

МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ



МАУП

НАВЧАЛЬНА ПРОГРАМА
дисципліни
**“УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ
ОРГАНІЗАЦІЙ ТА УСТАНОВ”**
(для спеціалістів)

МАУП

Київ
ДП «Видавничий дім «Персонал»
2012

ПОЯСНЮВАЛЬНА ЗАПИСКА

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

Затверджено на засіданні кафедри правоохоронної діяльності
(протокол № 8 від 16.03.06)

Схвалено Вченою радою Міжрегіональної Академії управління персоналом

Перезатверджено на засіданні кафедри правоохоронної діяльності
(протокол № 9 від 13.04.09)

Низенко Е. І. Навчальна програма дисципліни “Управління системою безпеки організацій та установ” (для спеціалістів). – К.: ДП «Вид. дім «Персонал», 2012. – 28 с.

Навчальна програма містить пояснювальну записку, тематичний план, зміст дисципліни “Управління системою безпеки організацій та установ”, питання для самоконтролю, вказівки до виконання контрольної роботи, теми контрольних робіт, а також список літератури.

- © Міжрегіональна Академія управління персоналом (МАУП), 2012
- © ДП «Видавничий дім «Персонал», 2012

Навчальна дисципліна “Управління системою безпеки організацій та установ” є спеціальним курсом у системі професійної підготовки фахівців з безпеки підприємництва і в галузі права, які змогли б утворити надійну систему безпеки установ і механізм управління в ній.

Зміст курсу відображає правові, організаційні та тактичні питання професійної діяльності працівників служби безпеки організацій та установ, спрямованої на захист суб'єктів господарювання від зовнішніх і внутрішніх загроз.

Мета вивчення курсу – опанувати існуючі методи захисту промислового шпигунства; здобути знання з комплексного використання типових систем тактичних прийомів у процесі протистояння загрозам; конструювання систем безпеки різних типів, класів і рівнів; перебування в постійному робочому стані служби безпеки установи; вивчити організаційні заходи охорони об'єктів і осіб, принципи управління службою безпеки; кадрову роботу.

Завдання курсу – навчитися виявляти ознаки, які б вказували на зародження та формування небезпеки; діагностувати загрози, прогнозувати їх наслідки; оцінювати ймовірності появи критичної ситуації; аналізувати фактори ризику; виробляти стратегії безпеки підприємства.

Контроль ефективності вивчення курсу передбачає відповіді на питання за темами курсу, тестування.

ТЕМАТИЧНИЙ ПЛАН дисципліни

“УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ ОРГАНІЗАЦІЙ ТА УСТАНОВ”

№ пор.	Назва змістового модуля і теми
1	2
	Змістовий модуль 1. Загальні положення забезпечення безпеки в організаціях та установах
1	Науково-пізнавальні засади вчення про безпеку
2	Правове забезпечення безпеки організацій та установ
3	Управління системою безпеки банку
4	Механізм захисту банківської таємниці

1	2
5	Змістовий модуль 2. Створення системи захисту організацій та установ від зовнішніх та внутрішніх загроз
6	Діагностування загроз безпеки
7	Система охорони організацій та установ
8	Група режиму в забезпеченні безпеки організацій та установ
	Детективна група у формуванні умов, які забезпечують стабільний розвиток та функціонування об'єкта, і захист від внутрішніх та зовнішніх загроз
9	Змістовий модуль 3. Тактика попереджувальної діяльності служби безпеки суб'єктів господарювання щодо загроз цілісності та функціональності організацій та установ
10	Тактика дій служби безпеки організацій та установ у нестабільних умовах внутрішнього та зовнішнього середовища
11	Тактичні особливості розвідувальної служби безпеки організацій та установ
12	Економічний шпіонаж як сфера таємної діяльності конкурентів і протидія йому
13	Характеристика зовнішнього середовища розвідувальної діяльності підприємства
14	Програма комплексних заходів забезпечення безпеки організацій та установ
15	Організаційні засади діяльності суб'єкта господарювання зі збереження комерційної таємниці
	Комерційна таємниця як об'єкт правової охорони
16	Змістовий модуль 4. Економічна безпека організацій та установ і її співвідношення з економічною безпекою держави
17	Концепція про місце і роль недержавних організацій та установ у системі захисту економічної безпеки України
18	Тенденції формування та реалізації державної політики в галузі безпеки організацій та установ приватної форми власності
19	Послуги суб'єктів недержавної системи безпеки із захисту і просування інтересів окремих громадян, організацій та установ
20	Канали витoku інформації з обмеженим доступом з організацій та установ
21	Напрями конструювання систем безпеки різних типів і рівнів
22	Економічна безпека в умовах конкурентної боротьби
	Конфлікт інтересів між власником інформації з обмеженим доступом і державними органами, організаціями, яким вона може бути передана

1	2
23	Змістовий модуль 5. Забезпечення безпеки у сфері комп'ютерних технологій
24	Особливості злочинної діяльності у сфері використання комп'ютерних технологій
	Приховування правопорушником передання розвіданої інформації, що опрацьовується в комп'ютерній мережі
Разом годин: 81	

ЗМІСТ *дисципліни*

“УПРАВЛІННЯ СИСТЕМОЮ БЕЗПЕКИ ОРГАНІЗАЦІЙ ТА УСТАНОВ”

Змістовий модуль 1. Загальні положення забезпечення безпеки в організаціях та установах

Тема 1. Науково-пізнавальні засади вчення про безпеку

Основні положення теорії виникнення, обмеження, усунення небезпек і загроз, що впливають на вироблення підходів до співвідношення державної і недержавної систем безпеки. Групування небезпек і загроз за кваліфікуючими ознаками.

Закономірності управління самоорганізаційною системою безпеки організацій та установ.

Пріоритети в застосуванні заходів, які повинні вживати підрозділи служби безпеки організацій та установ для виконання покладених на них завдань.

