МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ І ПРИКЛАДНИХ ТЕХНОЛОГІЙ
КАФЕДРА ПРИКЛАДНОЇ МАТЕМАТИКИ ТА КІБЕРБЕЗПЕКИ

ОСНОВИ КІБЕРБЕЗПЕКИ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Методичні рекомендації до самостійної роботи
Частина 1

для здобувачів СО «Бакалавр»
спеціальності 125 Кібербезпека та захист інформації

Вінниця
2024

УДК 004.056(075.4)
О-753

Затверджено на засіданні вченої ради
факультету інформаційних і прикладних технологій
Донецького національного університету імені Василя Стуса
(протокол № 9 від 24 січня 2024 р.)

Укладачі:

Михайло ПРОКОФЬЄВ, д-р техн. наук, професор кафедри прикладної математики та кібербезпеки ДонНУ імені Василя Стуса;

Людмила ПОЛОВЕНКО, канд. пед. наук, доцент кафедри прикладної математики та кібербезпеки ДонНУ імені Василя Стуса;

Олександр ГРЕСЬ, канд. техн. наук, асист. кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича.

Рецензенти:

Володимир КРИЖАНОВСЬКИЙ, д-р техн. наук, професор кафедри прикладної математики та кібербезпеки ДонНУ імені Василя Стуса;

Юрій ЯРЕМЧУК, д-р техн. наук, професор, директор Центру інформаційних технологій і захисту інформації, голова секції «Управління інформаційною безпекою» та професор кафедри менеджменту та безпеки інформаційних систем, науковий керівник науково-дослідної лабораторії технічного захисту інформації ВНТУ.

О-753 Методичні рекомендації до самостійної роботи з дисципліни «Основи кібербезпеки та національної безпеки» для здобувачів освіти спеціальності 125 Кібербезпека та захист інформації СО «Бакалавр» / укладачі М. І. Прокофьєв, Л. П. Половенко, О. В. Гресь. Вінниця: ДонНУ імені Василя Стуса, 2024. 88 с.

Розглядаються базові положення щодо проблеми забезпечення кібербезпеки і національної безпеки. Розкриваються питання щодо завдань кіберзахисту та шляхів його забезпечення в умовах інформаційної війни. Значну увагу приділено нормативно-правовим, технологічним та практичним аспектам забезпечення технічного захисту інформації в інформаційно-комунікаційних системах. Викладені технологічні рішення щодо питань створення технічних каналів витоку інформації в інформаційно-комунікаційних системах.

УДК 004.056(075.4)

ЗМІСТ

ВСТУП 4
ТЕМА 1. Кіберпростір і кібербезпека. Національна безпека і особливості захисту інформації у кіберпросторі 5
ТЕМА 2. Сучасна технічна розвідка. Інформаційна війна і національна безпека 11
ТЕМА 3. Правова основа забезпечення інформаційної безпеки в Україні 34
ТЕМА 4. Інформаційно-комунікаційні системи як об’єкт захисту 46
ТЕМА 5. Системи захисту інформації в ІКС від витоку технічними каналами 50
ТЕМА 6. Захист мовної інформації на ОІТ: пасивний захист, активний захист 57
ТЕМА 7. Методи та засоби технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наведень 64
ОРІЄНТОВНИЙ СПИСОК ПИТАНЬ ДО ІСПИТУ 75
ТЕСТИ ДЛЯ САМОПЕРЕВІРКИ 76
СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ 86

ВСТУП

Дисципліна «Основи кібербезпеки та національної безпеки» входить до циклу дисциплін професійної та практичної підготовки здобувачів вищої освіти спеціальності 125 Кібербезпека та захист інформації.

У сучасних умовах збройна боротьба ведеться із застосуванням високотехнологічного озброєння і військової техніки, високоефективних засобів розвідки, управління й ураження зі значним збільшенням розмаху і швидкоплинності операцій. Інформаційне забезпечення процесів управління та навантаження органів управління постійно зростають. Забезпечення ефективності управління своїми силами і засобами та порушення його у противника надає вагомі переваги над ним в умовах сучасного протиборства.

Метою вивчення навчальної дисципліни є формування знань та умінь, які необхідні для ідентифікації загроз, виявлення вразливостей у сучасних інформаційно-комунікаційних системах; основних методів їх усунення, а також практичного застосування відповідних методів і механізмів для захисту кібернетичного й інформаційного просторів.

У методичних рекомендаціях запропоновані допоміжні матеріали для опанування теоретичних питань, які виносяться на самостійне опрацювання за кожною темою, завдання для самостійного виконання.

Для закріплення самостійно опрацьованого матеріалу здобувач вищої освіти може використати питання для самоконтролю, які запропоновані після кожної теми, а також тести для самоперевірки.

ТЕМА 1. КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА. НАЦІОНАЛЬНА БЕЗПЕКА І ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ У КІБЕРПРОСТОРІ

ТЕОРЕТИЧНІ ВІДОМОСТІ

Завдання, які мають вирішуватись фахівцями з кібербезпеки – це:

– захист інформації;

– кіберзахист;

– забезпечення національної безпеки держави.

Основні завдання захисту інформації – сукупність методів і засобів, що забезпечують цілісність, конфіденційність і доступність інформації за умов впливу на неї загроз природного або штучного характеру, реалізація яких може призвести до завдання шкоди володільцям (власникам) і користувачам інформації.

Інформаційна безпека як складник національної безпеки – захищеність (стан захищеності) основних інтересів особистості, суспільства і держави у сфері інформації, зокрема, інформаційної і комунікаційної інфраструктури, інформація та значення її параметрів, що характеризують її повноту, об'єктивність, цілісність, доступність і конфіденційність. Особливістю інформаційної безпеки є те, що вона є невід'ємною частиною інших складників національної безпеки: економічної, воєнної, політичної безпеки тощо.

На сучасному етапі реальними та потенційними загрозами національній безпеці України в інформаційній сфері є:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, що становить державну або іншу, передбачену законом, таємницю, а також конфіденційної інформації, що становить державний інформаційний ресурс або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення у засобах масової інформації і комп'ютерних мережах дезінформації (недостовірної, неповної або упередженої інформації).

Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене внаслідок функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забез-

печуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включно з інформаційно-комунікаційними технологіями, програмними, програмно-апаратними засобами, іншими технічними та технологічними засобами і обладнанням) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту.

Кіберінцидент кібербезпеки (далі – кіберінцидент) – подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, зокрема внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (зокрема зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів.

Кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів.

Кіберзлочин (комп’ютерний злочин) – суспільно небезпечне злісне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України.

Кібероборона – сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та

інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії.

Кіберрозвідка – діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням.

Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням.

Кібершпигунство – шпигунство, що здійснюється у кіберпросторі або з його використанням.

Особливу увагу держава приділяє питанням забезпечення умов для безпечного функціонування об'єктів критичної інфраструктури.

Критична інформаційна інфраструктура – сукупність об'єктів критичної інформаційної інфраструктури.

Об'єкт критичної інформаційної інфраструктури – комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури. Критично важливі об'єкти інфраструктури (далі – об'єкти критичної інфраструктури) – підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей.

Національна безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої у державі забезпечується сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, діяльності Державної прикордонної служби та Міністерства оборони, міграційної політики, охорони здоров'я, дитинства, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова й інформаційної безпеки, кібербезпеки та кіберзахисту, соціальної політики, культурного розвитку громадян, захисту інформації, захисту екології і навколишнього середовища та інших сфер державного управління.

Основні засади забезпечення кібербезпеки України регламентує відповідний Закон України «Про основні засади забезпечення кібербезпеки України», який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних ін-

тересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Національна система кібербезпеки є сукупністю суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури.

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку покладені на них завдання.

Сьогодні основні завдання у сфері кібербезпеки вирішує Державна служба спеціального зв'язку та захисту інформації України, яка забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Націо-

нальної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Впровадження організаційно-технічної моделі кібербезпеки як складника національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних чинників системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об'єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту, системи взаємодії команд реагування на комп'ютерні надзвичайні події, а також у взаємодії з іншими суб'єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

Нині варто усвідомити, що є два шляхи забезпечення безпеки у кіберпросторі. Перший – чекати, поки відбудеться атака, і вже потім намагатися врятувати свої системи. Другий – завчасно шукати недоліки, серед іншого – і за допомогою фахівців державних установ і запроваджувати ефективну систему захисту та знижувати ймовірність успішної атаки до прийнятного рівня.

Кіберпростір не має кордонів, тому незалежно від регіону довільна система у кіберпросторі можете зазнати атаки з боку хакерів. Це спільна проблема, яка стосується держави, бізнесу, громадських організацій, ЗМІ тощо.

Державна служба спеціального зв'язку і захисту інформації є ключовим органом, відповідальним за розроблення регуляторної та нормативної бази, яка дає можливість усім використовувати найкращі практики у світі та впроваджувати їх, співпрацює з усіма провідними країнами, щоб забезпечити впровадження таких практик. Однак найкращі документи без їх практичного запровадження не мають жодного сенсу й не принесуть очікуваного результату. Щодня ворог атакує Україну у кіберпросторі. Тому пріоритет держави – безпечний кіберпростір.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ

Завдання 1. Підготувати глосарій українською та англійською мовами для термінів: інформація, інформаційна сфера, єдиний інформаційний простір країни, інформаційні ресурси, загроза інформаційній безпеці, незаконне використання інформаційних і комунікаційних систем і інформаційних ресурсів, інформаційна інфраструктура (організаційні структури, інформаційно-комунікаційні структури, національна комунікаційна мережа, національні електронні інформаційні ресурси, комунікаційні технології, системи засобів масової інформації).

Завдання 2. Підготувати глосарій англійською мовою для термінів: кіберпростір, кібербезпека, кіберзахист, кібератака, кіберінцидент, кіберзагроза, кіберзлочин, кібероборона, кіберрозвідка, кібертероризм, кібершпигунство.

ТЕМА 2. СУЧАСНА ТЕХНІЧНА РОЗВІДКА. ІНФОРМАЦІЙНА ВІЙНА І НАЦІОНАЛЬНА БЕЗПЕКА

ТЕОРЕТИЧНІ ВІДОМОСТІ

Вперше термін інформаційна війна з'явився у звіті Томаса Рона «Системи зброї та інформаційна війна», підготовленому у 1976 р. У ньому автор, зокрема, вказував, що інформаційна інфраструктура стає ключовим фактором економіки США, але вона одночасно перетворюється на вразливу мету у воєнний та мирний час. До 1980 р. вже склалося загальне уявлення про те, що інформація може бути як метою, так і зброєю (рис. 2.1).

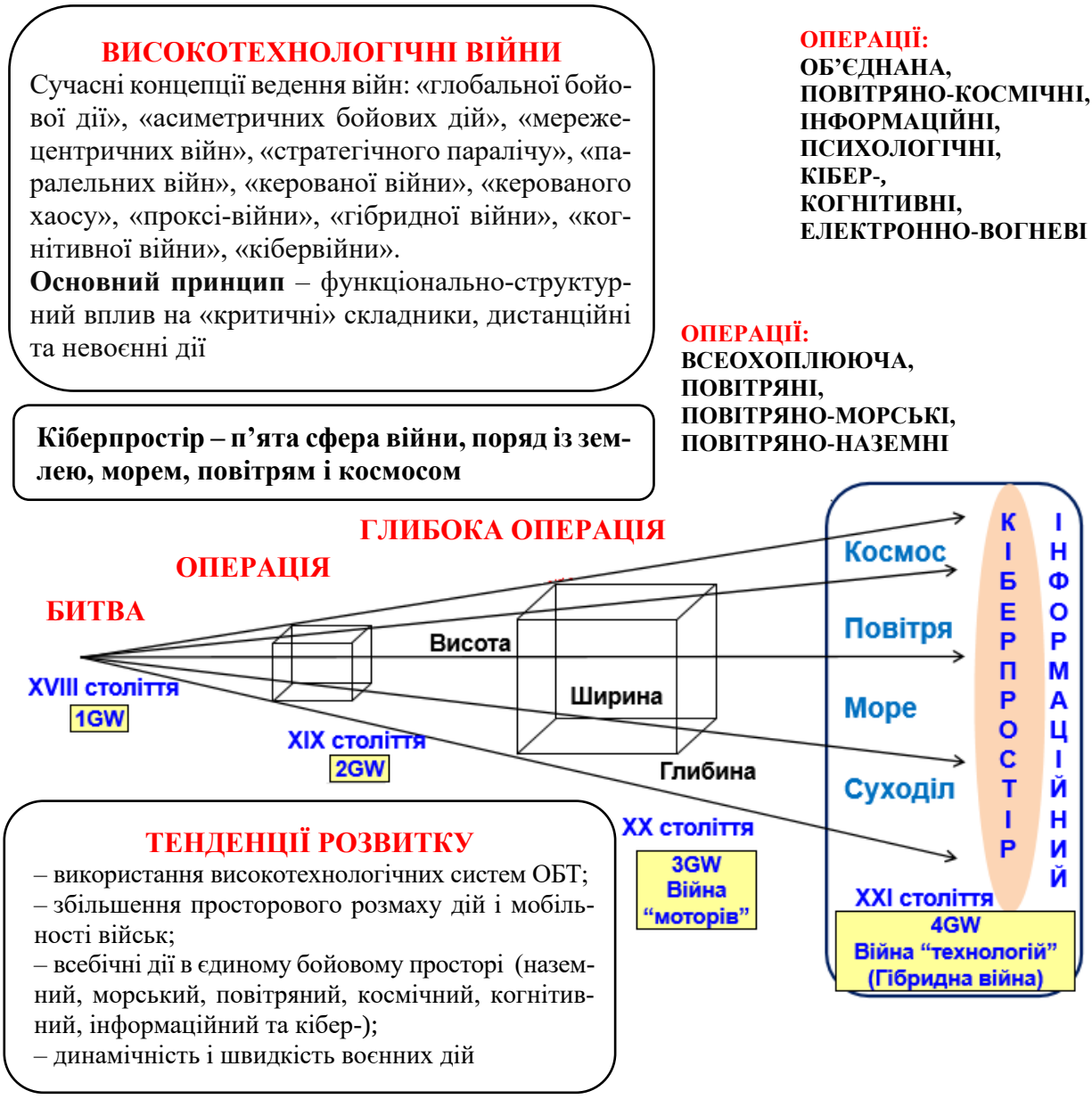

Рисунок 2.1. Еволюція основних концепцій ведення війн [3]

Через появу нових завдань після закінчення «холодної війни» термін інформаційна війна було введено в документи міністерства оборони США. Наприкінці

1996 р. Роберт Банкер, експерт Пентагону, представив доповідь, присвячену новій програмі будівництва і бойового застосування збройних сил США XXI століття. В її основу було покладено поділ всього театру бойових дій на два складники – традиційний і кіберпростір, причому останній має навіть більш важливе значення. Банкер запропонував доктрину «кіберманевру», яка повинна стати природним доповненням традиційних військових концепцій, що мають на меті нейтралізацію або придушення збройних сил противника. Отже, до сфер ведення бойових дій, крім землі, моря, повітря і космосу, тепер включається й інфосфера.

Як наголошують військові експерти, основними об'єктами поразки у нових війнах є інформаційна інфраструктура та психіка супротивника. У жовтні 1998 р. міністерство оборони США ввело в дію Об'єднану доктрину інформаційних операцій, що пов'язано з необхідністю розрізнення понять «інформаційна операція» та «інформаційна війна», які були сформульовані в такий спосіб.

Інформаційна операція – це дії, що вживаються з метою утруднення збирання, обробки, передавання та зберігання інформації системами противника під час захисту власної інформації та систем.

Інформаційна війна – комплексний вплив (сукупність інформаційних операцій) на систему державного та військового управління протилежної сторони, її військово-політичне керівництво.

У військовій справі настає новий етап – перехід від стратегії ядерного стримування до високоточної контр-силової інформаційної зброї.

Інформаційне протиборство – це суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, внаслідок якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють такі ступені інформаційного протиборства: інформаційна експансія, інформаційна агресія та інформаційна війна.

Інформаційна експансія – діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою:

– поступової, планової, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;

– витіснення положень національної ідеології та національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками;

– збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними ресурсами, інформаційно-телекомунікаційною структурою та національними засобами масової інформації (ЗМІ);

– нарощування присутності власних ЗМІ в інформаційній сфері об'єкта (системи), проникнення та ін. (приклад – завоювання інформаційної сфери у східних і південних районах України).

Яскравим прикладом використання інформаційного продукту як зброї є діяльність російської федерації, що веде війну проти нашої країни. Чи не головним методом цієї війни є інформаційна експансія, розв'язана російською федерацією з метою створення викривленої реальності та системи цінностей на користь агресора, послаблення та руйнування національної ідентичності і громадянської свідомості українців. Пропагандистські операції росії характеризуються дестабілізацією інформаційно-комунікативного простору, застосуванням великої кількості джерел інформування з метою дискредитації та фейкового спростування правдивих повідомлень.

Яскравим прикладом агресивних інформаційних кампаній є створення та розповсюдження пропагандистських наративів, як так звана доктрина «ДНР» «Русский Донбасс», просування змісту якої ґрунтується на тезах: «Донбас – історична частина Росії», «право розмовляти рідною мовою», «братовбивча війна на Донбасі» та ін. З допомогою таких інформаційних диверсій російські агресори намагаються змінити свідомість громадян, спотворити розуміння реальності та використати їх як безвольний ресурс у гібридній війні. Модель, що застосовується російськими пропагандистами, достатньо потужна. Сила її полягає в високій ресурсній забезпеченості, задіяності широкої мережі каналів передачі інформації. До того ж російські ЗМІ не турбуються про правдивість інформації, тому не витрачають часу на перевірку даних, вони самі створюють потрібні «новини», їх відповідність реальності абсолютно для них не важлива – головне, щоб досягалася поставлена мета.

Інформаційна агресія – незаконні дії однієї зі сторін в інформаційній сфері, спрямовані на нанесення супротивнику конкретної, відчутної шкоди в окремих областях його діяльності шляхом *обмеженого та локального* за своїми масштабами застосування сили.

Інформаційна війна – найвищий ступінь інформаційного протиборства, спрямованого на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, народами, націями, класами й соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї).

Можна вважати, що інформаційна агресія в інформаційній сфері переростає у війну в тому випадку, якщо одна зі сторін конфлікту починає широко застосовувати проти своїх супротивників інформаційну зброю.

Цей критерій дає змогу виділити з усього різноманіття процесів і явищ, що відбуваються в інформаційному суспільстві, такі, які становлять небезпеку для його нормального (мирного) розвитку.

Нині відсутні міжнародні та національні правові норми, які дозволяють у мирний час (за відсутності офіційного оголошення війни з боку агресора) юридично кваліфікувати ворожі дії іноземної держави в інформаційній сфері, що супроводжуються нанесенням збитку інформаційній або іншій безпеці країни, як акції інформаційної агресії або інформаційної війни матеріального, морального, іншого збитку.

Це дає змогу в мирний час активно використовувати найнебезпечніший і агресивний арсенал сил і засобів інформаційної війни як основний засіб досягнення політичної мети.

В інформаційній війні широко використовується інформаційна зброя, яка являє собою пристрої і засоби, призначені для нанесення протиборчій стороні максимальної шкоди під час інформаційної боротьби (шляхом небезпечних інформаційних впливів).

Для широкого застосування інформаційної зброї (як і будь-якої іншої) потрібно, щоб вона:

– максимально швидко, порівняно з іншими видами озброєння, могла бути застосована до об’єкта впливу;

– заподіяла об’єкту впливу необхідний збиток за заданий часовий інтервал;

– була досить простою і дешевою у виготовленні, порівняно з іншими видами зброї такого ж класу впливу.

На рубежі XX–XXI ст. виникли умови, які дали змогу говорити про інформаційну зброю як про найбільш значиму зброю сучасної епохи. До них належать:

– різке зниження вартості виробництва даних завдяки появі засобів обчислювальної техніки, виробництво інформації ставиться на конвеєр;

– створення автоматизованих засобів для отримання знань з даних;

– різке зниження вартості і скорочення часу на доставку повідомлень практично в будь-яку точку планети завдяки розвитку телекомунікаційних засобів та інтернету;

– різке підвищення ефективності інформаційного впливу завдяки появі розвинених теорій у галузі перепрограмування інформаційних самонавчальних систем: теорія програмування для ЕОМ і NLP (обробка природної мови);

– програмування для соціальних систем, включно з великою кількістю методів і прийомів інформаційно-психологічного впливу.

Розглянемо дві підгрупи інформаційної зброї.

Перша підгрупа засобів інформаційної зброї:

– засоби масової інформації (ЗМІ);

– психотропні генератори;

– психотропні препарати.

