МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний університет телекомунікацій

В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа

ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: СОЦІОТЕХНІЧНИЙ АСПЕКТ

Підручник

За загальною редакцією
доктора технічних наук, професора В. Б. Толубка

Затверджено Міністерством освіти і науки України
як підручник для студентів вищих навчальних закладів

Київ ДУТ 2015

ББК 351.86:004.056](075/8)
Б 91
УДК 67.401.212я73

Гриф надано Міністерством освіти і науки України
згідно з листом № 1/11-7193 від 14.05. 2014 р.

Рекомендовано вченою радою
Державного університету телекомунікацій
до друку та використання в навчальному процесі
(протокол № 9 від 26.02. 2014 р.)

А в т о р и:
В. Л. Бурячок, доктор технічних наук, професор;
В. Б. Толубко, доктор технічних наук, професор;
В. О. Хорошко, доктор технічних наук, професор;
С. В. Толюпа, доктор технічних наук, професор

Р е ц е н з е н т и:
доктор технічних наук, професор **Л. М. Щербак**;
доктор технічних наук, професор **В. Б. Дудикевич**;
доктор технічних наук, професор **Ю. Я. Самохвалов**

Б91 **Бурячок, В. Л.**
Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.
ISBN 978–966–2970–86–9

У підручнику висвітлено головні принципи забезпечення інформаційної та кібернетичної безпеки, розкрито їхню сутність, основний зміст та складові.

Значну увагу приділено типовим інцидентам у сфері високих технологій, а також методам і засобам соціального інжинірингу. Докладно розглянуто систему заходів із захисту від соціотехнічних атак. Наведено порядок здійснення процедур із тестування систем захисту інформації в інформаційно-комунікаційних системах на предмет проникнення, а також порядок оцінювання їхніх параметрів на різних рівнях.

Виклад зорієнтовано на майбутніх фахівців у галузі кібернетичної безпеки.

Пропонований матеріал буде корисний науковим і науково-педагогічним працівникам, профіль діяльності яких пов'язаний із забезпеченням інформаційної безпеки, а також аспірантам, магістрантам і студентам вищих навчальних закладів, що спеціалізуються у сфері управління інформаційною безпекою та систем захисту інформації згідно з освітнім напрямом «Інформаційна безпека».

ББК 67.401.212я73
УДК 351.86:004.056](075/8)

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АРМ — автоматизоване робоче місце
АСУ — автоматизована система управління
БД (БнД) — база даних (банк даних)
ДРР — дешифрувально-розвідувальна робота
ЕОМ — електронна обчислювальна машина
ЗІ — захист інформації
ЗПЗ — загальне програмне забезпечення
ІБ — інформаційна безпека
ІзОД — інформація з обмеженим доступом
ІКТ — інформаційно-комунікаційна технологія
ІР — інформаційний ресурс
ІС — інформаційна система
ІТ — інформаційна технологія
ІТС — інформаційно-телекомунікаційна система
КБ — кібернетична безпека
КбА — кібернетична атака
КбП — кібернетичний простір
КбТ — кібернетичний тероризм
КР — кібернетична розвідка
КСЗІ — комплексна система захисту інформації
ЛОМ — локальна обчислювальна мережа
МР — мережна розвідка
НСД — несанкціонований доступ
ОС — операційна система
ПАК — програмно-апаратний комплекс
ПЕОМ — персональна ЕОМ
ПЗ — програмне забезпечення
ПІБ — політика інформаційної безпеки
РІ — розвідувальна інформація
РІТС — розвідка інформаційно-телекомунікаційних систем
РСт — робоча станція
СЗІ — система захисту інформації
СІ — соціальний інжиніринг
СПЗ — спеціальне програмне забезпечення
СУБД — системи управління базами даних
ТЗІ — технічний захист інформації

ПЕРЕДМОВА

Науково-технічна революція початку XXI сторіччя спричинила в усьому світі глибокі системні перетворення. Передусім завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — *інформаційне суспільство*, а також *інформаційний* та *кібернетичний простори*, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу.

Проте через небачене досі поширення ІКТ та ІТС світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу. Тому цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи.

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 року № 2824-IV, а також відповідні закони України та Укази Президента України, присвячені цій проблемі, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України. Важливий практичний крок у реалізації наявної нормативно-правової бази було зроблено створенням 2007 року Центру реагування на комп'ютерні інциденти, що ввійшов до складу Державної служби спеціального зв'язку та захисту інформації України. На виконання статті 35 згаданої Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки (СБ) України на базі спеціального підрозділу для боротьби з кіберзагрозами запрацював Національний контактний пункт формату 24/7 із реагування та обміну терміновою інформацією про вчинені кіберзлочини. Окрім того, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення про початок створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року № 34 у структурі СБ України створено

Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ — Департамент боротьби з кіберзлочинністю та торгівлею людьми.

Такий стан справ фактично означає, що Україна поступово нагромаджує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Утім протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об'єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче. Одна з головних причин цих негараздів полягає в «незадовільному кадровому забезпеченні відомств відповідними фахівцями у сфері інформаційної безпеки», як наголошується в аналітичній доповіді Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України». Отже, найбільшу загрозу вітчизняним установам і відомствам становить відчутна нестача професіоналів з інформаційної та кібербезпеки, здатних:

- відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу;
- виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки;
- протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо.

Дедалі вища активність так званого когнітивного базису — звичайних користувачів, професійних шпигунів і/або хакерів (порушників), поряд зі стрімко зростаючою кількістю способів і методів, до яких вони вдаються з метою пошуку й збору інформації з відкритих і відносно відкритих джерел та її добування із закритих електронних джерел, потужний сплеск розвитку соціальних мереж — це ті чинники, що активізують кіберзлочинність, особливо з огляду на тенденції розвитку інтернету в напрямку інтеграції та об'єднання наявних можливостей у рамках єдиних багатокористувальницьких веб-платформ. Саме тому глобальна мережа перетворюється на засіб організації різного роду кібернетичних і соціотехнічних атак, несанкціонованого доступу (НСД) до чужих сайтів, створення сайтів-двійників тощо. Останнім часом такі дії неухильно виходять за межі окремих країн, випереджаючи за темпами зростання всі інші види організованої злочинності.

Вочевидь, чинити дієвий опір таким агресивним діям дуже складно. Адже заходи з ефективного запобігання небажаним витокам інформації мають крім суто технічних механізмів спиратися на методи й засоби соціального інжинірингу, систематизований виклад яких — одне з головних завдань пропонованого підручника. У кожному з п'яти його розділів поряд із теоретичними засадами забезпечення інформаційної та кібернетичної безпеки (розкриття змісту основних термінів і понять, визначень та математичних моделей процесів захисту від несакціонованого доступу тощо) висвітлюються найважливіші

аспекти відповідної діяльності, здійснюваної на базі чинних законодавчих і нормативних документів. Особливо важливі витяги з них наводяться в тексті.