Загальне завдання курсу “Управління системою безпеки організацій та установ”.

Література [1; 7; 12; 14; 17; 48]

Тема 2. Правове забезпечення безпеки організацій та установ

Нормативно-правові засади формування і функціонування системи забезпечення безпеки організацій та установ у сфері підприємницької діяльності. Зasadничі положення окремих норм права, що вказують на принципову допустимість здійснення суб'єктами недержавної системи безпеки заходів з надання послуг з охорони колективної, приватної власності та громадян.

Концепція (основи державної політики) національної безпеки, схвалена Верховною Радою України 16 січня 1997 р.

Погляди на забезпечення в Україні безпеки особи, суспільства у важливих сферах життєдіяльності.

Шляхи формування законодавства про недержавне забезпечення безпеки особи та підприємницької діяльності в Україні.

Література [12; 14; 17; 18; 21–23; 48; 53–54]

Тема 3. Управління системою безпеки банку

Основні напрями діяльності служби безпеки комерційного банку, що впливають з концепції безпеки цього підприємства. Оцінювання попереднього вивчення стану безпеки банку.

Загальна характеристика інформаційно-аналітичних досліджень щодо природи і технології криміногенних процесів, їх зв'язків із технологіями конкретних банківських та інших фінансово-господарських операцій.

Взаємозв'язок економічної та режимно-охоронної груп ризиків потенційних загроз з розробкою притаманних їм методів своєчасного виявлення, попередження та усунення можливої негативної діяльності на шкоду безпеці банку.

Основні функції управління підрозділами служби безпеки банку. Співвідношення інфраструктури економічної безпеки у сфері банківської діяльності із системою і засобами управління кредитними, страховими та іншими пов'язаними з ними ризиками.

Література [48; 52–54; 56; 62; 66; 73]

Тема 4. Механізм захисту банківської таємниці

Поняття безпеки комерційного банку. Співвідношення відмінних понять категорій “безпека”, “система забезпечення безпеки”, “небезпека”, “загроза”, їх аутентифікація.

Об'єкти системи безпеки комерційного банку.

Суб'єкти правовідносин при вирішенні проблеми безпеки.

Концепція безпеки комерційного банку. Види загроз безпеки банку і ресурси, що підлягають захисту.

Цілі та завдання системи безпеки комерційного банку. Принципи організації функціонування системи безпеки банку.

Форми забезпечення економічної безпеки банку.

Література [14; 27; 44; 47; 53; 66; 71]

Змістовий модуль 2. Створення системи захисту організацій та установ від зовнішніх та внутрішніх загроз

Тема 5. Діагностування загроз безпеки

Поняття критеріїв і показників безпеки. Критеріальне оцінювання системи безпеки, його зміст. Індикатори дослідження безпеки підприємства, що характеризують еволюцію розвитку об'єкта господарювання і загроз, рівень їх кількісних та якісних параметрів.

Порогові значення показників безпеки, їх структура, недотримання значень зумовлює формування руйнівних тенденцій у безпеці. Складові концепції ризику у стратегії безпеки.

Імовірнісний, експертний характер оцінювання ризику. Основні методи управління ризиком.

Порядок визначення “діагнозу” стану безпеки. Виявлення і усунення небезпечних тенденцій на основі моніторингу загроз безпеці та прогнозування їх наслідків. Зміст завдань діагностики небезпек.

Література [43; 44; 47; 48; 53; 71]

Тема 6. Система охорони організацій та установ

Мета охорони організацій та установ. Організація системи охорони установ. Основні причини зловмисних порушень охорони установ і організацій. Класифікація засобів і методів охорони організацій та установ.

Комплекс організаційних завдань з фізичної охорони особи в різних умовах. Виявлення порушників або ознак порушення зон заборони.

Системи автономної охорони. Застосування інженерно-технічних засобів охорони. Загальні принципи побудови системи охорони об'єкта.

Види охорони і сигналізації. Обов'язки охоронця на посту. Системи відеоспостереження і контролю.

Література [11; 21; 42; 53; 62; 66]

Тема 7. Група режиму в забезпеченні безпеки організацій та установ

Основні функції групи режиму. Механізм закритого діловодства. Положення і правила забезпечення роботи виконавцями закритих робіт.

Завдання, які вирішуються у процесі організації і ведення закритого діловодства, для забезпечення збереження секретної документарної інформації. Принципи, покладені в основу організації і ведення закритого діловодства.

Вимоги до приміщень, в яких виконуються роботи з документами — носіями відомостей про комерційну таємницю.

Планування і здійснення режимних заходів при виконанні всіх видів робіт, де використовується закрита інформація.

Службове розслідування фактів розголошення закритої інформації, втрата документів і виробів, що містять комерційну таємницю.

Встановлення на підприємстві загальної системи користування документами обмеженого допуску. Облік і зберігання конфіденційних документів. Знищення конфіденційних документів.

Правила внутрішнього трудового розпорядку. Робота співробітників групи режиму з персоналом підприємства з питань забезпечення збереження об'єктів захисту.

Література [27; 43; 44; 47; 53; 62; 71]

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

Поняття та зміст приватної детективної діяльності.

Завдання діяльності детективної групи. Питання законодавчого регулювання діяльності детективної групи. Поняття та зміст приватної детективної діяльності.

Суб'єкти, які здійснюють приватну детективну діяльність. Основні види професійних послуг, які суб'єкти приватної детективної діяльності матимуть право надавати замовникам з метою забезпечення захисту їх прав та інтересів.

Ліцензування приватної детективної діяльності. Вимоги до осіб, які можуть бути приватними детективами, помічниками детектива.

Право приватного детектива застосовувати при виконанні професійних обов'язків заходи фізичного впливу, а також використовувати спеціальні засоби активної оборони та примусу.

Складання карти ризиків з переліченням усіх можливих каналів витоку важливої інформації, що зберігається на підприємстві. Розробка запобіжних заходів витоку інформації.

