МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

МЕТОДИЧНІ МАТЕРІАЛИ ЩОДО ЗАБЕЗПЕЧЕННЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

з дисципліни

“ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ”

(для спеціалістів)

Київ
ДП «Видавничий дім «Персонал»
2012

Підготовлено професором кафедри правоохоронної діяльності
Е. І. Низенком

Затверджено на засіданні кафедри правоохоронної діяльності
(протокол № 4 від 23.11.09)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Низенко Е. І. Методичні матеріали щодо забезпечення самостійної роботи студентів з дисципліни "Забезпечення безпеки підприємницької діяльності" (для спеціалістів). — К.: ДП «Вид. дім «Персонал», 2012. — 58 с.

Методичні матеріали містять пояснювальну записку, тематичний план дисципліни, теми самостійної роботи студентів, методичні вказівки до написання самостійної роботи, питання для самоконтролю, задачі, практичні і тестові завдання, а також список літератури.

ЗМІСТ

Відповідальний за випуск *А. Д. Вегеренко*
Редактор *Г. Я. Кужільний*
Комп'ютерне верстання *С. А. Шередега*

Зам. № ВКЦ-4894

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

Ум. друк. арк. — 3,26. Обл. -вид. арк. — 1,08. 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 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

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

Мета самостійної роботи студентів з дисципліни "Забезпечення безпеки підприємницької діяльності" — сприяти засвоєнню в 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.

Завдання самостійної роботи студентів з дисципліни "Забезпечення безпеки підприємницької діяльності" — засвоєння відповідних знань, їх закріплення та систематизація, а також їх застосування при виконанні практичних завдань. Самостійна робота забезпечує підготовку студентів до поточних аудиторних занять.

Зміст самостійної роботи студентів з дисципліни "Забезпечення безпеки підприємницької діяльності" визначається навчальною програмою цієї дисципліни, а також цими методичними матеріалами.

Основними формами самостійної роботи студентів з дисципліни "Забезпечення безпеки підприємницької діяльності" є:

а) опрацювання прослуханого лекційного матеріалу, обов'язкових та додаткових літературних джерел;
б) вивчення окремих тем або питань, передбачених для самостійного опрацювання;
в) виконання домашніх завдань;
г) виконання та письмове оформлення задач, схем, порівняльних таблиць та інших робіт;
д) підготовка до практичних занять;
е) підготовка до різних форм поточного контролю;
є) пошук та огляд літературних джерел за заданою проблематикою;
ж) написання реферату за заданою проблематикою;
з) аналітичний розгляд наукової публікації;
і) підготовка контрольної роботи.

У процесі самостійної підготовки до практичних занять студенти повинні опрацювати прослуханий лекційний матеріал, всебічно розглянути зміст виносених на заняття питань, опрацювати навчальну літературу, відповідні нормативно-правові акти. Перевірку засвоєння знань студенти здійснюють за допомогою питань для самоконтролю.

Домашнє завдання з дисципліни "Забезпечення безпеки підприємницької діяльності" виконується з метою закріплення та поглиблення теоретичних знань та вмінь студента з винесеного на самостійне опрацювання навчального матеріалу. Поряд з оволодінням базовими теоретичними знаннями, доречно також вивчати і аналізувати практику їх реалізації, навички встановлення динаміки подій — механізму злочину, конструювання динамічної моделі поведінки злочинця. Вивченню підлягають в першу чергу передовий досвід слідчої, експертної та судової практики.

Практичні завдання (задачі) мають своєю метою закріпити теоретичні знання студентів і головне — привити їм навички роботи з нормативними актами. Практичні завдання (задачі) необхідно виконувати у письмовій формі з розгорнутим мотивованим рішенням. При виконанні домашніх завдань студенти повинні продемонструвати уміння самостійно аналізувати конкретні ситуації, аргументовано відповідати на поставлені в задачах питання, використовуючи відповідні нормативні акти. Відповіді на поставлені в задачах питання повинні бути повними та обґрунтованими.

Важливим засобом у засвоєнні знань є написання рефератів. Написання реферату за заданою проблематикою необхідно починати з власного, добре продуманого вступу. У вступі визначається мета дослідження, з максимально можливою точністю встановлюються рамки теми, що підлягає розгляду, визначаються методи її дослідження. Він служить перехідним містком до основного дослідження. В ньому повинно бути відображено практичне і теоретичне значення теми.

В основній частині роботи мова повинна йти перш за все про зміст досліджуваної проблеми. У цьому випадку необхідно дати чітке обґрунтування того, чому саме такому рішенню потрібно віддати перевагу.

Робота повинна завершуватись висновками.

Критерії оцінювання самостійної роботи студентів:

- оцінка "відмінно" — студент повно і всебічно розкриває винесені на самостійне опрацювання, питання теми, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, має власну точку зору стосовно відповідної теми і може аргументовано її доводити;
- оцінка "добре" — рівень знань студентів загалом, відповідає викладеному вище, але мають місце деякі упущення при виконанні завдань, винесених на самостійне опрацювання, обґрунту-

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. *ЦивилюкГ. Е.* Школа безопасности. Пособие по выживанию. — М.: ЭКСМО, 1995.
64. *Чернявский А. Д.* Безопасность предпринимательской деятельности. — К.: МАУП, 1998.
65. *Чернявский А. Д.* 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.
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. пособ. — М., 1993.

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., Зартръян В.* Разведка на службе вашего предприятия: Пер. с фр. — К. 1992.
50. *Криминология:* Учебник для учебных заведений МВД Украины / Под ред. В. Г. Лихолоба, В. П. Силонова. — К.: Донецьк, 1997.
51. *Крысин А. В.* Безопасность предпринимательской деятельности. — М.: Финансы и статистика, 1996.
52. *Методика* работы в кризисных ситуациях (Обзор конкретных методических ситуаций): Метод. разраб. — М.: Арсин ЛТД, 1996.
53. *Преступность* в Украине // Бюл. законодат. юрид. практики в Украине. — 1994. — № 2.
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 В. 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 св'язь, 1992.
58. *Стенг Д., Мун С.* Секреты безопасности сетей. — К.: Диалектика, 1995.

вання неточні, не підтверджуються достатньо обґрунтованими доказами;

- оцінка "задовільно" — студент розкрив винесені на самостійне опрацювання питання в загальних рисах, розуміє їх суть, намагається робити висновки, але при цьому допускає грубі помилки, матеріал викладає нелогічно і не самостійно;
- оцінка "незадовільно" — студент не в змозі дати відповідь на поставлене запитання або відповідь неправильна, студент не розуміє суті питання, не може зробити висновки.

ТЕМАТИЧНИЙ ПЛАН
дисципліни
“ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ”

Номер теми	Назва змістового модуля і теми
1	2
	Змістовий модуль І. Теоретичні засади забезпечення функціонування та розвитку системи безпеки підприємництва, що здійснюється недержавними структурами у межах забезпечення життєво важливих інтересів
1	Предмет, задачі та зміст діяльності, яка здійснюється задля забезпечення інтересів об’єкта через адекватне реагування на загрози
2	Основні обов’язки і права працівників служби безпеки господарюючого суб’єкта при виконанні задач по забезпеченню безпеки підприємства
3	Методи, принципи і організація керівництва силами служби безпеки підприємства банку в умовах проведення захисних операцій протидії загрозам господарюючому суб’єкту
4	Консультування і надання рекомендацій працівниками служби безпеки господарюючого суб’єкта, керівництву і персоналу підприємства з питань економічної, інформаційної, та особистої безпеки
5	Аналітична робота служби безпеки підприємства
6	Система економічної розвідки зарубіжних країн
	Змістовий модуль ІІ. Організація, порядок і способи виконання службових задач працівниками служби безпеки об’єкта задля забезпечення його нормального функціонування
7	Тактика дій персоналу служби безпеки підприємства при виконанні службових задач по охороні майна господарюючого суб’єкта
8	Тактика дій працівників служби безпеки господарюючого суб’єкта при реалізації заходів для недопущення здійснення протиправних зазіхань проти життя і здоров’я персоналу підприємства

нюк, В. Д. Павловський, М. В. Гуцалюк, В. М. Кутузов; 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. посібник. — К.: Вид-во Європ. ун-ту, 2003.
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. пособ. — 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.