Інформаційна зброя цієї підгрупи призначена для негативного впливу на людину. Зокрема, цей вплив може здійснюватися через різні ЗМІ. Відповідно до Закону України «Про засоби масової інформації» під цими засобами розуміються періодичні друковані видання, радіо-, теле-, відеопрограми, кінохронікальні програми, інші форми періодичного поширення масової інформації.

Під масовою інформацією розуміються призначені для необмеженого кола осіб друковані, аудіо-, аудіовізуальні та інші повідомлення й матеріали. Хронологія багатьох воєнних конфліктів останніх років включала, зазвичай, на початку їх розвитку етап психологічної обробки світової громадськості через ЗМІ.

Психотропні генератори – це пристрої, які впливають на людину шляхом передачі інформації через неусвідомлюване сприйняття. Вже давно встановлено, що різні органи людини мають власні резонансні частоти, використовуючи які, можна впливати на психіко-фізіологічний стан індивіда або колективу людей, викликаючи у них страх чи інші почуття. Ці та інші особливості людського організму використовуються під час побудови та підбору параметрів психотропних генераторів (частотний діапазон, потужність випромінювання, тривалість роботи та ін.).

Психотропні препарати – це лікарські (наркотичні) засоби, які здатні викликати стан залежності, здійснювати стимулюючий або депресивний вплив на центральну нервову систему, викликаючи галюцинації або порушення моторної функції організму, під впливом яких відбувається порушення мислення, змінюється настрій, поведінка.

Друга група засобів інформаційної зброї:

– засоби радіоелектронної боротьби;

– комплекси спеціального програмно-технічного впливу.

Засоби радіоелектронної боротьби (РЕБ) – це системи для виявлення і радіоелектронного придушення систем управління військами та радіоелектронного озброєння противника, його систем розвідки і навігації, а також системи для забезпечення стійкої роботи своїх систем.

РЕБ – це сукупність узгоджених за цілями, завданнями, місцем і часом дій зі здобування інформації про місцеперебування радіоелектронних засобів (РЕЗ), систем управління військами та зброєю противника, їх знищення або виведення з ладу всіма наявними засобами ураження, а також захист власних РЕЗ і систем управління від дій противника (контррадіоелектронна протидія).

Панування в електромагнітному просторі дає перевагу над противником в управлінні військами та озброєнням. Допомогти в цьому повинні засоби радіоелектронної боротьби (РЕБ), які є одними з провідних елементів нинішніх війн і збройних конфліктів і не випадково мають чи не найбільшу серед усіх сучасних видів озброєнь динаміку розвитку.

Основні об’єкти впливу в інформаційній війні:

1. Мережі зв’язку та інформаційно-обчислювальні мережі, які використовуються державними організаціями під час виконання їх управлінських функцій.

2. Військова інформаційна інфраструктура, вирішальне завдання якої полягає в управлінні військами.

3. Інформаційні та керуючі структури банків, транспортних і промислових підприємств.

4. ЗМІ (насамперед електронні).

Для досягнення мети в інформаційній війні особливе місце займає технічна розвідка. Виділяють такі класи технічних розвідок: космічна, повітряна, наземна, морська.

Із зазначених 4-х видів технічних розвідок нас насамперед цікавлять особливості наземної розвідки і такі її основні види: фотографічна і візуально-оптична, оптико-електронна, лазерна, радіоелектронна, радіолокаційна, гідро- і акустична, радіаційна, хімічна, сейсмічна, магнітометрична, комп’ютерна і вимірювально-сигнатурна розвідки.

Фотографічна і візуально-оптична розвідки передбачають отримання інформації під час безпосереднього спостереження / фіксації об’єктів неозброєним оком або з використанням оптичних приладів. Візуальне спостереження може використовуватися у всіх видах розвідки: наземної, морської, повітряної та космічної.

Повітряне спостереження з передачею даних по радіо вважається найбільш оперативним способом розвідки, який дає змогу отримувати розвідувальні відомості про об’єкти / війська та їх дії на велику глибину і в найкоротші терміни. Наземне спостереження ведеться зі спостережних постів у будь-якій обстановці та є важливим способом добування розвідданих.

Візуальне спостереження є також одним із основних способів ведення розвідки під час дій диверсійно-розвідувальних груп та агентури.

Під оптико-електронною розвідкою (ОЕР) розуміється процес добування інформації за допомогою засобів, що включають вхідну оптичну систему з фотоприймачем та електронні схеми обробки електричного сигналу, які забезпечують приймання й аналіз електромагнітних хвиль видимого та інфрачервоного діапазонів, випромінюваних або відбитих об’єктами і місцевістю.

ОЕР поділяють на телевізійну розвідку (ОТР), інфрачервону розвідку (ІЧР), лазерну розвідку (ЛР) та розвідку лазерних випромінювань (РЛВ). Апаратура ОЕР встановлюється на космічних і повітряних носіях, а також може застосовуватися в наземних умовах, наприклад, під час технічної розвідки.

Принцип роботи апаратури ОЕР заснований на прийманні власного інфрачервоного випромінювання об’єктів і фону або відбитого від них випроміню-

вання Сонця, Місяця, зоряного неба та штучних джерел підсвічування місцевості. Апаратура ОЕР дає змогу виявляти об'єкт на навколишньому фоні за умови, що його яскравість перевищує яскравість фону.

Апаратура ОЕР ділиться на пасивну та активну.

Пасивна ґрунтується на прийманні власного або перевідбитого випромінювання об'єктів розвідки.

Активна передбачає використання для підсвічування території свого випромінювача. Зондувальне випромінювання розсіюється об'єктами, місцевими предметами і місцевістю, частина цього випромінювання надходить на вхід оптичної системи апаратури розвідки з подальшим його перетворенням, обробкою та індикацією на відповідних пристроях.

Апаратура пасивної ОЕР поділяється на телевізійну, інфрачервону та розвідку лазерних випромінювань.

Апаратура телевізійної розвідки охоплює пристрої на ЕПТ і на РКП.

До апаратури ІЧР відносять тепловізори, телепеленгатори, радіометри та ПНС. Апаратура розвідки лазерних випромінювань призначена для виявлення, визначення розташування та розпізнавання засобів озброєння та військової техніки, до складу яких входять лазерні випромінювачі.

Апаратура активної ОЕР поділяється на лазерну зі скануванням зондуючого світлового променя та інфрачервону з використанням ІЧ-випромінювача для підсвічування місцевості.

Засоби лазерної розвідки

Як приклад розглянемо деякі особливості лазерного мікрофону LM-100.

Він забезпечує перехоплення мовної інформації на дистанціях до 100 метрів без проникнення до приміщення. Під тиском акустичного поля виникає вібрація предметів інтер'єру у приміщенні, тому розмова може бути прийнятою завдяки віддзеркаленню (навіть дифузному) лазерного променя від будь-яких поверхонь: метал, пластик, тканина, дерево тощо. Легка установка завдяки тому, що приймач та передавач в одному пристрої. Легке прицілювання за допомогою вбудованої відеокамери та штатива, керованого кроковими двигунами. Не відчуває шумів на трасі від мішені до приладу. Дає змогу працювати крізь скло (вікна приміщень, автомобільні вікна тощо). Реєструє відео- та аудіосигнали.

Переваги:

1) дальність перехоплення інформації – до 100 метрів;

2) легке прицілювання та налаштування за допомогою крокових двигунів;

3) дистанційне управління та моніторинг;

4) незалежність від поверхні та площі, з якої перехоплюється інформація;

5) гарна розбірливість мови;

6) компактні розміри.

Принцип роботи LM-100 – використання когерентного лазерного променя (генератор із великою довжиною когерентності) дає змогу сприймати вібрації з амплітудою менше довжини хвилі лазера без контакту з об'єктом вимірювань.

Лазерний промінь приймає вібрації мішені, викликані голосом з різних кутів і поверхонь незалежно від розташування мішені. Інформація лазерного променя модулюється зміною частоти в розсіяному (дифузному) світлі, тому прилад нечутливий до кута падіння променя на ціль і забезпечує хорошу розбірливість мови без будь-яких обробок.

Робоче місце оператора може розташовуватись у радіусі до 20 метрів навколо LM-100. Комп'ютер оператора з'єднується з LM-100 з допомогою WiFi.

Сьогодні для налаштування та керування LM-100 паралельно використовуються дві програми:

– програма управління струмом споживання лазером і демодуляцією звукового сигналу;

– програма управління камерою і штативом.

Радіоелектронна розвідка

Радіоелектронна розвідка (РЕР) – інформація отримується внаслідок приймання та аналізу електромагнітних випромінювань (ЕМІ) радіодіапазону, створюваних працюючими радіоелектронними засобами (РЕЗ). ЕМВ, створювані об'єктами розвідки, можуть бути первинними (власними) або вторинними (відбитими). Для нас особливістю є те, що існують ще і побічні ЕМВ.

Випромінювання РЕЗ – це насамперед їх основні (власні) випромінювання, що забезпечують функціонування РЕЗ. Особливість основних випромінювань – детермінований характер їх просторової, часової та спектральної структури (діаграма спрямованості випромінювання, тривалість і період слідування випромінюваних імпульсів, частота, вид амплітудного і фазового спектрів, ширина спектра тощо). Під час роботи передавачів РЕЗ, поряд з основними існують і неосновні, побічні випромінювання, які лежать поза смугою частот, необхідного для передавання інформації або створення перешкод, і містять певну інформацію про випромінюючі об'єкти.

Вторинні ЕМВ – це випромінювання, що виникають внаслідок відображення (розсіювання) електромагнітних хвиль (ЕМВ), що опромінюють об'єкт. ЕМВ, що падають на об'єкт, розсіюються ним у всіх напрямках, зокрема і на джерело зондуючого випромінювання.

Для вторинного випромінювання реальних об'єктів (літак, корабель, танк) характерна залежність його параметрів (інтенсивності, спектру, поляризації, нахилу фазового фронту) від відбивної здатності, геометричної форми та розмірів об'єкта, поляризації падаючої хвилі, взаємної орієнтації джерела випромінювання об'єкта, і, нарешті, від параметрів їх відносного руху.

Наявність первинних та вторинних ЕМВ об’єктів дає змогу вести розвідку об’єктів та їх розпізнавання. РЕР дає змогу вирішувати такі завдання:

− виявляти об’єкти, визначати їх місцезнаходження та параметри руху;

− визначати параметри об’єктів та характер їх зміни у часі;

− визначати призначення об’єктів та їх типи;

− перехоплювати інформацію, що передається каналами зв’язку.

Засоби РЕР працюють у пасивному чи активному режимі (без випромінювання ЕМВ або з випромінюванням) у широкому діапазоні спектра радіочастот.

РЕР має низку відмінностей:

− охоплює великі райони, межі яких залежать від особливостей поширення ЕМВ на різних ділянках спектра;

− функціонує безперервно у будь-яку пору року та за будь-яких метеоумов.

Засоби повітряної радіотехнічної і радіолокаційної розвідки

Прикладом засобу, що поєднує у собі усі ці три види розвідок, є стратегічний розвідувальний безпілотний літальний апарат ВПС США RQ-4 Global Hawk (рис. 2.2).

Рисунок 2.2. БПЛА RQ-4

Безпілотник літає на висоті понад 16 кілометрів, а його швидкість становить майже 500 кілометрів на годину. Global Hawk оснащений інтегрованою системою спостереження та розвідки HISAR. Комплекс включає радар SAR/MTI, а також оптичний та інфрачервоний сенсори. Усі три підсистеми можуть працювати одночасно, а їх дані обробляються єдиним процесором. Цифрові дані можуть передаватися на землю в режимі реального часу в межах прямої видимості або через супутниковий канал із швидкістю до 50 Мбіт/с.

Радар має можливість виявлення наземних рухомих об’єктів (moving target indicator – MTI) та передачі відомостей про подібні об’єкти (координати та швидкість) у текстових повідомленнях. У нормальному режимі роботи радар безпілотника забезпечує отримання радіолокаційного зображення місцевості з роздільною здатністю 1 метр. Підсистема SAR/MTI працює в X-діапазоні (8–12 ГГц) і забезпечує:

– сканування та виявлення рухомих цілей у радіусі 100 км;

– комбінований SAR/MTI режим дає можливість спостереження з роздільною здатністю 6 метрів у смузі шириною 37 км та завдовжки від 20 до 110 км;

– у режимі деталізації об'єктів радар забезпечує роздільну здатність 1,8 метра на території 10 км^2.

RQ-4 – це не маленька «пташка». За максимальний час у повітрі (понад 34 години) він має дальність польоту 22,7 тис. км, (наприклад, цього достатньо для того, щоб із Нью-Йорку долетіти до Києва, повернутися і знову долетіти до Києва).

РЛС із синтезованою апертурою дає змогу йому «бачити» цілі на землі навіть через хмари. Відомо, що у старих версіях дрона цей радар давав чітку картинку із роздільною здатністю до 1 метра на відстані у 100 км.

Також RQ-4 Global Hawk вміє «слухати», точніше, вести радіотехнічну розвідку, коли не тільки фіксується та перехоплюється радіовипромінювання ворога, а й встановлюються точні координати випромінювання. Це дає змогу локалізувати штаби, центри зв'язку, командні пункти, викрити позиції протиповітряної оборони тощо. Дальність роботи такої системи фактично становить понад півтисячі кілометрів.

США з 2014 року використовують RQ-4 Global Hawk у небі або поряд з Україною. На рівні 2020 року БПЛА в середньому прилітав у небо України від одного до чотирьох разів на місяць.

Global Hawk за кілька місяців до повномасштабного вторгнення РФ стали проводити моніторинг все частіше. У лютому польоти цих БПЛА стали майже щоденним явищем і проходили разом з іншими, вже пілотованими літаками-розвідниками. Зокрема, 23 лютого 2022 р. Global Hawk провів моніторинг усіх напрямів майбутніх ударів армії РФ, включно із територією Білорусі.

Після 24 лютого 2022 р. дрони не припинили роботу, зосередившись на моніторингу акваторії Чорного моря та Білорусі. І США не роблять із польотів RQ-4 Global Hawk, щонайменше щодо деяких із них, таємниці. Польоти здійснюються з транспондером, який передає інформацію про координати БПЛА, його швидкість та висоту.

Польоти Global Hawk – далеко не дешеве задоволення, одна година його перебування у повітрі коштує приблизно 18,5 тис. доларів. Орієнтовна вартість RQ-4 Global Hawk становить приблизно 130 млн доларів.

Характеристики RQ-4 Global Hawk:

Розмах крил: 39,8 м.

Довжина: 14,5 м.

Максимальна злітна вага: 14 628 кг.

Корисне навантаження: 1 360 кг.

Швидкість: 574 км/год.

Дальність: 22 700 км.

Автономність: більше 34 год.

Висота польоту: 18 288 м.

Наземна розвідувальна радіолокаційна станція СНАР-10М1 призначена для розвідки рухомих наземних цілей – колон різної техніки, живої сили, а також здатна фіксувати літальні апарати на малій висоті, засікати техніку, живу силу противника, розриви артилерійських снарядів залежно від відстані, а також помічати танки на відстані до 35–40 км, здатна помітити навіть окрему людину на відстані 15 км (рис. 2.3).

Рисунок 2.3. Наземна розвідувальна радіолокаційна станція СНАР-10М1

48Я6-К1 «Підліт» – універсальна мобільна трикоординатна радіолокаційна станція кругового огляду і виявлення повітряних цілей на малих і гранично малих висотах у складній завадовій обстановці (рис. 2.4).

Рисунок 2.4. Радіолокаційна станція РФ 48Я6-К1 «Підліт»

Комплекс призначений для видачі цілевказівки для ЗРК С-300, С-400 і їм подібних. Перші поставки РЛС «Підліт-К1» у війська ППО росії були розпочаті в 2015 році.

Оснащені такими РЛС зенітні ракетні комплекси виявились ефективним засобом закриття неба від українських літаків. Найбільша відстань ураження укра-

їнського літака, що летів на надмалій висоті – менше 15 м над землею, становить приблизно 150 км.

Цілодобове відеоспостереження на віддалених рубежах:

– дальнє відеоспостереження 24 години на добу;

– дальність виявлення людини до 10 км;

– автономне електроживлення комплексу на основі енергії сонця та вітру;

– автоматичне виявлення рухомих цілей за допомогою радіолокатора;

– спільна робота з охоронними сповіщувачами.

Автономний пост технічного спостереження «Аванпост» призначений для організації охорони та інтелектуального відеоспостереження на великих відкритих просторах та рубежах державного кордону (рис. 2.5).

Рисунок 2.5. Автономний пост технічного спостереження «Аванпост»

Комплекс забезпечує цілодобовий візуальний контроль за наземною та надводною обстановкою з виявленням нерухомих і рухомих цілей різних типів на відстанях до 10 км. Дає змогу відображати та архівувати відеоінформацію та тривожні події в реальному часі.

Гідроакустична розвідка

Гідроакустична розвідка (ГАР) призначена для отримання інформації шляхом приймання та аналізу акустичних сигналів інфразвукового, звукового та ультразвукового діапазонів, що поширюються у водному середовищі від надводних та підводних об’єктів. За принципом використання енергії акустичного випромінювання засоби ГАР поділяються на активні (гідролокатори) та пасивні. Гідролокатор працює за принципом випромінювання у водному середовищі зондуючих акустичних сигналів з наступним прийманням та аналізом відбитих від об’єктів та морського дна ехосигналів.

Під час ведення пасивної ГАР використовують шумопеленгатори, які приймають і аналізують шумові акустичні випромінювання у водному середовищі, що виникають під час роботи двигунів, гребних валів, машин і механізмів різних

агрегатів надводних кораблів (НК), підводних човнів (ПЛ) та інших плавзасобів, а також засоби розвідки, призначені для прийому та аналізу акустичних сигналів, створюваних гідролокаторами, ехолотами, системами гідроакустичного зв'язку тощо.

ГАР вирішує такі основні завдання визначення параметрів:

– первинних шумових полів об'єктів, що функціонують у водному середовищі, з метою виявлення їх класифікаційних ознак;

– випромінювання активних гідроакустичних засобів (ГАС) кораблів мінно-торпедної зброї та засобів гідроакустичного придушення з метою отримання даних, необхідних для організації гідроакустичного придушення;

– рівня розвитку гідроакустичної техніки, виявлення профілю ВПО і напрямів робіт, що проводяться в прибережних районах;

– гідролокаційних характеристик підводного човна, ПК, мінно-торпедного озброєння;

ГПР забезпечує:

– перехоплення інформації, що передається каналами гідроакустичного зв'язку;

– картографування рельєфу дна на підходах до узбережжя, проток та фарватерів, військово-морських баз, а також виявлення місць встановлення та елементів конструкцій підводних стаціонарних споруд;

– виявлення дислокації та маршрутів переміщення об'єктів ВМС за їх шумовими полями та сигналами активних ГАС;

– виявлення підводних стартів ракет і торпед, визначення їх місць, глибини і кількості.

У гідролокаторах і шумопеленгаторах приймання корисних сигналів відбувається на тлі гідроакустичних перешкод різного походження. До того ж, під час роботи гідроакустичної апаратури існують складні взаємозв'язки.

Акустична розвідка

Під акустичною розвідкою розуміється отримання інформації шляхом приймання та аналізу акустичних сигналів інфразвукового, звукового, ультразвукового діапазонів, що поширюються в повітряному середовищі від об'єктів розвідки. Акустична розвідка (АР) забезпечує отримання інформації, що міститься безпосередньо у вимовному або відтворюваному мовленні (акустична мовна розвідка), а також у параметрах акустичних сигналів, супутніх роботі озброєння і військової техніки, механічних пристроїв оргтехніки та інших технічних систем (акустична сигнальна розвідка).

АР вирішує такі завдання:

− дистанційне перехоплення смислової мовної інформації;

− визначення технічних та тактичних характеристик озброєння (О) та військової техніки (ВТ) (оцінка потужності вибухів боєприпасів та вибухових речовин під час випробувань, визначення параметрів авіаційних та ракетних двигунів під час стендових випробувань тощо);

− визначення характеру та спрямованості робіт на військово-промислових об’єктах;

− визначення шумових сигнатур О та ВТ.

Для вирішення зазначених завдань АР використовує портативну апаратуру приймання та реєстрації акустичних сигналів та стаціонарну апаратуру їх обробки та аналізу. Апаратура АР полягає в використанні властивостей середовища передавати звукові коливання.

Можливими каналами витоку інформації можуть бути:

− повітряне середовище, через яке поширюються як мовні сигнали, що виникають під час ведення розмов, так і шумове акустичне випромінювання, що створюється працюючими двигунами, технікою (військовою, озброєнням, вибухами) тощо;

− вібраційні канали, в яких середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалення, каналізація тощо;

− канали акустоелектричного типу, пов’язані з перетворенням акустичних сигналів в електричних елементах різних допоміжних технічних засобів і систем (ДТЗС), наприклад, електромагніти вторинних електрогодинників, дзвінкові ланцюги телефонних апаратів, трансляційні динаміки;

− канали оптико-акустичного типу, в яких за допомогою зондувального лазерного променя здійснюється знімання інформації з вібруючих в акустичному полі тонких поверхонь, що відбивають (віконного скла, предметів інтер’єру, картин, дзеркал).