Моделі порушення безпеки підприємства та можливості детективів щодо їх розпізнання.

Література [29; 43; 44; 50; 51; 53; 62; 69]

Змістовий модуль 3. Тактика попереджувальної діяльності служби безпеки суб'єктів господарювання щодо загроз цілісності та функціональності організацій та установ

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

Сучасні методології і методики управління забезпеченням безпеки організацій та установ у нестабільних умовах функціонування. Актуалізація загроз внутрішнього характеру. Виживання підприємства в умовах постійної конкуренції.

Характеристика факторів, які заважають нормальній діяльності підприємства та загрожують його безпеці. Мета забезпечення безпеки підприємства в нестабільних умовах функціонування.

Поняття сутності кількісного вимірювання загроз безпеці підприємства; завдання, реалізація яких необхідна для досягнення мети забезпечення безпеки. Менеджмент кризових ситуацій.

Компоненти готовності до подолання кризових ситуацій. Роль власної служби безпеки підприємства у збиранні інформації з питань, що становлять інтерес для представників адміністрації.

Література [27; 45; 47; 49; 53; 54]

Тема 10. Тактичні особливості розвідувальної служби безпеки організацій та установ

Особливості роботи інформаційних підрозділів розвідки служби безпеки підприємства у процесі опрацювання сирих фактів об'єктивної дійсності та перетворення їх на кінцеву продукцію розвідувальної діяльності.

Класифікація розвідувальної інформації за категоріями на основі напрямів її кінцевого використання. Форми подання керівництву підприємства зібраної та опрацьованої розвідувальної інформації. Зміст інформації цих документів.

Критерії, з урахуванням яких керівники підприємства оцінюють результати діяльності розвідувального підрозділу служби безпеки підприємства. Показники, що розкривають ці критерії.

Порядок складання документограми, що допомагає виявити слабкі місця в системі захисту комерційних секретів. Взаємозв'язок методів і джерел розвідувальної інформації.

Література [33–35; 37; 53; 55; 67; 72; 73]

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

Суб'єкти кримінологічних загроз безпеки об'єктів економіки. Зрошення економічної злочинності із загальнокримінальною.

Уявлення про економічну безпеку та її основне завдання. Роль комерційних і промислових секретів в умовах економічного суперництва підприємств. Характерні дестабілізаційні методи економічного протистояння підприємств усіх видів та розмірів. Пріоритетні напрями діяльності приватних служб безпеки та їх спецпідрозділів економічної розвідки.

Економічна розвідка і стратегія підприємств в умовах конфронтації в економічній сфері. Умовний поділ конфронтації за так званою сіткою Бернара Наумка.

З'ясування за допомогою розвідки намірів конкурентів у сфері ринкової економіки. Тактичні та стратегічні плани економічної розвідки. Механізм економічної розвідки, зорієнтованої на світовий ринок.

Література [24; 28; 30; 60; 73]

Тема 12. Характеристика зовнішнього середовища розвідувальної діяльності підприємства

Роль і значення розвідки безпеки підприємства. Потреби вітчизняних підприємців в одержанні інформації випереджаючого характеру про тенденції, факти, явища, які існують поза підприємством. Мета розвідки.

Зовнішнє середовище — об'єкт розвідувальної діяльності, його характеристика. Завдання, реалізація яких сприяє досягненню мети розвідки служби безпеки підприємства. Склад інформаційних підрозділів розвідки.

Засоби розвідувальної діяльності. Умови застосування технічних засобів розвідувальної діяльності. Інформаційні системи, покликани допомагати детективам у збиранні, опрацюванні та аналізі розвідувальної інформації.

Стандартні вимоги, які повинні задовольняти службові приміщення розвідувальних підрозділів.

Література [48; 53; 60; 63; 69; 71]

Тема 13. Програма комплексних заходів забезпечення безпеки організацій та установ

Пріоритетні напрями програми комплексних заходів забезпечення безпеки організацій та установ. Принципи співробітництва різних систем безпеки організацій та установ з правоохоронними органами.

Основні функції системи безпеки. Система заходів захисту організацій та установ.

Основні розділи і положення програми комплексних заходів забезпечення безпеки організацій та установ.

Організація адміністрацією установи нагляду за реалізацією на основі програми комплексних заходів протидії посяганням на безпеку установ і підприємств.

Література [27; 29; 31; 36; 42; 48–50; 57; 61]

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

Прийняття керівником підприємства рішення про необхідність захисту комерційної таємниці та створення системи інформаційної безпеки установи.

Закріплення в установчих документах права на використання комерційної таємниці.

Визначення складу та обсягу комерційної таємниці. Складання переліку відомостей, що становлять комерційну таємницю підприємства.

Закріплення прав і обов'язків працівників підприємства щодо порядку захисту комерційної таємниці в колективному договорі, правилах внутрішнього трудового розпорядку, контрактах, попередженнях — зобов'язаннях про збереження комерційної таємниці при прийнятті на роботу і звільненні.

Управління організацією захисту комерційної таємниці в умовах її обороту у виробничих інтересах підприємства та при передаванні іншим установам тощо.

Література [37; 60; 61; 66; 68]

Тема 15. Комерційна таємниця як об'єкт правової охорони

Потреба в нормативному закріпленні комерційної таємниці. Форми правової охорони та правового захисту комерційної таємниці. Законодавчі гарантії забезпечення права на інформацію.

Поняття та ознаки комерційної таємниці. Вартість інформації, що становить комерційну таємницю.

Об'єкти і суб'єкти права власності на інформацію, яка становить комерційну таємницю. Система правового захисту комерційної таємниці підприємства, її складові.

Поняття про режим доступу до інформації ділового, професійного, виробничого, банківського та іншого характеру.

