснення охоронної діяльності у формі надання на договірній основі послуг громадянам та юридичним особам з охорони належного їм майна.
3. У чому полягають гарантії прав громадян і юридичних осіб під час виконання персоналом охорони покладених на нього обов'язків.
4. Схарактеризуйте гарантії правового та соціального захисту персоналу охорони.
5. Дайте характеристику ліцензійних умов провадження господарської діяльності з надання послуг, пов'язаних з охороною державної та іншої власності, надання послуг з охорони громадян, затверджених наказом Держкомпідприємства та Міністерства внутрішніх справ від 14 грудня 2004 р. № 145/1501.

б) пристроями для аварійної зупинки і відкриття вручну розсувних чи двостулкових воріт;
в) оглядовими майданчиками чи естакадами для огляду автотранспорту;
г) шлагбаумом;
д) вишкою і майданчиком для огляду поїзда, що рухається;
е) запобіжниками або фіксаторами для запобігання довільного відкриття воріт;
ж) пультом керування воротами, який повинен міститися в приміщенні КПП або на його зовнішньому боці;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

2. У приміщенні КПП повинна бути необхідна службова документація:
а) інструкція з пропускного режиму;
б) інструкція з техніки безпеки і надання першої долікарської допомоги;
в) наказ власника об'єкта про введення пропускного режиму в дію;
г) схема безпечного руху працівників недержавної охорони на території об'єкта;
д) зразки всіх видів накладних;
е) зразки перепусток;
ж) зразки підписів осіб, яким надано право їх підписувати;
з) зразки відбитків печаток, пломб, штампів;
и) книги обліку товарно-матеріальних цінностей, що транспортуються, та обліку оглядів осіб і правопорушень;
к) списки телефонів усіх чергових служб, керівників об'єктів;
л) усі відповіді правильні;
м) усі відповіді неправильні;
н) не всі відповіді правильні.

3. Для посилення охорони об'єктів застосовують такі системи сигналізації охоронного призначення:
а) системи охоронної сигналізації (СОС);

б) системи телевідеоконтролю (СТВК);
в) системи телевідеоспостереження (СТВС);
г) система контролю доступу (СКД);
д) система ручної (ніжної) тривожної сигналізації (СРТС), що забезпечує можливість термінового виклику наряду охорони;
е) системи пожежної сигналізації (СПС);
ж) системи сигналізації комбіновані (ССК), що вміщують вищезгадані системи в будь-якій комбінації;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [5; 17; 20–25; 30]

Тема 8. Детективна група у формуванні умов, які забезпечують стабільний розвиток та функціонування об'єкта і захист від внутрішніх та зовнішніх загроз.

Питання для самоконтролю

1. Поняття та зміст приватної детективної діяльності.
2. Напрями діяльності детективної групи служби безпеки підприємства.
3. Законодавче регулювання детективної діяльності, яка зареєстрована у Державному класифікаторі професій України за № 3450 і введена в дію наказом Держстандарту України № 257 від 27.07.1995 р.
4. Суб'єкти, які здійснюють приватну детективну діяльність.
5. Ліцензування приватної детективної діяльності.
6. Вимоги до осіб, які можуть бути приватними детективами, помічниками детективів.
7. Шляхи удосконалення правової бази приватної детективної діяльності.
8. Технологічні основи детективної діяльності, що складаються з елементів: особистого пошуку, аналізу, моделювання "поведінки" системи безпеки об'єкта в умовах дестабілізації й самої системи дестабілізації; екстраполяція, яка використовується як метод прогнозування активізації дестабілізую-

в) вчинювати дії, які ставлять під загрозу життя, здоров'я, честь і гідність і схоронність майна громадян;
г) здійснювати відео- і аудіозапис, фото- кіно- і відеозйомки у службових та інших приміщеннях без письмової згоди на це відповідних посадових або приватних осіб;
д) збирати відомості, які пов'язані із приватним життям, політичними або релігійними переконаннями;
е) застосовувати дії, які посягають на права свободи громадян;
ж) видавати себе за співробітників правоохоронних органів;
з) приховувати від правоохоронних органів факти вчинених злочинів або злочинів, що готуються;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не усі відповіді правильні.

3. Діяльність по недержавному забезпеченню безпеки особи та підприємницької діяльності здійснюється за такими напрямами:
а) забезпечення безпеки фізичних осіб;
б) підготовка кадрів;
в) консультативна діяльність;
г) інформаційно-аналітична діяльність;
д) охоронно-технічна діяльність;
е) приватна детективна діяльність;
ж) приватна охоронна діяльність;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не усі відповіді правильні.

Література [25; 30; 34; 55]

Тема 18. Послуги суб'єктів недержавної системи безпеки із захисту і просування інтересів окремих громадян, організацій та установ

Питання для самоконтролю

1. Компетенція суб'єктів недержавної системи безпеки і правоохоронних органів щодо розслідування правопорушень.

10. Поясніть, як може здійснюватись координація діяльності суб'єктів забезпечення безпеки особи та підприємництва.
11. Що передбачає стратегія економічної і соціальної політики в плані розвитку підприємництва, яка визначена Президентом України.

Тестові завдання

Зазначте правильну відповідь.

***1. Суб'єкти забезпечення безпеки особи та підприємницької діяльності можуть взаємодіяти з правоохоронними органами та спеціальними службами за такими напрямами*:**

а) інформування про виявлення загрози Україні;
б) повідомлення про факти злочинів, що готуються, вчиняються або вже вчинені;
в) допомога при затриманні осіб, які підозрюються у вчиненні злочину;
г) допомога при розшуку осіб, що переховуються від слідства чи суду;
д) допомога при розшуку осіб, які ухиляються від кримінальної відповідальності;
е) одержувати інформацію про загрозу безпеці особи і підприємницької діяльності;
ж) одержувати консультативну допомогу;
з) одержувати допомогу при підготовці кадрів;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

***2. Суб'єктами недержавного забезпечення безпеки особи та підприємництва забороняється*:**

а) застосування заходів фізичного впливу, спеціальних засобів та вогнепальної зброї проти працівників правоохоронних органів та спеціальних служб, які діють у межах повноважень, що надані їм відповідним законодавчим актом;
б) розголошувати зібрану інформацію у будь-яких цілях всупереч інтересів суб'єктів підприємницької діяльності;

чих чинників, а тому сприяє прийняттю доцільних адекватних рішень з урахуванням певних обставин; прогнозування в умовах складової обстановки та виявлення тенденцій її розвитку під час організації і ведення розшуку.
9. Мета і засоби детективної діяльності.
10. Роль і завдання спостереження у розшуковій діяльності детективів.