Радіаційна розвідка

Під радіаційною розвідкою (РДР) розуміють процес отримання інформації внаслідок аналізу радіоактивних випромінювань, пов’язаних із викидами і відходами атомного виробництва, зберіганням і транспортуванням матеріалів, що розщеплюються, ядерних зарядів і боєприпасів, виробництвом і експлуатацією реакторів, двигунів і радіоактивним зараженням місцевості.

З допомогою РДР визначають:

− характеристики доз радіоактивного випромінювання навколо об’єкта розвідки та їх зміни у часі;

− маршрути перевезення джерел радіоактивних випромінювань;

− райони з підвищеним рівнем радіації;

− джерела радіоактивних випромінювань у транспортному засобі;

− вміст окремих видів ізотопів у навколишньому середовищі (ґрунті, повітрі, природних та промислових водоймах);

− ізотопний склад випромінювачів, типи джерел випромінювання і навіть дозиметричний контроль атмосфери Землі.

Хімічна розвідка

Хімічна розвідка (ХР) – добування інформації шляхом контактного або дистанційного аналізу зміни хімічних властивостей складу навколишнього середовища під впливом викидів і відходів виробництва, роботи двигунів, внаслідок вибухів і пострілів, навмисного розсіювання хімічних речовин, випробувань і застосувань хімічної зброї.

ХР вирішує такі основні завдання:

− виявлення та аналіз хімічного складу навколишнього середовища з метою визначення дислокацій підприємств з виробництва хімічної продукції військового призначення;

− вимірювання концентрації хімічних речовин у повітрі з метою визначення профілю виробництва, проведених наукових досліджень та випробувань, а також характеристик хімічного виробництва, військової техніки та її елементів (палива, вибухових речовин тощо);

− отримання інформації про хімічне зараження місцевості в умовах можливого застосування хімічної зброї;

− контроль хімічного складу навколишнього середовища на підприємствах хімічної промисловості для забезпечення безпеки персоналу.

ХР ведеться за допомогою апаратури, яка використовує як методи дистанційного аналізу (дистанційна ХР), так і аналізу проб (контактна ХР).

До апаратури дистанційної ХР належать: лідари, радіометри, ІЧ-спектрометри. Апаратура контактного аналізу включає газоаналізатори, газосигналізатори, пробовідбірні пристрої тощо.

Апаратура дистанційної ХР використовує принципи активної чи пасивної оптичної локації. Прикладом апаратури, що використовує принципи активної локації, є лідар. Хімічні речовини в атмосфері виявляють шляхом зондування її імпульсами лазерного випромінювання та реєстрації ефектів взаємодії лазерного випромінювання з речовиною.

Радіометри використовують принцип пасивної оптичної локації. Вони виявляють речовини за їх тепловим випромінюванням.

ІЧ-спектрометри також виявляють речовини шляхом аналізу спектрального складу власного випромінювання речовини або перевідбитого речовиною випромінювання природного джерела (Сонця).

Застосування приладів локальної дії та пристроїв для відбору проб дає змогу визначити хімічний склад речовин у районі розвідки або в лабораторії після відбору проби та її доставки до місця обробки.

Апаратура ХР може встановлюватися на космічних апаратах (КА), ракетах, літаках, вертольотах, кораблях, автомобілях, а також використовуватися в портативному варіанті.

Сейсмічна розвідка

Сейсмічна розвідка (СР) призначена для добування інформації шляхом виявлення та аналізу деформаційних та зсувних полів у земній поверхні, що виникають під впливом різних вибухів.

Основний напрям СР – розвідка ядерних вибухів та визначення їх параметрів. СР визначає:

– координати епіцентру вибуху;

– потужність та час вибуху;

– кількість вибухів у групі.

Сейсмічний метод виявлення та ідентифікації ядерних вибухів отримав загальне визнання як один із основних, крім вибухів, що створені у космосі та у повітрі на великих висотах (понад кілька десятків кілометрів). Сейсмічний метод застосовний для виявлення ядерних вибухів як на малих, так і на великих епіцентральних відстанях, що досягають 16 000–17 000 км. Особливо ефективний цей метод під час виявлення та ідентифікації підземних та підводних ядерних вибухів. Для виявлення та ідентифікації підземних вибухів, що здійснюються з повним камуфлетом, він поки є єдиним.

Під терміном виявлення розуміється встановлення за сейсмічними даними факту та часу виникнення сейсмічного явища, координат епіцентру та визначення його енергії (або магнітуди).

Під терміном ідентифікація розуміється встановлення сукупності характеристик зареєстрованих сейсмічних хвиль явища: землетрусу, підземного, підводного, контактного чи повітряного ядерного вибуху.

Під час виявлення ядерних вибухів сейсмічним методом найбільш складним є виявлення та ідентифікація підземних.

На відміну від інших видів ядерних вибухів, що повністю приховані (камуфлетних – підземних вибухів на великих епіцентральних відстанях), не вдається отримати безперечних доказів – виявити радіоактивні продукти. Сейсмічний метод наразі є єдиним методом виявлення та ідентифікації. Ідентифікація проводиться за сейсмічними записами і ґрунтується на відмінностях у динамічних характеристиках сейсмічних хвиль вибухів і землетрусів. Ці відмінності-критерії пов’язані з різним характером джерел сейсмічних коливань під час вибухів і землетрусів.

Сейсмічна розвідка є складною динамічною системою. У ній відбуваються процеси перетворення енергії та інформації, найважливішими з яких є збудження сейсмічним джерелом первинних хвиль, поширення їх у геологічному середовищі

з утворенням на неоднорідностях вторинних хвиль, приймання та запис пружних коливань у точках спостереження, обробка та інтерпретація сейсмічних записів.

Магнітометрична розвідка

Магнітометрична розвідка (ММР) призначена для добування інформації шляхом виявлення та аналізу локальних змін магнітного поля Землі під впливом об'єктів з великою магнітною масою.

ММР вирішує такі завдання:

− виявлення та визначення об'єктів, що знаходяться на землі, у землі та у водному середовищі;

− визначення «магнітних портретів» об'єктів та проведення їх класифікації.

Основним джерелом інформації засобів ММР є локальні зміни магнітного поля.

Вимірювально-сигнатурна розвідка

Новий напрям в американській технічній розвідці – система МАСИНТ (MASINT – Measurement And Signature INTelligence). Метою спостереження є об'єкт. Система МАСИНТ є багатоспрямованою, це найбільш інформативний напрям технічної розвідки. Вона дає змогу повніше реалізувати найважливіший принцип комплексності ведення технічної розвідки.

Відповідно ідеологія та цілі цього напряму технічної розвідки формулюються так: вимірювально-сигнатурна розвідка ведеться в інтересах забезпечення успіху військових операцій збройних сил, створення нових поколінь озброєння та військової техніки, визначення напрямів модернізації збройних сил, контролю над поширенням зброї, довкіллям і навіть виконанням військових договорів.

Сутність розвідки МАСИНТ полягає у комплексному характері збирання розвідувальної інформації:

– вимірювання геометричних розмірів і співвідношень статичних, динамічних та інших фізичних характеристик розвідуваних об'єктів (стаціонарних та рухомих);

– реєстрація сигнатур характерних фізичних полів, створюваних цими об'єктами (електромагнітних, магнітних, радіаційних, акустичних, сейсмічних та інших);

– виявлення хімічних та біологічних агентів і навіть складу конструкційних матеріалів об'єктів та їх елементів.

Для ведення розвідувальних заходів використовуються всі наявні датчики: оптичні, радіолокаційні, лазерні, радіочастотні, акустичні, сейсмічні, радіаційні, хімічні, оптико-електронної та радіолокаційної зйомки з перекриттям практично всього спектра електромагнітних коливань.

Варто мати на увазі, що фізичні вимірювання та зняття сигнатур не є самоціллю розвідки МАСИНТ. Головне в ній – виявлення призначення, тактики за-

стосування, можливостей та основних характеристик, а також вразливих місць розвідуваного об'єкта.

Наприклад, якщо розроблено корабельне тактичне лазерне озброєння для ППО, вимірювально-сигнатурна розвідка повинна буде насамперед розкрити, що це – лазерна зброя, далі тип лазера і вид накачування, довжину хвилі і режими випромінювання, потужність і ширину розбіжності променя (довжину когерентності), скорострільність, спосіб корекції хвильового фронту в атмосфері, ширину спектра огляду в просторі, швидкість сканування, принцип пошуку цілей та наведення, вразливість озброєння.

Захист об'єктів інформаційної діяльності (ОІД), на яких циркулює / обробляється інформація, що відповідно до законодавства України підлягає захисту від засобів технічної розвідки (ЗТР), являє собою сукупність організаційних та технічних заходів, що проводяться з метою виключення або суттєвого унеможливлення добування за допомогою ЗТР відомостей про:

– інформацію, що обробляється на ОІД;
– озброєння;
– військову техніку та військово-промислові об'єкти;
– створення хибних уявлень про них.

Під час здійснення заходів щодо захисту ОІД керуються певними принципами, дотримання яких забезпечує вирішення поставлених завдань захисту з максимальною ефективністю та мінімальною вартістю.

Усе різноманіття завдань захисту об'єктів від ЗТР можна звести до трьох типових задач:

– приховування об'єктів, що захищаються, або їх елементів від виявлення ЗТР;

– виключення можливості вимірювання (або зниження точності вимірювань) значень характеристик об'єктів, що приховуються;

– унеможливлення (або утруднення) розпізнавання об'єктів (або їх елементів) ЗТР, що приховуються.

Вирішення завдань захисту від ЗТР здійснюється шляхом застосування різних способів захисту. Залежно від характеру розв'язуваних завдань захисту об'єктів від ЗТР застосовуються способи приховування і дезінформації.

Приховування включає пасивний захист, активний захист і спецзахист.

Пасивне приховування повинно виключати або суттєво ускладнювати виявлення та визначення характеристик об'єктів розвідки шляхом усунення або ослаблення їх демаскуючих ознак. Воно забезпечується проведенням організаційних та технічних заходів (застосуванням технічних засобів).

До організаційних заходів належать:

– запровадження територіальних, просторових, часових, енергетичних та частотних обмежень на використання та режими роботи об’єктів, що приховуються, та їх елементів;

– використання маскуючих (екрануючих) властивостей місцевості та місцевих предметів, гідрологічних і гідроакустичних умов, метеоумов та часу доби, що обмежують можливості ведення технічної розвідки;

– виключення випадків зберігання та складування техніки, що приховується, та її елементів на відкритих майданчиках (Чорнобаївка);

– складання спеціальних схем перевезень техніки, що приховується, та їх елементів;

– встановлення меж територій, що охороняються (контрольованих зон);

– своєчасне оповіщення ОІД та полігонів про дії технічних розвідок.

До технічних заходів захисту належать:

– технічні рішення, що забезпечують зниження контрастності об’єктів за різними фізичними полями щодо відповідного фону;

– технічні рішення, що забезпечують зниження рівня різних випромінювань та акустичних шумів об’єктів, що приховуються;

– використання маскуючих поглинаючих та відбивних (розсіюючих) покриттів, штучних масок, навісів, екранів, поглинаючих насадок, екрануючих та безехових споруд;

– фарбування об’єктів, що приховуються (в тони, відповідні місцевості та пори року, радіопоглинаючі покриття);

– створення аерозольних, водяних, пухирцевих та вибухових завіс;

– застосування для налаштування та перевірки функціонування об’єктів імітаторів, вбудованої апаратури, екранованих приміщень та камер, закритих водойм (для гідроакустичних засобів);

– зменшення в атмосфері, природних водоймах, земній корі концентрації компонентів продуктів функціонування об’єктів, що приховуються, та їх елементів (хімічна, радіаційна розвідки).

Активне приховування передбачає застосування:

– засобів створення помилкової обстановки;

– активних та пасивних завад із різними фізичними полями (електромагнітні, акустичні, радіаційні, сейсмічні, гідроакустичні тощо).

На етапі розробки зразків продукції, що приховується, та її елементів (озброєння та військової техніки) активне приховування дає змогу приховати залишкові випромінювання різних фізичних полів, а на етапі випробувань захистити інформацію, що передається, комунікаційними каналами (радіо-, радіорелейного зв’язку, телеметрії) від зовнішньотраєкторних вимірювань.

Активні засоби приховування застосовуються в основному як додатковий захід до пасивних засобів приховування (найбільш доцільних), коли останні не забезпечують необхідного зменшення рівня демаскуючих ознак (випромінювань, що маскуються).

Спеціальний захист полягає у:

– застосуванні апаратурних, криптографічних і програмних засобів та способів захисту;

– встановленні спеціальних правил використання інформації;

– проведенні організаційних та технічних заходів, що виключають можливість перехоплення інформації шляхом несанкціонованого доступу або за допомогою ЗТР.

Дезінформація передбачає:

– технічну дезінформацію;

– імітацію;

– легендування.

Технічна дезінформація полягає у створенні умов, що виключають або істотно ускладнюють достовірне розпізнавання противником за допомогою ЗТР об’єктів, що приховуються, характеру і змісту проведених спеціальних робіт.

Технічна дезінформація забезпечується шляхом:

– створення хибних об’єктів, хибної обстановки щодо випромінюваних фізичних полів;

– відтворення на зразках техніки, що захищаються (озброєння), демаскуючих ознак, властивих застарілим зразкам, або зразкам, що не мають істотної цінності;

– порушення (спотворення) звичного для противника поєднання характерних ознак, властивих певним класам, типам, зразкам (озброєння та військової техніки або їх елементів).

Технічна дезінформація може застосовуватися як на етапах розробки та створення спеціальної техніки, так і на етапах їх випробувань, коли використання способів приховування складне або неможливе.

Імітація – елемент технічної дезінформації, що полягає у відтворенні демаскуючих ознак об’єкта прикриття шляхом реалізації планувальних, об’ємно-планувальних, архітектурних і конструкційних рішень, а також у застосуванні технічних засобів імітації (макетів техніки, помилкових споруд, різних імітаторів).

Легендування полягає в навмисному створенні умов, за яких у поєднанні з іншими можливими способами захисту переконливо забезпечується хибне уявлення про об’єкти, що приховуються, і характер виконуваних робіт. Водночас наявність об’єктів і спрямованість робіт повністю не приховується, а маскується дійсне призначення об’єктів і характер робіт, що проводяться шляхом навмисного показу та застосування іншої або застарілої техніки.

Захист від візуальних і фотографічних – оптичних ЗТР

Заходи захисту від оптичних засобів розвідки ґрунтуються на зміні обсягу та змісту інформації, що надходить до розвідувального засобу від фону та об'єктів, що приховуються. Ці заходи повинні проводитися цілеспрямовано для отримання необхідного маскувального ефекту, який оцінюється зниженням ймовірності правильного вирішення завдань розвідкою противника. Чим якісніше проведені заходи щодо приховування об'єкта, тим менша ймовірність його виявлення та розпізнавання, тим вищий маскувальний ефект.

Для приховування об'єкта від візуально-оптичної розвідки противника можуть застосовуватися такі заходи:

– екранування об'єкта, що усуває його пряму видимість із боку противника;

– зниження його видимості до порогу виявлення;

– імітація під місцевий чи другорядний об'єкт.

Усунення прямої видимості з боку противника досягається під час розміщення об'єкта, що приховується, за складками рельєфу, лісовими масивами, будівлями, місцевими предметами, а також під час використання природних і штучних хмар, туману, димових завіс.

Зниження рівня видимості об'єктів, що маскуються, до порогу виявлення досягається шляхом зменшення яскравого контрасту і колірних відмінностей між об'єктом і фоном, а також збільшення порогового контрасту.

Яскравий контраст об'єкта з фоном можна знизити такими шляхами:

– зменшенням відмінностей між коефіцієнтами яскравості поверхонь об'єктів та природних фонів;

– екрануванням об'єктів матеріалами, що просвічують, розсіюють падаюче на них випромінювання, як розріджені сітчасті тканини або маскувальні покриття на мережевій основі із несуцільним заповненням;

– зменшенням інтенсивності тіней.

Усунення або зниження колірного розмаїття між об'єктом і фоном досягається застосуванням маскувального фарбування, а також використанням маскувальних матеріалів, які краще відповідають навколишньому фону за кольором та своїми спектральними характеристиками у видимій частині спектру (0,38–0,75 мкм).

Збільшення порогового розмаїття досягається такими способами:

– зменшенням геометричних розмірів об'єктів і тіней від них;

– зміною геометричної форми об'єктів із переходом, за можливості, від протяжних форм до компактних;

– використанням видових властивостей місцевості, наприклад, строкатих фонів, що дають збільшення порогового контрасту виявлення, порівняно з монохромними тонами.

Щоб ускладнити розпізнавання об’єктів, необхідно знижувати їх видимість до порога розпізнавання.

Існує й інший шлях протидії вирішення розвідувального завдання. Необхідно так змінити сигнали, що надходять від об’єкта і фону, щоб утворювалися ознаки, невластиві об’єкту, який приховується. Під час приховування об’єкта це мають бути ознаки місцевого предмета або другорядного об’єкта, а під час імітації – ознаки об’єкта, що імітується.

Імітуючі макети та помилкові споруди повинні відтворювати імітовані об’єкти за формою, деталями та розмірами з таким ступенем точності, який визначається роздільною здатністю та стереоскопічним порогом зору, а також використовуваних оптичних приладів. Допуски на відтворення кольору та яскравості об’єктів визначається контрастною чутливістю зору.

У Силах оборони Таврійського напрямку заявили про те, що російська армія на своїх позиціях встановлює гумові танки, щоб Збройні сили України завдавали ударів по хибних позиціях, а не по справжніх бойових машинах.

Вартість одного танка та одного макета незіставні. Це також один зі способів введення в оману, створення ілюзії посилення якогось окремого напрямку і неправдиві дані про кількість озброєння та військової техніки.

Заходи захисту від радіо- та радіотехнічної розвідки (РР, РТР, РЛР) спрямовані на виключення або утруднення виявлення та перехоплення випромінювання радіоелектронних засобів (РЕЗ), утруднення вимірювання параметрів сигналу, виділення смислової інформації та визначення ТТХ. Для захисту від РР та РТР застосовуються всі загальні організаційні заходи.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ

Завдання 1. Підготувати доповідь на тему «Інформаційна агресія та розвідувальна діяльність: як маємо протидіяти таким елементам російської агресії».

Завдання 2. Підготувати глосарій українською та англійською мовами для визначення різновидів інформаційної війни: командно-управлінська; розвідувальна; психологічна; хакерська; економічна; електронна; кібервійна; гібридна війна, основні види наземної розвідки.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Цілі та стратегії інформаційної війни.
2. Які основні способи управління масами?
3. У чому полягає концепція гібридної війни?

4. Навести приклади імітації зразків військової техніки.

5. Назвіть переваги та недоліки лазерної розвідки.

6. Вкажіть основні способи маскування, які треба застосовувати для захисту об’єктів від візуально-оптичних і фотографічних засобів розвідки?

7. Які особливості, обмеження і режими роботи треба враховувати під час захисту від радіоелектронних засобів розвідки?

ТЕМА 3. ПРАВОВА ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ

ТЕОРЕТИЧНІ ВІДОМОСТІ

Україна – правова держава. Тому під час вирішення питань щодо забезпечення національної безпеки і її складника – інформаційної безпеки – ми маємо насамперед керуватись положеннями Законів України в інформаційній сфері.

Правовою основою у сфері забезпечення національної і інформаційної безпеки виступають Конституція України, Закони України, акти Президента України та Кабінету Міністрів України, нормативно-правові акти Служби безпеки України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України, з питань технічного захисту інформації та кіберзахисту.

Основний Закон України – «Конституція України»

Конституція України проголошує: «Кожен має право вільно збирати, зберігати, використовувати та поширювати інформацію будь-яким законним способом (ч. 1 ст. 34).

Кожен має право на недоторканність приватного життя, особисту та сімейну таємницю (ч. 1 ст. 32).

Захист конституційних прав на недоторканність приватного життя, особисту та сімейну таємницю регулюються Законом України «Про захист персональних даних».

Ніким не може бути засекречена інформація про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення (ст. 50).

Усі громадяни мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, що передбачає рівний доступ до державних інформаційних ресурсів, за винятком інформації, що відноситься до державної таємниці (ст. 40).

Конституції України забороняє цензуру та на законодавчому рівні визнає свободу масової інформації, що прямим чином пов'язано з правом на доступ до інформації (ст. 15).