Література [10; 47; 52; 53; 56; 60; 61; 66–68; 71]

Змістовий модуль 4. Економічна безпека організацій та установ і її співвідношення з економічною безпекою держави

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

Розуміння про концепцію, яка становить собою найвищий щабель системи документів щодо окремих сфер життєдіяльності.

Доцільність окреслення власного бачення змісту концепції про місце і роль недержавних організацій та установ у системі захисту економічної безпеки України.

Методологія побудови концепції про місце і роль недержавних організацій та установ у системі захисту економічної безпеки України.

Потреба адекватного відображення у змісті концепції питань про правову базу діяльності недержавних підприємств безпеки в системі економічної безпеки України. Можливості взаємодії цих структур з державними органами. Напрями діяльності суб'єктів недержавної системи безпеки.

Література [16; 24; 28; 34; 48; 56; 62]

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

Основна мета державної політики в галузі безпеки організацій та установ приватної форми власності. Парадигма безпеки з позиції

державницьких реалій на сучасному історичному етапі, концепцій, стратегій, доктрин та програм.

Співвідношення державної і недержавної підсистем безпеки відповідно до рівня потреби інтересів у безпеці, який нині існує в різних сферах життєдіяльності.

Комплекс правових, організаційно-управлінських, соціально-психологічних державних заходів утворення середовища функціонування системи безпеки заради управління загрозами та небезпеками в соціальних відносинах.

Література [17; 24; 48; 52–54]

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

Компетенція суб'єктів недержавної системи безпеки і правоохоронних органів щодо розслідування правопорушень. Послуги суб'єктів недержавної системи безпеки, що надаються згідно з чинним законодавством України окремим громадянам, організаціям і установам.

Умови, за яких може здійснюватися відповідна діяльність суб'єктів недержавної підсистеми безпеки у формі взаємодопомоги правоохоронним органам. Збирання відомостей у кримінальній справі, порушеній у зв'язку зі злочинним посяганням проти персоналу підприємства або власності засновника. Збирання відомостей у цивільних справах на договірній основі з учасниками процесу.

Зміст письмового повідомлення суб'єкта недержавної безпеки у правоохоронний орган про дані з виявленого злочину проти підприємства, не очікуючи порушення кримінальної справи. Пошук втраченого майна підприємства.

Документування фактів неправомірного використання товарних (фірмових) знаків підприємства. Виявлення ненадійних майбутніх ділових партнерів.

Охорона майна підприємства. Захист життя і здоров'я персоналу підприємства від протиправних зазіхань.

Забезпечення порядку в місцях здійснення підприємством представницьких, конфіденційних і масових заходів.

Література [28; 29; 31; 36; 47; 49; 52; 59; 65]

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

Класифікація методів збирання інформації залежно від вирішуваних завдань розвідки. Зasadничі положення загальних, особливих та приватних методів економічної розвідки на рівні підприємства. Джерела інформації про конкурентів.

Застосування найефективніших методів збирання, відбору і передавання інформації користувачу-конкуренту. Методи проникнення на охоронюваний об'єкт.

Придбання на підприємстві конкурента джерела постановлення конфіденційної інформації, яке таємно передає за винагороду комерційні секрети.

Таємне дослідження окремих екземплярів продукції конкурентів у лабораторії “вивсекції” для виявлення їх технологічних параметрів. Виток інформації в каналах зв'язку.

Перехоплення інформації з комп'ютерних систем без дозволу компетентних органів за допомогою технічних засобів, за рахунок випромінювань центрального процесора, дисплея, комунікаційних каналів, принтера.

Електромагнітне перехоплення через зовнішні комунікаційні канали комп'ютерної системи або шляхом підімкнення до ліній периферійних пристроїв. Добір пароля для доступу до чужого комп'ютера із застосуванням спеціально розроблених програм.

Література [30; 31; 55; 59–61; 63; 71]

Тема 20. Напрями конструювання систем безпеки різних типів і рівнів

Характеристика інтенсивного та екстенсивного видів розвитку систем безпеки організацій та установ. Самоорганізаційні засади систем безпеки об'єкта змішаного типу розвитку.

Формування адекватної загрозам і небезпекам системи внутрішньої безпеки організацій та установ.

Аналіз сучасного стану напрямів діяльності самоорганізаційних систем у сфері надання послуг з безпеки фірмам-клієнтам.

Рівні, типи, моделі в загальному контексті теорії самоорганізації, положення якої необхідно враховувати при побудові систем безпеки.

Література [44; 47–49; 53; 59; 60; 62; 66; 68]

Тема 21. Економічна безпека в умовах конкурентної боротьби

Конкурентне середовище і економічна безпека. Економічне суперництво.

Недобросовісна конкуренція, її зміст. Основні напрями конкурентної боротьби підприємств у галузі економіки і технології.

Захист службою безпеки господарюючого суб'єкта життєздатності підприємства від ворожих дій конкурентів і негативного впливу дестабілізуючих соціально-економічних факторів.

Фактори, на які слід зважати при вирішуванні питання про вибір службою безпеки організації, установи стратегії і тактики запобігання правопорушень в умовах ринкової економіки.

Література [26; 27; 33; 43; 47; 53; 54; 56; 60; 64; 71]

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

Суперечності в нормах Закону України “Про банки і банківську діяльність” щодо правового регулювання режиму використання організаціями банківської таємниці та конфіденційної інформації. Розбіжності у правових актах, що регулюють надання відомостей кредитними, митними та іншими установами контролюючим органам, які становлять конфіденційну інформацію та комерційну таємницю.

Підстави, які породжують зазначені права витребування контролюючими органами закритої інформації з обмеженим доступом у суб'єктів підприємницької діяльності.

Нормативне регулювання інформаційних відносин банків з органами служби безпеки України прокуратури і судами. Створення єдиного банку даних про імідж, платоспроможність і надійність суб'єктів підприємницької діяльності.