Практичні завдання

1. Поясніть, з яких етапів складається процес провадження службового розслідування працівниками детективної групи СБ підприємства стосовно протиправних посягань щодо господарюючого суб'єкта.
2. Визначте ваше ставлення стосовно того, що метою службового розслідування працівниками детективної групи СБ підприємства протиправних дій є не лише викриття винних, а й відновлення порушених прав та інтересів суб'єкта господарювання, загальна та індивідуальна превенція правопорушень.
3. Оцінювання приводів порушення провадження щодо службового розслідування працівниками детективної групи СБ підприємства протиправних дій, що стосуються господарчого суб'єкта.
4. У чому полягає безпосередній етап провадження службового розслідування протиправних дій, що стосуються господарчого суб'єкта?
5. На підставі чого приймається рішення про направлення зібраних матеріалів у зв'язку зі здійсненням перевірки до правоохоронних чи контрольних органів за територіальною належністю?
6. Визначте, чому детектив, що веде спостереження, повинен мати міцне здоров'я, відмінну пам'ять, залізне терпіння, гарний слух, повноцінний зір, миттєву реакцію, уміння імпровізувати й орієнтуватися у будь-якій ситуації, не виключаючи критичну ситуацію.
7. Схарактеризуйте види зовнішнього спостереження, яке може вестися під час детективної діяльності.

8. Схарактеризуйте технічні засоби, які використовуються при здійсненні спостереження детективами.
9. Тактичні особливості ведення спостереження детективами.
10. Підготуйте реферат на тему: "Роль детективної групи у забезпеченні безпеки підприємства".

Тестові завдання

Зазначте правильну відповідь.

***1. Напрям діяльності детективної групи служби безпеки підприємства*:**

а) розробляє і здійснює спеціальні заходи щодо спостереження за окремими клієнтами банку, серед яких можуть бути мешканці найбільшого оточення до банку, які висловлюють намір або готовність спричинити шкоду цьому підприємству чи його працівникам;
б) здійснює спільно з групою режиму СБ банку, перевірку кандидатів для прийому на роботу в банківську систему;
в) здійснює в рамках взаємодії з групою режиму СБ підприємства спеціальні заходи щодо контролю з лояльності окремих працівників до банку;
г) підтримує контакти з правоохоронними органами з усіх питань, пов'язаних з превентивними діями щодо забезпечення безпеки банку;
д) сприяє забезпеченню повернення банкам прострочених кредитів;
е) разом з аналітичною групою проводить спеціальні превентивні заходи щодо організацій-клієнтів і конкурентів банка;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

***2. Основними цілями створення і роботи детективних підрозділів СБ суб'єктів господарювання є*:**

а) виявлення загроз фінансово-економічного, соціально-психологічного й іншого характеру всередині підприємства й у сфері його інтересів;

6. Прокурорський нагляд за недержавним забезпеченням безпеки особи та підприємницької діяльності.
7. Координація діяльності суб'єктів забезпечення безпеки особи та підприємницької діяльності, а також здійснення з ними взаємодії з державними та іноземними установами.
8. Взаємодія суб'єктів забезпечення безпеки особи та підприємницької діяльності із правоохоронними органами та спеціальними службами відповідно до чинного законодавства України.
9. Напрями діяльності по недержавному забезпеченню безпеки особи та підприємництва.
10. Охорона життя, здоров'я, конституційних прав та законних інтересів фізичних осіб.

Практичні завдання

1. У чому полягає недержавне забезпечення безпеки особи та підприємницької діяльності?
2. Схарактеризуйте правові засади недержавного забезпечення безпеки особи та підприємницької діяльності.
3. Зазначте завдання недержавного забезпечення безпеки особи та підприємницької діяльності.
4. Схарактеризуйте принципи недержавного забезпечення безпеки особи та підприємницької діяльності.
5. Визначте ваше ставлення щодо дотримання конституційних прав та свобод людини та громадянина при недержавному забезпеченні безпеки та підприємницької діяльності.
6. Поясніть, які державні органи беруть участь у забезпеченні безпеки особи та підприємницької діяльності і які функції покладені на них.
7. Визначте ваше ставлення стосовно того, що у забезпеченні безпеки особи та підприємницької діяльності мають право брати учать громадяни України (фізичні особи) як суб'єкти недержавного забезпечення безпеки особи та підприємницької діяльності.
8. Поясніть, чому з метою забезпечення безпеки особи та підприємницької діяльності можуть створюватись підприємства та громадські об'єднання і в якому порядку.
9. Зазначте основні напрями забезпечення безпеки підприємницької діяльності.

***3. Для основних напрямів забезпечення безпеки підприємницької діяльності належать*:**

а) інформаційне та правове забезпечення для укладання угод та контрактів;
б) вжиття заходів своєчасного повернення кредитів чи інших фінансових матеріалів;
в) збирання даних по справах, що підлягають розгляду чи розглядаються в арбітражних судах;
г) встановлення осіб, які допустили розголошення комерційної чи банківської таємниці;
д) виявлення та попередження неправомірних дій конкурентів;
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не усі відповіді правильні.

Література [5; 7; 10; 12; 18; 20; 24; 26; 30; 34; 45]

Тема 17. Тенденції формування та реалізації державної політики в галузі безпеки організацій та установ приватної форми власності

Питання для самоконтролю

1. Основна мета державної політики в галузі безпеки організацій та установ приватної форми власності.
2. Парадигма безпеки з позиції державницьких реалій на сучасному історичному етапі, концепцій, стратегій, доктрин та програм.
3. Співвідношення держаної і недержавної підсистем безпеки відповідно до рівня потреби інтересів у безпеці, який нині існує в різних сферах життєдіяльності.
4. Комплекс правових, організаційно-управлінських, соціально-психологічних державних заходів утворення середовища функціонування системи безпеки заради управління загрозами та небезпеками в соціальних відносинах.
5. Створення сприятливого клімату для підприємництва, необхідних умов його цивілізованого розвитку, захисту прав і інтересів від протиправних зазіхань.

