ЗМІСТ

ВСТУП

Навчальний посібник відображає сучасні погляди на стан розвитку теорії і практики технічного захисту інформації з обмеженим доступом.

Причому, основні визначення дисципліни сформульовані відповідно до законодавчих актів України [23]: технічний захист інформації — це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особистості, суспільства і держави; система технічного захисту інформації — це сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правова та матеріально-технічна база.

Особливого значення технічний захист інформації набуває як один із основних напрямів кіберзахисту в системах забезпечення кібербезпеки [18], а також у забезпеченні безпеки об'єктів критичної інфраструктури [18; 24].

У **першій частині** посібника наведені основні положення системного підходу щодо захисту інформації, загальних концептуальних підходів щодо побудови системи технічного захисту інформації в державі і в організації, характеристик інформації як предмета захисту, загроз безпеці інформації та методів технічного захисту інформації.

У **другій частині** посібника розглядаються особливості організаційного та методичного забезпечення системи технічного захисту інформації, основи побудови системи і основних підсистем технічного захисту інформації, що включає: типовий

підхід до побудови системи технічного захисту інформації організації, що включає застосування засобів технічної охорони об'єктів, засобів протидії спостереженню і підслухуванню, засобів попередження витоку інформації через побічні електромагнітні випромінювання і наведення.

Посібник містить також словники додаткових термінів і понять, одиниць вимірювання та покажчик ключових термінів і понять. Ключові терміни і поняття технічного захисту інформації, які формулюються у основному тексті посібника та у словнику додаткових термінів і понять, виділені жирним шрифтом, а посилання на них — курсивом. Наведені також англійські еквіваленти термінів і понять, а також їхня етимологія, тобто визначення походження слова шляхом співставлення його зі спорідненими словами тієї або іншої мови. Це дозволяє досить докладно окреслити предметну частину технічного захисту інформації та використовувати посібник як тлумачний словник.

Автори висловлюють щиру вдячність рецензентам: доктору педагогічних наук наук, професору С. М. Мамченку та доктору технічних наук, професору В.О.Хорошку за змістовні зауваження та рекомендації, які безумовно сприяли покращенню книги.

ПЕРЕЛІК АБРЕВІАТУР

Україномовні

АТС - БД -	автоматична телефонна станція база даних база знань
БЗ - ДРР -	дешифрувально-розвщувальна робота
ЕОТ - ЕПР -	електронно-обчислювальна техшка ефективна площа
ЕРС - ІТС -	розаювання електрорушшна сила
ЗТО - КА -	інформаційно-телекомунікаційна система зааб ТЄХНІЧНОЇ
КОПС - КПП	охорони космічний апарат
- МДН - НСД	комплекс охоронно-пожежної сигналізації
- ОС - ПВЧ -	контрольно-пропускний пункт
ПЗ - ПЗЗ -	метал-діелектрик-напівпровідник несанкціонований
ПКП -	доступ операційна система підсилювач високої частоти
ПЕМВН -	програмне забезпечення прилад із зарядовим зв'язком
ПЕОМ -	приймально-контрольний прилад
ПНБ - ПНЧ -	побічні електромагнітні випромінювання і наведення
ППЧ - ПЦС -	персональна електронно-обчислювальна машина
РЕЗ - РЛС -	прилад нічного бачення
СКУД - ТЗІ -	шдсилювач низької частоти
ТТХ -	підсилювач ПРОМІЖНОЇ частоти
	пульт централізованого спостереження
	радіоелектронний засіб
	радіолокаційна станція
	система контролю управління доступом
	ТЄХНІЧНИЙ захист інформації
	тактико-технічна характеристика

Англомовні

	ACOUStic INTelligence
	Domain Name System
	Code Division Multiple Access
	Charge-Coupled Device
	COMmunications INTelligence
	Estimate of Adversary Sequence Interruption
ACOUSINT -	Enhanced Data rates for Global Evolution
DNS - CDMA -	ELectronic INTelligence
CCD - COMINT	International Organization for Standardization
- EASI - EDGE -	Metal Insulator-Semiconductor Field-Effect Transistor
ELINT - ISO -	NUClear INTelligence
MISFET -	RADar INTelligence
NUCINT -	Wired Equivalent Privacy
RADINT - WEP	Wireless Local Area Network
- WLAN -	Wireless Metropolitan Area Networks
WMAN - WPA -	Wi-Fi Protected Access
WPAN -	Wireless Personal Area Network

Розділ 1

Системний підхід до технічного захисту інформації

1.1. Основні положення системного підходу до технічного захисту інформації

Сформувати уявлення про комплекс завдань щодо побудови системи технічного захисту Інформації, методів, заходів і засобів щодо її реалізації на об'єктах інформаційної діяльності організації найбільш доцільно на основі системного підходу
[3; 26].

Системний підхід [systems approach] — це дослідження об'єкта або процесу за допомогою моделі, званою системою. Цей підхід передбачає найвищий рівень опису об'єкта дослідження — системний. Найнижчим рівнем є рівень опису параметрів об'єкта — параметричний. Між ними розташовуються структурний і функціональний рівні (рис. 1.1).