Ряд принципових положень, що стосуються гарантій інформаційної безпеки і на законодавчому рівні задекларовані Конституцією України:

– права і свободи людини і громадянина захищаються судом;

– кожен має право на повагу до його гідності;

– кожен має право на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень (обмеження цього права допускається лише на підставі судового рішення);

– не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом;

– органи державної влади та органи місцевого самоврядування, установи і організації, їх посадові особи зобов'язані забезпечити кожному можливість ознайомлення з документами і матеріалами, що безпосередньо зачіпають його права і свободи, відомостями про себе, якщо інше не передбачено законом;

– кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації;

– інтелектуальна власність охороняється законом (ст. 54).

Проте в умовах воєнного та надзвичайного стану для забезпечення безпеки громадян і захисту конституційного ладу відповідно до конституційного закону можуть встановлюватися окремі обмеження прав і свобод із зазначенням терміну їх дії.

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»

Державна служба спеціального зв'язку та захисту інформації України – це державний орган, який призначений для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону, і спрямовує свою діяльність на забезпечення національної безпеки України від зовнішніх і внутрішніх загроз та є складником сектору безпеки й оборони України.

Основними завданнями Державної служби спеціального зв'язку та захисту інформації України є:

– формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі – інформаційно-телекомунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів у частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку;

– участь у формуванні та реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), електронних довірчих послуг (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг);

– забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

Закон України «Про інформацію»

Основними принципами інформаційних відносин є:

- гарантованість права на інформацію;
- відкритість, доступність інформації, свобода обміну інформацією;
- достовірність і повнота інформації;
- свобода вираження поглядів і переконань;
- правомірність одержання, використання, поширення, зберігання та захисту інформації;
- захищеність особи від втручання в її особисте та сімейне життя.

Основні напрями державної інформаційної політики:

- забезпечення доступу кожного до інформації;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
- створення умов для формування в Україні інформаційного суспільства;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
- створення інформаційних систем і мереж інформації, розвиток електронного урядування;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- забезпечення інформаційної безпеки України;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Закон визначає: право на інформацію, гарантії права на інформацію, порядок охорони права на інформацію, мову інформації, основні види інформаційної діяльності.

Види інформації за змістом: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля.

За порядком доступу інформація поділяється на: відкриту інформацію; інформацію з обмеженим доступом. Інформація з обмеженим доступом: конфіденційна, таємна та службова інформація.

Закон України «Про захист інформації в інформаційно-комунікаційних системах»

Цей Закон регулює відносини у сфері захисту інформації в інформаційних, комунікаційних та інформаційно-комунікаційних системах (далі – система).

Об'єкти захисту в системі – інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.

Підтвердження відповідності комплексної системи захисту інформації здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

Підтвердження відповідності та проведення державної експертизи засобів технічного і криптографічного захисту інформації здійснюються в порядку, встановленому законодавством.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації, та засоби технічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері технічного захисту інформації або сертифікат відповідності, виданий органом з оцінки відповідності.

Забезпечення захисту інформації в системі покладається на власника системи. Особливості захисту інформації в системах, які забезпечують банківську діяльність, встановлюються Національним банком України.

Закон України «Про захист інформації в комунікаційних системах»

Закон адаптує українське законодавство до вимог ЄС у сфері захисту інформації. Верховна Рада ухвалила Закон щодо підтвердження відповідності інформаційної системи вимогам із захисту інформації.

Зміни до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» стосуються підтвердження відповідності інформаційної системи вимогам із захисту інформації ЄС. Так впроваджуються вимоги стандар-

тів сімейства системи управління інформаційною безпекою (СУІБ) для окремих категорій інформації. Ці вимоги діють для забезпечення інформаційної та кібербезпеки в ЄС і наближують Україну до європейських норм.

За Законом, підтвердження відповідності комплексної системи захисту інформації (КСЗІ) відбуватиметься за результатами держекспертизи.

Зміни до Закону передбачають, що державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, може оброблятися в системі без застосування КСЗІ, у разі виконання умов:

1) підтвердження відповідності системи управління інформаційною безпекою національним стандартам України щодо систем управління інформаційною безпекою;

2) використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи;

3) жоден з елементів системи не може бути розташований на території України, де органи державної влади тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції», та на територіях держав, які належать до митних союзів з такими державами;

4) виконання особливих вимог, встановлених Урядом до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Схвалений закон запроваджує альтернативний спосіб підтвердження відповідності інформаційної системи вимогам із захисту інформації.

Закон України «Про державну таємницю»

Цей Закон регулює суспільні відносини, пов’язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України. Дія цього Закону поширюється на органи законодавчої, виконавчої та судової влади, органи прокуратури України, інші державні органи.

Державну політику щодо державної таємниці як складову засад внутрішньої та зовнішньої політики визначає Верховна Рада України.

Президент України, забезпечуючи національну безпеку, видає укази та розпорядження з питань охорони державної таємниці, віднесених цим Законом та іншими законами до його повноважень.

Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сфері охорони державної таємниці.

Кабінет Міністрів України спрямовує та координує роботу міністерств, інших органів виконавчої влади щодо забезпечення здійснення державної політики у сфері охорони державної таємниці.

Спеціально уповноваженим державним органом у сфері забезпечення охорони державної таємниці є Служба безпеки України.

Забезпечення охорони державної таємниці відповідно до вимог режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях, діяльність яких пов'язана з державною таємницею, покладається на керівників зазначених органів, підприємств, установ і організацій.

До державної таємниці у порядку, встановленому цим Законом, відноситься інформація у сферах: оборони; економіки, науки і техніки; зовнішніх відносин; державної безпеки та охорони правопорядку.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності «особливої важливості», «цілком таємно» та «таємно» лише за умови, що вони належать до категорій, зазначених у частині першій цієї статті, і їх розголошення завдаватиме шкоди інтересам національної безпеки України та з дотриманням вимог статті 6 Закону України «Про доступ до публічної інформації».

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Засекречуванню підлягає інформація, а не документ. Якщо документ містить державну таємницю, то для ознайомлення може надаватися інформація, доступ до якої не обмежений. Засекречування матеріальних носіїв інформації здійснюється шляхом надання на підставі Зводу відомостей, що становлять державну таємницю (розгорнутих переліків відомостей, що становлять державну таємницю), відповідному документу, виробу або іншому матеріальному носію інформації грифа секретності посадовою особою, яка готує або створює документ, виріб або інший матеріальний носій інформації.

Оперативно-розшукові заходи щодо охорони державної таємниці здійснюються відповідно до Закону України «Про оперативно-розшукову діяльність».

Керівники державних органів, органів місцевого самоврядування, підприємств, установ і організацій зобов'язані здійснювати постійний контроль за забезпеченням охорони державної таємниці.

Закон України «Про захист персональних даних»

Цей Закон: регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з

обробкою персональних даних; поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Законодавство про захист персональних даних складають Конституція України, цей Закон, інші закони та підзаконні нормативно-правові акти, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України.

Персональні дані можуть бути віднесені до конфіденційної інформації про особу законом або відповідною особою. Не є конфіденційною інформацією персональні дані, що стосуються здійснення особою, уповноваженою на виконання функцій держави або місцевого самоврядування, посадових або службових повноважень.

Персональні дані, зазначені у декларації особи, уповноваженої на виконання функцій держави або місцевого самоврядування, оформленій за формою, визначеною відповідно до Закону України «Про запобігання корупції», не належать до інформації з обмеженим доступом, крім відомостей, визначених Законом України «Про запобігання корупції».

Не належить до інформації з обмеженим доступом інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, крім випадків, передбачених статтею 6 Закону України «Про доступ до публічної інформації».

Законом може бути заборонено віднесення інших відомостей, що є персональними даними, до інформації з обмеженим доступом.

Ст. 6 Закону визначає загальні вимоги до обробки персональних даних.

Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, та відповідати законодавству про захист персональних даних. Обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки.

Склад та зміст персональних даних мають бути відповідними, адекватними. Первинними джерелами відомостей про фізичну особу є: видані на її ім'я документи; підписані нею документи; відомості, які особа надає про себе.

Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.

Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних, обробляти персональні дані без його згоди можна до часу, коли отримання згоди стане можливим.

Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися.

Подальша обробка персональних даних в історичних, статистичних чи наукових цілях може здійснюватися за умови забезпечення їх належного захисту.

Контроль за додержанням законодавства про захист персональних даних у межах повноважень, передбачених законом, здійснюють такі органи: Уповноважений; суди.

Закон України «Про доступ до публічної інформації»

Цей Закон визначає порядок здійснення та забезпечення права кожного на доступ до інформації, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом, та інформації, що становить суспільний інтерес.

Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом. Публічна інформація є відкритою, крім випадків, встановлених законом.

Метою цього Закону є забезпечення прозорості та відкритості суб'єктів владних повноважень і створення механізмів реалізації права кожного на доступ до публічної інформації.

Закон України «Про основи національної безпеки України»

Цей Закон відповідно до пункту 17 частини першої статті 92 Конституції України визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Правову основу у сфері національної безпеки України становлять Конституція, цей та інші закони України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, а також видані на виконання законів інші нормативно-правові акти.

Основними принципами забезпечення національної безпеки є: пріоритет прав і свобод людини і громадянина; верховенство права; пріоритет договірних (мирних) засобів у розв'язанні конфліктів; своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам; чітке розмежу-

вання повноважень та взаємодія органів державної влади у забезпеченні національної безпеки; демократичний цивільний контроль над воєнною організацією держави та іншими структурами в системі національної безпеки; використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки.

Загрози національним інтересам і національній безпеці України за сферами: у зовнішньополітичній сфері; у сфері державної безпеки; у воєнній сфері та сфері безпеки державного кордону України; у внутрішньополітичній сфері; в економічній сфері; у соціальній та гуманітарній сферах; у науково-технологічній сфері; у сфері цивільного захисту; в екологічній сфері; в інформаційній сфері.

Повноваження суб'єктів забезпечення національної безпеки

Відповідно до Конституції і законів України:

– Президент України як глава держави, гарант державного суверенітету, територіальної цілісності України, додержання Конституції України, прав і свобод людини і громадянина, Верховний Головнокомандувач Збройних Сил України і Голова Ради національної безпеки і оборони України здійснює загальне керівництво у сферах національної безпеки та оборони України;

– Верховна Рада України в межах повноважень, визначених Конституцією України, визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного і воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних Сил України та інших військових формувань, створених відповідно до законів України;

– Рада національної безпеки і оборони України координує та контролює діяльність органів виконавчої влади у сферах національної безпеки і оборони; з урахуванням змін у геополітичній обстановці вносить Президенту України пропозиції щодо уточнення Стратегії національної безпеки України, Стратегії кібербезпеки України та Воєнної доктрини України;

– Кабінет Міністрів України як вищий орган у системі органів виконавчої влади забезпечує державний суверенітет і економічну самостійність України, вживає заходів щодо забезпечення прав і свобод людини і громадянина, обороноздатності, національної безпеки України, громадського порядку і боротьби із злочинністю;

– Національний банк України відповідно до основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику в інтересах національної безпеки України;

– Міністерства, інші центральні органи виконавчої влади, Служба безпеки України та Служба зовнішньої розвідки України в межах своїх повноважень за-

безпечують виконання передбачених Конституцією і законами України, актами Президента України, Кабінету Міністрів України завдань, здійснюють реалізацію концепцій, програм у сфері національної безпеки, підтримують у стані готовності до застосування сили та засоби забезпечення національної безпеки;

– місцеві державні адміністрації та органи місцевого самоврядування забезпечують вирішення питань у сфері національної безпеки, віднесених законодавством до їхньої компетенції;

– Воєнна організація держави забезпечує оборону України, захист її суверенітету, територіальної цілісності і недоторканності кордонів; протидіє зовнішнім загрозам воєнного характеру;

– органи і підрозділи цивільного захисту здійснюють заходи щодо захисту населення і територій від надзвичайних ситуацій у мирний час та в особливий період;

– правоохоронні органи ведуть боротьбу із злочинністю і протидіють тероризму;

– суди загальної юрисдикції здійснюють судочинство у справах про злочини, що завдають шкоди національній безпеці України;

– прокуратура України здійснює повноваження у сфері національної безпеки України відповідно до Конституції України та Закону України «Про прокуратуру України»;

– громадяни України через участь у виборах, референдумах та через інші форми безпосередньої демократії, а також через органи державної влади та органи місцевого самоврядування, які вони обирають, реалізують національні інтереси, добровільно і в порядку виконання конституційних обов’язків здійснюють заходи, визначені законодавством України щодо забезпечення її національної безпеки; як безпосередньо, так і через об’єднання громадян привертають увагу суспільних і державних інститутів до небезпечних явищ і процесів у різних сферах життєдіяльності країни; у законний спосіб і законними засобами захищають власні права та інтереси, а також власну безпеку.

Основними функціями суб’єктів забезпечення національної безпеки є:

– розроблення і періодичне уточнення Стратегії національної безпеки України, Стратегії кібербезпеки України і Воєнної доктрини України, доктрин, концепцій, стратегій і програм у сфері національної безпеки, планування і здійснення конкретних заходів щодо протидії і нейтралізації загроз національним інтересам України;

– створення нормативно-правової бази, необхідної для ефективного функціонування системи національної безпеки;

– удосконалення її організаційної структури;

– комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення життєдіяльності складових системи;

– підготовка сил та засобів суб'єктів системи до їх застосування згідно з призначенням;

– постійний моніторинг впливу на національну безпеку процесів, що відбуваються в політичній, соціальній, економічній, екологічній, науково-технологічній, інформаційній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;

– систематичне спостереження за станом і проявами міжнародного та інших видів тероризму;

– прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин їх виникнення та наслідків прояву;

– розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України;

– запобігання та усунення впливу загроз і дестабілізуючих чинників на національні інтереси;

– локалізація, деескалація та врегулювання конфліктів і ліквідація їх наслідків або впливу дестабілізуючих чинників;

– оцінка результативності дій щодо забезпечення національної безпеки та визначення витрат на ці цілі;

– участь у двосторонньому і багатосторонньому співробітництві в галузі безпеки, якщо це відповідає національним інтересам України;

– спільне проведення планових та оперативних заходів у рамках міжнародних організацій та договорів у галузі безпеки.

Контроль за реалізацією заходів у сфері національної безпеки здійснюється відповідно Президентом України, Верховною Радою України, Кабінетом Міністрів України, Радою національної безпеки і оборони України в межах їх повноважень, визначених Конституцією і законами України.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ

Завдання 1. Підготувати глосарій українською та англійською мовами для термінів: державні інформаційні ресурси, об'єкт інформаційної діяльності, система технічного захисту інформації, протидія технічним розвідкам, засіб криптографічного захисту інформації, засіб спеціального зв'язку, спеціальний зв'язок, документ, суб'єкт владних повноважень, відкрита інформація, конфіденційна, таємна та службова інформація, державна таємниця, гриф секретності, блокування інформації в системі, база персональних даних, публічна інформація.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які обов’язки Державної служби спеціального зв’язку та захисту інформації України?

2. На які види поділяється інформація за змістом?

3. На які види поділяється інформація за порядком доступу?

4. Розподіл інформації за ступенем секретності.

5. Назвіть основні принципи забезпечення національної безпеки України.

6. Які загрози національним інтересам і національній безпеці України у зовнішньополітичній сфері?

7. Які загрози національній безпеці в інформаційній сфері?

8. Які основні напрями державної політики з питань національної безпеки?

ТЕМА 4. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ЯК ОБ'ЄКТ ЗАХИСТУ

ТЕОРЕТИЧНІ ВІДОМОСТІ

Інформаційно-комунікаційна система (ІКС) – сукупність інформаційних та комунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Комунікаційна система (КС) – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Інформаційна система (ІС) – взаємозв'язана сукупність засобів, методів і персоналу, використовувана для зберігання, оброблення та видачі інформації з метою вирішення конкретного завдання.

Термін ІС передбачає використання комп'ютера як основного технічного засобу обробки інформації. Комп'ютери, оснащені спеціалізованими програмними засобами, є технічної базою та інструментом ІС.

Виток інформації – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним чи юридичним особам, які не мають права доступу до неї.

За режимом комунікації та за швидкістю мережі можуть бути такі КС:

1) «пункт-пункт» – кожна пара вузлів має взаємозв'язок; цей зв'язок не використовується іншими вузлами;

2) комутована – у мережі «пункт-пункт» необхідна кількість зв'язків зменшена за допомогою комутаторів;

3) широкомовна (багатопунктова) – спільний комунікаційний канал використовується всіма вузлами мережі;

4) низькошвидкісна: швидкості від кбіт/с до Мбіт/с;

5) високошвидкісна: швидкості від сотень Мбіт/с до Гбіт/с.

У більшості мереж КС складається з двох компонентів: передавальних ліній та комутаційних елементів.

Передавальні лінії (вживаються також терміни: кола ~ circuits або канали ~ channels) призначені для транспортування бітів між комп'ютерами.

Комутаційні елементи використовуються для сполучення двох або більше передавальних ліній і зазвичай є спеціалізованими комп'ютерами. Замість терміна «комутаційний елемент» вживають також терміни «вузол комутації пакетів» (packet switch node) або «комутаційний вузол».

Комунікаційна підмережа може бути віднесена до одного з двох типів:

- з каналами типу пункт-пункт (point-to-point);
- з широкомовними каналами (broadcast).

Основні компоненти КС:

- термінали – є вихідними і кінцевими пунктами у будь-якому середовищі телекомунікаційної мережі. Будь-який вхід або вихід пристрою, який використовуються для передачі або прийому даних, може бути класифікований як термінал компонента;
- комунікаційні процесори підтримують передавання і приймання даних між терміналами та комп'ютерами шляхом надання різних функцій керування та допоміжних функцій (наприклад, перетворення даних із цифрового в аналоговий і навпаки);
- комунікаційні канали – шлях, яким дані передаються і приймаються.

Телекомунікаційні канали створюються за допомогою різних фізичних носіїв, із яких найпопулярнішими є мідні дроти, коаксіальні і волоконно-оптичні кабелі.

Волоконно-оптичні кабелі використовуються для більш швидкого і надійного зв'язку для бізнесу та домашніх потреб.

Комп'ютери обробляють інформацію лише в чисельному вигляді. Вся відео-, символьна, звукова, графічна інформація перетворюється у числа. Інформація подається у двійковій системі числення інформації. Дані є складовою частиною інформації, що являють собою зареєстровані сигнали. Під час інформаційного процесу дані перетворюються з одного виду в інший за допомогою певних методів. Обробка даних містить у собі множину різних операцій.

З допомогою програмного забезпечення (ПЗ) здійснюється керування комунікаціями. ПЗ присутнє у всіх комп'ютерах мережі і відповідає за контроль мережевої активності та функціональності. Сьогодні комутаційні центри КС комп'ютеризовані або замінені комп'ютерними мережами.

У кожній комунікаційній мережі можна виділити такі три частини:

- сигналізація – передавання керуючої інформації;
- трафік користувачів мережі – площина даних або площина користувача;
- площина операцій – керування трафіком передавання даних.

Локальна мережа (Local Area Network – LAN) – комунікаційна система даних, яка розміщена у просторово обмеженій області (зазвичай максимальна відстань між робочими станціями не перевищує декількох сотень метрів), має визначені групу користувачів і топологію, не є публічною комутованою комунікаційною мережею, однак може бути сполучена з нею.

У підмережах типу «пункт-пункт» кожна передавальна лінія увімкнена між двома комутаційними елементами. Коли повідомлення або пакет висилається від одного комутаційного елемента до іншого через один або більше проміжних комутаційних вузлів, то цей пакет запам'ятовується після приймання на час, доки звільниться потрібна вихідна лінія. Тоді пакет висилається далі. Такі підмережі

називають також підмережами з буферизацією (store-and-forward) або підмережами з комутацією пакетів. Більшість підмереж WAN належить до цього типу. У такій підмережі, крім комутації пакетів, може використовуватися комутація кіл (каналів). Це типове рішення для підмереж, що використовують традиційну телефонну мережу.

Коли ініціюється сесія зі заданою швидкістю передавання, то створюється фізичне з'єднання між джерелом повідомлення і його призначенням. Швидкість передавання даних не може перевищувати повної інформаційної ємності утвореного каналу зв'язку.

Широкомовна мережа позбавлена процедур маршрутизації (раутингу) – передавання від кожного вузла може бути прийняте усіма іншими вузлами в мережі. Широкомовна мережа має тільки один комунікаційний канал.

Локальні кабельні комп'ютерні мережі – це широкомовні мережі, де кожен користувач сполучений з будь-яким іншим, і мережа має топологію шини, зірки або кільця.

Безпровідні локальні мережі використовують радіо- або оптичні хвилі. Супутникові радіосистеми також є широкомовними – наземна станція в системі може приймати всі повідомлення, які ретранслює сателіт.