ня 1998 р. № 1020 // Офіц. вісн. України. — 1998. — № 27. — С. 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 політикі) національної безпеки України" // Голос України. — 1997. — 4 лют.
21. *Постанова* Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці" від 9 с.рпня 1993 р. № 611 // З. П. — 1993. — № 12. — С. 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. пособ. — К., 1994.
25. *Батурин Ю. М., Жодзинский А. М.* Компютерная преступность и компютерная безопасность. — М.: Юрид. лит., 1991.
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. пособ. // 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. посіб. / Б. В. Рома-

1	2
9	Тактика дій працівників служби безпеки господарюючого суб'єкта при забезпеченні порядку в місцях проведення підприємством представницьких, конфіденційних і масових заходів
10	Технології здійснення працівниками служби безпеки господарюючого суб'єкта діяльності, яка ґрунтується на збиранні детальної інформації про учасників майбутніх ділових переговорів
11	Порядок, зміст і методика роботи працівників служби безпеки підприємства при проведенні заходів, спрямованих на вивчення негативних аспектів ринку
12	Порядок, зміст і методика роботи працівників служби безпеки підприємства при організації та проведенні заходів, спрямованих на виявлення ненадійних ділових партнерів
13	Технології збирання необхідних відомостей працівниками служби безпеки підприємства з цивільних справ
14	Тактика дій працівників служби безпеки господарюючого суб'єкта по розшуку безвісті зниклих співробітників підприємства, якщо їх відсутність на роботі приведе до реального або потенційного збитку
15	Тактика дій працівників детективної групи служби безпеки господарюючого суб'єкта при виконанні службових задач щодо ведення спостереження за об'єктом
16	Провадження службового розслідування працівниками служби безпеки підприємства.
17	Методи і засоби захисту інформації в сфері використання господарюючим суб'єктом електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж
18	Організація та проведення заходів з контролю за ефективністю технічного захисту електронної інформації з обмеженим доступом в організаціях та установах
Разом годин: 108	

ТЕМИ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ з дисципліни "ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ"

Змістовий модуль І. Теоретичні засади забезпечення функціонування та розвитку системи безпеки підприємництва, що здійснюється недержавними структурами у межах забезпечення життєво важливих інтересів

Тема1. Предмет, задачі та зміст діяльності, яка здійснюється задля забезпечення інтересів об'єкта через адекватне реагування на загрози

Питання для самоконтролю

1. Предмет навчального курсу "Забезпечення безпеки підприємницької діяльності".
2. Теоретичні засади дисципліни "Забезпечення безпеки підприємницької діяльності".
3. Система дисципліни "Забезпечення безпеки підприємницької діяльності".
4. Процес забезпечення безпеки та ефективного функціонування системи безпеки підприємництва.
5. Значення недержавної системи безпеки, для системи забезпечення національної безпеки.
6. Погляди на природу забезпечення безпеки, як самостійного напряму знань в структурі науки безпекознавство.
7. Формування механізму безпеки господарюючого суб'єкта.
8. Роль права у процесі забезпечення безпеки господарюючого суб'єкта.
9. Організаційно-управлінський аспект у створенні ефективної системи забезпечення безпеки об'єкта в умовах конкурентної боротьби.
10. Завдання курсу "Забезпечення безпеки підприємницької діяльності".

Практичні завдання

1. Зазначте специфічні закономірності, характерні для практичної діяльності по забезпеченню безпеки підприємництва.

СПИСОК ЛІТЕРАТУРИ

Основна

1. *Конституція* України. — К., 2001.
2. *Кримінальний* кодекс України. — К., 2001.
3. *Кодекс* України про адміністративні правопорушення // Кодекси України. — 1998. — Кн. 1.
4. *Закон* України "Про захист інформації в автоматизованих системах".
5. *Закон* України "Про пожежну безпеку".
6. *Закон* України "Про захист економічної конкуренції".
7. *Закон* України "Про телекомунікації".
8. *Закон* України "Про рекламу".
9. *Закон* України "Про ліцензування певних видів господарської діяльності".
10. *Закон* України "Про господарські товариства".
11. *Закон* України "Про власність".
12. *Закон* України "Про банки і банківську діяльність".
13. *Закон* України "Про Службу безпеки України".
14. *Закон* України "Про оперативно-розшукову діяльність".
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 28.02.1994 № 112.
16. *Наказ* Ліцензійної палати України і СБУ "Про умови і правила провадження підприємницької діяльності (ліцензійні умові) 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 07.04.1999. — 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 лип-

з) не всі відповіді правильні.

2. Середовищем поширення електромагнітних перешкод є:
   а) простір з побічними електромагнітними випромінюваннями;
   б) металеві частини корпусів, вузлів і блоків;
   в) паразитні ланцюги монтажу;
   г) паразитні міжобпліткові ємкості розподільчих трансформаторів;
   д) міжвиткові ємності дроселів фільтрів;
   е) джерело живлення і заземлений контур;
   є) усі відповіді правильні;
   ж) усі відповіді неправильні;
   з) не всі відповіді правильні.

3. Пошук радіоелектронних засобів несанкціонованого знімання інформації включає:
   а) вивчення службою безпеки підприємства оперативної обстановки біля об'єкта інформації;
   б) перевірку радіоефіру за межами приміщення;
   в) перевірку (моніторинг) радіоефіру у приміщенні за допомогою нелінійних локаторів у діапазоні частот 0,1–2000 МГц;
   г) перевірку комп'ютерів, телефонних апаратів та електротехнічних засобів за допомогою скануючого приймача;
   д) перевірку стін приміщення за допомогою діапазонного скануючого приймача або індикаторів поля;
   е) обстеження меблів та інших предметів у приміщенні за допомогою детектора випромінювання;
   є) перевірку телефонної та електронної лінії за допомогою комплексу "Scanner 99";
   а) усі відповіді правильні;
   б) усі відповіді неправильні;
   в) не всі відповіді правильні.

Література [25; 27; 29; 30; 32; 39; 43; 45; 48]

Тема18. Організація та проведення заходів з контролю за ефективністю технічного захисту електронної інформації з обмеженим доступом в організаціях та установах

Відповідно до програми курсу, самостійне вивчення студентами цієї теми не передбачається.

2. Підготуйте письмові відповіді на такі запитання:
   2.1. Як у теорії безпекознавства розглядають категорію безпека?
   2.2. У чому полягає зміст концепції безпеки підприємництва?
   2.3. Окресліть об'єкт і предмет курсу "Забезпечення безпеки підприємницької діяльності".
   2.4. Які завдання курсу забезпечення безпеки підприємницької діяльності.
   2.5. Розкрийте зміст структури курсу забезпечення безпеки підприємницької діяльності.
   2.6. Яку роль посідає самоорганізація у забезпеченні безпеки підприємства.
   2.7. З урахуванням яких даних визначається найбільш оптимальна структура створюваної служби безпеки на об'єкті.
   2.8. Охарактеризуйте сутність забезпечення безпеки господарюючого суб'єкта.
   2.9. Поясніть власне бачення обставин, що впливають на можливість вирішення проблеми більш активної участі державної системи в забезпеченні безпеки підприємництва.
3. Підготуйте реферат за темою "Предмет, завдання і зміст навчального курсу "Забезпечення безпеки підприємницької діяльності".
4. Підготуйте реферат за темою: "Методологічні засади і наукові принципи пізнання змісту курсу "Забезпечення безпеки підприємницької діяльності".

Тестові завдання

Зазначте правильну відповідь:

1. У числі задач системи безпеки підприємства необхідно назвати наступні:
   а) захист законних інтересів підприємства і його співробітників;
   б) збір, аналіз, оцінка і прогнозування даних, що характеризують обстановку на підприємстві;
   в) своєчасне виявлення злочинних посягань, спрямованих на добування секретів у персоналу підприємств;
   г) вивчення конкурентів, партнерів, клієнтів;
   д) захист співробітників підприємства від насильницьких посягань;

е) контроль за ефективністю функціонування системи безпеки підприємства;
є) своєчасне виявлення конфліктних ситуацій серед персоналу підприємства;
ж) виявлення спроб ведення несумлінної конкуренції;
з) добування необхідної надійної і всебічної інформації в конкурентному середовищі, що може мати значення для вироблення управлінських рішень з питань стратегії і практики економічного розвитку підприємства;
і) усі відповіді правильні;
к) не всі відповіді правильні;
л) усі відповіді неправильні.

2. До принципів побудови недержавної системи безпеки підприємництва належать:
а) централізоване керування;
б) координація взаємодії з правоохоронними органами;
в) розумна достатність;
г) відповідність зовнішнім і внутрішнім загрозам;
д) комплексне використання сил і засобів;
е) ієрархічність;
є) цілісність;
ж) відповідність нормам права;
з) усі відповіді правильні;
і) усі відповіді неправильні;
к) не всі відповіді правильні.

