МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

Толюпа С. В., Оксіюк О.Г., Бурячок В.Л., Вялкова В.І.

ЗАХИСТ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Навчальний посібник

Київ – 2018

УДК 389 Д 439

Рецензенти:
Наконечний В.С. доктор технічних наук, с.н.с. Державний університет телекомунікацій
Субач І.Ю. доктор технічних наук, професор Інститут спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Рекомендовано Вченою радою ФІТ КНУ імені Тараса Шевченка "КПІ" в якості навчального посібника для студентів за напрямами підготовки "Інформаційні технологіїї", "Кібербезпека".

Толюпа С. В., Оксіюк О.Г., Бурячок В.Л., Вялкова В.І.
Захист об'єктів інформаційної діяльності.. Навчальний посібник. – К.: ККБ та ЗІ ФІТ КНУ імені Тараса Шевченка, 2018. – 322 с.

Це видання є навчальним посібником написаний у відповідності до курсу "Комплексні системи захисту інформації" та "Системи технічного захисту інформації". Матеріал, що міститься у ньому дасть можливість ознайомити студентів з основними положеннями системної концепції забезпечення безпеки об'єктів інформаційної діяльності, питаннями категоруванія об'єктів, класифікації порушників та технічних засобів, системами збору, обробки, відображення та документування інформаціїї. Даний посібник розкриває поняття витоку інформації та засоби її виявлення: радіохвильові, радіопроменеві, оптичні, магнітометричні, комбіновані. розкрито поняття системи і засобів контролю доступу до об'єктів інформаційної діяльності, особливості їх застосування, застосування технічних засобів спостереження для контролю території об'єкта.

Навчальний посібник призначений для використання в навчальному процесі КНУ імені Тараса Шевченка, а також може застосовуватися в інших вищих та середніх спеціальних навчальних закладах за фахом інформаційні технології та кібернетична безпека.

ISBN 966-7714-82-9 УДК 389 Д 59
КНУ імені Тараса Шевченка,

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ..... 5
ВСТУП……... 6
РОЗДІЛ 1. РОЗДІЛ 1. ОСНОВНІ ПОЛОЖЕННЯ СИСТЕМНОЇ КОНЦЕПЦІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ. ПИТАННЯ КАТЕГОРУВАНІЯ ОБ'ЄКТІВ, КЛАСИФІКАЦІЇ ПОРУШНИКІВ ТА ТЕХНІЧНИХЗАСОБІВ 8
1.1. Початкові положення для розробки системної концепції забезпечення безпеки об'єктів охорони ……..…… 8
1.2. Системний підхід-основа методології розробки концепції комплексного забезпечення безпеки об'єктів охорони ……..…..... 14
1.3. Загальний підхід до категорування об'єктів охорони ……..……..……... 21
1.4. “Модель” порушника можливі шляхи і способи його проникнення на об'єкт, що охороняється ……..…….…..... 23
1.5. Класифікація технічних засобів охорони, їх основні тактико-технічні характеристики та сфери застосування ……..…….. 39
Висновки по розділу 1……..…….……..…….. 70
Контрольні питання до розділу 1……. 72
РОЗДІЛ 2. СИСТЕМИ ЗБОРУ, ОБРОБКИ, ВІДОБРАЖЕННЯ І ДОКУМЕНТУВАННЯ ІНФОРМАЦІЇЇ 74
2.1. Введення. СЗОІ - апаратно-програмна система забезпечення взаємодії людини з КТЗО ……..... 74
2.2. Питання класифікації СЗОІ ……..... 78
2.3. Функції СЗОІ у складі комплексів ТЗОС …..……..…….. 92
2.4. Варіанти структур побудови СЗОІ, їх переваги і недоліки……..... 100
2.4. Висновки по розділу 2……..……..……..……... 104
Контрольні питання до розділу 2……. 105
РОЗДІЛ 3. РАДІОХВИЛЬОВІ І РАДІОПРОМЕНЕВІ ЗАСОБИ ВИЯВЛЕННЯ 106
3.1. Призначення, види і основні характеристики радіохвильових і радіопроменевих засобів вивлення ……..……..……..…… 106
3.2. Передавач, антенна система і приймач як блок формування корисного сигналу ……..... 109
3.3. Два підходи до побудови РХЗВ……. 113
Висновки по розділу 3……..…….…..... 121
Контрольні питання до розд. 3…….. 121
РОЗДІЛ 4. ОПТИЧНІ ЗАСОБИ ВИЯВЛЕННЯ 123
4.1. Призначення, класифікація і основні характеристики оптичних засобів виявлення ……..…..... 123
4.2. Активні оптичні ЗВ. Принцип дії, особливості застосування ……..... 126
4.3. Пасивні інфрачервоні ЗВ……. 130
4.4. Інфрачервоне випромінювання. Основні поняття та характеристики… 150
Висновки по розділу 4……..……..……..... 183
Контрольні питання до розділу 4……. 184