У мережах із широкомовними каналами застосовують принцип розсіювання повідомлень. У такій мережі існує тільки один комунікаційний канал, який спільно використовується всіма вузлами. Широкомовна мережа, що використовує радіоканали, в загальному випадку, не має адекватного графічного зображення.

Неодмінна риса широкомовних систем – повідомлення, вислане будь-яким вузлом, досягає всіх інших вузлів. Тому повідомлення обов'язково мусить містити інформацію про те, кому воно адресоване. Пакети, вислані в мережі одним комп'ютером, приймаються усіма іншими, однак перед його опрацюванням кожен комп'ютер перевіряє адресне поле пакету. Якщо пакет не призначений цьому комп'ютеру, він ігнорується. Широкомовні системи мають можливість адресування пакетів до багатьох або всіх можливих призначень шляхом використання спеціального коду в адресному полі пакету. Повідомлення, отримане станцією, для якої воно не призначене, ігнорується цією станцією.

Основні операції інформаційного процесу ІКС

Захист даних – комплекс дій, що скеровані проти порушення конфіденційності, запобігання втрат, несанкціонованого відтворення та модифікації даних.

Транспортування даних – приймання та передавання даних між віддаленими користувачами інформаційного процесу. Джерело даних прийнято називати сервером, а споживача – клієнтом.

Перетворення даних – перетворення даних з однієї форми представлення в іншу, або з однієї структури в іншу, або зміна типу носія.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ

Завдання 1. Підготувати глосарій українською та англійською мовами для визначення понять: комунікаційна система, інформаційна система, інформаційно-комунікаційна система, комунікації (електрозв'язок), комунікаційна мережа, комунікаційна мережа загального користування, комунікаційна мережа доступу, комунікаційна послуга (послуга), телемережі.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Етапи функціонування ІКС.
2. У яких мережах застосовують принцип розсіювання повідомлень?
3. Основні операції інформаційного процесу ІКС.

ТЕМА 5. СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІКС ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ ТЕОРЕТИЧНІ ВІДОМОСТІ

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Об'єктами захисту в системі є інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Суб'єктами відносин, пов'язаних із захистом інформації в системах, є: користувачі; спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (Держспецзв'язку) і підпорядковані йому регіональні органи.

Володілець (власник) інформації – фізична або юридична особа, якій належать права на інформацію. Власник системи – фізична або юридична особа, якій належить право власності на систему. На підставі укладеного договору або за дорученням власник системи може надати право розпоряджатися системою іншій фізичній або юридичній особі – розпоряднику системи.

Порядок доступу до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються володільцем інформації. Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, перелік користувачів та їх повноваження стосовно цієї інформації визначаються законодавством. У випадках, передбачених законом, доступ до інформації в системі може здійснюватися без дозволу її володільця в порядку, встановленому законом.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації в ІКС, або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за станом захисту інформації.

Про спроби та/або факти несанкціонованих дій у системі щодо державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, власник системи повідомляє відповідно спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган. Умови оброблення інформації в системі визначаються власником системи відповідно до договору з володільцем інформації, якщо інше не передбачено законодавством.

Державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із

застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. КСЗІ – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Для створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації.

Підтвердження відповідності та проведення державної експертизи цих засобів здійснюються в порядку, встановленому законодавством.

Захисту в ІКС підлягає:

- відкрита інформація, що належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в інтернеті, інших глобальних інформаційних мережах і системах, або передається комунікаційними мережами (далі – відкрита інформація);
- конфіденційна інформація, що перебуває у володінні розпорядників інформації, визначених частиною першою статті 13 Закону України «Про доступ до публічної інформації»;
- службова інформація;
- інформація, що становить державну або іншу передбачену законом таємницю (таємна інформація);
- інформація, вимога щодо захисту якої встановлена законом.

Основні загрози інформації:

1. Отримання технічними засобами відомостей у сфері оборони, економіки, науки та техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

2. Несанкціонований доступ до інформації, що обробляється та циркулює в ІКС, а також спеціальний вплив на інформацію – спотворення, руйнування, знищення, порушення нормального функціонування систем обробки інформації.

3. Виток інформації з обмеженим доступом технічними каналами унаслідок виникнення побічних електромагнітних випромінювань та наведень, ведення акустичної та оптико-електронної розвідки в безпосередній близькості від об'єкта інформаційної діяльності.

Захист інформації в ІКС (рис. 5.1).

В Україні створена, функціонує та розвивається система ТЗІ, яка є сукупністю організаційних структур, нормативно-правової та матеріально-технічної бази. ТЗІ визначена як частина забезпечення національної безпеки України. Під час оброблення в системі повинна зберігати цілісність, що забезпечується шляхом

захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією.

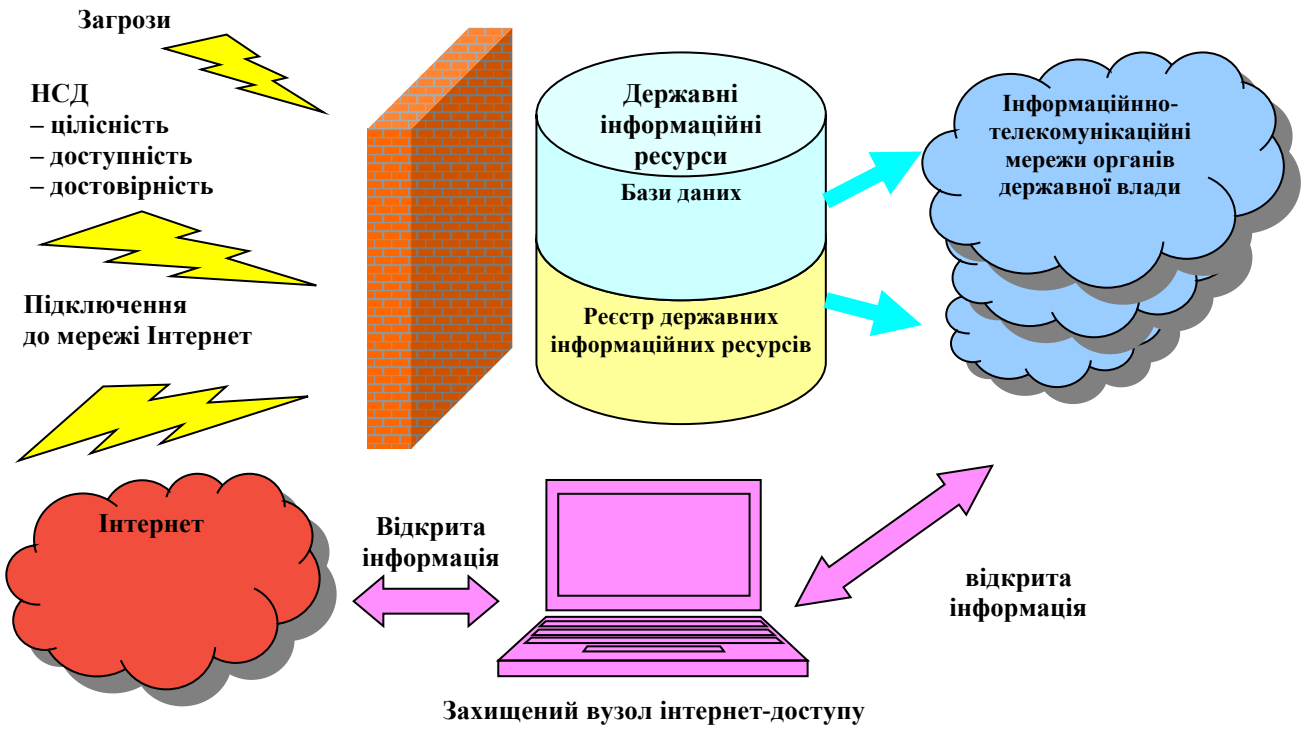

Рисунок 5.1. Захист інформації в ІКС

Модифікувати або знищувати відкриту інформацію в інформаційній (автоматизованій) системі можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора, повинні блокуватися.

Захист інформації в ІКС від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником системи.

В ІКС має здійснюватися контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Контролюється цілісність програмних та технічних засобів захисту інформації.

У разі порушення їх цілісності обробка в системі інформації припиняється.

Під час обробки службової і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

Доступ до службової інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У системі має забезпечуватися можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації, або позбавлення його такого права.

Вимоги до захисту в системі інформації, що становить державну таємницю, визначаються Правилами та законодавством у сфері охорони державної таємниці.

Забезпечення захисту в системі таємної інформації, яка не становить державну таємницю, та конфіденційної інформації здійснюється згідно з вимогами до захисту службової інформації, якщо інше не передбачено законом.

Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються розпорядником системи, якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

У системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;
- результатів виконання користувачем операцій з обробки інформації;
- спроб несанкціонованих дій з інформацією;
- фактів надання та позбавлення користувачів права доступу до інформації та її обробки;
- результатів перевірки цілісності засобів захисту інформації.

В системі забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки).

Реєстрація має здійснюватися автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, а також конфіденційної інформації про фізичну особу, яка законом віднесена до персональних даних, повинна супроводжуватися повідомленням про них адміністратора безпеки.

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

- Порядок підключення інформаційних систем, у яких обробляється службова і таємна інформація, до глобальних мереж передачі даних визначається законодавством.

• Передавання службової і таємної інформації з однієї системи до іншої (через незахищене середовище) здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

Рисунок 5.2. Організаційна структура системи ТЗІ в Україні

Системи ТЗІ в ІКС мають унеможливити:

• виток технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустоелектричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

• несанкціоновані дії з інформацією, зокрема з використанням комп'ютерних вірусів;

• спеціальний вплив на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування.

Державна служба спеціального зв'язку та захисту інформації України є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, комунікаційних систем, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону про Держспецзв'язку.

Керівництво Державною службою спеціального зв'язку та захисту інформації України здійснює Голова Державної служби спеціального зв'язку та захисту інформації України, який призначається на посаду та звільняється з посади Кабінетом Міністрів України за поданням Прем'єр-міністра України.

Повноваження Державної служби спеціального зв'язку та захисту інформації України визначаються законодавством України.

Організація та проведення робіт із захисту інформації в системі в організаціях здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проєктування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

У разі, коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

Виконавцем робіт із оцінювання ефективності створеної системи захисту може бути суб'єкт господарської діяльності або орган виконавчої влади, який має ліцензію або дозвіл на право провадження хоча б одного виду робіт у сфері ТЗІ, необхідність проведення якого визначено технічним завданням на створення системи захисту.

Для проведення робіт з технічного захисту інформації, на провадження яких виконавець не має ліцензії (дозволу), залучаються співвиконавці, що мають відповідні ліцензії.

Якщо для створення системи захисту необхідно провести роботи з криптографічного захисту інформації, виконавець повинен мати ліцензії на провадження робіт у сфері криптографічного захисту інформації або залучати співвиконавців, що мають відповідні ліцензії.

Контроль за забезпеченням захисту інформації в системі полягає у перевірці виконання вимог з технічного та криптографічного захисту інформації та здійснюється у порядку, визначеному Адміністрацією Держспецзв'язку.

У системі, яка складається з кількох ІКС (КС або ІС / АС), оцінюється ефективність ТЗІ кожного складника окремо.

Послуги в галузі ТЗІ надають ліцензіати.

Види ліцензійної діяльності:

1. Оцінювання захищеності інформації, що не становить державної таємниці.

2. Оцінювання захищеності інформації усіх видів, зокрема інформації, що становить державну таємницю.

3. Виявлення закладних пристроїв.

Перелік видів ліцензійної діяльності в галузі КЗІ:

1. Розроблення і складення конструкторської та іншої технічної документації, виробництво криптосистем і засобів криптографічного захисту інформації (з наданням права провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

2. Постачання, монтаж (встановлення), налаштування, технічне обслуговування (супроводження), ремонт та/або утилізація криптосистем і засобів криптографічного захисту інформації (з наданням права провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

3. Тематичні та експертні дослідження криптосистем і засобів криптографічного захисту інформації (з наданням права провадження діяльності у галузі криптографічного захисту інформації, що становить державну таємницю; з наданням права провадження діяльності у галузі криптографічного захисту службової інформації).

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ

Завдання 1. Підготувати глосарій українською та англійською мовами для визначення понять: ТЗІ, КЗІ, ІКС, ідентифікація, автентифікація, розподіл повноважень, адміністратор безпеки, Держспецзв’язок.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Описати структуру Держспецзв’язку.

2. Які заклади, установи та підприємства входять до сфери управління Держспецзв’язку?

3. Вимоги до захисту в системі інформації, що становить державну таємницю.

ТЕМА 6. ЗАХИСТ МОВНОЇ ІНФОРМАЦІЇ НА ОІТ: ПАСИВНИЙ ЗАХИСТ, АКТИВНИЙ ЗАХИСТ

ТЕОРЕТИЧНІ ВІДОМОСТІ

Акустоелектричний і параметричний канали витоку мовної інформації

Акустичний сигнал – коливання повітря, що несе мовну інформацію.

Усі джерела сигналів, що виникають внаслідок побічного впливу акустичного поля, можна розділити на дві основні групи:

– джерела з прямим перетворення тиску акустичного поля в електричний сигнал (п'єзоефект, магнітострикція);

– джерела утворення такого сигналу внаслідок параметричної залежності параметрів елементу від акустичного (віброакустичного) поля, що призводить до модуляції струму, який протікає крізь цей елемент.

Джерела з прямим перетворенням тиску акустичного поля в електричний сигнал створюють електричний сигнал у мовній смузі частот. Завдяки впливу акустичного поля на параметри елементів електричний сигнал може утворюватися як у мовній смузі частот, так і на високих частотах. У разі протікання постійного струму крізь параметричний елемент частота акустоелектричного сигналу співпадає з частотою акустичного поля.

Перетворення зовнішніх акустичних сигналів в електричні сигнали називаються акустоелектричними перетвореннями. Акустоелектричний канал витоку мовної інформації – канал, у якому інформативні мовні сигнали утворюють електричні або електромагнітні сигнали, що поширюються за межі КЗ у проводах ліній комунікацій або у повітряному середовищі.

До акустоелектричних перетворювачів належать фізичні пристрої, елементи, деталі та матеріали, здатні під дією змінного тиску акустичних хвиль створювати аналогічні зміни значень (амплітуди, фази, частоти) електричних сигналів.

Перехоплення цих сигналів може здійснюватися приймальними пристроями засобів акустоелектричної розвідки (підсилюючі, радіоприймачі тощо) з-поза меж контрольованої зони.

Параметричний канал витоку мовної інформації – канал, де інформативні мовні сигнали за допомогою дії акустичної хвилі викликають лише зміни значень параметрів пасивних акустоелектричних перетворювачів (індуктивності та ємності електричних кіл, магнітних властивостей феромагнітної речовини під час її деформації – розтягування, стискання, згинання, скручування).

Канал витоку мовної інформації завдяки ВЧ-нав'язуванню – канал, де інформативні мовні сигнали з допомогою дії акустичної хвилі викликають модуляцію підведених / наведених до джерела побічних випромінювань електричних і радіосигналів:

- нелінійні елементи, на які одночасно надходять електричні низькочастотний і високочастотний гармонійний сигнал. Під час цього високочастотний гар-

монійний сигнал модулюється низькочастотним електричним сигналом і перехоплюється спеціальним приймачем за межами контрольованої зони;

- струмопровідні механічні конструкції, що змінюють свій розмір або положення у просторі під дією акустичної хвилі і перевипромінюють високочастотний гармонійний сигнал, змінюючи його фазу, у зовнішній простір.

Класифікувати акустоелектричні перетворювачі доцільно так:

- активні – електродинамічні, електромагнітні, п'єзоелектричні;
- пасивні (параметричні) – індуктивні, магнітострикційні, ємнісні.

На виході активних акустоелектричних перетворювачів (електродинамічних, електромагнітних і п'єзоелектричних) під впливом акустичної хвилі виникають електричні сигнали.

У пасивних акустоелектричних перетворювачах ті ж дії акустичної хвилі викликають лише зміни значень параметрів перетворювачів – параметричні перетворювання.

Сигнали в електродинамічних акустоелектричних перетворювачах виникають відповідно до закону електромагнітної індукції під час переміщення проводу в магнітному полі під дією акустичних хвиль.

Електричні сигнали індукуються в котушках електромагнітних пристроїв внаслідок зміни напруженості створюваних у них полів, викликаних змінами під дією акустичних хвиль повітряного зазору між сердечником і якорем електромагніту або статора (нерухомої частини) і ротора (рухомої частини) електродвигуна.

Прикладом таких пристроїв можуть бути: електромагніти електромеханічних дзвінків і капсул телефонних апаратів, крокові двигуни вторинних годинників, кнопкові сповіщувачі ручного виклику пожежної служби охорони об'єкта та ін.

Активними акустоелектричними перетворювачами також є деякі кристалічні речовини (кварц, сегнетова сіль, титанат і ніобат барію та ін.), що широко застосовуються в радіоелектронній апаратурі для стабілізації частоти та фільтрації сигналів, в акустичних випромінювачах сигналів виклику телефонних апаратів замість електромеханічних дзвінків. На поверхні цих речовин під час механічної деформації їх кристалічної решітки (натискання на поверхню, згинання, скручування) виникають електричні заряди.

У пасивних акустоелектричних перетворювачах під дією акустичних хвиль змінюються значення параметрів – індуктивності та ємності електричних кіл. Відповідно до цього акустоелектричні перетворювачі називаються індуктивними та ємнісними.

Різновидом індуктивного є магнітострикційний акустоелектричний перетворювач. Магнітострикція проявляється у зміні магнітних властивостей феромагнітної речовини (електротехнічної сталі та її сплавів) під час їх деформації (розтягування, стискання, згинання, скручування).

До найбільш поширених випадкових акустоелектричних перетворювачів належать:

- пристрої виклику в телефонних апаратах;
- динамічні головки гучномовців, електромагнітні капсули телефонних трубок, електричні двигуни побутових електроприладів;
- котушки індуктивності контурів, дроселі, трансформатори, проводи монтажних джгутів, пластини (електроди) конденсаторів;
- п’єзоелектричі речовини (кварці генераторів, віброакустичні випромінювачі акустичних генераторів завад);
- феромагнітні матеріали у вигляді сердечників трансформаторів і дроселів.

Інформаційні сигнали, утворені внаслідок акустоелектричного перетворення, можуть:

- поширюватися дротами за межі контрольованої зони;
- випромінюватись у простір;
- модулювати інші сигнали.

Паразитні зв’язки і наведення

Постійні електричні заряди і електричний струм в елементах і колах радіоелектронних і електричних пристроїв створюють відповідні електричні і магнітні поля, а електричні заряди і струм змінної частоти – електромагнітні поля.

Електромагнітні поля поширюються в просторі і наводяться на елементи та кола інших технічних засобів і систем. Для функціонування засобів і систем необхідно забезпечити також і гальванічне з’єднання їх елементів. Внаслідок гальванічних з’єднань виникають додаткові шляхи для поширення сигналів одних вузлів і блоків по колах інших. Внаслідок впливу побічних полів та через провідники та резистори сигналів одних вузлів і блоків на сигнали інших блоків і вузлів виникають паразитні зв’язки та наведення – як всередині основних радіоелектронних засобів, так і на розташовані поряд засоби.

Виділяють такі види паразитних зв’язків: ємнісні, індуктивні, гальванічні.

Ємнісний зв’язок утворюється внаслідок впливу електричного поля. Індуктивний зв’язок утворюється внаслідок впливу магнітного поля, а гальванічний зв’язок утворюється через наявність загального активного опору.

Можливість витоку інформації через паразитні зв’язки та наведення залежить від багатьох факторів, зокрема від конфігурації, розмірів і взаємного положення випромінюючих і приймаючих струмопровідних елементів основних технічних засобів – ці елементи можна назвати випадковими антенами (монтажні проводи, сполучні кабелі, виводи радіодеталей та ін.).

Усі джерела сигналів, що виникають внаслідок побічного впливу акустичного поля, можна розділити на дві основні групи:

– джерела з прямим перетворенням тиску акустичного поля в електричний сигнал (п’єзоефект, магнітострикція);

– джерела утворення такого сигналу внаслідок параметричної залежності параметрів елементу від акустичного (віброакустичного) поля, що призводить до модуляції струму, який протікає крізь цей елемент.

Джерела з прямим перетворенням тиску акустичного поля в електричний сигнал створюють електричний сигнал у мовній смузі частот. Через вплив акустичного поля на параметри елементів електричний сигнал може утворюватися як у мовній смузі частот, так і на високих частотах. У разі протікання постійного струму крізь параметричний елемент частота акустоелектричного сигналу співпадає з частотою акустичного поля.

Для гармонійного струму залежність параметрів елементу джерела сигналу (ємності, індуктивності тощо) призводить до модуляції цього струму і появи бокових частот у спектрі гармонійного сигналу. Ці бокові частоти несуть інформацію щодо акустоелектричного мовного сигналу.