б) інформаційна експрес-оцінка партнерів, клієнтів, контрактників на предмет зв'язку з джерелами ризику;
в) інформаційний контроль розвитку інфраструктури ринку, конкурентів їхніх рекламних заходів;
г) забезпечення координації і взаємодії функціональних підрозділів підприємства на основі взаємного обміну інформацією про конкурентне оточення;
д) аналіз інвестиційних пропозицій підприємству;
е) первинна оцінка і поточний контроль економічного стану партнерів і контрагентів підприємства;
ж) оцінка надійності і стійкості банків та інших категорій партнерів підприємства;
з) пошук конкретних учасників, виконавців, які нанесли збитки підприємству, що компенсуються або не компенсуються, а також виявлення обставин, за яких готувалось і було скоєно посягання;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

***3. Принципи проведення працівниками детективної групи СБ підприємства службового розслідування*:**

а) законність;
б) неухильне дотримання прав і свобод громадян;
в) загально-управлінський принцип єдиноначальності та колегіальність у вирішенні поточних питань службового розслідування;
г) наступальність;
д) конфіденційність;
е) конспіративність у роботі з негласними джерелами інформації;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

Література [25; 30; 34; 55]

Змістовий модуль ІІІ. Тактика попереджувальної діяльності служби безпеки суб'єктів господарювання щодо загроз цілісності та функціональності організацій та установ

Тема 9. Тактика дій служби безпеки організацій та установ у нестабільних умовах внутрішнього та зовнішнього середовища

Питання для самоконтролю

1. Сучасні методології і методики управління забезпеченням безпеки організацій та установ у нестабільних умовах функціонування.
2. Поняття надзвичайної ситуації.
3. Актуалізація дестабілізуючих факторів, які можна умовно назвати надзвичайними ситуаціями і поділити за характером їх виникнення на певні види.
4. Загальна характеристика об'єкта захисту.
5. Види та характеристики загроз безпеки підприємницьким структурам.
6. Поняття кризової ситуації.
7. Поняття ефективного управління загрозами та кризовими ситуаціями підрозділами СБ, що забезпечують безпеку підприємництва.
8. Способи вчинення актів кримінального тероризму.
9. Визначте поняття антикризової оперативної технології забезпечення безпеки підприємницьких структур.
10. Схарактеризуйте сутність готовності до роботи служби безпеки підприємства до кризових ситуацій, тобто функціонування в умовах ускладнення обстановки навколо підприємницької структури.

Практичні завдання

1. Схарактеризуйте напрями антикризових оперативних технологій (перший напрям — це технології підготовки та підтримання системи безпеки підприємницької структури в готовності до можливих проявів загроз; другий напрям — це технологічні переходи до антикризового оперативного

б) захист державою законних інтересів недержавних організацій у відповідних сферах їх діяльності;
в) взаємодія в боротьбі з кримінальним сектором в економічній та фінансовій сферах діяльності;
г) надання пріоритетної допомоги недержавним організаціям, які беруть безпосередньо участь у захисті безпеки найважливіших для держави підприємств;
д) повага і дотримання прав і свобод людини і громадянина;
е) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не усі відповіді правильні.

***2. Практика і тенденції розвитку в умовах формування ринкових відносин дають змогу визначити перелік охоронних послуг і забезпечення економічної безпеки, серед яких уже сформовані*:**

а) фізична охорона різного роду об'єктів і приватних осіб із використанням сучасних технічних та спеціальних засобів;
б) патрулювання в громадських місцях спільно з підрозділами патрульно-постової служби ОВС під час проведення масових культурно-просвітницьких і соціальних заходів;
в) надання підприємницьким структурам гарантій з безпеки та інформування щодо надійності партнерів при здійсненні комерційних операцій;
г) забезпечення безпеки міжнародних і вітчизняних виставок, конгресів, симпозіумів, фестивалів тощо;
д) інформаційно-аналітичне забезпечення підприємницького розвитку і захисту комерційної таємниці;
е) економічна безпека об'єктів і приватних осіб засобами прогресивно технічних комплексів інформаційних систем;
ж) інформаційна безпека недержавних суб'єктів економічних відносин;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не усі відповіді правильні.

Практичні завдання

1. Обґрунтуйте необхідність прийняття Верховною Радою України спеціального закону, який би визнав право існування недержавних структур, діючих у сфері захисту підприємництва і особи.
2. Які дві групи суб'єктів нині діють в системі забезпечення безпеки економічних відносин, сформованих в Україні?
3. Схарактеризуйте тактику забезпечення силами недержавних служб безпеки громадського порядку в місцях проведення спортивних і видовищних заходів.
4. Визначте ваше ставлення щодо підготовки та перепідготовки кадрів як у державних, так і в недержавних навчальних закладах.
5. Необхідність розроблення механізму взаємодії державної і недержавної підсистем безпеки у системі захисту економічної безпеки України.
6. Мета комплексної системи економічної безпеки підприємств.
7. Управління процесами інформаційного забезпечення у сфері економічної безпеки підприємства на базі методології збалансованої системи показників, які можуть бути використанні для прогнозування безпеки.
8. Формування стратегічних карт, які є групуванням цілей і показників, що надає можливість керівнику здійснювати управління, орієнтуючись на значення індикаторів (обставин тимчасового характеру, що склалися у сфері безпеки).
9. Ключові фактори управління інформаційними процесами економічної безпеки підприємства.

Тестові завдання

Зазначте правильну відповідь.

1. Основними принципами, якими необхідно керуватись державі, яка діє у сфері забезпечення безпеки приватної власності, підприємництва і особи та недержавним структурам діючим в цьому напрямі, є:

а) взаємна відповідальність держаних і недержавних структур перед законом за дії, що завдають збитки національним інтересам;

управління підприємницькою структурою; третій напрям — це технології антикризового оперативного управління; четвертий напрям — це технології переходу від антикризового оперативного управління до повсякденного управління)

2. Обґрунтуйте необхідність створення антикризової оперативної групи для управління підприємницькою структурою при настанні кризової ситуації, коли повсякденне управління стає неможливим.
3. Зазначте, який, на вишу думку, може мати вигляд структура антикризової оперативної групи.
4. Який зв'язок існує між національною безпекою, підприємницькою діяльністю і тероризмом?
5. Визначте ваше ставлення щодо процедури взаємодії, спільних дій служби безпеки підприємства і правоохоронних органів, які можуть відбуватися як на договірній, так і на недоговірній основі, якій передує усна домовленість.
6. Визначте ваше ставлення стосовно того, що раціонально організована взаємодія недержавної системи безпеки підприємництва з правоохоронними органами є однією з найважливіших складових ефективності захисту підприємства.
7. Зазначте специфічні завдання служби безпеки підприємництва, які діють у нестабільних умовах внутрішнього та зовнішнього середовища.
8. На основі яких принципів повинна здійснюватись побудова недержавної системи безпеки підприємства?
9. Підготуйте реферат на тему: "Антикризові оперативні технології як засіб забезпечення безпеки підприємництва".
10. Підготуйте реферат на тему: "Недержавна система безпеки у боротьбі з тероризмом та організованою злочинністю як невід'ємна складова національної безпеки України".

Тестові завдання

Зазначте правильну відповідь.