3. Методологія дослідження сфери забезпечення безпеки підприємницької діяльності охоплює:
а) синергетику;
б) діалектичний метод;
в) генетичний метод (спосіб дослідження системи безпеки, який заснований на аналізі її розвитку);
г) системно-структурний метод;
д) статистичний метод;
е) спостереження;
є) абстрагування і конкретизація;
ж) порівняння та зіставлення;
з) аналіз та синтез;
і) індукція та дедукція;
к) аналогія і прогнозування;
л) моделювання;

електроживлення персонального комп'ютера застосовують мережеві перешкодоусувачі — фільтри?
5. Чому зміни напруги називають мережевими перешкодами в промисловій мережі (220В, 50Гц)?
6. Визначте, чому кабельна мережа відіграє роль антени для побічних випромінень комп'ютера і сервера?
7. За допомогою якого обладнання приймаються і декодуються електромагнітні коливання, які виникли за рахунок високочастотних струмів, що подаються через мережу електроживлення комп'ютера на нелінійні елементи?
8. Чи можна, на вашу думку, прослуховувати приміщення, де є ЕОМ, виходячи з того, що побічні коливання у пристроях комп'ютера можуть бути промодульовані голосовою інформацією (акустичним полем), оскільки деякі конструктивні елементи комп'ютера мають мікрофонний ефект?
9. Які фізичні явища, характерні для форм зберігання інформації на об'єктах ЕОМ?
10. Криптографічний захист інформації.

Тестові завдання

Зазначте правильну відповідь:

1. Серед умов для формування технічних каналів відтоку інформації через ланцюги електроживлення у пристроях комп'ютера можна назвати такі обставини:
а) неоптимізовану кількість паразитних контурів;
б) наявність у паразитних контурів загальної точки, що забезпечує взаємний обмін побічними електромагнітними коливаннями;
в) безліч видів побічних коливань багатоканального блока вторинного живлення;
г) наскільки послаблено паразитне випромінювання, викликане сигналами, що передаються через кабельну систему під час мережевого обміну інформацією;
д) некваліфіковане та необережне прокладення кабелю;
е) опосередковане випромінювання, що виникає в елементах комп'ютера, наводиться на всі прокладки кабелю локальної мережі;
є) усі відповіді правильні;
ж) усі відповіді неправильні;

3. Ціль діяльності групи ПДТР, яка є відносно самостійним структурним підрозділом служби безпеки підприємства.
4. Роль нормативних документів, національних і міжнародних стандартів з обробки та захисту інформації в діяльності групи протидії технічній розвідці (ПДТР).
5. Пріоритети у діяльності розвідок світу в галузі наукового шпигунства і перехоплення інформації, що обертається у локальних та корпоративних мережах установ і підприємств.
6. Особливості напрямку захисту інформації в інформаційних системах, базовим елементом яких є комп'ютер, з урахуванням того, що інформація крім основного середовища передачі даних має ще декілька побічних середовищ.
7. Поняття середовища ПДТР з точки зору процесу захисту інформації і контролю її захищеності.
8. Шкала електромагнітних коливань, її межі (від інфразвукових до рентгенівських випромінювань).
9. Класифікація та сутність принципів захисту інформації від витоку по технічних каналах (маскування небезпечного сигналу шумовинням, фізичне усунення тракту поширювання небезпечного сигналу, обмеження дії небезпечного сигналу в тракті його поширення, зменшення рівня небезпечного сигналу на виході передавача тощо).

Практичні завдання

1. Зазначте відмінності стосовно цілі дій групи протидії технічній розвідці та іншої групи захисту інформації від несанкціонованого доступу (НСД) в ЕОМ.
2. Визначте, чому спроби неправомірного доступу до чужих інформаційних мереж здійснюється одночасно з декількох робочих місць (персональних комп'ютерів) шляхом автоматичного перебору абонентських номерів доти, доки на іншому кінці лінії не "відгукнеться" чужий комп'ютер, тобто частина атакуючих комп'ютерів одержує необхідний доступ?
3. Чи може, на ваш погляд, незаконний користувач, підібравши необхідний пароль, одержати доступ до комп'ютерної інформації та проводити з нею будь-які дії під виглядом законного користувача?
4. Висловіть вашу думку, чому для зниження рівня паразитного електромагнітного випромінювання, що проникає у мережу

м) усі відповіді правильні;
н) усі відповіді неправильні;
о) не всі відповіді правильні

Література [1; 19; 20; 23; 26; 35; 36; 38; 41; 60]

Тема2. Основні обов'язки і права працівників служби безпеки господарюючого суб'єкта при виконанні задач по забезпеченню безпеки підприємства

Питання для самоконтролю

1. Охарактеризуйте діючу на території України законодавчу базу, яка дозволяє створювати підрозділ служби безпеки підприємства.
2. Система забезпечення безпеки підприємницької діяльності має певні принципи побудови. Проаналізуйте їх.
3. Охарактеризуйте принцип комплексного системного підходу до вирішення проблем забезпечення безпеки підприємства.
4. Хто несе відповідальність за організацію і забезпечення безпеки підприємства і який спеціальний підрозділ має певні права, пов'язані із цим напрямом діяльності?
5. Керівник якого підрозділу підприємства може виступати як уповноважена особа власника підприємства з питань захисту інформації з обмеженим доступом?
6. Охарактеризуйте основні вимоги щодо захисту конфіденційної інформації, які повинні знати співробітники підприємства та ступінь їх особистої відповідальності за їх порушення.
7. Яким вимогам повинні відповідати відомості, які виробляються підприємством та його робітниками, перед тим як мають бути спрямовані в загальні внутрішні та зовнішні інформаційні потоки з урахуванням можливої необхідності їх захисту?
8. Назвіть застережні заходи в роботі з чернетками документів, що використовуються при підготовці документів обмеженого користування. Проаналізуйте їх.
9. Наведіть особливості попередження витоку конфіденційних відомостей, які підготовлені на підприємстві для засобів масової інформації і пов'язані з його діяльністю.
10. У чому полягає організація на підприємстві відповідного режиму поводження з конфіденційною інформацією в місцях проведення виробничих нарад, ділових переговорів?

Практичні завдання

Завдання 1. Підготуйте письмові відповіді на наступні запитання:

1. Дайте перелік фахівців, із яких складається підрозділ інформаційної безпеки служби безпеки підприємства і охарактеризуйте їх функціональні обов'язки.
2. Розкрийте головні завдання підрозділу інформаційної безпеки служби безпеки підприємства.
3. Яка роль підрозділу інформаційної безпеки СБ підприємства у організації і ведені належного обліку документів з грифом "комерційна таємниця"?
4. Яким чином здійснюється працівниками підрозділу безпеки підприємства співробітництво з правоохоронними органами?
5. Що розуміють під принципом, який на практиці часто називається "політикою чистих столів"?
6. Охарактеризуйте заходи співробітників підрозділу інформаційної безпеки щодо запобігання розголошення і витоку комерційних секретів при веденні діловодства, а також при веденні відкритого службового листування.
7. Яким чином органи судової влади та прокуратури забезпечують охорону права юридичних осіб на комерційну таємницю?
8. Назвіть нормативно-правові акти, що регулюють суспільні відносини в сфері охорони комерційної таємниці.
9. Розкрийте повноваження співробітників підрозділу безпеки підприємства у сфері забезпечення стійкості функціонування господарюючого суб'єкта.
10. Охарактеризуйте порядок обліку і зберігання конфіденційної інформації, що є власністю підприємств, які не підпадають під державне управління (комерційні банки, господарські товариства, асоціації, концерни і т. ін.).

Завдання 2. Підготуйте реферат на тему "Основні обов'язки і права працівників служби безпеки господарюючого суб'єкта при виконанні задач по забезпеченню безпеки підприємства".

Завдання 3. Підготуйте реферат на тему "Обов'язки і права працівників підрозділу інформаційної безпеки підприємства".

Завдання 4. Підготуйте реферат на тему "Основні обов'язки і права співробітників комерційної розвідки підприємства".

ж) пошук конкретних учасників чи виконавців, що нанесли збитки підприємству, які компенсуються або не компенсуються, а також виявлення обставин, при яких готувалось і було скоєно посягання;
з) усі відповіді правильні;
і) усі відповіді неправильні;
к) не всі відповіді правильні.