Підручник має передусім спонукати читачів до самостійного пошуку практичних заходів із протидії сторонньому кібернетичному впливу за тих чи інших конкретних умов.

Поглибленому опрацюванню матеріалу підручника посприяє добірка питань для самоконтролю, якою завершується кожний його розділ.

Практичну спрямованість підручника підсилюють шість тематичних додатків, що охоплюють найширше коло споріднених питань.

РОЗДІЛ 1

КІБЕРПРОСТІР, КІБЕРБЕЗПЕКА ТА КІБЕРТЕРОРИЗМ: ПОНЯТТЯ І ВИЗНАЧЕННЯ

1.1. Кіберпростір і кібербезпека — головні ознаки нової інформаційної цивілізації. Заходи України із забезпечення кібербезпеки національної інфосфери та протидії проявам кіберзлочинності

Процеси формування та розвитку сучасного інформаційного суспільства, факт створення якого офіційно визнали представники держав Великої вісімки в ході Окінавської зустрічі в липні 2000 року, базуються, як відомо [1], на синтезі двох технологій — комп'ютерної і телекомунікаційної. Ці процеси підпорядковуються двом простим, але дуже змістовним законам.

Перший закон сформулював один із засновників корпорації Intel Гордон Мур: ***Кількість транзисторів у процесорах збільшуватиметься вдвічі протягом кожних півтора року***. Цей закон фактично пояснює виникнення нових, специфічних за формою і способами функціонування суб'єктів та об'єктів інформаційної інфраструктури, гарантоване зростання швидкості обчислень і обсягів оброблюваної інформації, а також формування на рубежі тисячоліть ***інформаційного простору*** — *глобального інформаційного середовища, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протиборчі сторони та їх навколишнє оточення з метою підтримання ухвалюваних рішень щодо створення оптимального задля досягнення поставлених цілей складу сил і засобів та їх ефективного застосування в різних умовах навколишньої обстановки.*

Другий закон належить Роберту Меткалфу — винахіднику мережі Інтернет: ***Цінність мережі перебуває у квадратичній залежності від кількості вузлів, що входять до її складу***. Отже, цей закон констатує, що основу сучасного інформаційного суспільства становлять мережі різного функціонального призначення, сукупність і взаємозв'язок яких, власне, і створюють інформаційний простір [1], а також новітні інформаційно-телекомунікаційні (ІТ) технології, які останнім часом:

1) стали важливою складовою суспільного розвитку та розвитку світової економіки в цілому, змінивши значною мірою механізми функціонування багатьох суспільних інститутів та інститутів державної влади;

2) увійшли до групи найбільш істотних факторів, що впливають на формування сучасного високоорганізованого інформаційного середовища й дають змогу на якісно новому рівні інформаційного обслуговування як у віртуальному, так і в реальному просторі вести повсякденну оперативну роботу, здійснювати аналіз стану і перспектив діяльності інформаційно-аналітичних підрозділів, а також добувати вихідні дані, необхідні для ухвалення раціональних і науково-обґрунтованих управлінських рішень.

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ-систем (ІТС) і мережних технологій різного функціонально-

го призначення, які в процесах обробки, передавання та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення (ПЗ) призвело, зрештою, до формування ***кіберпростору*** (КбП) (рис. 1.1) — високорозвиненої моделі об'єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів:

♦ подаються в деякому математичному, символьному (як сигнали, знаки, звуки, рухомі або нерухомі зображення) або в будь-якому іншому вигляді;

♦ розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для зберігання, обробки й передавання інформації;

♦ перебувають у постійному русі по сукупності ІТ-систем і мереж.

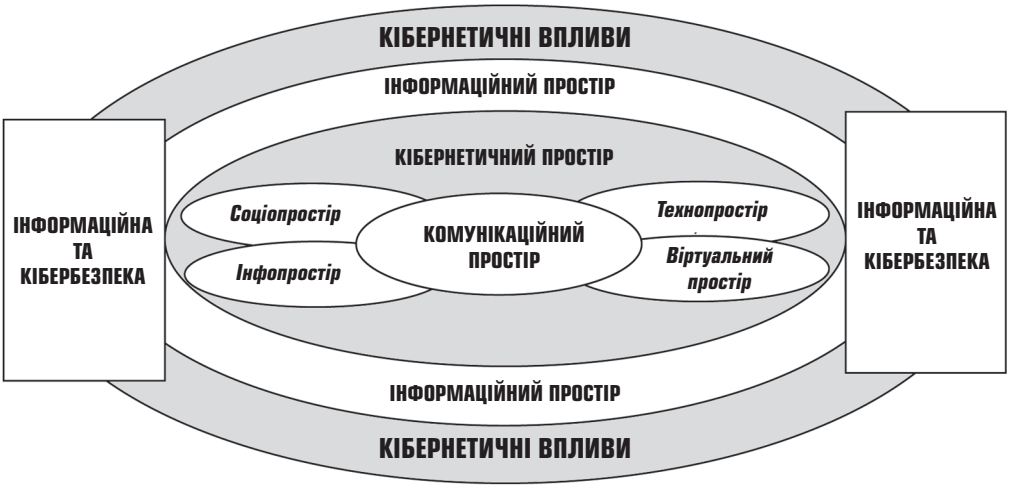


Рис. 1.1. Взаємозв'язок інформаційного та кіберпросторів

Уперше термін «кіберпростір» було використано у згаданій раніше Окінавській хартії глобального інформаційного суспільства та в Конвенції про злочинність у сфері комп'ютерної інформації від 23 листопада 2001 року. Сфера його дії на той час перебувала під впливом загальних механізмів правового регулювання суспільних відносин, обмежуючись специфічними об'єктами й інтересами суб'єктів правовідносин, а також комп'ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах. Нині кіберпростір має чимало визначень.

Наприклад:

1) відповідно до міжнародного стандарту [2], ***кіберпростір*** — це середовище існування, що виникло в результаті взаємодії людей, програмного забезпечення і послуг в інтернеті за допомогою технологічних пристроїв і мереж, під'єднаних до них, якого не існує в будь-якій фізичній формі;

2) відповідно до нормативної бази США [2], ***кіберпростір*** — це сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережні системи та пов'язану з ними фізичну інфраструктуру;

3) відповідно до офіційних документів Євросоюзу [2], ***кіберпрострір*** — це віртуальний простір, в якому циркулюють електронні дані світових персональних комп'ютерів (ПК);

4) відповідно до офіційних документів Великобританії [2], ***кіберпростір*** — це всі форми мережної, цифрової активності, що включають у себе контент та дії, здійснювані через цифрові мережі;

5) відповідно до офіційних документів Німеччини [2], ***кіберпростір*** — це вся інформаційна інфраструктура, доступна через інтернет поза будь-якими територіальними кордонами.