РОЗДІЛ 5. СЕЙСМІЧНІ ЗАСОБИ ОХОРОННОЇ СИГНАЛІЗАЦІ 185
5.1. Основні поняття і визначення……. 185
5.2. Основи теорії збудження і розповсюдження сейсмічних хвиль …….…. 187
5.3. Перешкоди в СЗВ……. 193
5.4. Чутливі елементи СЗВ……. 196
5.5. Рекомендації по закріпленню знань……... 197
Висновки по розділу 5……..……....……..... 198
Контрольні питання до розділу 5…….. 199
РОЗДІЛ 6. МАГНІТОМЕТРИЧНІ ЗАСОБИ ВИЯВЛЕННЯ 200
6.1. Види магнітометричних ЗВ, принципи їх дії ……... 200
6.2. Основні характеристики МЗВ…… 202
6.3. Характерні перешкоди при застосуванні МЗВ і способи їх компенсації.. 203
6.4 Особливості розробки і застосування МЗВ……..... 205
6.5. Структурна схема МЗВ……..…… 207
6.6. Основи теорії розробки засобу магнітометричного виявлення (на прикладі феррозондів)…… ……. 208
Висновки по розділу 6……..……....……..... 218
Контрольні питання до розділу 6…….. 219
РОЗДІЛ 7. КОМБІНОВАНІ ЗАСОБИ ВИЯВЛЕННЯ 220
7.1. Призначення, види і способи комбінування засобів виявлення …… 220
7.2. Формалізація вибору різних варіантів комбінування засобів виявлення на одному рубежі охорони……. 223
Висновки по розділу 7…… 258
Контрольні питання до розділу 7…….. 258
РОЗДІЛ 8. ЗАСТОСУВАННЯ ТЕХНІЧНИХ ЗАСОБІВ СПОСТЕРЕЖЕННЯ ДЛЯ КОНТРОЛЮ ТЕРИТОРІЇ ОІД 259
8.1. Телевізійні камери і пристрої для їх оснащення…….. 259
8.2. Пристрої передачі, комутації і обробки відеосигналів……... 264
8.3. Класифікація телевізійних систем відео контролю…….. 270
8.4. Вибір засобів відеоконтролю для устаткування об'єктів, особливості їх експлуатації……...…….. 274
Висновки по розділу 8……..……....…… 285
Контрольні питання до розділу 8…… 286
РОЗДІЛ 9. СИСТЕМИ І ЗАСОБИ КОНТРОЛЮ ДОСТУПУ, ОСОБЛИВОСТІ ЇХ ЗАСТОСУВАННЯ 287
9.1. Особливості побудови систем контролю доступу…… 287
9.2. Периферійне устаткування і носії інформації систем контролю доступу. 297
9.3 Засоби ідентифікації і аутентифікації……. 298
9.4. Функціональні можливості систем контролю доступу…… 310
9.5. Рекомендації по вибору засобів і систем контролю доступу…….. 313
Висновки по розділу 9……..……....…… 318
Контрольні питання до розділу 9…….. 318
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……..... 320