1. Перший (підготовчий) напрям антикризової оперативної технології полягає у розробці й підготовці типових спеціальних планів дій співробітників та служб безпеки підприємницької структури, серед яких можуть бути:

а) план дій при захопленні заручників;

б) план дій при нападі на приміщення;
в) план дій при загрозі вибуху;
г) план дій при нападі на інкасаторів;
д) план дій при вимаганні;
е) план дій при викраденні співробітників підприємства чи їх близьких;
ж) план дій при погрозах співробітникам підприємства викраденням їхніх рідних чи близьких з метою отримання викупу чи конфіденційної інформації;
з) план дій при спробі проникнення до електронних баз даних з метою отримання конфіденційної інформації або руйнування цих масивів інформації;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

2. Другий напрям — технологія переходу до антикризового оперативного управління загрозами безпеці підприємницькій структурі та виходу з кризових ситуацій, що виникли у результаті дії загроз, передбачає послідовність таких дій:

а) отримання інформації про можливу загрозу;
б) аналіз інформації;
в) прогнозування можливого розвитку загрози;
г) прийняття рішення про введення антикризового оперативного управління;
д) вибір плану дій та засобів відповідно до ситуації, що виникла;
е) дії згідно з вибраним планом дій у контексті ситуації;
ж) оцінювання ситуації та прийняття рішення про можливість її локалізації своїми силами та засобами чи залучення до вирішення кризової ситуації правоохоронних органів;
з) визначення щодо ліквідації кризової ситуації чи загрози та механізмів переходу до нормативного повсякденного функціонування;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

Змістовий модуль IV. Економічна безпека організацій та установ та її співвідношення з економічною безпекою держави

Тема 16. Концепція про місце і роль недержавних організацій та установ у системі захисту економічної безпеки України

Питання для самоконтролю

1. Розуміння про концепцію, яка становить собою найвищий щабель системи документів щодо окремих сфер життєдіяльності.
2. Доцільність окреслення власного бачення змісту концепції про місце і роль недержавних організацій та установ у системі захисту економічної безпеки України.
3. Потреба адекватного відображення у змісті концепції питань про правову базу діяльності недержавних підприємств безпеки в системі економічної безпеки України.
4. Можливості взаємодії цих структур з державними органами.
5. Напрями діяльності суб'єктів недержавної системи безпеки.
6. Методологія побудови концепції про місце і роль недержавних організацій та установ у системі захисту економічної безпеки України.
7. Суб'єкти недержавної системи безпеки.
8. Напрями діяльності недержавної системи безпеки у сфері економічної безпеки.
9. Недержавні структури захисту безпеки підприємництва і особи — найбільш надійний резерв держави для вирішення проблеми зростання злочинності у сфері економіки в умовах економічної кризи.
10. Створення благодатного клімату для розвитку національного підприємства, забезпечення безпеки, захисту прав та інтересів підприємців від протиправних нападів.

***2. До предмета захисту інформації можна віднести*:**

а) комерційні задуми, комерційно-політичні цілі форми, результати нарад та засідань органів управління підприємства, розміри і умови банківського кредиту, за рахунок цін, комп'ютерні програми;
б) цінна інформація у формі комерційної ідеї або плану, теоретичної розробки щодо промисловості, картотеки клієнтів;
в) нові технології, ноу-хау;
г) унікальне обладнання, що використовують у виробничому процесі;
д) дослідні зразки виробів;
е) відомості про партнерів, конкурентів;
ж) результати маркетингових досліджень ринків збуду;
з) річні та інші звіти, технологічні карти;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не усі відповіді правильні.

***3. Комерційна таємниця підприємства 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 розробку внутрішніх правил засекречення;
е) не захищатися авторським і патентним правом;
ж) не стосуватися негативної діяльності підприємства;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [25; 30; 34; 55]

***3. Заходи організаційно-правового характеру щодо мінімізації негативних наслідків дій, пов'язаних зі здійсненням кримінального тероризму, включають*:**

а) моделювання прогностичних сценаріїв діяльності СБ об'єкта у надзвичайній ситуації при вчиненні або загрозі вчинення актів кримінального тероризму з конкретним поділом функцій і закріпленням персональної відповідальності за використанням вказаних у планах дій;
б) складання моделі організації взаємодії СБ підприємства з іншими силами (у тому числі правоохоронними органами) щодо забезпечення безпеки об'єкта;
в) розробка планів управління об'єктом в умовах підвищеної можливості вчинення актів кримінального тероризму;
г) розробка рекомендацій поведінки для осіб, яких захопили в заручники;
д) проведення співробітниками служби безпеки підприємства з метою запобігання тероризму інформаційно-аналітичної роботи щодо виявлення або здатності персоналу до співробітництва з конкуруючими об'єктами;
е) запровадження спеціальних методів управління кадровими ресурсами в умовах можливості вчинення актів кримінального тероризму;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні.

Література [25; 30; 34; 40–42; 50]

Тема 10. Тактичні особливості розвідувальної діяльності служби безпеки організації та установ

Питання для самоконтролю

1. Поняття конкурентної розвідки.
2. Реалізація конкурентною розвідкою заходів протидії усім видам шпіонажу (промислового, економічного, науково-технічного тощо).
3. Характеристика оргструктури конкурентної розвідки.

4. Всестороннє вивчення конкурентною розвідкою ділових партнерів.
5. Організація та проведення конкурентною розвідкою заходів по недопущенню надзвичайних ситуацій.
6. Виявлення конкурентною розвідкою негативних тенденцій у поведінці персоналу підприємництва, інформування про нього керівництва та розробка відповідних рекомендацій.
7. Організація конкурентною розвідкою взаємодії з правоохоронними органами з метою попередження та недопущення правопорушень, націлених проти інтересів підприємств.
8. Максимально повне інформаційне забезпечення інформаційно-аналітичним підрозділам конкурентної розвідки діяльності підприємства та підвищення його ефективності.
9. Джерела конкурентної розвідки.
10. Відмінність між конкурентною розвідкою та промисловим шпигунством.