Серед інших варто також відзначити й такі визначення поняття КбП [2]:

• поліморфний віртуальний простір, що генерує інформаційна система (ІС) як у формі складних світів, так і у простих реалізаціях (типу електронної пошти, глобальної навігації тощо);

• комунікаційне середовище, утворене системою зв'язків між об'єктами кіберінфраструктури — електронними обчислювальними машинами, комп'ютерними мережами, програмним забезпеченням та інформаційними ресурсами, використовуване для забезпечення певних інформаційних потреб;

• штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп'ютерних систем управління і обробки інформації, що забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, а також обмін електронними повідомленнями, даючи змогу із застосуванням електронних інформаційних образів у режимі реального часу вступати у відносини (взаємодіяти) щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання інформаційних послуг, ведення електронної комерції тощо);

• простір, сформований інформаційно-комунікаційними системами, в якому відбуваються процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, поданої у вигляді електронних комп'ютерних даних;

• об'єкти інформаційної інфраструктури що керуються інформаційними (автоматизованими) системами управління та інформації, що в них циркулює;

• середовище, утворене організованою сукупністю інформаційних процесів на основі взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Як випливає зі щойно викладеного, найбільш відмітними ознаками кіберпростору як субстанції, створенню якої сприяли передусім такі чинники: зміна характеру діяльності людини з ухвалення рішень; упровадження електронно-цифрових форм створення, обробки, зберігання та переміщення інформації, перехід від паперового діловодства до електронного тощо,— **абсолютна більшість фахівців *вважає його неперевершені можливості зі створення незлічених зв'язків між окремими індивідами і соціальними групами та з надання різнопланових інформаційних послуг.*** З урахуванням характерних особливостей кіберпростору як сфери вчинення заздалегідь спланованих деструктивних дій на кшталт проникнення в ІТС один одного, блокування або виведення з ладу найбільш уразливих елементів цих систем, дезорганізації оборонних автоматизованих систем управління (АСУ) протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (поряд із наземною, морською й повітряно-космічною сфера-

ми) і своєрідної сполученої ланки між такими поняттями, як інтернет і кібернетика, усе це, у свою чергу, дає змогу:

• виокремити в цьому просторі систему певних відношень між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури;

• схарактеризувати злочини, втручання і загрози, пов'язані з особливостями існування та передавання інформації;

• визначитись із можливими його дійовими особами (рис. 1.2) [1];

• розглядати кіберпростір із позицій власне віртуального і реального (електронного, комунікаційного, кібернетичного, інформаційного, особливого психологічного) тлумачення як додатковий вимір бойового простору, розрізняючи при цьому фізичний (інфраструктура, кабелі та роутери), семантичний (дані) і синтаксичний (протоколи передавання даних) рівні тощо.

Рис. 1.2. Дійові особи кіберпростору та їхній вплив на інформаційну і кібербезпеку

З огляду на сказане, а також з урахуванням результатів проведеного багатокритеріального аналізу (табл. 1.1) [2] і відсутності в Україні стандартизованого визначення розумітимемо під ***кіберпростором*** *віртуальне комунікаційне середовище, утворене системою зв'язків між користувачами та об'єктами інформаційної інфраструктури*, такими як ***електронний інформаційний ресурс*** (ІР), ***системи й мережі*** всіх форм власності, керовані автоматизованими системами управління, що використовуються не лише для перетворення та передавання інформації, котра в них циркулює, із метою забезпечення інформаційних потреб суспільства, а й для впливу на аналогічні об'єкти протиборчої сторони.

Таблиця 1.1

Аналіз дефініцій поняття кібербезпеки за базовими критеріями

Походження дефініції чи її автори	Базовий критерій									
	Virt	HF	Soft	PhI	Net	INet	IServ	IRes	MSys	IPr
Стандарт ISO/IES 27032	+	+	+	+	+	+	+			
Нормативна база США				+	+			+		+
Офіційні документи ЄС	+							+		
Концепція кібербезпеки Великобританії					+			+		+
Законодавство Німеччини				+		+				
В. Харченко, О. Корченко та ін.	+									+
В. Бурячок	+		+	+	+			+		+
М. Погорецький, М. Шеломенцев				+	+		+	+	+	+
С. Мельник, О. Тихомиров					+			+		+
Д. Дубов, М. Ожеван								+	+	

Примітка. Для позначення базових критеріїв використано такі ідентифікатори [2]: **Virt** — критерій віртуальності; **HF** — критерій урахування людського чинника; **Soft** — критерій урахування ПЗ; **PhI** — критерій наявності фізичної інфраструктури; **Net** — критерій наявності мережної складової; **INet** — критерій урахування поняття «Інтернету»; **IServ** — критерій можливості надання інформаційних послуг; **IRes** — критерій урахування інформаційних ресурсів; **MSys** — критерій наявності системи управління; **IPr** — критерій урахування інформаційних процесів.

Нині важливість кіберпростору підтверджується появою концепцій ведення боротьби в ньому та створенням у складі збройних сил багатьох країн світу спеціальних структур на зразок (рис.1.3):

- об'єднаного Кіберкомандування (U. S. Cyber Command-USCYBERCOM) та спеціалізованого кібернетичного розвідувального центру у США;
- Управління мережних операцій у Німеччині;
- Центрального управління з кібербезпеки, Оперативного центру забезпечення кібербезпеки (CSOC) та Центру державного зв'язку (GCHQ) у Великобританії;
- Центру інформаційних систем Служби безпеки (CISSS) та Національного агентства безпеки інформаційних систем (ANSSI) у Франції;
- спеціалізованого центру захисту національного кіберпростору Tehila в Ізраїлі;
- кіберпідрозділів у складі Федеральної служби безпеки Росії тощо.

Усі ці підрозділи призначено для ведення ***кіберборотьби*** — *комплексу заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані IT-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань.*

Такий стан справ зумовлює небачені досі глибинні зміни у ставленні більшості держав світу до безпеки власного інформаційного та кіберпростору, а отже, і до посиленого захисту інформації, засобів її обробки та кіберсередовища, в якому ця інформація циркулює (рис. 1.4), тобто до вжиття заходів із забезпечення інформаційної та кібербезпеки.