3. Принципи проведення працівниками детективної групи СБ підприємства службового розслідування:
а) законність;
б) неухильне дотримання прав і свобод громадян;
в) загальноуправлінський принцип єдиноначальності та колегіальності у вирішені поточних питань службового розслідування;
г) наступальність;
д) конфіденційність;
е) конспіративність у роботі з негласними джерелами інформації;
є) усі відповіді правильні;
ж) усі відповіді неправильні;
з) не всі відповіді правильні.

Література [26; 35; 38; 41]

Тема16. Провадження службового розслідування працівниками служби безпеки підприємства.

Відповідно до програми курсу, самостійне вивчення студентами цієї теми не передбачається.

Тема17. Методи і засоби захисту інформації в сфері використання господарюючим суб'єктом електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж

Питання для самоконтролю

1. Місце групи протидії технічній розвідці (ПДТР) у складі служби безпеки підприємства.
2. Вимоги, що висовуються для забезпечення безпеки інформації, яка в процесі діяльності підприємства циклічно актуалізується.

1. Напрям діяльності детективної групи служби безпеки підприємства:
   а) розробляє і здійснює спеціальні заходи щодо спостереження за окремими клієнтами банку, серед яких можуть бути представники найближчого оточення до банку, котрі 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 окремих працівників з лояльності 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 банку;
   є) усі відповіді правильні;
   ж) усі відповіді неправильні;
   з) 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 в середині підприємства та в сфері його інтересів;
   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;
   є) оцінка надійності і стійкості банків та інших категорій партнерів підприємства;

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь:

1. У структуру підрозділу інформаційної безпеки СБ підприємства можуть входити:
   а) керівник підрозділу інформаційної безпеки (заступник керівника служби безпеки підприємства);
   б) юрист;
   в) фахівці в галузі економічної розвідки, промислової контррозвідки;
   г) фахівці, які вміють застосовувати спеціальну техніку для захисту приміщень;
   д) системний адміністратор;
   е) системний програміст;
   є) криптограф;
   ж) аудитор;
   з) спеціаліст інформаційної системи.
2. Основні напрямки захисту комп'ютерної системи підприємства:
   а) захист апаратури та носіїв інформації від пошкодження, викрадення, знищення;
   б) захист інформації в мережах зв'язку та вузлах комутації;
   в) захист від витоку інформації через побічні канали електромагнітних випромінювань та наведень;
   г) захист інформаційних ресурсів від несанкціонованого доступу;
   д) захист юридичної значущості електронних документів (забезпечення доказу правдивості того, що документ був створений і відправлений справді автором);
   е) захист від незаконного проникнення в комп'ютерні системи і мережі, автоматизовані системи, здатного спричинити перекручення або знищення інформації чи то носіїв інформації;
   є) захист від втручання в роботу комп'ютерних мереж банків через мережу "Інтернет" для отримання доступу до конфіденційної інформації шляхом "зламу систем захисту";
   ж) оптимізація організаційних і організаційно-технічних заходів опрацювання конфіденційної інформації з метою попередження її викрадення чи знищення.

3. Виходячи з вимог безпеки інформації, пошук радіоелектронних засобів несанкціонованого знімання інформації можна представити у вигляді відповідних етапів:
   а) вивчення службою безпеки підприємства оперативної обстановки біля об'єкта інформації;
   б) перевірка радіоефіру за межами приміщення;
   в) перевірка монітору радіоефіру у приміщенні за допомогою нелінійних локаторів у діапазоні частот 0,1–2000 МГц;
   г) перевірка комп'ютерів, телефонних апаратів, електротехнічних засобів за допомогою скануючого приймача;
   д) перевірка стін приміщення за допомогою діапазонного скануючого приймача або індикаторів поля;
   е) обстеження меблів та інших предметів у приміщенні за допомогою детектора випромінювання;
   є) перевірка телефонної та електричної лінії за допомогою комплексу "Scanner 99";
   ж) технічний контроль за спеціальною апаратурою, що використовується для забезпечення безпеки і таємності інформації.
4. Роботи із захисту інформації, що обертається в комп'ютерах і комп'ютерних мережах проводяться в таких напрямках:
   а) протидія несанкціонованому доступу до інформаційних потоків підприємства за допомогою програмного забезпечення і засобів інженерно-технічної розвідки;
   б) блокування несанкціонованого доступу до зберігання і опрацювання інформації за допомогою засобів обчислювальної техніки, що передається через лінії зв'язку абонентів;
   в) попередження несанкціонованої модифікації інформації;
   г) обстеження підрозділом інформаційної безпеки підприємства об'єктів, на яких використовуються комп'ютерні технології;
   д) атестування системи комп'ютерної безпеки з метою підтвердження відповідності вимогам стандарту безпеки інформації;
   е) категоріювання об'єктів, що мають комп'ютерні системи;
   є) використання рубіжної системи захисту підприємницької інформації;
   ж) здійснення тотального контролю об'єктів захисту з ЕОМ.

Література [26; 33–36; 38; 39; 41; 52; 54; 67]

тому сприяє прийняттю доцільних адекватних рішень з урахуванням даних обставин.
9. Мета і засоби детективної діяльності.
10. Роль і задачі спостереження в 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'єкту господарювання, загальна та індивідуальна превенція правопорушень.
3. Оцінка 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 з 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 в будь-якій з ситуацій, не виключаючи й критичну.
7. Охарактеризуйте види зовнішнього спостереження, яке може вестися у ході детективної діяльності.
8. Охарактеризуйте технічні засоби, які використовуються при здійсненні спостереження детективами.
9. Тактичні особливості ведення спостереження детективами.
10. Підготуйте реферат за темою: "Роль детективної групи у забезпеченні безпеки підприємства"

Тестові завдання

Зазначте правильну відповідь:

Тема13. Технології збирання необхідних відомостей працівниками служби безпеки підприємства з цивільних справ

Відповідно до програми курсу, самостійне вивчення студентами цієї теми не передбачається.

Тема14. Тактика дій працівників служби безпеки господарюючого суб'єкта по розшуку безвісті зниклих співробітників підприємства, якщо їх відсутність на роботі приведе до реального або потенційного збитку

Відповідно до програми курсу, самостійне вивчення студентами цієї теми не передбачається.

Тема15. Тактика дій працівників детективної групи служби безпеки господарюючого суб'єкта при виконанні службових завдань щодо ведення спостереження за об'єктом

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 в Державному класифікаторі професій України під номером 3450 і введена в дію наказом Держстандарту України № 257 від 27.07.1995.
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; екстраполяції, яка використовується як метод прогнозування активізації дестабілізуючих чинників, а

Тема3. Методи, принципи і організація керівництва силами служби безпеки підприємства банку в умовах проведення захисних операцій протидії загрозам цьому суб'єкту

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. Методи управління, від яких значною мірою залежить ефективність процесу досягнення мети безпеки банку (пізнавально-програмуючий і організаційно-регулюючий).
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 задач системи безпеки банку (стратегічні, тактичні, оперативні).
8. Чому без засобів групи управління в 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 у письмову вигляді 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 і т. д.
2. Схарактеризуйте основні методи керування службою безпеки банку (економічні, розпорядницькі і соціально-психологічні).
3. Ваша думка щодо структури процесу керування діяльністю служби безпеки банку, яка складається з трьох блоків, кожне 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. Охарактеризуйте методологію дослідження процесів формування, функціонування та 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 власне 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 повинна 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 за часом, місцем і видом 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.
   є) не всі відповіді правильні.
2. Управлінський вплив, спрямований на забезпечення банківської безпеки залежить від рис засобів управління, основними з яких є такі:
   а) забезпечують злагодженість та 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;

   а) з електроживленням радіотрансляторів (закладок) від телефонної лінії або від батарейки;
   б) радіомікрофони, які можна монтувати в телефонний провід;
   в) напівактивний мікрофон без джерела живлення;
   г) радіомікрофон, розташований в безпосередній близькості від телефонної лінії;
   д) постійно діючі радіомікрофони;
   е) радіомікрофони з дистанційним керуванням;
   є) з передачею інформації в ефір за допомогою радіохвилі;
   є) усі відповіді правильні;
   ж) усі відповіді неправильні;
   з) не всі відповіді правильні.
2. Акустичний контроль приміщення можливий за допомогою:
   а) мікрофону, з виводом сигналу по телефонній лінії;
   б) диктофону;
   в) стетоскопу;
   г) радіомікрофону;
   д) телефонної лінії;
   е) лазерного зняття інформації із віконного скла;
   є) усі відповіді правильні;
   ж) усі відповіді неправильні;
   з) не всі відповіді правильні.
3. Для захисту телефонних ліній від радіозакладок і диктофонів, використовуються:
   а) прилади активного захисту;
   б) аналізатори телефонних ліній;
   в) склемблери;
   г) фільтри;
   д) випалювачі засобів з'йому;
   е) універсальні прилади;
   є) джерела радіошуму;
   ж) детектори диктофонів;
   з) прилади, що дистанційно стирають запис з касетних диктофонів;
   з) усі відповіді правильні;
   і) усі відповіді неправильні;
   к) не всі відповіді правильні.