Література [1; 3; 5; 7; 14; 53; 61]

Змістовий модуль 5. Забезпечення безпеки у сфері комп'ютерних технологій

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

Класифікація способів скоєння злочинів залежно від об'єкта злочину з використанням інформаційних технологій. Кібер-тероризм.

Проникнення до баз даних через мережу Інтернет з метою змінення інформації. Електронний “злам” захисту через комп’ютерну мережу.

Знищення за допомогою комп’ютерних вірусів інформаційних інфраструктур.

Незаконний доступ до комп’ютерних систем у фінансово-кредитних організаціях за допомогою хакерів. Шахрайство з пластиковими картками, пов’язане з використанням фантомної картки. Фізичні поля, завдяки яким може бути здійснено несанкціонований доступ до систем зв’язку.

Класифікація електромагнітних передавачів інформації (за діапазоном випромінювання, середовищем поширення, за способом утворення). Особливості поширення звукових хвиль залежно від середовища. Поняття про структурний звук.

Перехоплення комп’ютерної інформації при її передаванні телекомунікаційними каналами і комп’ютерними мережами. Об’єкти безсереднього підслуховування.

Вистежування і перехоплення зловмисника в каналі зв’язку; контролювання дій порушника.

Література [25; 26; 31; 60; 63; 64; 69]

Тема 24. Приховування правопорушником передання розвіданої інформації, що опрацьовується в комп’ютерній мережі

Поняття про методи приховування інформації — криптографії і стегографії. Зміст понять “стегосистема”, “контейнер”, “приховуване (вбудоване) повідомлення”, “стегоключ”. Формула загального процесу стегографії.

Основні вимоги, яких необхідно дотримуватися для того, щоб сформований таємний канал передавання інформації не викликав підозри. Поняття “файл-контейнер” і “файл-повідомлення”.

Комп’ютерні стегоситеми, застосовувані зловмисниками. Уявлення про те, як встановити в комп’ютерну систему “програму-закладку”. Механізм маскуванню процесу встановлення програми-закладки в комп’ютер.

SOFT TEMPESS — технології таємного передавання даних керованим каналом паразитних електромагнітних випромінювань і наводок. Передавання розвіданої інформації через випромінювання монітора.

Література [25; 30; 34; 55; 73]

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Характеристика законодавства у сфері забезпечення безпеки організацій та установ.
2. Поняття і зміст навчального курсу “Управління системою безпеки організацій та установ”.
3. Показники суспільних загроз.
4. Складові проблеми збереження безпеки.
5. Організаційні принципи захисту організацій та установ від зовнішніх та внутрішніх загроз.
6. Межі правового простору для превентивних засобів, які здійснюються детективною групою.
7. Державна політика в галузі безпеки підприємницької діяльності.
8. Структура комплексної безпеки організацій, установ.
9. Функції служби безпеки організацій та установ.
10. Принцип стратегії попередження, властивої структурам економічної розвідки, в умовах тактичної ситуації “один проти всіх”.
11. Спеціалізація підрозділів служби безпеки організацій та установ за напрямками комплексного забезпечення захисту суб’єкта господарювання від зовнішніх та внутрішніх загроз.
12. Програмно-цільове планування діяльності із забезпечення безпеки підприємства.
13. Взаємодія і координація зусиль зацікавлених підрозділів підприємства, пов’язаних із забезпеченням безпеки господарюючого суб’єкта.
14. Здійснення заходів безпеки в поєднанні з необхідною конспірацією.
15. Створення шляхом діяльності служби безпеки організацій, установ нормативних, організаційних і матеріальних гарантій для персоналу господарюючого суб’єкта.
16. Інформаційно-аналітичні дослідження відомостей про конкурентів і зовнішнє середовище.
17. Джерела інформації про конкурента для визначення політики економічного розвитку організації, установи.
18. Реалізація цілей контррозвідки в роботі аналітико-інформаційного підрозділу служби безпеки.
19. Аналітична робота детективної групи служби безпеки з профілактики шахрайства, здійснювана співробітниками підприємства.
20. Поняття захисту інформації з обмеженим доступом від технічної розвідки.

21. Права Департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України з контролю за дотриманням суб'єктами підприємництва ліцензійних умов здійснення діяльності з технічного захисту інформації.
22. Запобігання загрозам несанкціонованого доступу до інформації в електронно-обчислювальних машинах.
23. Поняття спеціального захисту інформації в каналах зв'язку.
24. Поняття криптографічного захисту інформації.
25. Організація службою охорони служби безпеки пропускнуго та внутрішньооб'єктного режимів на підприємствах.
26. Поняття пропускнуго та внутрішньооб'єктного режимів.
27. Режимні вимоги при роботі з інформацією, яка містить державну чи комерційну таємницю.
28. Основні категорії об'єктів, що охороняються.
29. Класифікація методів і засобів охорони.
30. Інженерно-технічні засоби охорони.
31. Захист від тероризму.
32. Охоронні системи приватного підприємства.
33. Взаємодія приватної охорони підприємства з органами внутрішніх справ.
34. Документування порушень у сфері контрольно-пропускнуго режиму.
35. Забезпечення безпеки людей при пожежі.
36. Забезпечення охоронно-пожежної спеціалізації організацій та установ.
37. Особливості стеження з автомобіля.
38. Контрзаходи щодо стеження (таємного спостереження) на вулиці.
39. Стеження на вулиці.
40. Вимоги до розміщення.
41. Відрив від переслідувачів, які ведуть спостереження.
42. Основні завдання детективної групи у процесі службового розслідування.
43. Принципи економічної розвідки.
44. Несанкціоноване отримання і використання інформації, яка містить комерційну таємницю.