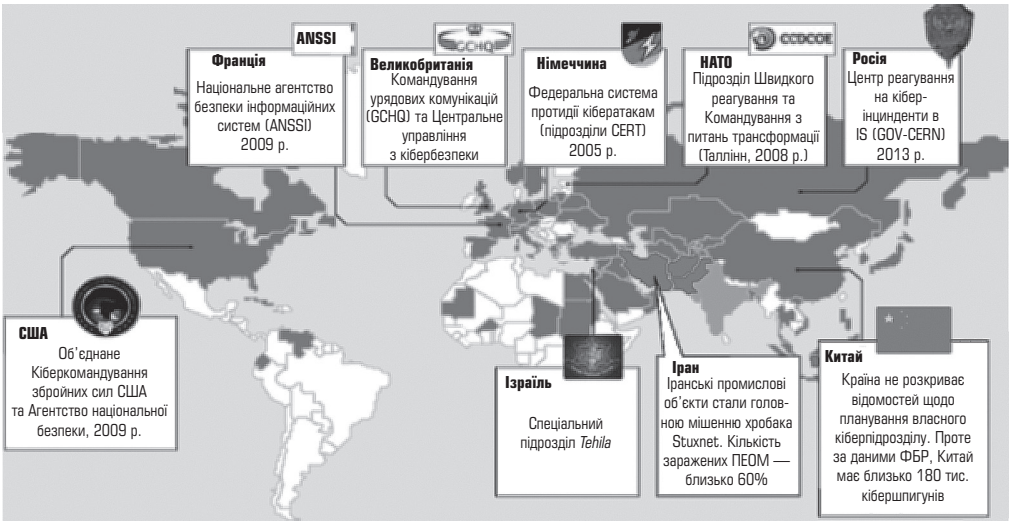


Рис. 1.3. Маштаби ураження та протидії сторонньому кібервпливу

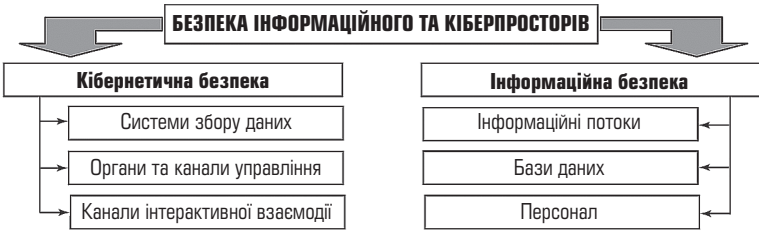


Рис. 1.4. Об'єкти впливу в інформаційному та кіберпросторі

При цьому ***інформаційну безпеку*** (ІБ) у найзагальнішому розумінні можна визначити як *такий стан захищеності інформаційного простору держави, за якого неможливо завдати збитку властивостям об'єкта безпеки, що стосуються інформації та інформаційної інфраструктури, і який гарантує безперешкодне формування, використання й розвиток національної інфосфери в інтересах оборони* (рис. 1.5).

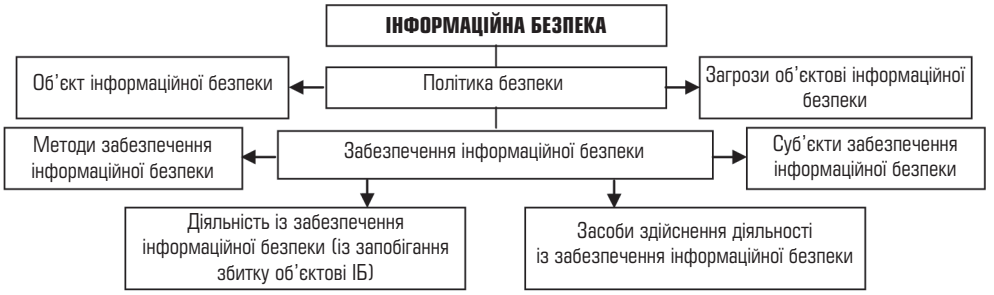


Рис. 1.5. Структура поняття «інформаційна безпека»

Спектр інтересів ІБ щодо інформації, інформаційних систем та інформаційних технологій як об'єктів безпеки можна поділити на такі основні категорії: ***доступність*** — можливість за прийнятний час отримати певну інфор-

маційну послугу; ***цілісність*** — актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованого змінювання; ***конфіденційність*** — захищеність від несанкціонованого ознайомлення (рис. 1.6).