Література [26; 28; 33; 34; 37; 41; 49; 54; 66]

1. Чому ризик — це завжди кількісна та якісна оцінка небезпеки певним суспільним відносинам, з якими зокрема пов'язана діяльність з правового захисту підприємництва?
2. Зазначте основні питання, що вирішуються у ході перевірки партнерів у підприємницькій діяльності.
3. Охарактеризуйте сучасні методи перевірки надійності комерційних партнерів, щоб мінімізувати ризики при укладанні договорів, адже у сфері підприємництва часто вдаються до шахрайства.
4. Наведіть приклади шахрайських дій при укладанні договору, визначіть типові способи вчинення та приховування цього виду злочину.
5. Визначте чи можна уявити собі методику перевірки повноважної особи, яка підписує договір, не ознайомившись з документом, що підтверджує повноваження особи на укладання самого контракту, не отримавши дані про його право не тільки брати участь в переговорах, а й приймати рішення з конкретних питань від імені контрагента.
6. Як можна дізнатися, що лише перший керівник має право виступати від імені підприємства без доручення, а за дорученням у переговорах може брати участь заступник директора підприємства-контрагента, якому можуть бути делеговані значні повноваження, та головний бухгалтер.
7. Обґрунтуйте, чому уже на першому етапі підготовки угоди, велике значення має чітка та повна фіксація фірмових назв контрагентів згідно з державним реєстром.
8. Методика перевірки доручення.
9. Обґрунтуйте, чому угода, що укладається від імені іншої особи, є перевищенням прав, однак не тягне за собою ніяких правових наслідків до особи, від імені якої вона укладається.
10. Обов'язок служби безпеки підприємства щодо перевірки партнера.

Тестові завдання

Зазначте правильну відповідь:

1. "Радіомікрофони", які встановлені у приміщенні і ретранслюють інформацію в підходяще для підслуховування місце, де працює розшифровуючий бесіди оператор, бувають різних видів:
   в) інформаційні технології є найбільш активними і рухомими елементами в системи управління;
   г) носять альтернативний характер.
   д) усі відповіді правильні.
   е) усі відповіді неправильні.
   є) не всі відповіді правильні.
3. Головне призначення системи забезпечення безпеки банку полягає у досягненні цілей безпеки, а основною функцією даної системи є забезпечення інтересів об'єкта через:
   а) моніторинг 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;
   є) усі відповіді неправильні;
   ж) не всі відповіді правильні;

Література [26; 33–35; 41; 43; 45; 48; 52]

Тема4. Консультування і надання рекомендацій працівниками служби безпеки господарюючого суб'єкта керівництву і персоналу підприємства з питань економічної, інформаційної та особистої 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, ризики 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 ставленням до них.
8. Необхідність у розробці чітких критеріїв, показників, параметрів безпеки.
9. Поняття, критерії, 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 і методика його проведення.
2. З яких двох найважливіших елементів складається концепція ризику в стратегії безпеки.
3. Наведіть вашу точку зору, чому оцінка рівня безпеки організацій та установ, поряд з аналізом фактів ризику, передбачає також використання категорій збитків — фактичних, очікуваних, потенційних та их, 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, а саме зародження, розвиток та безпосередню їх актуалізацію.
6. Обґрунтуйте завдання діагностики небезпек, що 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, завдячуючи яким можна вирішувати завдання щодо ідентифікації ознак, які б вказували на формування і розвиток небезпек, чи можуть знаходитись у взаємній суперечці. Внаслідок чого це трапляється?
10. Поясніть, чому у випадку "конфлікту аксіологій" (аксіологія — грецьк. Axsa — цінність, logos — вчення, "вчення про цінність") постає необхідність у виробленні поміркованого управлінського

Тема12. Порядок, зміст і методика роботи працівників служби безпеки підприємства при організації та проведенні заходів, спрямованих на виявлення ненадійних ділових партнерів.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Охарактеризуйте зміст концепції ризику.
2. Розкрийте зміст поняття методології ризик-менеджменту або управління ризиками.
3. Обґрунтуйте необхідність моделювання процесів виникнення небезпек і загроз за моделями вивчуваних об'єктів, оскільки модель у певному сенсі відображає певні його сторони і властивості.
4. Ймовірнісний характер оцінки ризику у силу невизначеності багатьох негативних наслідків як дії об'єктивних факторів, так і прийнятих управлінських рішень.
5. Розкрийте зміст процедури оцінки деякої події, процесу або явища.
6. Обґрунтуйте, чому оцінка рівня безпеки передбачає поряд із аналізом факторів ризику, також і використання категорій збитків — фактичних, очікуваних, потенційних, компенсованих і некомпенсованих.
7. Охарактеризуйте механізм розвитку небезпек, тому що вони не виникають раптово, здебільшого їм передують деякі події, процеси або явища.
8. Обґрунтуйте необхідність у виявленні тих ознак, які б вказували на зародження та формування небезпек, терміни їх виникнення, можливу шкоду.
9. Об'єктивні показники, які на ранніх стадіях зародження та формування небезпек дають можливість вважати їх чинниками, що визначають формат небезпеки, здійснювати моделювання імовірних загроз.
10. Обґрунтуйте твердження вчених, що найвища міра безпеки досягається за умови, коли весь комплекс показників перебуває у межах допустимих порогових значень.

Практичні завдання

є) виявлення внутрішніх логічних зв'язків в отриманні інформації;
ж) створення більш логічної інформації ніж була, що відбиває новий погляд на проблему;
з) складання загальної картини на небезпечні тенденції стану безпеки підприємства в залежності від негативних факторів системосередовища (середовища існування підприємства, як системи);
і) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

3. Інформаційно-аналітичний підрозділ конкурентної розвідки СБ підприємства може бути "Мозковим центром" комерційної структури, що обумовлено наступними факторами:
а) використанням у конкретній боротьбі найефективніших форм і методів;
б) величезним тиском кримінальних елементів на банки, підприємства, організації, установи та подальшої криміналізації ринку;
в) недосконалістю правової захищеності підприємницьких структур;
г) знаходженням більш надійних партнерів;
д) необхідністю вивчення доступних джерел сировини, комплектуючих чи товарів в інтересах їх переробки та реалізації;
е) необхідністю перевірки надійності вірогідних партнерів;
є) можливістю встановлення таємного співробітництва персоналу з представниками структур, що являють небезпеку для підприємства;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
і) не всі відповіді правильні.

Література [26; 28; 33; 35; 39; 41; 46; 48; 62]

рішення, яке має ґрунтуватися на оцінці 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 і не сприймаються належним чином;
б) суб'єктивні показники залежать не лише від фізичного, але й від інтелектуального розвитку людини, які обумовлюють критеріальну шкалу оцінок тих чи інших чинників у якості загрозливих або небезпечних;
в) кожна небезпека і загроза є оригінальною і характеризується специфічними та 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 й наголошуючи на їх системній 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 відтворенням їх у вигляді графіків і 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;
є) усі відповіді правильні;
ж) усі відповіді неправильні;
з) 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;

є) критерії, за допомогою яких обираються ті чи інші стратегії забезпечення безпеки організацій та установ.
ж) усі відповіді правильні;
з) усі відповіді неправильні;
і) не всі відповіді правильні.

3. Небезпеки та загрози вимірюють за такими ознаками:
а) за кількістю загиблих людей та тих, що зазнали ушкоджень;
б) за розмірами шкоди;
в) за розмірами матеріальних втрат у процентах від загального доходу об'єкта;
г) за щорічним зростанням шкоди у процентах із прогнозом подальшого розвитку;
д) за кількісним порівнянням втрат від небезпек на конкретному підприємстві з втратами на інших;
е) рівнем економічного розвитку організацій, установ;
є) рівнем заробітної плати;
ж) максимально можливим зниженням сумарного ризику;
з) дослідженням небезпек за моделями об'єктів, що вивчають за певними критеріями з послідуючим розповсюдженням результатів на оригінал;
і) усі відповіді правильні;
к) усі відповіді неправильні;
л) не всі відповіді правильні.