Практичні завдання

1. Поясніть, чому в умовах сучасної конкурентної боротьби першочергове значення набуває розвідка намірів конкурентів, вивчення основних тенденцій розвитку бізнесу, аналіз можливих ризиків.
2. Схарактеризуйте особливості організації і проведення конкурентної розвідки, яка розв'язує свої завдання легальним способом у межах існуючих законів.
3. Зазначте, чому для конкурентної розвідки дотримання етичних норм і принципів діяльності має бути важливою передумовою діяльності?
4. Наведіть вашу точку зору стосовно того, що збирати інформацію може кожен, єдина умова — не використовувати заборонені методи, не порушувати гарантованих Конституцією прав і свобод людини.
5. Визначте ваше ставлення до того, що поява професійних баз даних й пошукових систем дають можливість аналітикам конкурентної розвідки готувати якісні матеріали, придатні для прийняття рішень керівником підприємств, без доступу до таємних матеріалів.
6. Чому всі конкуруючі між собою фірми повинні надійно захищати від несанкціонованого доступу відомості стосовно

Практичні завдання

1. Схарактеризуйте, які відомості не можуть бути віднесені до комерційної таємниці.
2. Об'єктом яких правовідносин може бути інформація?
3. Визначте, чи можна забезпечити надійне збереження комерційних секретів, керуючись лише національним законодавством України.
4. Схарактеризуйте, у чому полягає суть концепції захисту фірмових секретів, яка була розроблена спеціалістом з США в галузі захисту інформації А. Патоксом.
5. Визначте етапи процесу організації інформації та методу "opsec".
6. Правові гарантії захисту інформації з обмеженим доступом, що не становить державну таємницю, передбаченні чинним законодавством України.
7. Поясніть чинний правовий механізм охорони персональної інформації з обмеженим доступом.
8. Схарактеризуйте механізм правового регулювання захисту інформації в автоматизованих системах.
9. Ознаки комерційної таємниці.
10. Створення системи захисту комерційної таємниці.

Тестові завдання

Зазначте правильну відповідь.

1. Персональними даними про особу є:

а) національність;
б) освіта;
в) величина вкладу на банківському рахунку;
г) місце роботи;
д) дата і місце народження;
е) стан здоров'я;
ж) адреса;
з) сімейний стан;
и) релігійність;
к) усі відповіді правильні;
л) не усі відповіді правильні;
м) усі відповіді неправильні.

г) увагу умов роботи з конфіденційною інформацією, до якої він буде допущений;
д) наведення позитивних та негативних прикладів із практики захисту комерційної таємниці;
е) врахування наявності в оформлюваного працівника підозрілих зв'язків з числа співробітників фірм;
ж) виявлення недостовірних відомостей у процесі підготовки матеріалів до оформлення допуску до комерційної таємниці;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

Література [25; 30; 34; 55]

Тема15. Комерційна таємниця як об'єкт правової охорони

Питання для самоконтролю

1. Співвідношення понять "комерційна таємниця" і "інтелектуальна власність".
2. Потреба в нормативному закріпленні комерційної таємниці.
3. Законодавчі гарантії забезпечення права на інформацію.
4. Поняття та ознаки комерційної таємниці.
5. Вартість інформації, що становить комерційну таємницю.
6. Об'єкти і суб'єкти права власності на інформацію, яка становить комерційну таємницю.
7. Складання та підписання суб'єктами підприємства протоколів про наміри в процесі ділових зустрічей, якщо в діловій бесіді повідомляється конфіденційна інформація.
8. Зобов'язання партнерів не розголошувати інформацію про предмет та умови майбутньої угоди.
9. Поняття про режим доступу до інформації ділового, професійного, виробничого, банківського та іншого характеру.
10. Форми правової охорони та правового захисту комерційної таємниці.

технологічних процесів, стратегії маркетингу, результатів науково-дослідних і дослідно-конструктивних робіт?
7. Чи можна з позиції чинного законодавства України застосовувати детективу — працівнику конкурентної розвідки СБ підприємства спеціальні технічні пристрої негласного отримання інформації в умовах сучасної конкурентної боротьби?
8. Зазначте вашу точку зору з приводу того, що в складі видобувного підрозділу конкурентної розвідки СБ підприємства повинні бути співробітники по: роботі з інформаторами, виявленню та збиранню відкритих публікацій, здійсненню зашифрованого спостереження, технічному забезпеченню проведенню розшукових заходів з елементами конспірації, здійсненню службових розслідувань і документуванню дій об'єкта у ході зовнішнього спостереження.
9. Підготуйте реферат на тему: "Конкурентна розвідка — легальний інструмент дослідження ринку".
10. Підготуйте реферат на тему: "Історія розвитку та становлення конкурентної розвідки".

Тестові завдання

Зазначте правильну відповідь.

***1. Розрізняють такі завдання інформаційно-аналітичного підрозділу конкурентної розвідки служби безпеки підприємства*:**

а) вивчення криміногенної обстановки в регіоні, де функціонує підприємство;
б) збирання, обробка, аналіз й прогнозування процесів розвитку ринку;
в) вивчення конкурентів, їх намірів відносно підприємства, в якому функціонує інформаційно-аналітичний підрозділ СБ;
г) вивчення платоспроможності клієнтів кредитоспроможності банків, фінансового та економічного стану у партнерів;
д) здійснення аналізу розвитку відносин підприємства з іншими об'єктами системосередовища і розроблення шкали ворожості, за допомогою якої може вимірюватися ця небезпека;

е) зазначення кількісного значення ознак і властивостей небезпек та загроз, щоб надати їм узагальнену кількісну оцінку для поповнення поглиблення якісної характеристики;
ж) сприяння виявленню наявних каналів витоку інформації за допомогою виявлення наявних каналів витоку інформації за допомогою вимірювання і оцінки якісних і кількісних ознак ступеня поінформованості конкурентів про фінансовий економічний стан підприємства, а також ефективності його роботи в цілому.
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні.

2. Для обробки інформації, отриманої з різних джерел, інформаційно-аналітичний підрозділ конкурентної розвідки служби безпеки підприємства застосовує такі способи:
а) поділ інформації на теми і блоки;
б) осмислення частини питань, що мають ідентичний характер;
в) виділення головного і другорядного;
г) виділення із цілого масиву інформації відомостей, які є дезінформормацією, але мають помилковий характер;
д) поділ інформації на відкриту й закриту;
е) компонування різноманітної інформації в нову логічну систему;
ж) виявлення внутрішніх логічних зв'язків в отриманні інформації;
з) створення більш логічної інформації, ніж була, що відбиває новий погляд на проблему;
и) складання загальної картини на небезпечні тенденції стану безпеки підприємства залежно від негативних факторів системосередовища (середовища існування підприємства, як системи);
к) усі відповіді правильні;
л) усі відповіді неправильні;
м) не всі відповіді правильні.