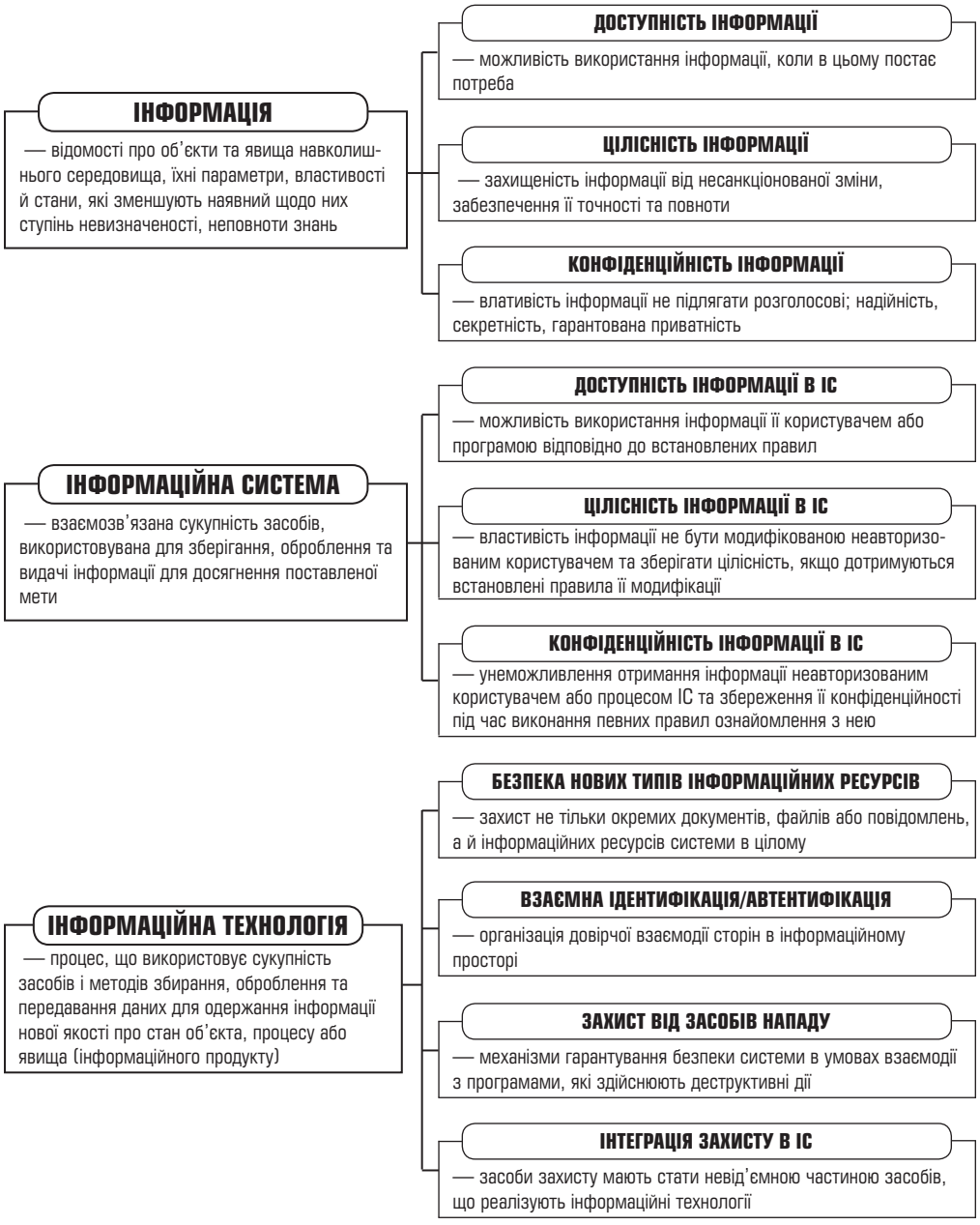


Рис. 1.6. Інформаційні системи та технології як об'єкти ІБ

Головні загрози, які можуть спричинити порушення цих категорій, а також негативно вплинути на компоненти ІС, призвівши навіть до їх втрати, знищення чи збою функціонування, такі: *розголошення інформації*, її *витік* або *несанкціонований доступ* до такої інформації (рис. 1.7).

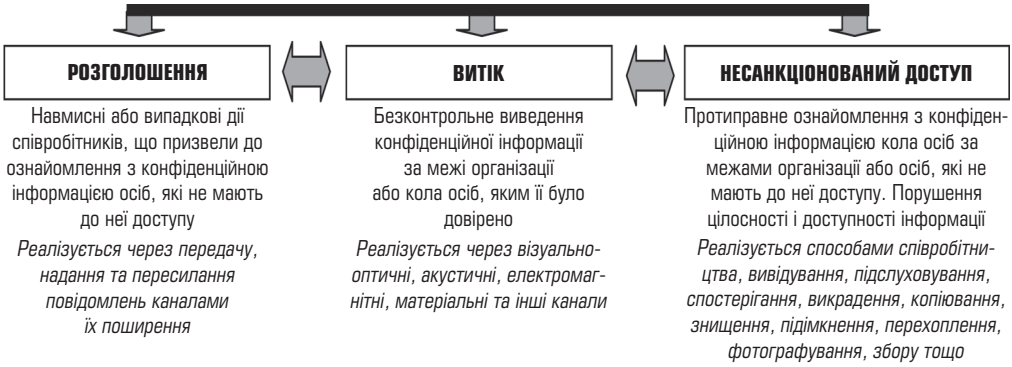


Рис. 1.7. Способи нанесення збитку інформаційній безпеці

Методи (рис. 1.8), завдяки яким цьому можна запобігти, забезпечивши відповідний рівень ІБ, доцільно класифікувати так:

• *сервіси мережної безпеки* (механізми захисту інформації, оброблюваної в розподілених обчислювальних системах і мережах);

• *інженерно-технічні методи* (мають на меті забезпечення захисту інформації від витоку по технічних каналах);

• *правові та організаційні методи* (створюють нормативну базу для організації різного роду діяльності, пов'язаної із забезпеченням ІБ);

• *теоретичні методи забезпечення* (розв'язують завдання формалізації різного роду процесів, пов'язаних із забезпеченням ІБ).

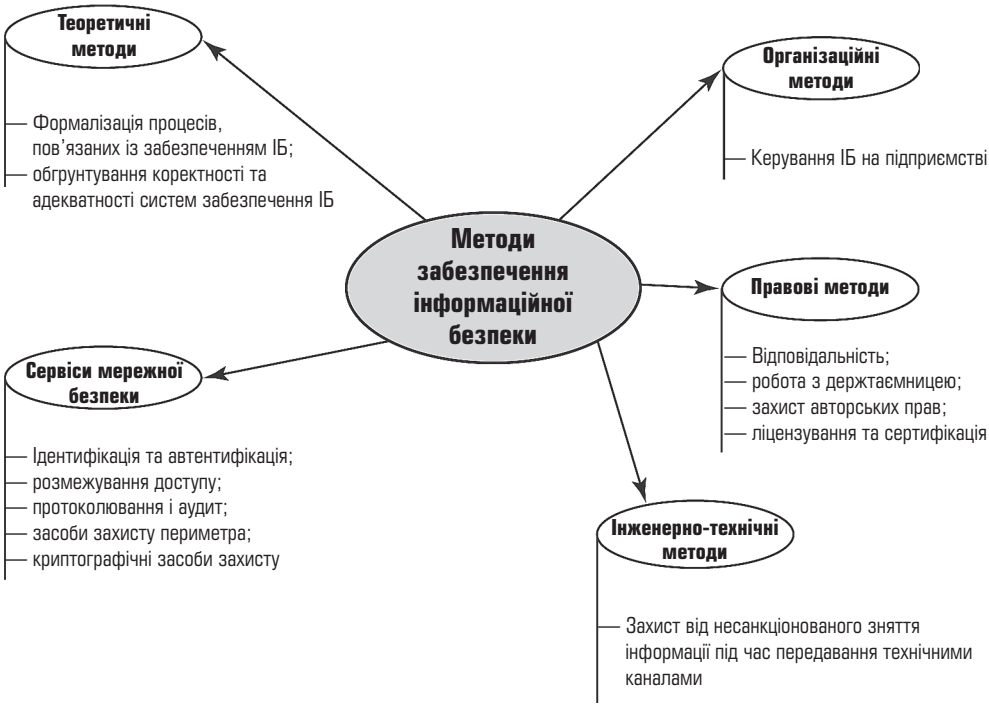


Рис. 1.8. Основні методи забезпечення інформаційної безпеки

Кібербезпеку (рис. 1.9) можна визначити як *стан захищеності кіберпростору держави в цілому або окремих об'єктів її інфраструктури від ризику стороннього кібервпливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним і/або національним інтересам* [1; 3–9].

Рис. 1.9. Складові кібернетичної безпеки

Досягається такий стан завдяки сукупності активних захисних і розвідувальних дій, що у процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо IP, ІКТ і ІТС (рис. 1.10).

Рис. 1.10. Взаємозв'язки і мотивація здійснення кібервпливів

Такі дії спрямовуються на досягнення і утримання потенційними протиборчими сторонами переваги у протидії новим загрозам безпеці для власних об'єктів критично важливої фізичної, інформаційної та кіберінфраструктури (рис. 1.11).

Головні проблеми забезпечення кібернетичної безпеки постають з таких причин:

- відсутності чіткого усвідомлення ролі та значення кібербезпекової складової в системі забезпечення національної безпеки держави;
- дефініційної, термінологічної та нормативно-правової неврегульованості у сфері кібербезпеки;
- залежності держави від програмних і технічних продуктів іноземного виробництва;

Рис. 1.11. Критично важливі складові фізичної, інформаційної та кіберінфраструктури

• відсутності належної координації діяльності відповідних відомств, а отже, і неузгодженості дій зі створення окремих елементів системи кібербезпеки;

• дефіциту щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів.