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСО- автоматизована система охорони
АСОІ - автоматизованих системах обробки інформації
ДП - допоміжні пристрої
ДТА - диверсійно-терористичний акт
ДТЗ - диверсійно-терористичних засобів
ЗВ – засоби виявлення
ЗСКД - засоби систем керування доступом
КОС – комплекс охоронної сигналізації
КТЗО – комплекс технічних засобів охорони
ЛОМ - локальних обчислювальних мережах
НСД - несанкціонований доступ
НСК - несанкціоноване копіювання
ОЗГ – організовані злочинні групи
ОЗФ – організовані злочинні формування
ОО – об’єкти охорони
СБ - служби безпеки
СБО - служби безпеки об’єкта
СЗОІ - система збору та обробки інформації
СТС - системи телевізійного спостереження
ТЗО – технічні засоби охорони
ТЗОС – технічні засоби охоронної сигналізації
ТЗС - технічні засоби спостереження
СКД – система контролю доступу
ЧЕ - чутливий елемент
ПКП - приймально-контрольний прилад
МТМ - міська телефонна мережа
СПС - система передачі сповіщень
КП - кінцеві пристрої
Р- ретранслятор
АТС - автоматичні телефонні станції
ПЦС - пульт централізованого спостереження
ПЦО - пункт централізованої охорони
ІСБ - інтегрованою системою безпеки
ТТХ - тактико-технічні характеристики
ПВ - пристрої відображення
ВЛІ - вакуумні люмінесцентні індикатори
ВКП - відеоконтрольні пристрої
ВДЖ - вторинні джерела живлення
РКІ - рідкокристалічний індикатор
ПП - пороговий пристрій
ПБ - периферійних блок
СА - станційна апаратура
СТС - системою тривожного сповіщення

ВСТУП

У цьому навчальному посібнику викладено основні положеннями системної концепції забезпечення безпеки об'єктів інформаційної діяльності, питання категорування об'єктів, класифікації порушників та технічних засобів, системами збору, обробки, відображення та документування інформації. Розкривається поняття витоку інформації та засоби її виявлення: радіохвильові, радіопроменеві, оптичні, магнітометричні, комбіновані. розкрито поняття систем і засобів контролю доступу до об’єктів інформаційної діяльності, особливості їх застосування, а також використання технічних засобів спостереження для контролю території об’єкта.

Інформаційні системиоб’єктів інформаційної діяльності являють собою цінність та мають відповідне матеріальне вираження й вимагають захисту від різноманітних за своєю сутністю впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

Інформація для своготіснування завжди вимагає наявності носія. Як матеріальні носії інформації може виступати поле або речовина. В деяких випадках у вигляді носія інформації може розглядатися людина. Втрата інформацією своєї цінності (порушення безпеки інформації) може статися внаслідок переміщення інформації або зміни фізичних властивостей носія.

Інформація в інформаційній системі існує у вигляді даних, тобто представляється в вигляді, придатному для введення, виведення, зберігання, передачі тощо.При аналізі проблеми захисту інформації від несанкціонованому доступу, яка може циркулювати в інформаційно-телекомунікаційний системі, як правило, розглядаються лише інформаційні об’єкти, що служать приймальниками/джерелами інформації, і інформаційні потоки (порції інформації, що пересилаються між об’єктами) безвідносно до фізичних характеристик їх матеріальних носіїв.

Захист інформації, що обробляється в інформаційній системі, полягає в створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Іншими словами, захист інформації спрямовано на забезпечення безпеки оброблюваної інформації на об’єктах інформаційної діяльності.

Істотна частина проблем забезпечення технічного захисту інформації в інформаційних системах може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту.

Навчальний посібник призначено для використання в навчальному процесі студентами вищих навчальних закладів за напрямом підготовки “Кібербезпека”.

Автори висловлюють щиру подяку рецензентам доктору технічних наук, професору Конаховичу Георгію Філімоновичу (Національний авіаційний університет), доктору технічних наук (Національний авіаційний університет), професору Рудницькому Володимиру Миколайовичу (Черкаський технологічний університет) та доктору технічних наук, професору Дружиніну Володимиру

Анатолійовичу (Державний університет телекомунікацій) за уважне та доброзичливе рецензування та зауваження, яке сприяло значному поглибленню та покращенню підручника.

Зогляду на те, що у навчальному посібнику систематизовано викладаються питання технічного захисту інформації на об’єктах інформаційної діяльності, він не може бути без недоліків, тому автори будуть щиро вдячні за висловлені зауваження та пропозиції щодо покращення його.