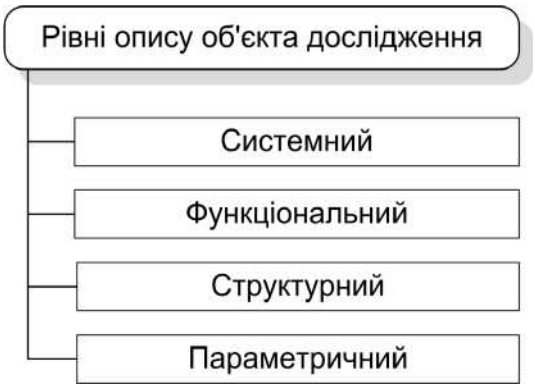

Рис. 1.1. Рівні опису об'єкта

Сутність системного підходу полягає в наступному:

— СУКУПНІСТЬ сил і засобів, ЯКІ забезпечують вирішення завдання, представляється у вигляді моделі, званою системою; система описується сукупністю параметрів;

— будь-яка система розглядається як підсистема більш складної системи, що впливає на структуру і функціонування розглянутої системи;

— будь-яка система має ієрархічну структуру, елементами і зв'язками якої не можна нехтувати без достатніх підстав;

— при аналізі системи необхідний облік зовнішніх і внутрішніх факторів, що впливають, прийняття рішень на основі частини з них без розгляду інших може привести до невірних результатів;

— властивості системи перевищують суму властивостей її елементів за рахунок якісно нових властивостей, відсутніх у її елементів — системних властивостей.

Ефективність реалізації системного підходу на практиці залежить від уміння фахівця виявляти і об'єктивно аналізувати все різноманіття факторів і зв'язків досить складного об'єкта дослідження, яким є, наприклад, організація як об'єкт захисту.

Необхідною умовою такого вміння є наявність у фахівця так званого системного мислення, що формується в результаті відповідного навчання та практики вирішення завдань, що слабо формалізуються.

Системне мислення [systems thmkmg] — це форма мислення, що характеризує здатність людини на несвідомому рівні вирішувати завдання дедуктивними методами. Ці методи стосовно до технічного захисту інформації передбачають:

— чітку постановку задачі, що включає визначення тематичних питань інформації та її джерел як об'єктів захисту, виявлення загроз цій інформації та формулювання цілей і завдань захисту інформації;

— розробку принципів і шляхів вирішення завдання;

— розробку методів вирішення завдань;

— створення програмного, технічного та методичного забезпечення вирішення завдань.

Системне мислення — це найважливіша якість не тільки фахівця із захисту інформації, а й будь-якого організатора і керівника. Якщо керівник не може швидко виявити фактори, що впливають на те чи інше рішення, і оцінити їх вагу, то неврахо-вані або необґрунтовано відкинуті фактори постійно будуть про себе нагадувати. Такий керівник перетворюється на борця з ним же створюваними проблемами.

Якщо системний підхід характеризує концептуальні погляди на шляхи вирішення завдань, що слабо формалізуються, то основу їх вирішення становить системний аналіз.

Системний аналіз [system analysis] — 1) Аналіз об'єкта дослідження як сукупності елементів, що утворюють систему. У наукових дослідженнях він передбачає оцінку поведінки об'єкта як системи з усіма факторами, які впливають на його функціонування. Системний аналіз можна здійснювати у відповідності до етапів системного аналізу. Кінцевим результатом системного аналізу є побудова моделі системи і розробка пропозицій з її удосконалення або зміни. 2) Аналіз призначення системи, яку передбачається проектувати, і встановлення множини вимог, яким вона повинна відповідати. Єдиної методики системного аналізу у наукових дослідженнях поки що немає. У практиці досліджень він застосовується з використанням таких методик:

— процедур теорії дослідження операцій, яка дає змогу дати кількісну оцінку об'єктам дослідження;
— аналізу систем дослідження об'єктів в умовах невизначеності;
— системотехніки, яка включає проектування і синтез складних систем у процесі дослідження їхнього функціонування.

Відповідно до вимог системного підходу сукупність взаємопов'язаних елементів, функціонування яких спрямоване на забезпечення безпеки інформації, утворює систему захисту інформації.

Такими елементами є люди, інженерні конструкції і технічні засоби, що забезпечують захист інформації незалежно від їх приналежності до інших систем.

Ядро системи захисту утворюють сили і засоби, основними

функціями яких є забезпечення інформаційної безпеки. Однак вони становлять лише частину сил і засобів системи захисту інформації.

Наприклад, в систему захисту інформації входять не тільки структурні підрозділи (служба безпеки, відділ режиму і секретності 1-й відділ тощо), призначені для захисту інформації, але й всі співробітники організації, зобов'язані в міру своєї відповідальності забезпечувати захист інформації. Отже, вони також є елементами системи захисту інформації організації. І якщо який-небудь співробітник організації порушить правила поводження з секретними документами, то можливий величезний збиток, незважаючи на бездоганну роботу інших елементів системи захисту.

Отже, структура (елементи та їх взаємозв'язок) системи захисту інформації держави, відомства, організації пронизує структуру держави, відомства, організації.

1.2. Цілі, завдання і ресурси системи захисту інформації

Цілі являють собою очікувані результати функціонування системи захисту інформації, а завдання те, що треба зробити для того, щоб система могла забезпечити досягнення поставлених цілей (рис. 1.2) [26].

Можливість вирішення завдань залежить від ресурсу, що виділяється на захист інформації.

Ресурс включає в себе людей, що вирішують завдання захисту інформації, фінансові, технічні та інші засоби, що витрачаються на захист інформації.

Входами системи захисту інформації є загрози інформації, а виходами — заходи, які треба застосувати для запобігання реалізації загроз або зниження їх до допустимого рівня.

Нарешті, заходи, дії і технології, що визначають заходи захисту, відповідні загрозам, утворюють процес.

Основною метою технічного захисту інформації є забезпечення її безпеки, при якій ризик зміни, знищення або розкрада-