Комплексну сутність кібербезпеки за таких умов унаочнює схема, подана на рис. 1.12.

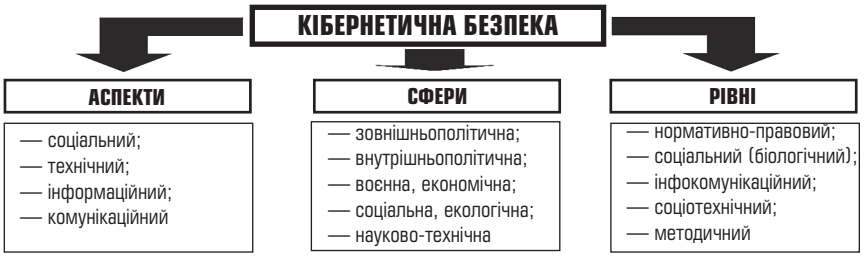


Рис. 1.12. Сутність кібернетичної безпеки

Протягом останніх років Україна, як і більшість країн світу, робить певні кроки в розбудові інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також у боротьбі з кіберзлочинністю. Нормативно-правову базу в цих сферах діяльності становлять такі документи:

• Конвенція Ради Європи про кіберзлочинність [10], ратифікована Законом України від 7.09.2005 року № 2824-IV;

• Закони України «Про інформацію» [11], «Про основи національної безпеки України» [12], «Про Державну службу спеціального зв'язку та захисту інформації України» [13], «Про телекомунікації» [14], «Про захист інформації в інформаційно-телекомунікаційних системах» [15], «Про доступ до публічної інформації» [16], «Про оборону України» [17], «Про засади внутрішньої і зовнішньої політики» [18], «Про об'єкти підвищеної небезпеки» [19];

• Укази Президента України, зокрема про Доктрину інформаційної безпеки [20], Стратегію національної безпеки України [21] та Воєнну доктрину України [22];

• окремі положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБОУ.

При цьому ключову роль у забезпеченні кібербезпеки відіграють:

1) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та IT-системах;

2) Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007–2015 роки» [23], у запропонованих змінах до якого наголошується на необхідності створення національної системи кібербезпеки;

3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» [24], яким має бути впроваджено низку термінів, пов'язаних із кібербезпекою.

Практичними кроками щодо реалізації чинної нормативно-правової бази стало створення 2007 року в складі Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ) України Центру реагування на комп'ютерні інциденти. На виконання статті 35 Конвенції про кіберзлочинність у червні 2009 року при Службі безпеки України на базі спеціального підрозділу для боротьби з кіберзагрозами утворено Національний контактний пункт формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені кіберзлочини. Окрім цього, Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» від 10 грудня 2010 року № 1119/2010 ухвалено рішення щодо початку створення Єдиної загальнодержавної системи протидії кіберзлочинності. Іншим Указом Президента України «Про внесення змін до деяких законів України про структуру і порядок обліку кадрів Служби безпеки України» від 25 січня 2012 року №34 у структурі СБ України створено Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки. З огляду на ступінь та динаміку поширення комп'ютерних інцидентів теренами України в липні 2010 року в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ — Департамент боротьби з кіберзлочинністю і торгівлею людьми.

Сьогодні фахівці з кіберзахисту від ДССЗЗІ, СБ та МВС України стикаються у своїй роботі з численними труднощами, не маючи змоги самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному та кіберпросторі. Через це їм доводиться дедалі активніше шукати шляхів співробітництва з аналогічними організаціями світового співтовариства, використовуючи для цього всі наявні можливості й механізми, які є в розпорядженні кожної з країн [25].

Відчутний поштовх до активізації зусиль у цьому напрямку дало ухвалення організацією НАТО програмного документа під назвою «Рамки для співробітництва у питаннях кібернетичного захисту між НАТО та державами-партнерами», який було розповсюджено у Штаб-квартирі Альянсу 2 квітня 2009 року. У документі наголошується, що головний елемент політики НАТО у сфері кіберзахисту полягає в тому, що держави — члени Альянсу несуть пряму відповідальність за захист власних національних комунікацій та інформаційних систем. Альянс, у свою чергу, повинен бути здатний надати підтримку своїм партнерам, які зазнали кібератак міжнаціонального значення. Цим документом передбачено, зокрема, що головні цілі співпраці НАТО з державами-партнерами у сфері кіберзахисту полягають у підвищенні здатності НАТО та держав-партнерів у сфері захисту критичних комунікаційних та інформаційних інфраструктур проти кібератак, наданні допомоги у відновленні нормального функціонування відповідної інфраструктури після кібератак, а також у створенні основ для вжиття заходів із підтримки потерпілих від кібератак. Відповідно до головних положень згаданого документа країни-партнери закликаються до невідкладної гармонізації національного законодавства у сфері кібернетичної безпеки з відповідними міжнародними нормами, такими як Конвенція Ради Європи з питань кіберзлочинності, із неодмінним дотриманням таких головних принципів.

1. Співпраця між НАТО та країною-партнером має бути взаємовигідною в такому сенсі: Альянс може надати країні-партнерові інформацію та підтримку у сфері кібербезпеки, якщо ця країна неухильно виконує умови взаємодії.

2. НАТО може надати країні-партнерові як експертну допомогу, так і свої технічні можливості для захисту від кібернетичних атак.

3. Країни-партнери можуть звертатися з пропозиціями щодо співпраці у сфері кіберзахисту та отримання підтримки з боку НАТО, якщо зазнають кібератак національного масштабу.

4. Альянс і партнери мають уникати дублювання зусиль, що докладаються в рамках інших міжнародних організацій, залучених до захисту ІС від кібератак.

5. Наявність угоди про безпеку між НАТО та країною-партнером має визначати обсяги допомоги та інформаційного обміну. Проте інформацію стосовно захисту критичної інфраструктури національних комунікаційних та інформаційних систем буде позначено та передано належним чином лише в разі потреби ознайомлення з нею.

Документ, про який ідеться, визначає також сфери співробітництва НАТО з державами-партнерами у сфері кіберзахисту, а саме: узагальнений обмін інформацією щодо відповідної політики та доктрин; обговорення технічних засобів захисту комунікаційної та інформаційної інфраструктури (може бути передбачено на більш змістовному рівні співробітництва). Окремо в згадуваному документі наголошується на таких моментах.

По-перше, країни-партнери можуть звертатися з пропозиціями стосовно проведення консультацій із питань кібернетичного захисту у форматі «28+1» або «28+*n*»;

По-друге, процес планування та оцінювання сил, а також щорічні національні програми мають слугувати головними інструментами налагодження співпраці з державами-партнерами в питаннях кіберзахисту з якомога повнішим урахуванням їхніх індивідуальних потреб і обставин. Загальна

кількість Цілей партнерства в рамках ППОС, схвалених для України, дорівнює 96, з них на Збройні сили України покладено 70; на МВС України — 8; на МЗС України — 6; на СБУ — 11; на Мінфін України — одну.