45. Методика роботи з відомостями про конкурентів і ділових партнерів, зосередженими в інформаційно-довідкових картотеках служби безпеки організації, установи.
46. Умови забезпечення конкурентних переваг.
47. Системи економічної розвідки.
48. Структурні підрозділи у внутрішніх організаціях системи забезпечення безпеки організацій та установ.
49. Юридична природа охоронних підприємств, детективних агентств, служб безпеки підприємств різних форм власності.
50. Основні функції підрозділу з фізичної охорони осіб і транспортних засобів.
51. Функції управління в системі забезпечення безпеки організацій та установ.
52. Тактичні особливості забезпечення охорони особи в умовах руху автотранспортом.
53. Організація дій групи охорони, що перебуває в автомобілі супроводу, при короткочасній зупинці автомобіля з охоронюваною особою.
54. Порядок дій водія при виявленні у процесі огляду автомобіля ознак його мінування.
55. Організаційно-технологічні засоби забезпечення безпеки особи в місцях скупчення громадян під час пішої прогулянки.
56. Технологія несанкціонованого прослуховування чужих розмов.
57. Організація та здійснення заходів щодо знаходження підслуховуючих пристроїв.
58. Ознаки прослуховування кімнати із застосуванням "жучка" з кодовим увімкненням.
59. Методи і технічні засоби захисту інформації.
60. Методика використання зовнішньоспостережуваних фізіологічних, поведінкових ознак міміки, жестів зі справжнім станом співбесідника в запобіганні загроз від фізичних осіб.
61. Організація діловодства та контролю за секретними документами організацій та установ.
62. Економічна оцінка наслідків втрати комерційної таємниці установи, підприємства.
63. Специфіка дій з контролю за використанням фотокопіювальної апаратури.

64. Поняття про комплекс заходів, що закріплюють права підприємства, організації, установи на комерційну таємницю.
65. Джерела витоку інформації з підприємства.
66. Поняття “система забезпечення безпеки”, “загроза”, “управління системою безпеки”.
67. Поняття про концепцію безпеки установи, підприємства.
68. Правовий статус служби безпеки організації, установи.
69. Забезпечення порядку в місцях проведення установою представницьких конфіденційних і масових заходів.
70. Класифікація загроз за ознакою природи їх виникнення.
71. Мета забезпечення безпеки підприємства.
72. Принципи, на яких будується система безпеки організацій та установ.
73. Підсистеми, які містить система безпеки установи, підприємства.
74. Політика і стратегія безпеки організації, установи.
75. Суб’єкти безпеки підприємства, організації, установи.
76. Засоби забезпечення безпеки організацій, установ.
77. Зміст загрози і безпеки.
78. Основні види послуг із забезпечення безпеки, які суб’єкти приватної діяльності матимуть право надавати замовникам.
79. Побудова карти ризиків витоку інформації.
80. Правила, які слід виконувати, щоб запобігти витоку інформації.
81. Причини розголошення комерційних секретів працівниками підприємств.
82. Основні напрями забезпечення безпеки підприємницької діяльності.
83. Поняття інформаційної безпеки та її мета.
84. Класифікація методів збирання інформації в економічній розвідці.
85. Система інформаційної безпеки організації, установи.
86. Завдання та організація інформаційної безпеки підприємства, установи.
87. Завдання та основні напрями діяльності Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.
88. Засоби і методи захисту інформації та інформаційних систем.
89. Технічний та криптографічний захист інформації з обмеженим доступом.
90. Способи неправомірного доступу до комп’ютерної інформації.

ВКАЗІВКИ ДО ВИКОНАННЯ КОНТРОЛЬНОЇ РОБОТИ

Згідно з навчальним планом дисципліни “Управління системою безпеки організацій та установ” студенти виконують контрольну роботу.

Мета виконання контрольної роботи — поглибити і закріпити здобуті теоретичні знання, вивчити вітчизняний і зарубіжний передовий досвід діяльності підрозділів служби безпеки суб’єктів підприємницької діяльності.

Перед тим як виконувати контрольну роботу, необхідно вивчити відповідні першоджерела зі списку літератури.

Контрольна робота повинна містити план. У вступі розкривають роль і значення вибраної теми. Основна частина повинна складатися з двох-трьох питань вибраної теми. Окремою частиною роботи повинні бути висновки, де слід викласти і обґрунтувати пропозиції та рекомендації щодо вдосконалення чинного законодавства або теоретичних положень за темою контрольної роботи і список використаної літератури.

Наприкінці виконання роботи слід належно оформити титульну сторінку, підписати роботу і у встановленні терміни подати її на перевірку.

Варіант теми контрольної роботи студенти вибирають за останньою цифрою номера своєї залікової книжки; якщо остання цифра “5”, то студент виконує варіант на вибір відповідно 5, 15, чи 25.

За консультацією зі складних питань контрольної роботи студенти можуть звернутися до викладачів кафедри з правоохоронної діяльності.

ТЕМИ КОНТРОЛЬНИХ РОБІТ

1. Правове забезпечення безпеки організацій та установ.
2. Науково-пізнавальні засади вчення про безпеку.
3. Природа загроз функціонуванню системи безпеки та розвитку організацій та установ.
4. Діагностування загроз безпеки об’єкта-системи.
5. Концептуальні засади управління рівнем безпеки організації, установи.
6. Системи безпеки організацій та установ.
7. Канали витоку інформації з підприємства.