(контрактів), які передбачають розрахунки в іноземній валюті";
г) Указом Президента Украйни від 4 жовтня 1994 р. "Про застосування Міжнародних правил інтерпретації комерційних термінів";
д) правилами "Інкотермс" (у середині 1990 р.);
е) Конвенцією ООН про договори купівлі-продажу товарів, 1980 (Віденська конвенсія);
ж) наказом міністерства зовнішньоекономічних зв'язків та торгівлі від 5 жовтня 1995 р. № 75 "Про затвердження Положення про форму зовнішньоекономічних договорів".
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не всі відповіді правильні;

2. Перевірка на благонадійність громадян, що отримують допуск до комерційної таємниці, включає в себе:
а) ґрунтовне вивчення досьє кандидата на роботу;
б) перевірку його біографічних даних за останні 10 років;
в) з'ясування мети та обставин змінювання місця роботи;
г) вивчення фінансового становища кандидата;
д) перевірку за основними картотеками МВС;
е) встановлення за місцем проживання кандидатів контактів з дільничими інспекторами міліції з метою перевірки способу життя, поведінки, виявлення компрометуючих зв'язків;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
и) не всі відповіді правильні;

3. Надання допуску до комерційної таємниці передбачає:
а) перевірку співробітника підприємства у зв'язку з допуском до комерційної таємниці;
б) ознайомлення співробітника зі ступенем відповідальності за порушення законодавства, пов'язані з розголошенням ним комерційної таємниці;
в) звертати увагу майбутнього працівника на характерні особливості режиму майбутньої діяльності;

ційна таємниця з документів, підготовлених структурними підрозділами підприємства?
3. На які підрозділи суб'єкта господарювання покладається обов'язок щодо ведення обліку, зберігання, розмноження та використання документів з грифом "комерційна таємниця"?
4. Який діє порядок приймання і обліку документів з грифом "КТ"?
5. Що перевіряється працівниками канцелярії після того, як приймається і розкривається кореспонденція з грифом "ДСК" (для службового користування)?
6. Як здійснюється допуск штатного співробітника підприємства, який має допуск найвищого рівня "комерційна таємниця — особливо важливо", до інформації більш нижчого рівня секретності?
7. В якому випадку співробітник підприємства може отримати право на ознайомлення з будь-якою комерційною таємницею у зв'язку з виконання ним посадових обов'язків?
8. Порядок доступу представників органів державної влади та управління до комерційної таємниці підприємства у процесі виконання ними посадових обов'язків.
9. Порядок юридичного закріплення факту ознайомлення особою з конкретною конфіденційною інформацією.
10. Яким шляхом оформлюється надання доступу представнику сторонньої організації до конкретної комерційної таємниці підприємства?

Тестові завдання

Зазначте правильну відповідь.

***1. При укладенні угод з іноземною фірмою необхідно керуватись такими нормативно-правовими актами*:**

а) Законом України "Про зовнішньоекономічну діяльність" від 16 квітня 1991 р.;
б) міжнародними договорами України;
в) Постановою КМ України та Національного банку України від 21 червня 1995 р. № 444 "Про типові платіжні умови зовнішньоекономічних угод (контрактів) та типових формах захисних застережень до зовнішньоекономічних угод

***3. Інформаційно-аналітичний підрозділ конкурентної розвідки СБ підприємства повинен бути "Мозковим центром" комерційної структури, що обумовлено такими факторами*:**

а) використанням у конкретній боротьбі небезпечних раніше форм і методів протиборства;
б) величезним тиском кримінальних елементів на банки, підприємства, організації, установи та участю подальшої криміналізації ринку;
в) недосконалістю правової захищеності підприємницьких структур;
г) знаходженням більш надійних партнерів;
д) необхідністю вивчення доступних до джерел сировини, комплектуючих чи товарів в інтересах їх переробки та реалізації;
е) необхідністю перевірки надійності вірогідних партнерів, їх класифікований підбір;
ж) можливістю встановлення таємного співробітництва персоналу з представниками структур, що являють небезпеку для підприємства;
з) необхідністю забезпечення готовності до подання високого рівня невизначеності управлінських завдань;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

Література [3; 5; 30; 47]

Тема 11. Економічний шпіонаж як сфера таємної діяльності конкурентів і протидія йому

Питання для самоконтролю

1. Поняття економічної безпеки підприємства.
2. Взаємозв'язок необхідності постійного дотримання економічної безпеки підприємства з наявним для кожного суб'єкта господарювання завданням забезпечення головних цілей своєї діяльності.
3. Зміст поняття кримінологічної загрози безпеки економіки.
4. Характеристика факторів і умов, що становлять небезпеку для нормального функціонування будь-яких об'єктів економіки.

5. Суб'єкти кримінологічних загроз безпеки об'єктів економіки.
6. Характерні дестабілізаційні методи економічного протистояння підприємств усіх видів та розмірів.
7. Боротьба держав світу між собою в області економіки і технології та її мета.
8. Основні прийоми ведення сучасного економічного протистояння.
9. Сітка Бернара Надулека, яку застосовують, розглядаючи можливі варіанти конфронтації в економічній сфері на стратегічному рівні.
10. Механізм економічної розвідки американської, японської, німецької, зорієнтованої на світовий ринок.

Практичні завдання

1. Схарактеризуйте складові економічної розвідки (макроекономічна, мікроекономічна розвідка, економічна контррозвідка).
2. Схарактеризуйте тактичні особливості діяльності мікроекономічної розвідки.
3. Зазначте особливості і призначення різноманітних дестабілізаційних методів.
4. Схарактеризуйте тактику реалізації "Доктрини наведення мостів", яку застосовують з метою широкомасштабного проникнення в країну для ведення агресивної економічної політики по відношенню до конкретної країни.
5. Схарактеризуйте практику створення сумісних підприємств, яка відкриває широкі потенційні можливості для ведення економічної розвідки.
6. Зазначте напрями діяльності економічної розвідки і характерні риси їх функціонування.
7. Схарактеризуйте завдання макроекономічної розвідки.
8. Схарактеризуйте завдання економічної контррозвідки.
9. Що становить найбільший інтерес економічної розвідки?

Тестові завдання

Зазначте правильну відповідь.

1. Недержавні організації, які займаються промисловим шпіонажем, проявляють найбільшу зацікавленість в таких питаннях конкуруючих з ними фірм, організацій, банків, як:

а) фінансові звіти та прогнози;

Тема 14. Організаційні засади діяльності суб'єкта господарювання зі збереження комерційної таємниці

Питання для самоконтролю

1. Правове забезпечення діяльності суб'єкта господарювання щодо збереження комерційної таємниці.
2. Закріплення в установчих документах права на використання комерційної таємниці.
3. Визначення складу та обсягу комерційної таємниці.
4. Складання переліку відомостей, що становлять комерційну таємницю підприємства.
5. Закріплення прав та обов'язків працівників підприємства щодо порядку захисту комерційної таємниці в колективному договорі.
6. Закріплення прав і обов'язків працівників підприємства в правилах внутрішнього трудового розпорядку.
7. Закріплення прав і обов'язків працівників підприємства в контрактах, попередженнях-зобов'язаннях про збереження комерційної таємниці при прийняті на роботу і звільненні.
8. Управління організацією захисту комерційної таємниці в умовах її обороту у виробничих інтересах підприємства та при передаванні іншим установам.
9. Створення системи інформаційної безпеки суб'єкта господарювання.
10. Поняття "конфіденційна інформація", що не є власністю держави.