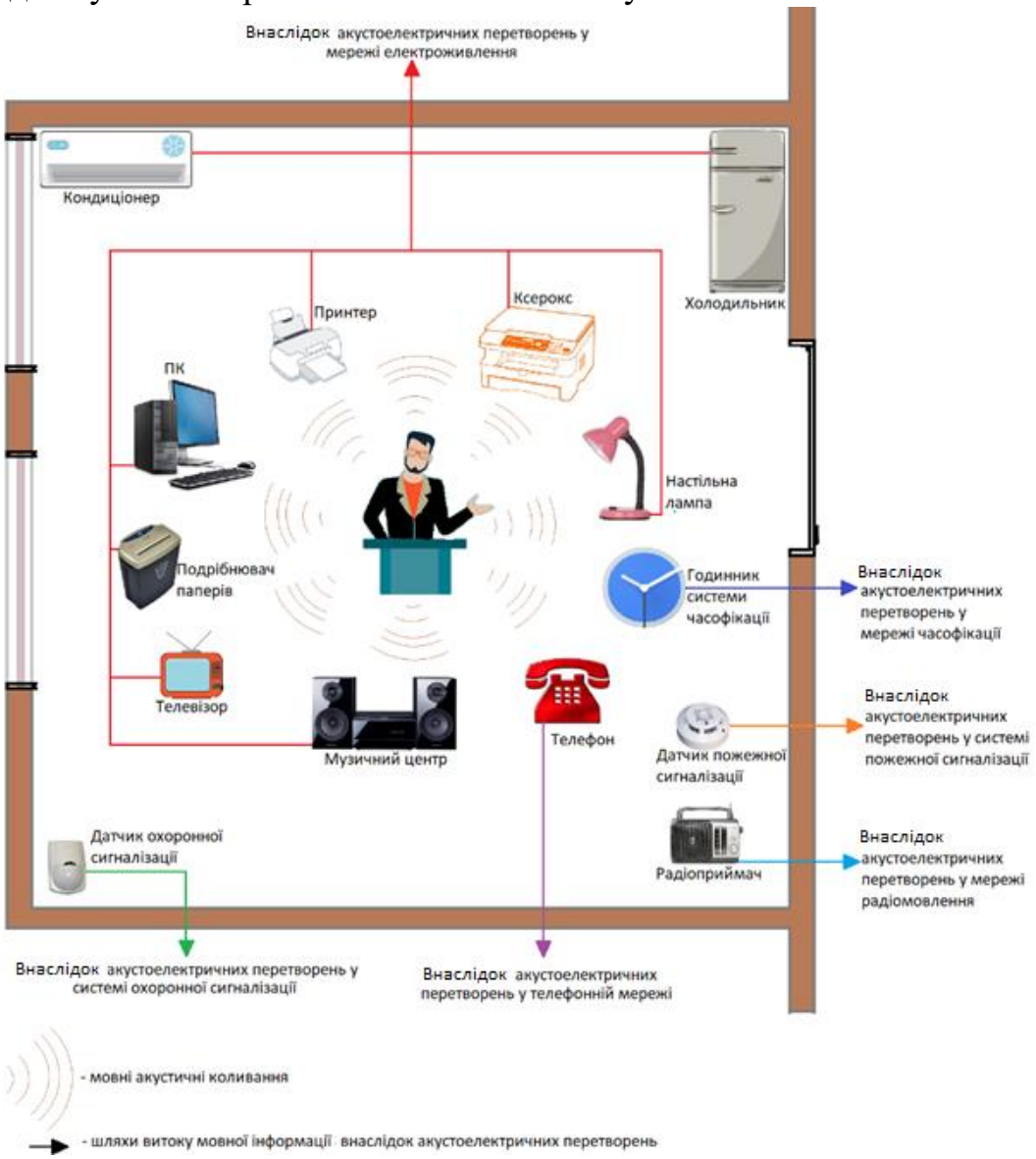

Рисунок 6.1. Утворення акустоелектричних каналів витоку інформації на об’єкті

Основні типи акустоелектричних перетворювачів

Електродинамічні перетворювачі. Електродинамічними називають системи, електричний контур яких переміщується у постійному магнітному полі. Прикладом такого елементу є електродинамічний мікрофон.

Електромагнітні перетворювачі. На відміну від електродинамічних, у електромагнітних перетворювачах нерухомим є контур котушки, а поле змінюється шляхом переміщення постійного магніту.

До типових електродинамічних та електромагнітних перетворювачів належать: електродинамічний гучномовець, абонентський гучномовець, вторинний електричний годинник, електромеханічний дзвінок телефонного апарату. Значення чутливості таких елементів наведено в таблиці 6.1.

Таблиця 6.1 – Чутливості типових електродинамічних та електромагнітних перетворювачів

Тип акустоелектричного перетворювача	**Чутливість, мВ/ПА**
Електродинамічний мікрофон	4–6
Електродинамічний гучномовець	2–3
Абонентський гучномовець	30–45
Вторинний електричний годинник	0,1–0,5
Електромеханічний дзвінок телефонного апарату	0,05–0,6

Наведені в табл. 1 акустоелектричні перетворювачі мають високі значення чутливості до акустичного поля і у разі їх прямого під’єднання до ліній утворюють канал витоку мовної інформації з високим показником розбірливості мови. Небезпечний електричний сигнал створюється у мовному діапазоні частот. Водночас на відстані до 1 км не треба враховувати мале загасання НЧ сигналу в лінії. Тому без додаткових пристроїв захисту електродинамічні та електромагнітні перетворювачі не повинні розміщуватися на об’єктах, де озвучується мовна інформація.

До п’єзоелектричних перетворювачів належать елементи, у яких під час дії на них тиску на обкладинках п’єзоелементу виникає електрична напруга. Більшість конденсаторів мають цей ефект.

Пасивний захист інформації на об’єктах інформаційної діяльності

Радіопоглинаючі матеріали можуть застосовуватися в якості покриттів різних поверхонь з метою зменшення віддзеркалення від цих поверхонь електромагнітних хвиль. Принцип дії таких матеріалів полягає в тому, що падаюча на них електромагнітна хвиля перетвориться всередині їх структури в інші види енергії.

Водночас відбуваються явища розсіювання, поглинання, інтерференції, а в низці покриттів і дифракції електромагнітних хвиль. Залежно від властивостей радіопоглинаючі матеріали / покриття можуть бути широкодіапазонними і вузькодіапазонними.

РПМ складаються зазвичай з електроізоляційних (тканини) і електропровідних (фольга, металізовані плівки та ін.) шарів, що чергуються між собою, спінених композицій (електроізоляційний матеріал – смола, електропровідний матеріал – волокна, фольга тощо). Є також керамічні РПМ у вигляді плиток з феритів. Основні вимоги до РПМ – високі механічні властивості, стійкість до впливу метеорологічних умов. Цими матеріалами покривають поверхню наземних споруд, морських та ін. об'єктів, щоб радіолокаційні станції не могли їх виявити. РПМ використовують також в елементах надвисокочастотних пристроїв, у камерах, де досліджують антенні системи, тощо.

Таблиця 6.2 – Характеристики РПМ, що випускаються

Матеріал	**Тип, марка**	**Діапазон довжин хвиль, см**	**Коефіцієнт відображення, –дБ**	**Товщина, мм**	**маса 1м^2, кг**
Гумові килимки	В2Ф-2	0,8–4	15–20	19–30	4–5
Магнітодіелектричні пластини	ХВ-0,8	0,8	15–20	1–3	3–10
Поглинаючі покриття на основі поролону	«Болото»	0,8–100	15–20	–	–
Феритові пластини	СВЧ-0,68	15–200	14–15	4–20	20–70

Основною вимогою, що пред'являється до РПМ, є поєднання високих магнітних і діелектричних властивостей.

Загальні положення та вимоги щодо розміщення режимних приміщень

Проєктування режимних приміщень, у яких дозволяється зберігати секретні матеріали та зразки секретної техніки у неробочий час, здійснюється з дотриманням вимог «Порядку організації та забезпечення режиму секретності в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях», затвердженого постановою Кабінету Міністрів України від 18 грудня 2013 року № 939.

Режимні приміщення розміщуються в громадських будинках та спорудах, будівлях виробничого та адміністративного призначення I або II ступенів вогнестійкості за ДБН В.1.1-7.

Режимні приміщення в багатоповерхових будівлях треба розміщувати, зазвичай, не нижче другого і не вище передостаннього (не враховуючи технічного) поверху.

Взаємопов'язані за функціональними ознаками режимні приміщення повинні розміщуватись групами і мати загальні для групи входи зі сторони загального коридору.

Під час розміщення режимних приміщень треба враховувати, що біля їх вікон не повинно бути пожежних драбин, водостічних труб, балконів, покрівель прибудов та інших будівельних елементів (карнизів, виступів стін тощо), з яких можливе проникнення через вікна сторонніх осіб.

Розміщення обладнання, технічних засобів у режимних приміщеннях повинно відповідати вимогам із технічного захисту інформації, безпеки праці, санітарним нормам та відповідати вимогам пожежної безпеки.

Режимні приміщення оснащуються охоронною сигналізацією, яка повинна бути виведена на пульт поста охорони будинку, групи приміщень, чергового по установі (підприємству) або пульт централізованого спостереження підрозділу охорони. Типи та види охоронної сигналізації повинні відповідати встановленим Службою безпеки України вимогам. Для живлення охоронної сигналізації у аварійних випадках повинне передбачатись автономне джерело живлення. Переключення на автономне джерело живлення повинно бути автоматичним. Режимні приміщення повинні бути обладнанні автоматичною пожежною сигналізацією.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ

Завдання 1. Підготувати глосарій українською та англійською мовами для визначення термінів: акустичний сигнал, акустоелектричний канал витоку мовної інформації, параметричний канал витоку мовної інформації, канал витоку мовної інформації завдяки ВЧ-нав'язуванню, магнітострикційні перетворювачі, тензорезистивні перетворювачі, резонансні перетворювачі, перетворювачі на основі волоконно-оптичних кабелів зв'язку.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Назвіть основні типи акустоелектричних перетворювачів.
2. Принципи створення акустоелектричного каналу витоку інформації.
3. Які фактори впливають на рівень акустоелектричного сигналу?
4. Можливі середовища поширення акустоелектричних сигналів.
5. Основні перспективні технологічні напрями створення РП.
6. Вимоги до будівельних конструкцій режимних приміщень.

ТЕМА 7. МЕТОДИ ТА ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ КАНАЛАМИ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ І НАВЕДЕНЬ

КОРОТКІ ТЕОРЕТИЧНІ ВІДОМОСТІ

В основних технічних засобах (ОТЗ), що обробляють інформацію з обмеженим доступом (ІзОД), носієм інформації є електричний струм, параметри якого (амплітуда, частота або фаза) змінюються за законом зміни ІзОД. Під час проходження такого електричного струму у струмоведучих елементах ОТЗ навколо них виникає електромагнітне поле. Через це елементи ОТЗ слугують як побічні електромагнітні випромінювачі, завдяки чому і поширюються інформативні сигнали у просторі.

Побічні електромагнітні випромінювання наводяться також на випадкові антени – кола додаткових технічних засобів і систем (ДТЗС) або сторонні провідники, що розміщуються на певній відстані від ОТЗ. Випадкові антени можуть бути зосередженими і розподіленими.

Зосереджена випадкова антена являє собою компактний технічний засіб (наприклад, телефонний апарат). До розподілених випадкових антен належать кабелі, дроти, металеві труби та інші струмопровідні комунікації.

Шуми, що супроводжують всі фізичні процеси, наявні на вході засобів перехоплення інформації, і так обмежують розвідувальну здатність засобів технічної розвідки (ЗТР).

Канали витоку інформації шляхом побічних електромагнітних випромінювань та наведень (ПЕМВН) можуть утворювати не тільки струмопровідні елементи ОТЗ, а і високочастотні (ВЧ) генератори ОТЗ, самозбудження підсилювачів низької частоти (УНЧ) ОТЗ.

Вузли і елементи ОТЗ, в яких наявна велика напруга і протікають малі струми, створюють у ближній зоні електромагнітні поля з переважанням електричного складника. Переважний вплив електричного складника поля на елементи ОТЗ спостерігається і в тих випадках, коли ці елементи малочутливі до змін значень магнітного складника електромагнітного поля.

Вузли й елементи ОТЗ, в яких протікають великі струми і наявні малі перепади напруги, створюють у ближній зоні електромагнітні поля з переважанням магнітного складника. Переважний вплив магнітного складника поля на елементи ДТЗС спостерігається також тоді, коли вони малочутливі до змін значень електричного складника або останній набагато менший магнітний через властивості випромінювача.

Інтенсивність полів ПЕМВН у діапазоні частот від одиниць кілогерц до сотень-тисяч мегагерц така, що приймання сигналів може вестися за межами конт-

рольованої зони (КЗ) по ефіру, а також при безпосередньому підключенні ЗТР до ліній ДТЗС, що виходять за межі КЗ.

Крім з'єднувальних ліній ОТЗ і ДТЗС, за межі КЗ можуть виходити проводи та кабелі, що до них не належать, але транзитом проходять через приміщення, де встановлені ОТЗ. Такі дроти, кабелі та струмопровідні елементи називаються сторонніми провідниками.

Приймач ЗТР – це потенційний противник, що використовує технічні засоби перехоплення інформації. Якщо розглянути задачу захисту інформації від можливого її витоку, то в точці розміщення ЗТР противника необхідно забезпечити таке співвідношення сигнал / шум, що не дасть змоги противнику отримати інформацію, яку захищають, або істотно ускладнити отримання інформації.

Ця задача може бути вирішена у три способи – зменшувати рівень сигналу ПЕМВН, збільшувати загасання рівня сигналу ПЕМВН у каналі, збільшувати рівень шуму в каналі на вході ЗТР (рис. 7.1).

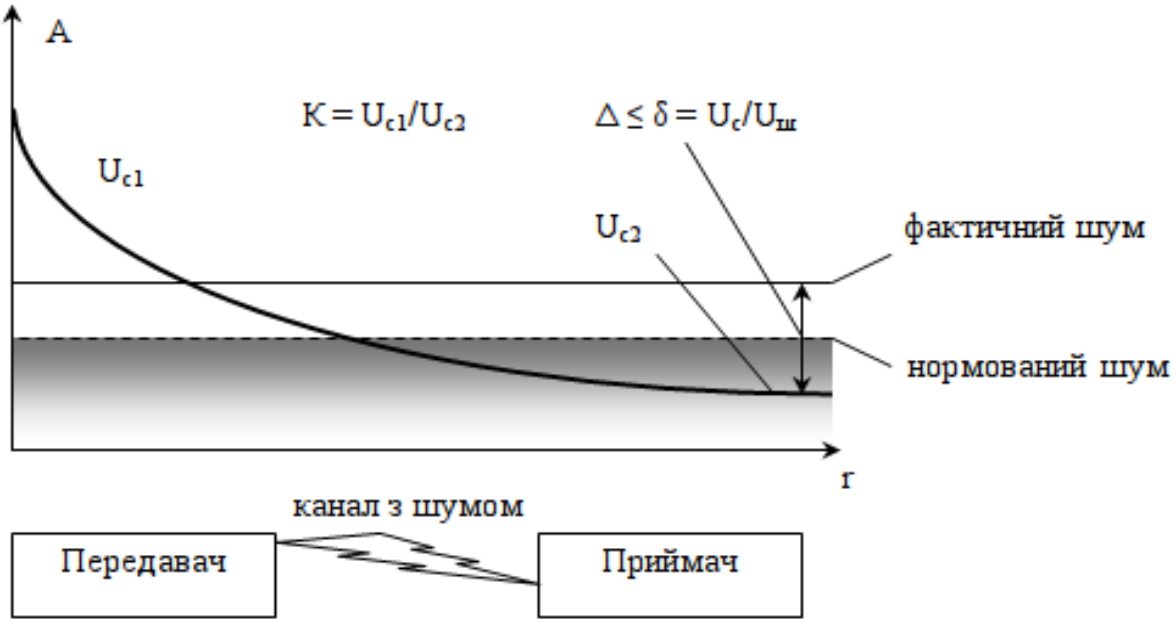

Рисунок 7.1. Задача захисту інформації від можливого її витоку

Розглянемо позначення, які використовуються у представленій на рис. 7.1 задачі:

r – відстань від ОТЗ до місця можливого розміщення приймача ЗТР;

U_{c1} – рівень сигналу ПЕМВ від ОТЗ на вході приймача ЗТР (визначається розмірами антени, зазвичай, 1 м);

U_{c2} – рівень сигналу ПЕМВ від ОТЗ на межі зони 2 на вході приймача ЗТР;

U_c – рівень сигналу ПЕМВ від ОТЗ у точці вимірювання на вході приймача ЗТР;

$U_ш$ – рівень шуму на вході приймача ЗТР у точці вимірювання (зазвичай, значення рівня нормованого шуму);

δ – співвідношення рівнів сигнал-шум;

$Д$ – нормоване значення співвідношення сигнал-шум;

$К$ – коефіцієнт запасу захищеності інформації від витоку каналами ПЕМВ.

На практиці, в загальному випадку, як це зображено на рис. 7.1, для технічного захисту інформації (ТЗІ) застосовують усі перераховані способи або їх комбінації.

Рівні ПЕМВ окремих складників полів ПЕМВ залежно від відстані r від ОТЗ до ЗТР пропорційні у ближній зоні r^{-3}, у проміжній зоні r^{-2} і у дальній зоні r^{-1}. На цьому факті ґрунтується можливість введення понять ближньої, проміжної та дальньої зон поширення ЕМВ. Ближня зона ЕЕВ, або зона індукції - це область, у якій доданок, пропорційний r^{-3} у виразах для полів, має перевагу над іншим доданком. Це область, радіус якої не перевищує значення 0,16 λ – довжини хвилі ПЕМВ. Дальня зона, або зона випромінювання – це область, у якій доданок, пропорційний r^{-1} у виразах для полів, має перевагу над іншими доданками. Це область, радіус якої перевищує значення 3λ. Проміжна зона знаходиться між 0,16 λ і 3λ.

Загроза витоку інформації з ОТЗ через канал побічних електромагнітних випромінювань та наведень нейтралізується методами пасивного та активного захисту інформації на ОІД.

Під пасивними методами прийнято розуміти методи зниження рівня паразитного випромінювання інформаційного сигналу на фоні природного, побутового, промислового або іншого наявного електромагнітного шуму.

Пасивні методи захисту інформації спрямовані на:

- екранування приміщень, у яких розташовані ОТЗ;
- видалення незадіяних струмопровідних елементів (випадкових антен);
- фільтрації паразитних сигналів у комунікаціях, що виходять за межі контрольованої зони;
- ослаблення побічних електромагнітних випромінювань (інформаційних сигналів) на межі контрольованої зони до величин, що забезпечують неможливість їх виділення засобом розвідки на фоні природних шумів шляхом збільшення радіусу КЗ;
- ослаблення наведень побічних електромагнітних випромінювань (інформаційних сигналів) на сторонні провідники і сполучні лінії ДТЗС, що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їх виділення засобом розвідки на фоні природних шумів шляхом віддалення їх від місця розміщення ОТЗ;

• виключення (ослаблення) просочування інформаційних сигналів у колах електроживлення, що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їх виділення засобом розвідки шляхом фільтрації.

Активні методи захисту інформації спрямовані на:

• створення просторових маскувальних електромагнітних завад з метою зменшення відношення сигнал-шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗ;

• створення маскувального лінійного електромагнітного зашумлення у сторонніх провідниках і сполучних лініях ДТЗС з метою зменшення відношення сигнал-шум на межі контрольованої зони до величин, шо забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗ.

Ослаблення побічних електромагнітних випромінювань і їх наведень у сторонніх провідниках здійснюється також шляхом заземлення ОТЗ і їх сполучних ліній.

Виключення (ослаблення) просочування інформаційних сигналів ОТЗ в колах електроживлення досягають шляхом фільтрації інформаційних сигналів.

Методи й засоби блокування каналів витоку інформації

Захист інформації від витоку технічними каналами забезпечують проєктно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також шляхом виявлення закладних пристроїв.

Організаційні заходи – це спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.

До основних організаційних заходів належать:

– залучення до робіт для захисту інформації організацій, що мають ліцензії на право надання послуг з оцінювання ефективності технічного захисту інформації (ТЗІ);

– категоріювання об’єктів інформаційної діяльності (приміщень, виділених для проведення робіт з оброблення ІзОД) щодо відповідності вимогам забезпечення захисту інформації;

– використання на об’єкті ОТЗ у захищеному виконанні, що мають експертні висновки у сфері ТЗІ;

– визначення КЗ навколо об’єкта;

– організація режимних заходів - контроль та обмеження доступу на об’єкти інформаційної діяльності та у виділені приміщення;

– введення територіальних, частотних, енергетичних, просторових і часових обмежень щодо режиму використання ОТЗ;

– блокування візуально-оптичного каналу витоку інформації шляхом встановлення ролет / штор на вікна, через які можна спостерігати за екранами моніторів ОТЗ;

– відключення технічних засобів, що мають можливість створення каналів ПЕМВН на період проведення / оброблення інформації з обмеженим доступом.