Література [34; 35; 40; 41; 51; 54; 69]

Тема5. Аналітична робота служби безпеки 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 та 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.

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 та 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 і поглиблення якісної характеристики;
є) сприяння виявленню наявних каналів витоку інформації за допомогою вимірювання і оцінки якісних і кількісних ознак ступеня поінформованості конкурентів про фінансовий, економічний стан підприємства, а також ефективність його роботи в цілому.
ж) усі відповіді правильні;
з) усі відповіді неправильні;
і) не всі відповіді правильні.

2. Для обробки інформації, отриманої з різних джерел, інформаційно-аналітичний підрозділ конкурентної розвідки служби безпеки підприємства застосовує наступні 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 не є дезінформацією, але носять помилковий характер;
д) поділ інформації на відкриту й закриту;
е) компонування різноманітної інформації в нову логічну систему;

вчення основних тенденцій розвитку бізнесу, аналіз можливих ризиків.
2. Схарактеризуйте особливості організації і проведення конкурентної розвідки, яка розв'язує свої задачі 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 окремої держави 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 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 та проведенню розшукових заходів з елементами конспірації, здійсненню службових розслідувань і документуванню дій об'єкта у ході зовнішнього спостереження.
9. Підготуйте реферат за темою: "Конкурентна розвідка — легальний інструмент дослідження ринку".
10. Підготуйте реферат за темою: "Історія розвитку та становлення конкурентної розвідки".

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 економічним 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 дане підприємство.
3. Поясніть роль інформаційно-аналітичного підрозділу комерційної розвідки в забезпеченні керівництва підприємства шляхом відповідної підготовки до веденню переговорів з партнерами в нестандартних ситуаціях.
4. Тактика добування комерційною розвідкою підприємства відомостей, на основі яких можна характеризувати ступень 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. Наведіть вашу думку, чому дані, одержані з відкритих джерел, інформації у будь-якому випадку перепровіряються розвід-

увальними методами (за допомогою притягнутих до співробітництва інформаторів тощо).

9. Обґрунтуйте, чому інформаційні системи належать до числа найважливіших засобів діяльності комерційної розвідки СБ підприємства.
10. Охарактеризуйте основні задачі аналітичного відділення, довідково-інформаційного фонду, групи експертів і консультантів, 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 наступні аналітичні методи:
   а) обробка зібраної інформації;
   б) установлення причинно-наслідкових взаємозв'язків зібраних фактів і явищ;
   в) асоціативні діаграми, за допомогою яких виявляються області ділових і особистих інтересів об'єкта спостереження;
   г) аналіз інформації для виявлення відсутніх ланок даних та 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;
   є) складання загальної картини на основі відомої інформації;
   ж) виявлення тенденцій розвитку подій і явищ;
   з) усі відповіді правильні;
   і) усі відповіді неправильні;
   к) не усі відповіді правильні.
2. Способи одержання інформаційно-аналітичним підрозділом комерційної розвідки служби безпеки підприємства про діяльність конкурентів, можуть мати такі законні форми:
   а) збір і аналіз інформації з офіційно опублікованих джерел;
   б) відвідування виставок та ярмарок, влаштованих конкурентами;

   є) підпис представника служби безпеки, який проінструктував співробітника, що підписав зобов'язання;
   ж) попередження-зобов'язання про нерозголошення робітником після звільнення комерційних секретів, до яких він мав доступ.

Література [26; 28; 33; 35; 39; 41; 46; 48; 62]

Тема11. Порядок, зміст і методика роботи працівників служби безпеки підприємства при проведенні заходів, спрямованих на вивчення негативних аспектів ринку

Питання для самоконтролю

1. Поняття конкурентної розвідки.
2. Реалізація конкурентною розвідкою заходів протидії всім 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 підприємства, 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 підрозділом 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, ви-

є) переведення співробітника на іншу ділянку роботи або посаду, яка не пов'язана з необхідністю доступу до відомостей, що складають комерційну таємницю;
ж) тяжіння до вживання алкоголю.

3. Перевірка на благодійність громадян, що отримують допуск до фірмових і банківських секретів на Заході включають наступні дії:
а) співбесіда в кадровому апараті, коли кандидат на роботу з комерційною таємницею заповнює необхідні документи;
б) намагання отримати максимум відомостей, зокрема: як часто і чому кандидат змінює місця роботи, за якими адресами мешкав, де служив;
в) перевірка за основними і додатковими картотеками МВС;
г) встановлення за місцем проживання кандидатів контактів з дільничними інспекторами поліції з метою перевірки способу життя, поведінки, виявлення компрометуючих зв'язків;
д) після всіх перевірочних заходів за спеціально розробленими методиками методистом-психологом проводиться тестування кандидата;
е) з'ясування мети та обставин поїздок за кордон;
є) перевірку біографічних даних кандидата за останні 10 р.ків;
ж) ґрунтовне вивчення досьє кандидата на роботу з комерційної таємниці.

4. Зобов'язання про нерозголошення комерційної таємниці повинно мати такі реквізити:
а) прізвище, ім'я, по-батькові співробітника;
б) займана посада;
в) зобов'язання не розголошувати відомості, що складають комерційну таємницю;
г) попередження про те, що у випадку розголошення довірених секретів з робітником може бути розірвана трудова угода за ініціативою власника підприємства;
д) попередження про те, що у випадку розголошення комерційної таємниці підприємства, робітник може бути притягнутий до відповідальності в порядку, встановленому законодавством України;
е) дата та особистий підпис співробітника, який дав зобов'язання;

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;
є) викрадення креслень, документів, зразків виробів;
ж) переманювання провідних спеціалістів для одержання потрібної інформації;
з) усі відповіді правильні;
і) усі відповіді неправильні;
к) не усі відповіді правильні.

3. Показники комплексної оцінки результатів роботи комерційної розвідки підприємства наступні:
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;
є) кількість виявлених ненадійних ділових партнерів;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
і) не усі відповіді правильні.

Література [33–35; 37; 45; 49]

Тема 6. Система економічної розвідки зарубіжних країн

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 кримінологічна загроза 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 технологій та її мета.
8. Основні прийоми ведення сучасного економічного протистояння.
9. Сітка Бернара Надулека, яку застосовують при розгляді можливих варіантів конфронтації в економічній сфері на стратегічному рівні.
10. Механізми економічної розвідки: американської, японської, німецької, зорієнтованих на світовий ринок.

Практичні завдання

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

Тестові завдання

Зазначте правильну відповідь:

Тестові завдання

Із запропонованих варіантів виберіть правильну відповідь:

1. Надання допуску до комерційної таємниці надається дієздатним громадянам України віком від 18 р.ків і передбачає враховувати наступні фактори:
   а) перевірку співробітника у зв'язку з допуском до комерційної таємниці;
   б) ознайомлення співробітника із ступінню відповідальності за порушення законодавства, пов'язаної з розголошенням ним комерційної таємниці;
   в) виявлення в оформлюваного підозрілих зв'язків з числа співробітників конкуруючих фірм;
   г) встановлення недостовірних відомостей про себе в процесі підготовки матеріалів до оформлення допуску;
   д) наявність у перевіряємого судимості за тяжкі злочини і перш за все — за протиправні дії, пов'язані з комерційним шпигунством, зловживаннями у сфері кредитно-фінансової та економічної діяльності;
   е) відсутність у співробітника підприємства обґрунтованої необхідності в роботі з комерційною таємницею;
   є) наявність у співробітника психічних захворювань, тяжіння до вживання наркотичних засобів;
   ж) тяжіння до вживання алкоголю, внаслідок чого може статися витік інформації.
2. Причинами та підставами позбавлення допуску можуть бути:
   а) розголошення співробітником довіреної йому конфіденційної таємниці;
   б) невиконання вимог режиму, який встановлений Положенням про комерційну таємницю та правилами її збереження;
   в) сприяння вітчизняним та іноземним конкурентам в здійсненні діяльності, яка завдає шкоди інтересам підприємства;
   г) грубе порушення співробітником "Положення про комерційну таємницю";
   д) втрата співробітником документів та інших матеріальних носіїв, які містять комерційну таємницю;
   е) надходження відносно співробітника компрометуючих його відомостей які він приховував і які не могли бути враховані при вирішенні питання про його допуск;

7. Характеристика триступеневої системи важливості комерційної таємниці.
8. Особливості оформлення допуску конкретному співробітникові до ступенів важливості комерційної таємниці.
9. Коли допуск до комерційної таємниці співробітників підприємства вважається правомірним, тобто має юридичну силу?
10. Хто має право позбавляти співробітника допуску до комерційної таємниці?