Практичні завдання

1. Схарактеризуйте діючий порядок встановлення триступеневої системи важливості комерційної таємниці, яка позначається обмежуючими грифами: "комерційна таємниця — особливо важливо" (КТ — ОВ), "комерційна таємниця — конфіденційно" (КТ — К), "комерційна таємниця — суворо конфіденційно" (КТ — СК).
2. Чи можуть керівники центральних органів виконавчої влади, місцевих органів виконавчої влади зняти гриф "комер-

***2. Принципи, з урахуванням яких може бути розроблена програма комплексних заходів забезпечення безпеки організацій та установ*:**

а) пріоритет заходів попередження злочинних посягань на об'єкт, який захищають;
б) законність заходів безпеки, які повинні розроблятися на основі та в межах діючих правових актів;
в) комплексне застосування сил та коштів для забезпечення безпеки підприємства;
г) координація дій щодо протидії загрозам безпеки підприємства;
д) компетентність працівників, які повинні вирішувати питання безпеки об'єкта, який захищають;
е) економічна доцільність фінансових витрат на захист безпеки підприємства;
ж) планова основа діяльності по захисту безпеки підприємства на базі програми комплексних заходів забезпечення безпеки цього об'єкта;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не усі відповіді правильні.

***3. Цілі захисту безпеки підприємства включають*:**

а) недопущення залежності від випадкових та нестійких ділових партнерів;
б) виконання виробничих програм;
в) орієнтація на світові стандарти та на лідерство в розробці й освоєнні нових технологій виробництва продукції;
г) максимально повне інформаційне забезпечення діяльності підприємства та підвищення його ефективності;
д) підвищення конкурентоздатності виробленої продукції;
е) збереження та примноження власності;
ж) зміцнення інтелектуального потенціалу підприємства;
з) захист законних прав та інтересів підприємства;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не усі відповіді правильні.

Література [1; 2; 5; 7; 15; 23; 66]

б) найважливіші елементи систем безпеки, кодів та процедур доступу до інформаційних мереж і центрів;
в) організаційна структура об'єкта;
г) умови продажу чи злиття об'єктів;
д) фінансовий стан об'єкта;
е) перспективні плани розвитку виробництва;
ж) умови контрактів;
з) технічна специфікація існуючої та перспективної продукції;
и) маркетинг та стратегія цін;
к) фінансові звіти та прогнози;
л) усі відповіді правильні;
м)усі відповіді неправильні;
н) не усі відповіді правильні.

***2. Для добування потрібної інформації організації, які займаються промисловим шпіонажем, користуються такими спеціальними методами розвідки*:**

а) незаконне одержання інформації через корумповані елементи у владних структурах;
б) шантаж і різноманітні способи тиску;
в) підслуховування розмов конкурентів;
г) використання професіональних агентів для одержання інформації;
д) обманні переговори з представником конкурента про придбання товарів і після одержання необхідної інформації відмова від предмета переговорів;
е) обманне запрошування на роботу спеціалістів, що працюють у конкурента, з пропонуванням заповнити тест із спеціально підібраними питаннями;
ж) завуальовані питання спеціалістам конкурента;
з) таємне спостереження за об'єктом, яким може бути спеціаліст, відділ чи установа;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не усі відповіді правильні.

***3. Характерні риси діяльності промислового шпіонажу*:**

а) створення умов для підготовки та проведення терористичних і диверсійних акцій;
б) шантаж окремих осіб;

в) перепродаж фірмових секретів;
г) дискредитація чи усунення конкурентів;
д) підробка товарів;
е) оволодіння ринками збуту;
ж) зрив переговорів по контрактах;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не усі відповіді правильні.

Література [15; 18; 20; 24; 29; 34; 43]

Тема 12. Характеристика зовнішнього середовища розвідувальної діяльності підприємства

Питання для самоконтролю

1. Питання вітчизняних підприємств в одержанні інформації випереджуючого характеру про тенденції, факти, явища, які існують поза підприємствами.
2. Зовнішнє середовище — об'єкт розвідувальної діяльності, його характеристика.
3. Інформаційно-аналітичний підрозділ комерційної розвідки служби безпеки підприємства, його призначення.
4. Роль інформаційних технологій, які застосовують інформаційно-аналітичні підрозділи у поліпшенні ринкових позицій компанії і підвищенні її фінансових результатів.
5. Принципи діяльності інформаційно-аналітичного підрозділу комерційної розвідки служби безпеки підприємства.
6. Видача інформаційно-аналітичним підрозділом комерційної розвідки рекомендацій керівництву підприємства на основі аналізу обстановки стосовно конфліктних ситуацій трудового колективу з адміністрацією.
7. Прогнозування розвитку подій на основі виявлених тенденцій їх загострення з метою попередження страйків на підприємстві.
8. Збір інформації про передбачуваних партнерів і конкурентів.
9. Запобігання підрозділом детективів комерційної розвідки проникнення на підприємство осіб, що займаються економічними контрагентами (постачальниками, торговими і збутовими посередниками, інвесторами, споживачами тощо).

жах свої функцій забезпечують інформаційну безпеку, і розкрийте зміст їх діяльності в цьому напрямі.
8. Схарактеризуйте силову складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах своїх функцій забезпечують силову безпеку, і розкрийте зміст їх діяльності в цьому напрямі.
9. Схарактеризуйте позавиробничу складову безпеки — ринкову та зазначте суб'єкти підприємства, що забезпечують ринкову безпеку, і розкрийте зміст їх діяльності в цьому напрямі (служба маркетингу, комерційна розвідка).
10. Схарактеризуйте інтерфейсну складову безпеки організацій та установ і зазначте суб'єкти, що забезпечують виявлення можливих непередбачених загроз зміни умов взаємодії (навіть до розриву відносин) з економічними контрагентами (постачальниками, торговими і збутовими посередниками, інвесторами, споживачами тощо).

Тестові завдання

Зазначте правильну відповідь.

1. До основних елементів програми комплексних заходів забезпечення безпеки організацій та установ можна віднести:

а) захист комерційної таємниці та конфіденційності інформації;
б) комп'ютерну безпеку;
в) внутрішню безпеку;
г) безпеку будинків та споруд;
д) фізичну безпеку;
е) технічну безпеку;
ж) конкурентну розвідку;
з) інформаційно-аналітичну роботу;
и) експертну перевірку механізму системи забезпечення безпеки підприємства;
к) усі відповіді правильні;
л) усі відповіді неправильні;
м) не усі відповіді правильні.