Технічні заходи – це спрямовані на захист інформації заходи, проведення яких передбачає використання спеціальних технічних засобів, а також реалізацію технічних рішень. Технічні заходи слугують для унеможливлення витоку інформації з обмеженим доступом через ослаблення рівня інформативних сигналів або зменшення відношення сигнал-завада у місцях можливого розміщення ЗТР або їх датчиків до рівнів, що унеможливлюють виділення інформативних сигналів засобами розвідки.

Під час проведення таких заходів використовують активні та пасивні методи.

До технічних заходів із використанням пасивних методів належать:

1. Обмеження доступу на об’єкти інформаційної діяльності та у виділені приміщення шляхом застосування технічних засобів і систем для обмеження та контролю доступу.

2. Локалізація випромінювання:

– екранування ОТЗ та з’єднувальних ліній;

– заземлення ОТЗ та екранів їх з’єднувальних ліній.

3. Розмикання кіл (навіть гальванічне), в яких циркулюють інформаційні сигнали. Встановлення автономних або стабілізованих пристроїв електроживлення ОТЗ (акумуляторів, мотор-генераторів). У мережах електроживлення ОТЗ, в лініях освітлювання (за потреби) застосування мережевих протизавадних фільтрів, а в лініях (телефонного зв’язку, сигналізації та ін.) фільтрів ВЧ.

До технічних заходів із використанням активних методів блокування каналів витоку інформації належать такі засоби ТЗІ:

- генератори просторового зашумлення (електромагнітного);
- знешкодження підключених до лінії закладних пристроїв з допомогою спеціальних генераторів імпульсів (випалювачів «жучків»).

Виявити закладні пристрої можна завдяки спеціальним обстеженням (візуальний огляд без залучення технічних засобів) і спеціальним перевіркам (із використанням технічних засобів) об’єктів ЕОТ та ОІД (виділених приміщень).

1. Просторове зашумлення:

- просторове електромагнітне зашумлення з використанням генераторів шуму чи створення направлених завад (під час виявлення і визначення чистоти випромінювання закладного пристрою чи побічних електромагнітних випромінювань ІД) з використанням засобів створення направлених завад.

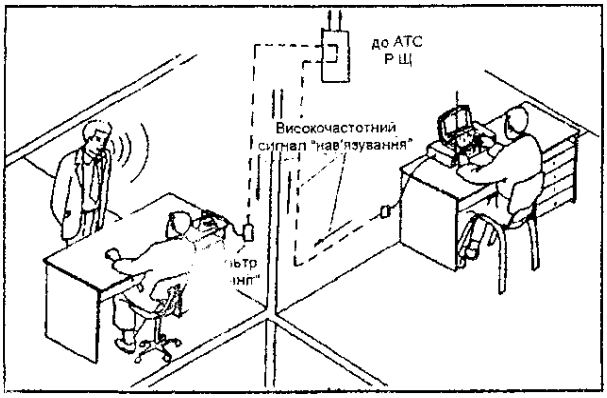

Рисунок 7.2. Встановлення спеціальних фільтрів у з'єднувальні лінії ДТЗС

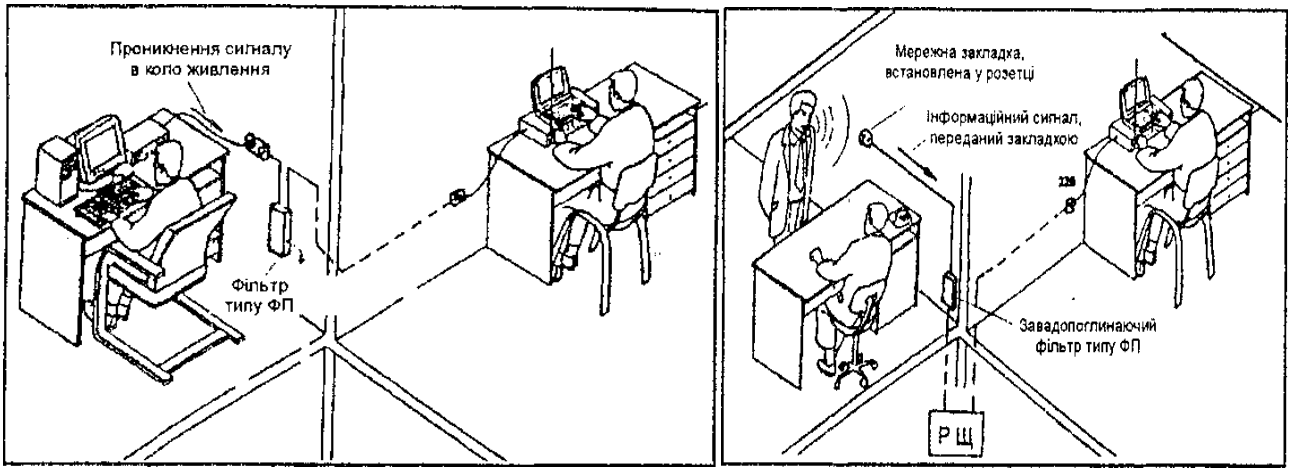

Рисунок 7.3 Встановлення в колах електроживлення ОТЗ протизавадних фільтрів

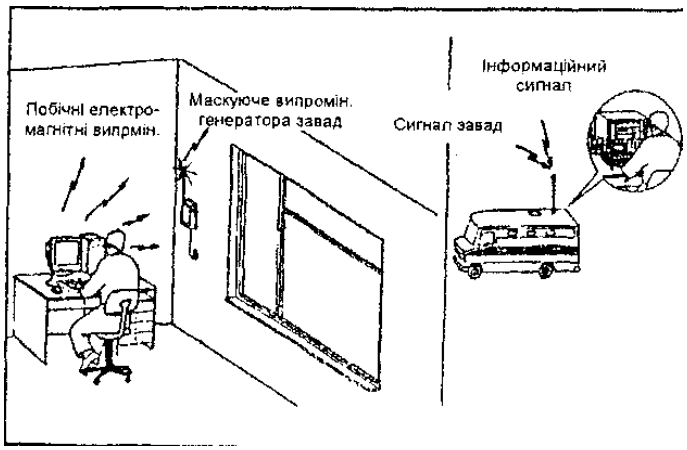

Рисунок 7.4. Просторове електромагнітне зашумлення
побічних електромагнітних випромінювань ОТЗ генератором шуму

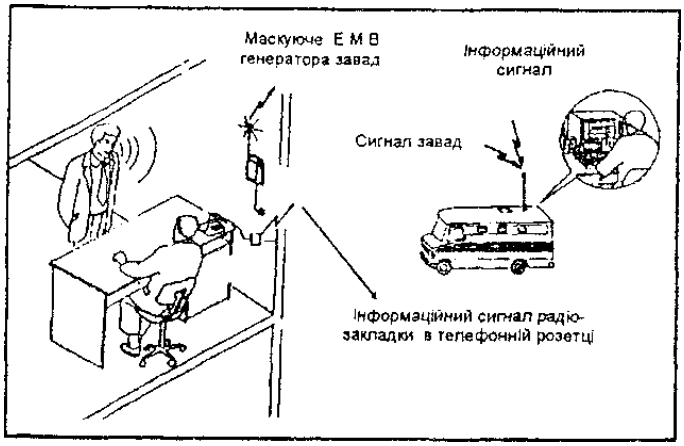

Рисунок 7.5. Створення направлених маскуючих радіозавад у каналах передачі інформації закладними пристроями

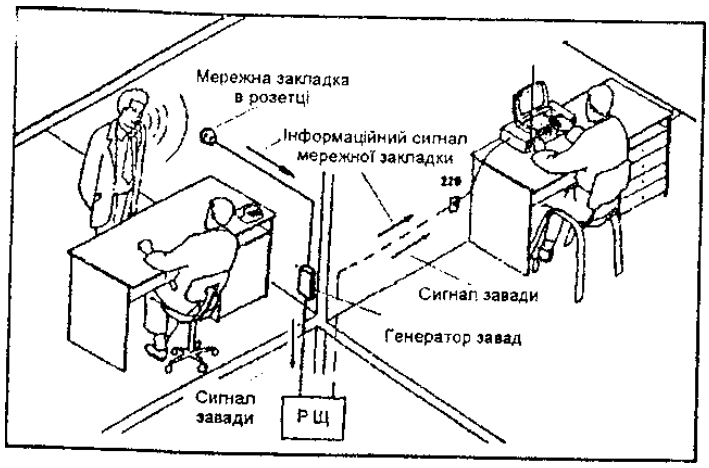

Рисунок 7.6. Лінійне зашумлення ліній електроживлення освітлювальної і мережі електроживлення ОТЗ

Виявлення портативних електронних пристроїв перехоплення інформації (закладних пристроїв) здійснюється шляхом проведення спеціальних обстежень, а також спеціальних перевірок ОІД і виділених приміщень. Спеціальні обстеження ОІД і виділених приміщень проводяться шляхом їх візуального огляду без застосування технічних засобів.

Спеціальна перевірка проводиться з використанням технічних засобів. Під час цього здійснюється:

1) виявлення закладних пристроїв з використанням пасивних засобів:

- пошук закладних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, сканерних приймачів і програмно-апаратних комплексів контролю;
- організація радіоконтролю (постійно чи на час оброблення ІзОД);

2) виявлення закладних пристроїв з використанням активних засобів:

- спеціальна перевірка ОІД з використанням нелінійних локаторів;

• спеціальна перевірка виділених приміщень, ІД і допоміжних технічних засобів з використанням рентгенівських комплексів.

Методи і засоби захисту інформації на ОІД від витоку технічними каналами

Активні методи захисту інформації спрямовані на:

• створення просторових маскувальних електромагнітних завад з метою зменшення відношення сигнал-шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ІД;

• створення маскувальних електромагнітних завад у сторонніх провідниках і сполучних лініях ДТЗС із метою зменшення відношення сигнал-шум на межі контрольованої зони до величин, шо забезпечують неможливість виділення засобом розвідки інформаційного сигналу ІД.

Ослаблення побічних електромагнітних випромінювань ІД і їх наведень у сторонніх провідниках здійснюється шляхом екранування і заземлення ІД і їх сполучних ліній. Виключення (ослаблення) витоку інформаційних сигналів на ОІД в колах електроживлення досягають шляхом фільтрації інформаційних сигналів.

Захист мобільних телефонів від витоку інформації

Сьогодні, коли зловмисникам доступна можливість установки на мобільні телефони спеціальних програм, які дають змогу використовувати телефон для прослуховування або отримувати дані, що зберігаються в пам’яті мобільного телефону. Мобільний телефон може перетворитися в пристрій, який становить загрозу незаконного отримання інформації та прослуховування.

Одним із таких способів є автоматична відповідь стільникового телефона на дзвінки з заданих номерів (телефон автоматично «відповість на дзвінок», але не повідомить власника про те, що на нього надійшов виклик).

У разі прийняття такого виклику мобільним телефоном він автоматично перетворюється на прилад, який прослуховує і здійснює запис та передавання звукової інформації на приймаючий пристрій. Приблизно так само буде виглядати передавання інформації з одного мобільного на інший пристрій, на який подібне передавання даних відбувається абсолютно непомітно для володільця телефона.

Для того, щоб забезпечити власну інформаційну безпеку, необхідно з обережністю ставитися до подарованих, знайдених або до телефонів, повернутих із ремонту. Такий пристрій необхідно перевірити на наявність шкідливого програмного забезпечення або придбати спеціальні пристрої, які допоможуть забезпечити захист від інформаційного шпигунства.

У чому полягає захист мобільного телефона?

Принцип роботи захисних пристроїв для мобільних телефонів полягає в детектуванні електромагнітного поля навколо телефона. Коли на телефон надходить дзвінок, то рівень активності електромагнітного поля суттєво збільшується і це фіксується приладом захисту. Це факт обов'язково буде супроводжуватися звуковими і світловими сигналами, які володілець мобільного телефону однозначно не пропустить. Під час такого виявлення пристрій для забезпечення захисту мобільного телефону вмикає генерацію білого шуму на тих частотах, на яких здійснюється передавання даних. Це не дасть змоги розпізнати / відновити текст розмови на приймаючому пристрої.

Акустичні сейфи для телефона – це одні з найпоширеніших засобів захисту стільникових телефонів від прослуховування. Такий пристрій не привертає уваги сторонніх, водночас дає змогу забезпечити надійний захист від незаконного отримання акустичної інформації, бо в ньому поєднані функції генератора акустичного шуму і детектора поля. Для використання необхідно лише помістити телефон у підставку для того, щоб активувати захист. Важливо, що під час цього телефон буде залишатися на зв'язку, і немає необхідності вимикати мобільний під час використання акустичного сейфа. Телефон буде реагувати на дзвінки як зазвичай, а «приховані» дзвінки заблокує підставка.

Але не варто забувати, що акустичний сейф захищає тільки тоді, коли всередині нього знаходиться телефон. Якщо ж стільниковий телефон, що захищається таким засобом, буде просто лежати на столі, то його власник не буде захищений від витоку мовної інформації.

До основних переваг використання акустичних сейфів можна віднести те, що такі пристрої мають високу чутливість і моментально виявляють факт передавання інформації по каналах GSM, 3G, Bluetooth, Wi-Fi, CDMA. Цей пристрій сумісний з будь-якою моделлю відповідного за розмірами телефона або смартфона і не шкодить здоров'ю володільця.

Захисні екрануючі чохли для мобільних телефонів складаються із двох відділень: спеціального, в якому блокуються сигнали GSM / CDMA / 3G / WiFI / Bluetooth, і звичайного відділення чохла. Для захисту володарю мобільного телефона необхідно просто помістити його в спеціальне відділення, а це виключить можливість прослуховування, оскільки радіосигнал не вийде за межі цього чохла. Мобільний телефон буде недоступний, ніби вимкнений або під час перебування поза мобільною мережею. Такий чохол-блокіратор зручно носити з собою і використовувати тоді, коли немає можливості скористатися акустичним сейфом і не потрібно залишатися в цей час на зв'язку. Наприклад, на переговорах, нарадах та ін.

Засіб подавлення мобільного стільникового зв'язку – це невелике обладнання, яке здатне блокувати передавання сигналів між стільниковими телефона-

ми та базовою станцією. Здебільшого це відбувається шляхом створення завад у робочих діапазонах частот стільникових телефонів, що призводить до відсутності сигналу або значної втрати якості сигналу. Хоча подавлювачі мобільного зв'язку можна використовувати практично скрізь, вони в основному використовуються в місцях, де очікується або вимагається тиша, або в тих місцях, де використання мобільного телефона заборонено. Зокрема такі засоби заборонено використовувати на об'єктах інформаційної діяльності, на яких обробляється інформація з обмеженим доступом і створюються комплекси технічного захисту інформації.

Засіб подавлення мобільного стільникового зв'язку блокує і приймання, і передавання сигналів мобільного зв'язку. Мобільні телефони використовують унікальні частоти для розмови та прослуховування. Більшість засобів подавлення мобільного стільникового зв'язку блокують будь-яку з двох частот, опосередковано забезпечуючи ефект запобігання використання обох частот.

Засоби подавлення мобільного стільникового зв'язку працюють за тими ж принципами, що й глушники, які використовуються для запобігання радіозв'язку. Вони або функціонують, порушуючи частоти від стільникового телефона до базової станції, або від базової станції до стільникового телефона. Вони ефективно блокують передавання сигналів з мереж, зокрема UMTS, 3G, CDMA, GSM та PHS. Один такий пристрій Jammer може не працювати на різних частотах, оскільки мобільні телефони працюють у різних діапазонах частот у різних країнах.

Пасивні методи захисту від витоку каналами ПЕМВН, параметричними і акустоелектричними ВЧ каналами витоку інформації

Електромагнітне екранування – це локалізація електричного та електромагнітного полів у певній частині простору. Екранування дає змогу захистити радіоелектронні прилади від впливу зовнішніх полів та локалізувати їх власні випромінювання, заважаючи їх появі в навколишньому просторі. Внаслідок цього стає практично неможливим несанкціоноване знімання інформації технічними каналами (до яких належить канал побічних електромагнітних випромінювань і наведень, електроакустичний канал, параметричний канал через просторове ВЧ-нав'язування, радіоканал та ін.). Отже, воно дає змогу знизити ефективність використання зловмисником радіомікрофонів з передачею інформації радіоканалом, просторового ВЧ-нав'язування та інших можливих засобів знімання інформації у просторі поза межами КЗ.

До недоліків електромагнітного екранування можна віднести великі габарити екрануючих конструкцій, і відповідно високу вартість робіт.

Для ефективного екранування ЕМП застосовують такі рішення: збільшення товщини екрана, розробка та застосування екрануючих та радіопоглинаючих матеріалів.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОГО ВИКОНАННЯ

Підготувати реферат за темою:

1. Правові засади організації і функціонування національної системи кібербезпеки.
2. Правові засади організації і функціонування системи національної безпеки.
3. Загальні принципи і задачі захисту інформації від засобів технічної розвідки.
4. Організація та функціонування системи забезпечення інформаційної безпеки.
5. Сучасні інформаційні технології в ІКС.
6. Організація захисту інформації в Україні – загальні принципи, структура системи захисту, правова основа організації захисту інформації.
7. Канали витоку інформації під час її оброблення в ІКС.
8. Канали витоку мовної інформації, що циркулює на об’єктах інформаційної діяльності.

ОРІЄНТОВНИЙ СПИСОК ПИТАНЬ ДО ІСПИТУ

1. Поняття кіберпростору.
2. Поняття інформаційного простору.
3. Визначення інформації, її основні властивості.
4. Явище кібертероризму.
5. Кіберпростір та кібернетичний простір – арена для проведення інформаційних операцій.
6. Об’єкти та суб’єкти інформаційної взаємодії.
7. Структура соціотехнічної системи.
8. Захист інформації від соціотехнічних атак.
9. Соціальні мережі: особливості, основні поняття та визначення.
10. Методи соціального інжинірингу.
11. Загрози соціального інжинірингу.
12. Засоби та заходи фізичного захисту інформації.
13. Засоби та заходи технічного захисту інформації.
14. Технічні канали витоку інформації і їх особливості.
15. Визначення термінів: захист інформації в системі, витік інформації, доступ до інформації в системі, знищення інформації в системі, криптографічний захист інформації.
16. Засоби та заходи криптографічного захисту інформації.
17. Тестування системи захисту інформації на проникнення.
18. Шляхи поширення акустичних хвиль.
19. Акустичний канал витоку інформації.
20. Акустовібраційні (віброакустичні) канали витоку інформації.
21. Що таке організаційні заходи захисту інформації?
22. Що таке технічні заходи захисту інформації?
23. Які активні і пасивні методи використовуються для виявлення закладних пристроїв на ОІД?
24. Заходи провідних країн світу щодо захисту кіберпростору.
25. Заходи України щодо захисту кіберпростору та інформаційного простору.
26. Загальні положення щодо вимог до конструкції і розміщення режимних приміщень.
27. Загальні положення ліцензійних умов надання послуг у галузі ТЗІ і КЗІ.
28. Правова основа технічного захисту інформації в Україні.
29. Організаційна структура системи захисту інформації на об’єктах інформаційної діяльності.
30. Властивості інформаційних технологій за ступенем охоплення завдань.
31. Інформаційні технології за способом побудови мережі.
32. Загрози оброблюваної засобами АС інформації.

ТЕСТИ ДЛЯ САМОПЕРЕВІРКИ

1. Прояви обмеження свободи слова та доступу громадян до інформації порушують таку властивість інформації:

а) конфіденційність;

б) цілісність;

в) доступність;

г) усі вищеперераховані властивості.

2. CERT-UA – це:

а) урядова команда реагування на комп'ютерні надзвичайні події України;

б) розвідувальний орган;

в) Державний центр кіберзахисту;

г) правильної відповіді немає.

3. Яка технологія створює маркер безпеки, який дає змогу користувачу ввійти на потрібний вебдодаток, використовуючи облікові дані з вебсайта в соціальних мережах?

а) менеджер паролів;

б) відкрита авторизація;

в) служба VPN;

г) приватний режим браузера.

4. Sandworm – це:

а) супутникова система;

б) хакерський підрозділ російської військової розвідки;

в) ісламська терористична організація;

г) контррозвідувальний орган України.

5. Споживач хоче роздрукувати фотографії, що зберігаються на обліковому записі у хмарному сховищі, використовуючи службу друку в інтернеті третьої сторони. Після успішного входу в обліковий запис у хмарі клієнту автоматично надають доступ до служби онлайн-друку третьої сторони. Що дозволило виконати цю автоматичну автентифікацію?