Практичні завдання

Завдання 1. Охарактеризуйте методологію вивчення та перевірки власником підприємства або уповноваженою ним особою кандидата для роботи, пов'язаної з відомостями, що складають комерційну таємницю.

Завдання 2. Підготуйте в довільній формі так зване попередження-зобов'язання про нерозголошення співробітником підприємства після звільнення комерційних секретів, до яких він мав доступ.

Завдання 3. Підготуйте реферат на тему "Юридичне поняття допуску до комерційної таємниці".

Завдання 4. Підготуйте реферат на тему "Перевірка осіб, що оформляються задля роботи з комерційними секретами".

Завдання 5. Охарактеризуйте дві різні юридичні категорії "допуск" і "доступ" до комерційної таємниці, визначте чим вони відрізняються.

Завдання 6. Розкрийте шляхи оформлення власником підприємства рішення про надання доступу до конкретної комерційної таємниці та її матеріальних носіїв представнику сторонньої організації і збереження цією особою конфіденційної інформації, з якою він був ознайомлений.

Завдання 7. Охарактеризуйте поняття "режим доступу до інформації" у відповідності до ст. 28 Закону "Про інформацію".

Завдання 8. Розкрийте особливості способів вирішення питання юридичних гарантій збереження в таємниці конфіденційної інформації підприємства, до якої отримали доступ представники органів державного управління та ділових кіл.

Завдання 9. Підготуйте в письмовій формі "Положення про дозвільну систему доступу співробітників підприємства і представників сторонніх організацій до відомостей, що складають комерційну таємницю підприємства".

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;
   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;
   є) умови контрактів;
   ж) технічна специфікація існуючої та перспективної продукції;
   з) маркетинг та стратегія цін;
   і) фінансові звіти та прогнози;
   к) усі відповіді правильні;
   л) усі відповіді неправильні;
   м) не усі відповіді правильні.
2. Для добування потрібної інформації, організації, які займаються промисловим шпіонажем, користуються таким спеціальними методами розвідки:
   а) незаконне одержання інформації через корумповані елементи у владних структурах;
   б) шантаж і різноманітні способи тиску;
   в) підслухування розмов конкурентів;
   г) використання професійних агентів для одержання інформації;
   д) обманні переговори з представником конкурента про придбання товарів і після одержання необхідної інформації відмова від предмету переговорів;
   е) обманне запрошення на роботу спеціалістів, що працюють у конкурента, з пропозицією заповнити тест із спеціально підібраними питаннями;
   є) завуальовані питання спеціалістам конкурента;
   ж) таємне спостереження за об'єктом, яким може бути спеціаліст, відділ чи установа;
   з) усі відповіді правильні;
   і) усі відповіді неправильні;
   к) 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;
є) зрив переговорів по контрактах;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
і) не усі відповіді правильні.

Література [28; 64–66]

Змістовий модуль ІІ. Організація, порядок і способи виконання службових задач працівниками служби безпеки об'єкта задля забезпечення його нормального функціонування

Тема7. Тактика дій персоналу служби безпеки підприємства при виконанні службових задач по охороні майна господарюючого суб'єкта

Питання для самоконтролю

1. Головні функції групи режиму.
2. На кого покладається здійснення пропускного режиму?
3. Хто встановлює пропускний режим на об'єкті охорони?
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 охорони?
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 охорони у зв'язку із закінченням терміну перебування на ньому.
10. Умови, при яких разова перепустка для одноразового відвідування об'єкта охорони дійсна.

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 конкурентноздатності виробленої продукції;
е) збереження та примноження власності;
є) зміцнення інтелектуального потенціалу підприємства;
ж) захист законних прав та інтересів підприємства;
з) усі відповіді правильні;
і) усі відповіді неправильні;
к) не усі відповіді правильні.

Література [26; 31; 33; 35; 41; 45; 48; 55]

Тема10. Технології здійснення працівниками служби безпеки господарюючого суб'єкта діяльності, яка ґрунтується на збиранні детальної інформації про учасників майбутніх ділових переговорів

Питання для самоконтролю

1. Право керівника підприємства, незалежно від форми власності, встановлювати спеціальні правила регулювання допуску до інформації категорії "комерційна таємниця", забезпечуючи тим самим умови для її збереження.
2. Вимоги, які доцільно взяти за основу організації роботи по допуску співробітників підприємства до комерційної таємниці.
3. Загальна характеристика змісту поняття "допуск до комерційної таємниці".
4. Правові навантаження, які несе поняття допуск персоналу до комерційних секретів.
5. Які юридичні зобов'язання виникають в зв'язку з існуючим порядком допуску персоналу підприємства до комерційної таємниці?
6. Які наслідки можуть наступити у випадках, коли співробітник порушує вимоги, пов'язані з зобов'язанням про збереження довіреної йому комерційної таємниці.

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
   є) конкурентну розвідку;
   ж) інформаційно-аналітичну роботу;
   з) експертну перевірку механізму системи забезпечення безпеки підприємства;
   і) усі відповіді правильні;
   к) усі відповіді неправильні;
   л) не усі відповіді правильні.
2. Принципи, з урахуванням яких може бути розроблена програма комплексних заходів забезпечення безпеки організацій та установ:
   а) пріоритет заходів попередження злочинних посягань на захищуваний об'єкт;
   б) законність заходів безпеки, які повинні розроблятися на основі та в межах діючих правових актів;
   в) комплексне застосування сил та засобів для забезпечення безпеки підприємства;
   г) координація дій щодо протидії загрозам безпеки підприємства;
   д) компетентність працівників, які повинні вирішувати питання безпеки, захищуваного об'єкту;
   е) економічна доцільність фінансових витрат щодо захисту безпеки підприємства;
   є) планова основа діяльності по захисту безпеки підприємства на базі програми комплексних заходів забезпечення безпеки цього об'єкта;
   ж) усі відповіді правильні;
   з) усі відповіді неправильні;
   і) не усі відповіді правильні.

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 відвідувача чи ні від КПП і назад уповноважений працівник охоронюваного об'єкта, що його приймає.
3. Визначте особливості допуску у неробочі дні осіб на територію об'єкта охорони.
4. Забороняється чи можна пропустити на територію об'єкта осіб у нетверезому стані, із спиртними напоями, господарюючими сумками, а також транспортні засоби особистого користування.
5. Забороняється чи ні співробітникам об'єктів, охорони і відвідувачам виносити (ввозиті) до нього вибухові речовини, горючі і легкозаймисті рідини та матеріали, зброю, боєприпаси й 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, яким доручено супроводження вантажу на територію об'єкта охорони.
9. Підготуйте реферат за темою: "Планування і здійснення режимних заходів при виконанні всіх видів робіт, де використається закрита інформація".
10. Підготуйте реферат за темою: "Порядок доступу представників сторонніх організацій до документів і відомостей, що містять комерційну таємницю".

Тестові завдання

Зазначте правильну відповідь.

1. КПП (контрольно-пропускний пункт) для транспортних засобів обладнуються:
   а) типовими розсувними чи розстібними воротами з електроприводами та дистанційним керуванням;

б) пристроями для аварійної зупинки і відкриття вручну розсувних чи розстібних воріт;
в) оглядовими майданчиками чи естакадами для огляду автотранспорту;
г) шлагбаумами;
д) вишкою і майданчиком для огляду поїзда, що рухається;
е) запобіжними або фіксаторами для запобігання довільного відкриття воріт;
є) пульт управління воріт, який повинен розташовуватися в приміщенні КПП або на його зовнішній стороні;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
і) не всі відповіді правильні.

2. У приміщенні КПП повинна бути необхідна службова документації:
а) інструкція з пропускного режиму;
б) інструкція з техніки безпеки і надання першої долікарняної 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 пропусків;
є) зразки підписів осіб, яким надано право їх підписувати;
ж) зразки відбитків печаток, пломб, штампів;
з) книги обліку товарно-матеріальних цінностей, що транспортуються та обліку оглядів осіб і правопорушень;
и) списки телефонів усіх чергових служб, керівників об'єктів;
к) усі відповіді правильні;
л) мусі відповіді неправильні;
м) не всі відповіді правильні.