По-третє, потенціал Центру передового досвіду із захисту від кібернетичних загроз в Таллінні (Естонія), Центру передового досвіду із боротьби проти тероризму в Анкарі (Туреччина), Програми НАТО «Наука заради миру та безпеки» і Комітету з планування цивільного зв'язку може використовуватися країнами-партнерами у плані підготовки відповідного персоналу.

Згідно зі сказаним основні напрямки подальшого співробітництва України з НАТО у сфері кіберзахисту, а отже, і створення загальнодержавної системи кібернетичної безпеки мають бути такі:

1. Формування культури та проведення інформаційно-пропагандистської кампанії про значущість проблематики кібербезпеки держави за допомогою:

• активного інформування про кібернетичні втручання і загрози, про потенційні уразливості ІТ-систем і мереж, а також способи їх компенсації;

• розширення співпраці державних органів з ІТ-компаніями, некомерційними організаціями з метою популяризації та впровадження на практиці безпечної поведінки в кіберпросторі;

• стимулювання заходів боротьби з кіберзлочинністю і кібертероризмом, кібершпіонажем і кіберактивізмом;

• підвищення рівня безпеки електронних послуг, що надаються державою власному населенню;

• організації профілактичної роботи з потенційними жертвами кіберзлочинів, керівниками малого і середнього бізнесу.

2. Створення механізму моніторингу кібернетичних втручань і загроз, а також своєчасного ухвалення рішень щодо реагування на їх прояви за рахунок:

1) розроблення ключових моделей кібернетичних втручань і загроз, а також систем моніторингу їх реалізації;

2) формування критеріїв (наприклад, прогнозованих людських втрат, масштабів економічних збитків, загроз щодо дестабілізації суспільства), згідно з якими об'єкти інформаційного та кіберпросторів віднесено до критичної інформаційної і кіберінфраструктури;

3) проведення активних розвідувальних дій у кіберпросторі потенційних протиборчих сторін, а також завдяки захисту власної інфосфери (рис. 1.8) від негативних чинників:

• деструктивного впливу на програмно-математичне забезпечення, комп'ютерні мережі та телекомунікаційні засоби обміну даними;

• електромагнітного та фізичного ураження елементів ІТ-систем та мереж;

• консцієнтального (вплив на свідомість і моральний стан) та семантичного (вплив на якість інтерпретації інформації) впливу, а також електромагнітного ураження працівників органів управління;

• радіоелектронного подавлення елементів систем передавання даних і радіонавігації, систем телефонного і супутникового зв'язку, а також систем зв'язку з рухомими об'єктами;

4) зменшення вартості усунення наслідків кібернетичних втручань і загроз (створення розподілених структур, створення бекапів) тощо.

3. Забезпечення безпеки державних інформаційних ресурсів за рахунок:

• стандартизації об'єктів зберігання ІР та регламентів міжвідомчої взаємодії;

• гарантування безпеки механізмів електронної міжвідомчої взаємодії;

• мінімізації кількості шлюзів, що сполучають державні інформаційні системи з мережею Інтернет для максимізації їхньої безпеки.

4. Підвищення надійності критичної кіберінфраструктури за рахунок:

• створення механізмів моделювання і прогнозування кібервтручань та кіберзагроз;

• упровадження системи обміну інформацією щодо захисту об'єктів критично важливої інформаційної та кіберінфраструктури;

• забезпечення прийнятної автономності кореневої інфраструктури інтернету;

• розроблення механізмів протистояння використання інтернету в терористичних цілях.

5. Підтримка вітчизняних виробників програмно-апаратного забезпечення шляхом:

1) стимулювання розробки власної елементної бази і апаратних засобів, а також вітчизняного ПЗ і СПЗ, що впливатимуть на процеси:

• виявлення, проведення аналізу та своєчасного реагування на нові види кібернетичних втручань і загроз, а також ідентифікації відомих;

• ідентифікації користувачів, персоналу та можливих порушників;

• забезпечення конфіденційності, цілісності та доступності до ІР;

• несанкціонованого отримання інформації з ІТ-систем та мереж;

• формування політики безпеки щодо контролю мережного доступу;

• проектування та створення систем виявлення атак і захисту від них;

• виділення ресурсів, ранжування обраних контрзаходів за ступенем важливості з реалізацією та тестуванням найбільш пріоритетних;

• проведення аудиту та сертифікації нових СПАК, використовуваних у державній і військовій системах управління;

2) ліцензування ПЗ, що має базовий функціонал нейтралізації кібервтручань і кіберзагроз.

6. Підвищення компетентності фахівців різних сфер діяльності у питаннях кібербезпеки за рахунок:

• розроблення і впровадження програми навчання фахівців у галузі кібербезпеки, здатних до прогнозування можливих ризиків від кібернападів та оцінювання їх наслідків;

• реалізації механізмів набору персоналу необхідної кваліфікації для забезпечення кібербезпеки державних ІТ-систем і мереж тощо;

7. Вироблення і реалізація єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та ІТ-інфраструктури від деструктивного кібернетичного впливу на базі:

• формування і реалізації цільових науково-технічних програм у галузі кібербезпеки;

• цільового фінансування, підтримання та проведення НДДКР із кібербезпеки.

8. Реалізація механізмів партнерства держави, бізнесу й громадян у сфері кібербезпеки за рахунок:

• упровадження механізмів обміну інформацією державних ситуаційних центрів і центрів реагування на прояви стороннього кібервпливу з представниками бізнесу та громадського суспільства;

• підвищення ефективності взаємодії провайдерів інтернет-послуг та користувачів в аспекті інформування про кібервтручання і загрози, потенційні уразливості ІТ-систем і мереж;

• організації співпраці державних і бізнесових інституцій, а також окремих громадян у питаннях розроблення сучасних програмно-апаратних засобів забезпечення кібербезпеки.

9. Удосконалення національного нормативно-правового та понятійно-термінологічного апарату кібербезпеки завдяки:

1) перегляду рекомендацій щодо придбання раціональних програмних засобів захисту від стороннього кібервпливу;

2) регулювання консультативних механізмів із питань забезпечення діяльності у сфері боротьби з кіберзлочинністю і кібертероризмом;

3) актуалізації нормативно-правових актів України відповідно до сучасних світових загроз, практик і технологій;

4) внесення змін до низки чинних нормативно-правових актів України, які регулюють відносини й визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів.