а) служба хмарного зберігання є довіреним програмним забезпеченням для служби онлайн-друку;

б) пароль, введений користувачем для служби онлайн-друку, аналогічний паролю, який використовується в службі хмарного зберігання;

в) користувач перебуває у незашифрованій мережі, і пароль служби хмарного зберігання доступний для перегляду службі онлайн-друку;

г) інформація про обліковий запис для служби хмарного зберігання була перехоплена шкідливою програмою.

6. Який інструмент використовується для надання списку відкритих портів на мережних пристроях?

а) Tracert;

б) Whois;

в) Ping4;

г) Nmap.

7. Користувач працює в інтернеті, використовуючи ноутбук та загальнодоступний WiFi у кафе. Що треба перевірити перш ніж підключитися до загальнодоступної мережі?

а) чи відімкнено адаптер Bluetooth на ноутбуці;

б) чи ноутбук вимагає автентифікації користувача для спільного використання файлів і медіа;

в) чи веббраузер ноутбука працює у приватному режимі;

г) чи встановлено на ноутбуці майстер-пароль для захисту паролів, що зберігаються у менеджері паролів.

8. Який тип технології може запобігти зловмисному програмному забезпеченню відстежувати дії користувачів, збирати особисту інформацію та створювати небажані оголошення, що з'являються на комп'ютері користувача?

а) антишпигунське ПЗ (antispyware);

б) двофакторна аутентифікація;

в) менеджер паролів;

г) фаєрвол (брандмауер).

9. Який тип атаки перериває роботу сервісів, навантажуючи мережні пристрої фіктивним трафіком?

а) нульовий день (zero-day);

б) сканування портів (port scans);

в) атака грубої сили (brute force);

г) DDoS.

10. Адміністратор вебсервера налаштовує параметри доступу так, щоб користувачі, перш ніж отримати доступ до певних вебсторінок, проходили автентифікацію. Яка вимога захисту інформації забезпечується завдяки цій конфігурації?

а) доступність (availability);

б) конфіденційність;

в) масштабованість (scalability);

г) цілісність.

11. Захист прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій щодо невтручання у приватне життя і захист персональних даних забезпечують таку властивість:

а) конфіденційність;

б) цілісність;

в) доступність;

г) усі вищеперераховані властивості.

12. Яка частина Ланцюга кібервбивства, що використовується зловмисниками, зосереджена на ідентифікації та виборі цілей?

а) експлуатація;

б) доставка;

в) розвідка;

г) озброєння.

13. Відповідають за забезпечення оборони України, захист її суверенітету, територіальної цілісності і недоторканності кордонів; протидіють зовнішнім загрозам воєнного характеру:

а) органи і підрозділи цивільного захисту;

б) суди загальної юрисдикції;

в) воєнна організація держави;

г) правоохоронні органи.

14. Отримання інформації під час безпосереднього спостереження / фіксації об'єктів неозброєним оком або з використанням оптичних приладів є цариною:

а) фотографічної і візуально-оптичної розвідки;

б) оптико-електронної розвідки;

в) радіоелектронної розвідки;

г) гідроакустичної розвідки.

15. Найбільш інформативним напрямом, що дає змогу повніше реалізувати найважливіший принцип комплексності ведення технічної розвідки, є:

а) вимірювально-сигнатурна розвідка;

б) магнітометрична розвідка;

в) сейсмічна розвідка;

г) комп'ютерна розвідка;

д) акустична розвідка.

16. Яке призначення руткітів?

а) відтворення себе незалежно від будь-яких інших програм;

б) маскування під легальну програму;

в) постачання реклами без згоди користувача;

г) отримання привілейованого доступу до пристрою, з приховання власної присутноті.

17. Адміністратор мережі проводить тренінг для співробітників офісу про те, як створити надійний і ефективний пароль. Який пароль, найімовірніше, буде найважче вгадати або зламати злочинцеві?

а) Drninjaphd;

б) super3secret2password1;

в) mk$$cittykat104#4;

г) 10characters.

18. Як користувач може завадити іншим прослуховувати мережний трафік під час роботи ПК через загальнодоступну точку доступу Wi-Fi?

а) з'єднуватися з використанням служби VPN;

б) відключити Bluetooth;

в) створити сильні та унікальні паролі;

г) використовувати шифрування WPA2.

19. Який інструмент може здійснювати аналіз трафіку та портів у режимі реального часу, а також дає змогу виявити сканування портів, атаки з ідентифікації та переповнення буфера?

а) Netflow;

б) SIEM;

в) Snort;

г) Nmap.

20. Яка основна мета кібервійни?

а) моделювання можливих сценаріїв війни між державами;

б) захист хмарних центрів обробки даних;

в) розвиток передових мережних пристроїв;

г) отримання переваги над супротивниками.

21. До сукупності основних суб'єктів національної системи кібербезпеки не належить:

а) Державна служба спеціального зв'язку та захисту інформації України;

б) Національна поліція України, Служба безпеки України;

в) Національний банк України;

г) Міністерство оборони України та Генеральний штаб Збройних Сил України;

д) правильної відповіді немає (усі вищеперераховані суб'єкти входять до національної системи кібербезпеки).

22. Кабінет Міністрів України:

а) визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного і воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних Сил України та інших військових формувань;

б) координує та контролює діяльність органів виконавчої влади у сферах національної безпеки і оборони; з урахуванням змін у геополітичній обстановці

вносить Президенту України пропозиції щодо уточнення Стратегії національної безпеки України, Стратегії кібербезпеки України та Воєнної доктрини України;

в) забезпечує державний суверенітет і економічну самостійність України, вживає заходів щодо забезпечення прав і свобод людини і громадянина, обороноздатності, національної безпеки України, громадського порядку і боротьби із злочинністю;

г) відповідно до основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику в інтересах національної безпеки України.

23. Ведуть боротьбу зі злочинністю і протидіють тероризму:

а) органи і підрозділи цивільного захисту;

б) суди загальної юрисдикції;

в) воєнні організації держави;

г) правоохоронні органи;

д) усі відповіді правильні.

24. Отримання інформації внаслідок приймання та аналізу електромагнітних випромінювань радіодіапазону, створюваних працюючими радіоелектронними засобами, є цариною:

а) фотографічної і візуально-оптичної розвідки;

б) оптико-електронної розвідки;

в) радіоелектронної розвідки;

г) гідроакустичної розвідки.

25. Діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу – це:

а) інформаційна експансія;

б) інформаційна агресія;

в) гібридна війна;

г) психологічна війна.

26. Яка найпоширеніша мета інфікування пошукової оптимізації (search engine optimization (SEO)?

а) побудувати ботнет зомбі;

б) змусити когось інсталювати шкідливе програмне забезпечення або розкрити особисту інформацію;

в) збільшити вебтрафік на шкідливі сайти;

г) переповнити мережний пристрій шкідливо сформованими пакетами.

27. Яке налаштування на бездротовому маршрутизаторі вважається нестандартним з погляду безпеки бездротової мережі?

а) заборона широкомовної трансляції SSID;

б) активація бездротової безпеки;

в) застосування шифрування WPA2;

г) зміна стандартного SSID та пароля бездротового маршрутизатора.

28. Який найкращий спосіб запобігти несанкціонованому використанню вашого Bluetooth?

а) використовуйте Bluetooth лише для підключення до смартфона або планшета;

б) використовуйте Bluetooth лише під час під'єднання до відомого SSID;

в) завжди відключайте Bluetooth, коли він активно не використовується;

г) завжди використовуйте VPN під час з'єднання з Bluetooth.

29. Який останній етап схеми Ланцюга кібервбивства (Cyber Kill Chain)?

а) зловмисні дії;

б) створення зловмисного навантаження;

в) збирання інформації про жертву;

г) дистанційне керування пристроєм-жертвою.

30. З якою метою мережний адміністратор використовує інструмент Nmap?

а) виявлення та ідентифікація відкритих портів;

б) ідентифікація конкретних мережних аномалій;

в) захист приватних IP-адрес внутрішніх хостів;

г) збір і аналіз попереджень щодо загроз і записів у журналах.

31. Яке твердження описує кібербезпеку?

а) це стандартна модель для розробки технологій брандмауера для боротьби з кіберзлочинцями;

б) це назва комплексного засобу безпеки для кінцевих користувачів, який захищає робочі станції від нападу;

в) це постійні зусилля, спрямовані на захист підключених до інтернету систем і пов'язаних з ними даних від несанкціонованого використання або пошкодження;

г) усі вищеперераховані властивості.

32. Верховна Рада України:

а) визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного і воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних Сил України та інших військових формувань;

б) координує та контролює діяльність органів виконавчої влади у сферах національної безпеки і оборони; з урахуванням змін у геополітичній обстановці вносить Президенту України пропозиції щодо уточнення Стратегії національної безпеки України, Стратегії кібербезпеки України та Воєнної доктрини України;

в) забезпечує державний суверенітет і економічну самостійність України, вживає заходів щодо забезпечення прав і свобод людини і громадянина, обороноздатності, національної безпеки України, громадського порядку і боротьби із злочинністю;

г) відповідно до основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику в інтересах національної безпеки України.

33. Sandworm – це:

а) супутникова система;

б) хакерський підрозділ російської військової розвідки;

в) ісламська терористична організація;

г) контррозвідувальний орган України.

34. Процес добування інформації за допомогою засобів, що включають вхідну оптичну систему з фотоприймачем та електронні схеми обробки електричного сигналу, які забезпечують приймання та аналіз електромагнітних хвиль видимого та інфрачервоного діапазонів, випромінюваних або відбитих об'єктами та місцевістю, є цариною:

а) фотографічної і візуально-оптичної розвідки;

б) оптико-електронної розвідки;

в) радіоелектронної розвідки;

г) гідроакустичної розвідки.

35. Який тип атаки дає змогу зловмиснику використовувати підхід грубої сили?

а) соціальна інженерія;

б) відмова в обслуговуванні (denial of service);

в) прослуховування пакетів (packet sniffing);

г) злам пароля (password cracking).

36. Яка технологія дає змогу користувачу уникнути витрат на обладнання та технічне обслуговування під час створення резервних копій даних?

а) магнітна стрічка;

б) мережне сховище (network attached storage);

в) зовнішній жорсткий диск;

г) хмарний сервіс.

37. Під час зберігання інформації на локальному жорсткому диску який спосіб захистить дані від несанкціонованого доступу?

а) двофакторна автентифікація;

б) створення копії жорсткого диска;

в) шифрування даних;

г) видалення важливих файлів.

38. Який інструмент може ідентифікувати шкідливий трафік, порівнюючи вміст пакету з відомими сигнатурами атаки?

а) NetFlow;

б) Zenmap;

в) IDS;

г) Nmap.

39. Що є прикладом Ланцюга кібервбивства (Cyber Kill Chain)?

а) група ботнетів;

б) серія хробаків, заснована на одному і тому ж базовому коді;

в) комбінація вірусів, хробаків і троянських коней;

г) сплановане розгортання кібератаки.

40. Під час опису зловмисного ПЗ в чому полягає різниця між вірусом і хробаком?

а) вірус може використовуватися для запуску DoS-атаки (але не для DDoS), а хробак може використовуватися для запуску як DoS-, так і DDoS-атак;

б) вірус націлений на отримання привілейованого доступу до пристрою, а хробак – ні;

в) на відміну від хробака, вірус може використовуватися як спосіб постачання реклами без згоди користувача;

г) вірус поширюється шляхом приєднання до іншого файла, тоді як хробак може розмножуватися самостійно.

41. Рада національної безпеки і оборони України:

а) визначає засади внутрішньої та зовнішньої політики, основи національної безпеки, формує законодавчу базу в цій сфері, схвалює рішення з питань введення надзвичайного і воєнного стану, мобілізації, визначення загальної структури, чисельності, функцій Збройних Сил України та інших військових формувань;

б) координує та контролює діяльність органів виконавчої влади у сферах національної безпеки і оборони; з урахуванням змін у геополітичній обстановці вносить Президенту України пропозиції щодо уточнення Стратегії національної безпеки України, Стратегії кібербезпеки України та Воєнної доктрини України;

в) забезпечує державний суверенітет і економічну самостійність України, вживає заходів щодо забезпечення прав і свобод людини і громадянина, обороноздатності, національної безпеки України, громадського порядку і боротьби із злочинністю;

г) відповідно до основних засад грошово-кредитної політики визначає та проводить грошово-кредитну політику в інтересах національної безпеки України.

42. Відповідають за забезпечення оборони України, захист її суверенітету, територіальної цілісності і недоторканності кордонів; протидіють зовнішнім загрозам воєнного характеру:

а) органи і підрозділи цивільного захисту;

б) суди загальної юрисдикції;

в) воєнна організація держави;

г) правоохоронні органи.

43. Найбільш інформативним напрямом, що дає змогу повніше реалізувати найважливіший принцип комплексності ведення технічної розвідки, є:

а) вимірювально-сигнатурна розвідка;

б) магнітометрична розвідка;

в) сейсмічна розвідка;

г) комп'ютерна розвідка;

д) акустична розвідка.

44. Який з прикладів ілюструє спосіб приховання шкідливого програмного забезпечення?

а) ботнет-зомбі передає хакеру особисту інформацію;

б) електронний лист надсилається працівникам організації із вкладенням (attachment), яке виглядає як антивірусне оновлення, але фактично містить шпигунську програму;

в) започатковано атаку проти публічного вебсайта інтернет-магазину з метою блокування відгуків на запити відвідувачів;

г) хакер використовує методики підвищення рейтингу вебсайта для перенаправлення користувачів на шкідливий сайт.

45. Чому пристрої IoT становлять більший ризик, ніж інші пристрої в мережі?

а) IoT-пристрої не можуть функціонувати в ізольованій мережі з єдиним підключенням до інтернету;

б) для пристроїв IoT потрібні незашифровані бездротові з'єднання;

в) більшість пристроїв IoT не вимагають підключення до Інтернету та не можуть отримувати нові оновлення;

г) більшість пристроїв IoT не отримують частого оновлення мікропрограми.

46. Користувачеві важко запам'ятовувати паролі для декількох облікових записів у інтернеті. Яке найкраще рішення варто спробувати користувачеві для вирішення цієї проблеми?

а) створити єдиний надійний пароль, який буде використовуватися для усіх облікових записів у інтернеті;

б) записати паролі на папері й ретельно їх заховати;

в) повідомити паролі адміністратору мережі або комп'ютерному спеціалісту;

г) зберегти паролі в централізованій програмі менеджера паролів.

47. Співробітник медичного бюро надсилає електронні листи пацієнтам з приводу нещодавніх відвідин ними медичного центру. Яка інформація піддаватиме ризику конфіденційність пацієнтів, якщо її долучити до електронного листа?

а) контактна інформація;

б) інформація про наступний візит;

в) записи пацієнтів;

г) ім’я та прізвище.

48. Компанія зазнає величезної кількості звернень до головного вебсервера. ІТ-відділ розробляє план додавання ще кількох вебсерверів для балансування навантаження і забезпечення надлишковості. Яка вимога інформаційної безпеки вирішується шляхом реалізації плану?

а) цілісність;

б) масштабованість (scalability);

в) конфіденційність;

г) доступність (availability).

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основна література

1. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін. Львів: Львівська політехніка, 2019. 580 с.

2. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ: Видавництво НА СБ України, 2020. 256 с.

3. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Видання друге, перероб. та доп. Одеса: ОНАЗ ім. О. С. Попова, 2019. 320 с.

4. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

5. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості Верховної Ради (ВВР)*. 2017. № 45.Ст. 403.

6. Закон України «Про захист персональних даних». (Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481).

7. Закон України «Про національну безпеку України», від 21.06.2018 № 2469-V.

8. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Редакція від 28.08.2021.

9. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури. Постанова КМУ від 19 червня 2019 р. № 518.

Допоміжна література

10. Декодування коду від RFID пристрою при скімінгу на частоті третьої гармоніки / В. Комаров, Д. Чернов, М. Прокофьєв, В. Крижановський. *Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф*. Львів: Видавництво Львівської політехніки. 2023. С. 157–158.

11. Захист NFC зв’язку від підслуховування на частотах вищих гармонік / В. Крижановський, Ю. Рассохіна, В. Комаров, М. Прокофьєв. *Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф*. Львів: Видавництво Львівської політехніки, 2023. С. 137–138.

12. Дереко В. Н. Теоретико-методологічні засади класифікації загроз об’єкту інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*, 2015. № 2(18). С. 16–23.

13. Дудатьєв А. В., Войтович О. П., Миронюк В. В. Моделі загроз соціотехнічній системі: соціальний аспект. *Вчені записки Таврійського національного університету. Технічні науки.* 2019. № 30(69). С. 97–102.

14. Дудатьев А. В., Войтович О. П., Миронюк В. В. Інформаційно-аналітичні центри в управлінні інформаційною безпекою держави. *Вісник Хмельницького національного університету*. 2020. № 1. С. 105–110.

15. Євграфов Д. В., Яремчук Ю. Є. Показники якості виявлення літер алфавіту спеціалізованим засобом перехоплення інформації з екранів моніторів на рідкокришталевих структурах. *Захист інформації.* 2021. Т. 23. № 4. С. 234–240.

16. Загоруйко Л., Половенко Л., Чернов Д. Структурування нейроподібної мережі для виявлення кібератак на інформаційно-комунікаційні системи. *Захист інформації і безпека інформаційних систем: матеріали IX Міжнар. наук.-техн. конф*. Львів: Видавництво Львівської політехніки. 2023. С. 99–101.

17. Прокофьєв М. І., Хорошко В. О., Хохлачева Ю. Є. Концепція застосування інформаційних впливів та протидія інформаційної зброї. *Правове, нормативне та матеріально-технічне забезпечення систем захисту інформації в Україні*. 2016. Вип. 1(31). С. 9–14.

18. Прокофьєв М. І., Хорошко В. О. Проблеми захисту інформації в Україні. *Правове, нормативне та матеріально-технічне забезпечення систем захисту інформації в Україні*. 2015. Вип. 2(30). С. 9–14.

19. Aleksieiev A., Prokofiev M., Shpatar P. A method of quantum communication using sideband-modulated infrared emission. *Proceedings Volume 12938. Sixteenth International Conference on Correlation Optics*; 129380T. 2024. DOI: 10.1117/12.3010050.

20. Hierl R., Neujahr H., Sandl P. Military Aviation. *Information Ergonomics*. 2012. P. 159–195.

21. Introducing the IBM Security Frameworkand IBM Security Blueprintto Realize Business-Driven Security. *International Technical Support Organization*. Dec. 2010.

22. Microwave food fat meter / K. Shevchenko, O. Yanenko, M. Prokofiev, S. Peregudov, V. Kuz. *Proceedings of the international scientific conference UNITECH'20 GABROVO*. Gabrovo: University publishing house «V. Aprilov», 2020. Vol. 1. P. 194–197.

23. Schneier B. Applied Cryptography. Protocols, Algorithms and Source Code in C. Indianapolis: John Wiley & Sons, 2016. 712 p.

24. Tsanov T., Terlemezyan L. Polymers & Polymer Composites. 1997. Vol. 6, № 7. P. 447–454.

Інформаційні ресурси в мережі Інтернет

25. Вступ до кібербезпеки: курс на освітній онлайн платформі Мережевої академії Cisco. URL: https://www.netacad.com/courses/cybersecurity/introduction-cybersecurity

26. Основи кібербезпеки: курс на освітній онлайн платформі Мережевої академії Cisco. URL: https://www.netacad.com/courses/cybersecurity/cybersecurity-essentials

27. Освітні курси Академії Cisco. URL: https://osvita.diia.gov.ua/korysni-posylannya?category=cisco-courses

28. Курси кібербезпеки Дія.Освіта – Протидія кіберзагрозам. URL: https://osvita.diia.gov.ua/signup?gclid=CjwKCAiA8YyuBhBSEiwA5R3-E-xlny5redljYcm4dnhtypTcfkuoMpWHCX0eGT_uA9WFCTOuWYU3BoCyCYQAvD_BwE

Навчальне видання

Михайло ПРОКОФЬЄВ
Людмила ПОЛОВЕНКО
Олександр ГРЕСЬ

ОСНОВИ КІБЕРБЕЗПЕКИ ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Методичні рекомендації до самостійної роботи
Частина 1

для здобувачів СО «Бакалавр»
спеціальності 125 Кібербезпека та захист інформації

Редактор Солдатова О. А.
Технічний редактор Гомон О. К.

Підписано до друку 20.02.2024 р.
Формат 60×84/16. Папір офсетний.
Друк – цифровий. Умовн. друк. арк. 5,12 .
Тираж 100 прим. Зам. № 6.

Донецький національний університет імені Василя Стуса
21021, м. Вінниця, вул. 600-річчя, 21.
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру
серія ДК № 5945 від 15.01.2018 р.