3. Для посилення охорони об'єктів застосовують наступні системи сигналізації охоронного призначення (ССОП):
а) системи охоронної сигналізації (СОС);
б) системи телевідеоконтролю (ТВК);
в) системи телевідеоспостереження (СТВС);
г) системи контролю доступу (СКД);

2. Схарактеризуйте фінансову складову безпеки організацій та установ та зазначте суб'єкти підприємства, що в межах виконання своїх функцій забезпечують фінансову безпеку.
3. Схарактеризуйте інтелектуальну складову економічної безпеки та зазначте суб'єкти підприємства, що в межах свої функцій забезпечують інтелектуальну безпеку й розкрийте зміст їх діяльності в цьому напрямку.
4. Схарактеризуйте кадрову складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах свої функцій забезпечують кадрову безпеку й розкрийте зміст їх діяльності в цьому напрямку.
5. Схарактеризуйте технологічну складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах свої функцій забезпечують технологічну безпеку й розкрийте зміст їх діяльності в цьому напрямку.
6. Схарактеризуйте правову складову безпеки організацій та установ і зазначте суб'єкти підприємства, що забезпечують правову безпеку.
7. Схарактеризуйте інформаційну складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах свої функцій забезпечують інформаційну безпеку й розкрийте зміст їх діяльності в цьому напрямку.
8. Схарактеризуйте силову складову безпеки організацій та установ і зазначте суб'єкти підприємства, що в межах своїх функцій забезпечують силову безпеку й розкрийте зміст їх діяльності в цьому напрямку.
9. Схарактеризуйте позавиробничу (ринкову) складову безпеки, та зазначте суб'єкти підприємства, що забезпечують ринкову безпеку і розкрийте зміст їх діяльності в цьому напрямку (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 і т. ін.).

б) захист державою законних інтересів приватних суб'єктів у відповідних сферах їх діяльності;
в) взаємодія в боротьбі з кримінальним сектором в економічній та фінансових сферах діяльності;
г) повага і дотримання прав і свобод людини і громадянина;
д) законність у використанні науково-технічних засобів;
е) усі відповіді правильні;
є) усі відповіді неправильні;
ж) не всі відповіді правильні.

Література [26; 31; 33; 35; 38; 41; 54; 59]

Тема9. Тактика дій працівників служби безпеки господарюючого суб'єкта при забезпеченні порядку в місцях проведення підприємством представницьких, конфіденційних і масових заходів

Питання для самоконтролю

1. Мета комплексної системи економічної безпеки підприємств.
2. Суть первинних заходів, які забезпечують безпеку підприємства.
3. Зв'язок об'єкта захисту та стабільного стану підприємства з основними характеристиками системи забезпечення економічної безпеки.
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 даного підприємства.
7. Визначення на концептуальному рівні стратегії запобігання та протидії злочинній діяльності криміналітету відносно підприємства.
8. Форми злочинних посягань 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.

д) системи ручної (ножної) тривожної сигналізації (СРТС), що забезпечують можливість термінового виклику наряду охорони;
е) системи пожежної сигналізації (СПС);
є) системи сигналізації комбіновані (ССК), що вміщують вищезгаданії системи в будь-якій комбінації;
ж) усі відповіді правильні;
з) усі відповіді неправильні;
і) не всі відповіді правильні.

Література [15; 16; 36; 38; 41; 44; 52; 54; 69]

Тема8. Тактика дій працівників служби безпеки господарюючого суб'єкта при реалізації заходів для недопущення здійснення протиправних зазіхань проти життя і здоров'я персоналу підприємства

Питання для самоконтролю

1. Ліцензійні умови провадження господарської діяльності з надання послуг, пов'язаних з охороною державної та іншої власності, надання послуг з охорони громадян (затверджені наказом Держкомпідприємництва та Міністерства внутрішніх справ від 14 грудня 2004 року № 145/1501).
2. Охарактеризуйте зміст Положення про підрозділи відомчої воєнізованої охорони Державного комітету зв'язку та інформатизації України від 18.07.2000 року № 103.
3. Об'єкти недержавної охоронної діяльності: фізичні особи та майно громадян і юридичних осіб усіх форм власності.
4. Суб'єкти недержавної охоронної діяльності: фізичні особи — суб'єкти підприємницької діяльності, а також суб'єкти господарювання, засновані на недержавній формі власності, які мають права юридичної особи та на професійній основі виконують заходи охорони і безпеки щодо належного їм майна і майна інших власників і фізичних осіб за цивільно-правовими угодами.
5. Заходи охорони та безпеки, які здійснюються під час перевезення вантажів та проїзду фізичних осіб.
6. Послуги, що надаються при здійсненні охоронної діяльності.
7. Здійснення контролю за охоронною діяльністю у межах своєї компетенції центральними органами виконавчої влади, місцевою державною адміністрацією, органами місцевого самоврядування та органами ліцензування;

8. Безпосередній контроль за охоронною діяльністю, який здійснює Міністерство внутрішніх справ України.
9. Вимоги щодо професійної підготовки суб'єктів охоронної діяльності, які надають охоронні послуги на підставі отриманих ліцензій за укладеними цивільно-правовими угодами.
10. Охарактеризуйте заборони, що висуваються у законопроекті Закону України "Про охоронну діяльність" № 1020 щодо використовування форменого одягу та несертифікованих в установленому порядку спеціально призначених технічних засобів охоронного призначення.

Практичні завдання

1. Чому охоронцю при здійсненні фізичної охорони дуже важливо досконало знати особливості постійних маршрутів руху і відпочинку охоронюваної особи?
2. Стверджується, що у випадках забезпечення фізичної охорони особи, необхідно складати перелік усіх найбільш небезпечних місць з погляду можливого нападу. Обґрунтуйте, що зобов'язаний розробити керівник групи охоронців.
3. Характерні тактичні особливості фізичної охорони особи, коли охоронювана особа керує автомобілем, у якому разом з ним знаходяться охоронці.
4. Характерні особливості фізичної охорони особи, коли охоронювана особа виступає як пасажир, а охоронці розташовуються в салоні поруч з ним.
5. Комбінований, посилений варіант охорони, якому властиве виділення додаткових сил охоронців, розміщених в автомобілі супроводу.
6. Як повинен діяти тілоохоронець відносно охоронюваної особи, що виступає в ролі водія у випадку ускладнення обстановки.
7. Розташування автомобілів при русі, якщо охорона забезпечується з використанням одного автомобіля супроводу;
8. Наведіть вашу думку про те, чому наприкінці руху, машина супроводу з охороною, обігнавши автомобіль охоронюваного з тілоохоронцями, прибуває на місце призначення першою.
9. Бойовий порядок особистої охорони особи після виходу охоронюваного з машини.
10. Особливості дій охоронців перед входом у під'їзд з охоронюваною особою.

Тестові завдання

Зазначте правильну відповідь:

1. Законопроект Закону України "Про охоронну діяльність" № 1020 визначає:
   а) організаційно-правові та економічні засади здійснення охоронної діяльності суб'єктами охоронної діяльності;
   б) перелік безпосередніх суб'єктів охоронної діяльності, зокрема суб'єктів господарювання усіх форм власності;
   в) види діяльності суб'єктів підприємництва у галузі охорони, що здійснюються на підставі ліцензій та у відповідності з ліцензійними умовами;
   г) спеціальний дозвільний порядок охоронної діяльності суб'єктів господарювання і видачі ліцензій на підприємницьку діяльність в галузі охорони;
   д) заходи забезпечення особистої безпеки працівників охорони;
   е) організаційні, правові та технічні умови здійснення охорони майна та забезпечення особистої безпеки фізичних осіб;
   є) охоронна діяльність, як робота особливого змісту з підвищеною небезпекою;
   ж) усі відповіді правильні;
   з) усі відповіді неправильні;
   и) не всі відповіді правильні.
2. Недержавна охоронна діяльність здійснюється у сфері:
   а) охорони майна фізичних і юридичних осіб;
   б) транспортування майна фізичних і юридичних осіб;
   в) забезпечення особистої безпеки фізичних осіб;
   г) проектування, монтажу, ремонту та експлуатаційного обслуговування засобів приватної сигналізації;
   д) ремонту технічних систем гласного аудіоконтролю, відео- та телеспостереження;
   е) усі відповіді правильні;
   є) усі відповіді неправильні;
   ж) не всі відповіді правильні.
3. Основними принципами, якими необхідно керуватися суб'єктам охоронної діяльності повинні стати:
   а) солідарна відповідальність державних і приватних суб'єктів охоронної діяльності перед законом;