8. Захист конфіденційної інформації від витоку за межі організації.
9. Роль детективної групи в забезпеченні безпеки підприємства.
10. Методи і технологія діяльності служби безпеки організацій та установ з фізичної охорони осіб.
11. Захист служби безпеки установи об'єктів інформації, інформаційних систем від технічних розвідок та інших засобів таємного отримання конфіденційної інформації.
12. Програма комплексного захисту безпеки підприємства.
13. Створення системи безпеки на підприємстві.
14. Характеристика засобів, методів збирання і вивчення інформації, яку добувають у процесі економічного шпіонажу.
15. Захист інформації за допомогою криптографії.
16. Правове регулювання відносин у сфері захисту комерційної таємниці.
17. Комерційний шпіонаж.
18. Управління системою попередження посягань на економічну безпеку господарюючого суб'єкта.
19. Організаційно-правове забезпечення, формування та реалізація державної політики у сфері безпеки підприємництва.
20. Економічна безпека банку.
21. Суб'єкти, що мають право ознайомлюватися з банківською документацією.
22. Комерційна таємниця за міжнародними договорами.
23. Технічні засоби в забезпеченні безпеки організацій та установ.
24. Економічна безпека підприємств України.
25. Захист інформації в контексті боротьби з "комп'ютерною" злочинністю.
26. Інформація як об'єкт інтелектуальної власності, що потребує охорони.
27. Попередження захоплення заручників як одне з основних завдань служби безпеки комерційного підприємства.
28. Правове регулювання порядку розробки, виготовлення, реалізації та застосування спеціальних технічних засобів негласного отримання інформації, що містить комерційну таємницю.
29. Синергетична парадигма безпекознавства.
30. Системи безпеки в конфліктогенному середовищі.

СПИСОК ЛІТЕРАТУРИ

Основна

1. Конституція України. — К., 2001.
2. Кримінальний кодекс України. — К., 2001.
3. Цивільний кодекс Української РСР // Кодекси України. — 1998. — Кн. 2.
4. Закон України "Про захист інформації в автоматизованих системах".
5. Кодекс України про адміністративні правопорушення // Кодекси України. — 1998. — Кн. 1.
6. Закон України "Про пожежну безпеку".
7. Закон України "Про захист економічної конкуренції".
8. Закон України "Про телекомунікації".
9. Закон України "Про рекламу".
10. Постанова Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці" від 9 серпня 1993 р. № 611 // З. П. — 1993. — № 12. — Ст. 269.
11. Закон України "Про ліцензування певних видів господарської діяльності".
12. Закон України "Про господарські товариства".
13. Закон України "Про власність".
14. Закон України "Про банки і банківську діяльність".
15. Закон України "Про Службу безпеки України".
16. Закон України "Про оперативно-розшукову діяльність".
17. Постанова Верховної Ради України "Про концепцію (основи державної політики) національної безпеки України" // Голос України. — 1997. — 4 лют.
18. Положення про порядок ліцензування підприємницької діяльності: Затв. постановою Кабінету Міністрів України від 3 липня 1998 р. № 1020 // Офіц. вісн. України. — 1998. — № 27. — Ст. 1004.
19. 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.

20. *Положення* про Державний комітет України з питань регуляторної політики та підприємництва: Затв. Указом Президента України від 25 травня 2000 р. № 721/2000.
21. *Інструкція* “О порядке выдачи субъектам предпринимательской деятельности лицензий на предоставление услуг по охране коллективной и частной собственности, а также охраны граждан, монтажа, ремонта и профилактического обслуживания средств охранной сигнализации”: Утвержд. приказом МВД от 28 февраля 1994 г. № 112.
22. *Інструкція* “Об условиях и правилах сопровождения предпринимательской деятельности (лицензионные условия), связанной с разработкой, изготовлением и реализацией специальных технических средств негласного получения информации с каналов связи, иных средств негласного получения информации и контроле за их соблюдением”: Утвержд. приказом Лицензионной палаты Украины и Службы безопасности Украины от 07.04.99 № 30/76, зарегистрирована в Министерстве юстиции Украины 30.04.99 № 275/3568, разработана в соответствии с законами Украины “О предпринимательстве”, “Об оперативно-розыскной деятельности”, “О государственной тайне”, Постановлением Верховного Совета Украины от 17 июня 1992 г. № 2471-ХІІ “О праве собственности на отдельные виды имущества”, Положением о порядке лицензирования предпринимательской деятельности, утвержденным приказом Государственного комитета Украины по вопросам государственных секретов от 31.07.95 № 47, зарегистрированным в Министерстве юстиции Украины 03.08.95 № 278/814.
23. *Приказ* Лицензионной палаты Украины, Департамента специальных телекоммуникационных систем и защиты информации СБ Украины от 13 октября 1998 г. № 92/80 “Об утверждении инструкции об условиях и правилах проведения предпринимательской деятельности (лицензионные условия), связанной с разработкой, изготовлением, ввозом, вывозом, реализацией и использованием средств технической защиты информации, а также оказания услуг по технической защите информации и контроля за их соблюдением”: Зарег. в Министерстве юстиции Украины 23 октября 1998 г. № 682/3122.
24. *Постанова* Верховной Рады Украины “Про Державну програму боротьби зі злочинністю” від 25 червня 1993 р. № 3225-ХІІ // ВВР України. — 1993.
25. *Шпионские* штучки и устройства для защиты объектов и информации: Справоч. пособие / В. И. Андрианов и др. — СПб.: Лань, 1996.
26. *Батурин Ю., Хозишский М.* Компьютерная преступность и компьютерная безопасность. — М.: Юрид. лит., 1991.
27. *Безопасность* бизнеса: Справоч. пособие / Под ред. Ю. И. Когута. — К., 1993.
28. *Боттом Н., Галатти Р.* Экономическая разведка и контрразведка: Практ. пособие: Пер. с англ. — Новосибирск, 1994.
29. *Бэскид Э.* Энциклопедия личной безопасности. — М.: Аквариум, 1994.
30. *Вартенесян В. А.* Радиоэлектронная разведка. — М.: Воениздат, 1991.
31. *Ведев Д. Л.* Защита данных в компьютерных сетях // Открытые системы. — 1995. — № 3.
32. *Выживание* в экстремальных условиях. — М.: Рус. раритет, 1993.
33. *Гасанов Р. М.* Шпионаж и бизнес. — М.: Междунар. отношения, 1993.
34. *Гасанов Р. М.* Промышленный шпионаж на службе монополий. — М.: Междунар. отношения, 1996.
35. *Голубев В. О.* Інформаційна безпека: проблеми боротьби з кіберзлочинами: Моногр. — Запоріжжя, 2003.
36. *Группа* личной охраны: Метод. разработка. — М.: Арсин ЛТД, 1996.
37. *Дориченко С. А., Яценко В. В.* 25 этюдов о шифрах. — М.: Текст, 1994.
38. *Зелинский А. Ф.* Криминология: Курс лекций. — Харьков, 1996.
39. *Заплатинський В. М.* Основи кримінологічної безпеки сучасного бізнесу: Навч. посіб. — К.: Вид-во КДТЕУ, 2000.
40. *Зубок М. І., Зубок Р. М.* Безпека підприємницької діяльності: Норм.-правові документи комерц. підприємства, банку. — К.: Істина, 2004.
41. *Зеленецкий В. С.* Общая теория борьбы с преступностью. — Харьков: Основы, 1994.