4. Поняття комплексної системи забезпечення економічної безпеки підприємства.
5. Основні функції системи безпеки.
6. Розділи програми комплексних заходів забезпечення економічної безпеки організацій та установ залежно від масштабу та значимості цього підприємства.
7. Визначення на концептуальному рівні стратегії запобігання та протидії злочинній діяльності криміналітету на підприємстві.
8. Форми злочинних діянь проти безпеки підприємства.
9. Норми і правила поведінки працюючого персоналу, включаючи керівництво, в тій чи іншій небезпечній ситуації.
10. Джерела негативних впливів на безпеку підприємства.

Практичні завдання

1. Складіть порівняльну таблицю внутрішньовиробничих та позавиробничих складових поняття безпеки підприємства з огляду на їх цілі.
2. Схарактеризуйте фінансову складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах виконання своїх функцій забезпечують фінансову безпеку і зміст їх діяльності в цьому напрямі.
3. Схарактеризуйте інтелектуальну складову економічної безпеки та зазначте суб'єкти підприємства, що в межах своїх функцій забезпечують інтелектуальну безпеку, і розкрийте зміст їх діяльності в цьому напрямі.
4. Схарактеризуйте кадрову складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах своїх функцій забезпечують кадрову безпеку, і розкрийте зміст їх діяльності в цьому напрямі.
5. Схарактеризуйте технологічну складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах своїх функцій забезпечують технологічну безпеку, і розкрийте зміст їх діяльності в цьому напрямі.
6. Схарактеризуйте правову складову безпеки організацій та установ і зазначте суб'єкти підприємства, що забезпечують правову безпеку в цьому напрямі.
7. Схарактеризуйте інформаційну складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах своїх функцій забезпечують інформаційну безпеку, і розкрийте зміст їх діяльності в цьому напрямі.

мічним шпіонажем, злочинців з наміром нанесення шкоди підприємству.
10. Профілактична робота з персоналом підприємства з приводу того, що на будь-якому підприємстві є своя цінна інформація і її потрібно захищати.

Практичні завдання

1. Зазначте, як здійснюється "легендування перспективної роботи, розпорядку дня керівництва підприємства".
2. Зазначте особливості пропагандистського забезпечення, що має напрям на формування в країні та за її межами позитивної думки про це підприємство.
3. Поясніть роль інформаційно-аналітичного підрозділу комерційної розвідки в забезпеченні керівництва підприємства відповідної підготовки до ведення переговорів з партнерами у нестандартних ситуаціях.
4. Тактика добування комерційною розвідкою підприємства відомостей, на основі яких можна характеризувати ступінь відповідності внутрішніх можливостей розвитку підприємства зовнішнім, які генеруються ринковим середовищем.
5. Організація і тактика добування комерційною розвідкою підприємства спільно зі службою маркетингу відомостей, на основі яких можна характеризувати надійність взаємодії з економічними контрагентами.
6. Поясніть, для чого необхідна документограма, коли добувають негласно той або інший документ для зняття з нього копії.
7. Зазначте джерела розвідувальної інформації.
8. Чому, на вашу думку, дані, одержані з відкритих джерел інформації, у будь-якому разі перевіряються розвідувальними методами (за допомогою притягнутих до співробітництва інформаторів тощо).
9. Обґрунтуйте, чому інформаційні системи належать до числа найважливіших засобів діяльності комерційної розвідки СБ підприємства.
10. Схарактеризуйте основні завдання аналітичного відділення, довідково-інформаційного фонду, групи експертів і консультантів, відділення, які є складовими інформаційно-аналітичного підрозділу комерційної розвідки служби безпеки підприємства.

Тестові завдання

Зазначте правильну відповідь.

***1. Інформаційно-аналітичним підрозділом комерційної розвідки служби безпеки підприємства для обробки інформації, отриманої з різних джерел, використовуються такі аналітичні методи*:**

а) обробка зібраної інформації;
б) установлення причинно-наслідкових взаємозв'язків зібраних фактів, явищ;
в) застосування асоціативних діаграм, за допомогою яких виявляють області ділових і особистих інтересів об'єкта спостереження;
г) аналіз інформації для виявлення відсутніх ланок даних, виділення головного і другорядного, помилкових і дезінформаційних відомостей;
д) компонування різноманітної інформації в нову логічну систему;
е) створення більш логічної інформації, що відбиває новий погляд на проблему;
ж) складання загальної картини на основі відомої інформації;
з) виявлення тенденцій розвитку подій і явищ;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не усі відповіді правильні.

***2. Способи одержання інформаційно-аналітичним підрозділом комерційної розвідки служби безпеки підприємства про діяльність конкурентів можуть мати такі законні форми*:**

а) збирання і аналіз інформації з офіційно опублікованих джерел;
б) відвідування виставок та ярмарок, влаштованих конкурентами;
в) придбання і дослідження виробів конкурентів (так звана зворотна інженерія);
г) вивідування потрібної інформації у спеціалістів конкурента;
д) підкуп співробітників із ключових відділів конкурента;

е) засилка агентів на фірму і в близьке оточення провідних спеціалістів;
ж) викрадення креслень, документів, зразків виробів;
з) переманювання провідних спеціалістів для одержання потрібної інформації;
и) усі відповіді правильні;
к) усі відповіді неправильні;
л) не усі відповіді правильні.

***3. Показники комплексної оцінки результатів роботи комерційної розвідки підприємства*:**

а) кількість даних, оглядів, довідок-меморандумів загального характеру;
б) кількість цивільних справ, виграних за допомогою детективів;
в) кількість успішно проведених ділових переговорів за допомогою фахівців інформаційно-аналітичного підрозділу комерційної розвідки;
г) кількість перевірок осіб, що уклали контракти з підприємством;
д) кількість виявлених некредитоспроможних ділових партнерів;
е) кількість виявлених несумлінних конкурентів;
ж) кількість виявлених ненадійних ділових партнерів;
з) усі відповіді правильні;
и) усі відповіді неправильні;
к) не усі відповіді правильні.

Література [20; 27; 30; 34; 44; 49]

Тема 13. Програма комплексних заходів забезпечення безпеки організацій та установ

Питання для самоконтролю

1. Мета комплексної системи економічної безпеки підприємств.
2. Суть первинних заходів, які забезпечують фундамент, основу системи безпеки підприємства.
3. Зв'язок об'єкта захисту — стабільного стану підприємства з основними характеристиками системи забезпечення економічної безпеки.