42. *Калиниченко В. И.* Основы оказания первой неотложной медицинской помощи при охранной деятельности: Сб. метод. матер. по мед. подготовке. — М.: Ось-89, 1994.
43. *Козлов С. Б., Иванов Е. В.* Предпринимательство и безопасность: В 2 т. — М.: Универсум, 1991.
44. *Козлов С. Б., Иванов Е. В.* Предпринимательство и безопасность. — М.: Агентство НТИ, 1991.
45. *Криминология.* Учебник для юрид. вузов / Под общ. ред. д-ра юрид. наук, проф. А. И. Долговой. — М.: ИНФРА-М-Норма, 1997.

Додаткова

46. *Криминология: Учебник (для учебных заведений МВД Украины) /* Под ред. В. Г. Лихолоба, В. П. Филонова. — К.: Донецк, 1997.
47. *Крысин А. В.* Безопасность предпринимательской деятельности. — М.: Финансы и статистика, 1996.
48. *Ліпкан В. А.* Безпекознавство: Навч. посіб. — К.: Вид-во Європ. ун-ту, 2003.
49. *Методика работы в кризисных ситуациях (Обзор конкретных методических ситуаций):* Метод. разработка. — М.: Арсин ЛТД, 1966.
50. *Низенко Э. И.* Научно-технические методы и средства в профилактической деятельности органов внутренних дел. — К., 1981.
51. *Низенко Э. И.* Теоретические предпосылки использования технических средств в деятельности службы профилактики // Тр. Всесоюз. науч.-исслед. ин-та МВД СССР № 49. — М., 1978. — С. 84–89.
52. *Нелін О. І., Низенко Є. І., Панфілов В. М.* Роль недержавних служб безпеки в захисті економічних інтересів підприємництва — К.: Поліграф-Сервіс, 2001.
53. *Низенко Э. И.* Обеспечение безопасности предпринимательской деятельности: Учеб. пособие — К.: МАУП, 2003.
54. *Низенко Е. І.* Організаційно-правове забезпечення, формування та реалізація державної політики в сфері безпеки підприємництва // Зб. наук. пр. — К.: Приватне право і підприємництво. — 2003. — Вип. 3. — С. 79–84.
55. *Преступность в Украине //* Бюл. законодав. юрид. практики в Украине. — 1994. — № 2.

56. *Рекомендации по повышению безопасности объектов.* — М., 1995.
57. *Рубанов В., Дмитриев Ю.* К вопросу о защите промышленных секретов совместных предприятий // Хозяйство и право. — 1989. — № 1.
58. *Самотуга В., Андреев С.* Коммерческая тайна и ее защита. — М.: Внешторгиздат, 1992.
59. *Сборник документов по порядку создания и функционирования негосударственных охранных и детективных организаций.*
60. *Спесивцев А. В., Вегнер В. А., Крутяков А. Ю.* Защита информации в персональных ЭВМ. — М.: Радио и связь, 1992.
61. *Стенг Д., Мун С.* Секреты безопасности сетей. — К.: Диалектика, 1995.
62. *Учебник телохранителя. Базовый курс.* — М.: Мир безопасности, 1996.
63. *Федоткин С., Гураев Ю.* Сборник материалов по основам организации охранной деятельности. — М., 1996.
64. *Фролов Г.* Тайны тайнописи. — М., 1992.
65. *Ханит Ч., Зартрян В.* Разведка на службе вашего предприятия: Пер. с фр. — К., 1992.
66. *Хуберт Г.* Искусственный интеллект как средство обеспечения безопасности. — М., 1989.
67. *Цивилюк Г. Е.* Школа безопасности. Пособие по выживанию. — М.: ЭКСМО, 1995.
68. *Чернявский А. Д.* Безопасность предпринимательской деятельности. — К.: МАУП, 1998.
69. *Чернявский А.* Краткая история развития промышленного шпионажа // Деловая Украина. — 1993. — № 67. — С. 69–71.
70. *Чернявский А.* Методы коммерческой и экономической разведки // Деловая Украина. — 1993. — № 74.
71. *Чигринов В. В.* Концепция безопасности коммерческого банка. — К.: Оптима, 2001.
72. *Шеннон К.* Работы по теории информации и кибернетике. — М.: Иностран. лит., 1963.
73. *Ярочкин В. И., Халятин Д. В.* Основы защиты информации. Служба безопасности предприятия: Учеб. пособие. — М., 1993.

ЗМІСТ

Пояснювальна записка	3
Тематичний план дисципліни “Управління системою безпеки організацій та установ”	3
Зміст дисципліни “Управління системою безпеки організацій та установ”	5
Питання для самоконтролю	17
Вказівки до виконання контрольної роботи	21
Теми контрольних робіт	21
Список літератури	23

Відповідальний за випуск *Ю. В. Нешкуренко*
Редактор *І. В. Хронюк*
Комп’ютерне верстання *Г. В. Макуха*

Зам. № ВКЦ-4715

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

Наклад 30 пр.

Міжрегіональна Академія управління персоналом (МАУП)

03039 Київ-39, вул. Фрометівська, 2, МАУП

ДП «Видавничий дім «Персонал»

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

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