10. Організація міжнародного співробітництва у сфері кібербезпеки шляхом:

1) створення міжнародного експертного центру з питань регулювання взаємовідносин у галузі телекомунікацій та зв'язку;

2) удосконалення механізмів надання взаємодопомоги в технічних і методологічних аспектах випереджувального виявлення джерел, фіксування та оперативного обміну інформацією про факти здійснення кібератак, а також запобігання їхньому деструктивному впливу на ІР;

3) удосконалення організаційно-правових норм міжнародної взаємодії у процесі боротьби з кіберзлочинністю і кібертероризмом та внесення змін і доповнень до низки чинних міжнародних нормативно-правових документів:

• Конвенції Ради Європи про кіберзлочинність 2001 року (зважаючи на те, що її положення порушують принцип державного суверенітету та узаконюють проведення наступальних міждержавних кібератак під виглядом оперативно-розшукових заходів);

• Рекомендацій Міжнародного союзу електрозв'язку (серія Х: Мережі передавання даних, взаємозв'язок відкритих систем та безпека. Безпека електрозв'язку. Огляд кібербезпеки), в яких вперше визначено зміст термінів «кіберсередовище» і «кібербезпека»;

• Положень Женевських і Гаазьких конвенцій, стислу характеристику яких наведено в табл. 1.2 [1] (з урахуванням нових меж кібервоєн конкретні пропозиції щодо коригування цих Положень внесли в лютому 2011 року фахівці з Нью-Йоркського інституту EastWest [1] на щорічній конференції Munich Security Conference).

Реалізація перелічених заходів має відбуватися в кілька етапів за неухильного дотримання таких принципів:

1) верховенства права, законності та пріоритету додержання прав і свобод людини і громадянина;

2) партнерства держави та приватного сектору з метою вироблення нових, більш оптимальних рішень;

3) пріоритетного розвитку та підтримки вітчизняного кібернетичного (або інформаційного) сектору;

Таблиця 1.2

Характеристика Женевських і Гаазьких конвенцій

Документ	Назва	Дата	Кількість статей
Женевська конвенція	Про поліпшення участі поранених на полі бою	1864 р.	10
Гаазька конференція II	Про закони й звичаї сухопутної війни	1899 р.	60 (55 у додатках)
Гаазька конференція IV	Про закони й звичаї сухопутної війни	1907 р.	64 (56 у додатках)
Женевський протокол	Про заборону застосування на війні задушливих, отрутних та інших подібних газів і бактеріологічних засобів	1925 р.	—
Женевська конвенція I	Про поліпшення долі поранених і хворих у діючих арміях	1864 р. (нова ред. 1949 р.)	77 (13 у додатках)
Женевська конвенція II	Про поліпшення долі поранених, хворих та осіб, які потерпіли при корабельних аваріях, зі складу збройних сил на морі	1949 р.	63
Женевська конвенція III	Про поводження з військовополоненими	1929 р., (нова ред. 1949 р.)	143
Женевська конвенція IV	Про захист цивільного населення під час війни	1949 р.	180 (21 у додатках)
Женевська конвенція	Про заборону розробки, виробництва й накопичення запасів бактеріологічної (біологічної) і токсичної зброї та про їх знищення	1975 р.	15
Протокол I	Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року стосовно захисту жертв міжнародних збройних конфліктів	1977 р.	102
Протокол II	Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року стосовно захисту жертв збройних конфліктів неміжнародного характеру	1977 р.	28
Протокол III	Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року стосовно прийняття додаткової відмітної емблеми	2005 р.	17

4) відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури, дієвості, комплексності і постійності заходів забезпечення кібербезпеки держави;

5) участі інституцій громадянського суспільства в забезпеченні кібернетичної безпеки держави.

Відповідну роботу слід проводити поетапно.

На *першому етапі* з урахуванням досвіду інших країн та особливостей українських реалій має бути вдосконалено понятійно-термінологічний та нормативно-правовий апарат, створено ключові елементи Єдиної загальнодержавної системи кібербезпеки, проведено заходи з підготовки структурних підрозділів спецпризначення та ЗС України до ведення дій в умовах кібервійни, сформовано базис підготовки спеціалізованих кадрів, створено міжвідомчі та

центральні органи, а також удосконалено підрозділи власної інформаційної (кібернетичної) безпеки державних установ (відомств) та комерційних організацій (структур).

На *другому етапі* — удосконалено міжнародні правила поведінки держав у кіберпросторі та відповідне нормативно-правове підґрунтя, упроваджено програми підтримання вітчизняної інноваційної продукції щодо протидії сторонньому кібернетичному впливу, розгорнуто мережі CERT по всій Україні.

На *третьому етапі* — проведено коригування Стратегії за результатами оцінювання ефективності її реалізації та нових викликів.

Проте існує ціла низка проблем, які заважають Україні створити дієздатну систему протидії внутрішнім і зовнішнім загрозам власному інформаційному та кіберпростору. Головні з них такі [1]:

- складність структури ІКТ та національного кіберпростору;
- наявність якісних відмінностей кіберзброї від зброї звичайної;
- ускладненість щодо розмежування воєнних і цивільних об'єктів критичної інфраструктури держави в кіберпросторі;
- можливість недержавних суб'єктів та неавторизованих (індивідуальних) користувачів виступати в ролі гравців у кіберпросторі та проблематичність щодо їх виявлення;
- можливість прихованого проведення протиборчими сторонами кібератак та кібероперацій у кіберпросторі один одного;
- значна вразливість інфосфери України через надмірну присутність у ній західних програмних продуктів (зокрема, фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва;
- деградація науково-технічного потенціалу України, нерозвиненість національної інноваційної системи в інфосфері та низький рівень конкурентоспроможності в ній;
- непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами та силовими структурами України, що спеціалізуються на проблемах кіберзахисту, а також їх незадовільне кадрове забезпечення кваліфікованими фахівцями з цих питань;
- відсутність єдиного понятійно-термінологічного поля кібербезпеки України як головної складової безпеки інформаційної, а також системних нормативно-правових документів, які б регламентували діяльність зазначених відомств, правоохоронних і силових структур у сфері кіберзахисту;
- відсутність у вітчизняному законодавстві визначень таких важливих термінів, як «*кібервійна*», «*кіберзахист*» та «*кібербезпека*» (на відміну від *інформаційної безпеки*, сутність якої викладено в ст. 17 Конституції України), «*комп'ютерна злочинність*» і «*комп'ютерний тероризм*» (останні два поняття знайшли певне відображення в Законі України «Про основи національної безпеки» та доктрині ІБ України);
- відсутність загальнонаціонального координаційного центру, здатного узгоджувати й координувати діяльність правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпростору України та керувати проведенням комплексних навчань із забезпечення кібернетичної безпеки держави в інфосфері на кшталт навчань «Cyber Storm», які проводяться в США, і/або «Cyber Europe», що проводяться в ЄС (див. додаток Б).

Такий стан справ фактично є каталізатором для ініціювання втручань в інфосферу України, результатом чого може стати порушення управління державою, її інституціями та окремими об'єктами критично важливої інформаційної і кіберінфраструктури, виникнення техногенних катастроф. Саме тому найбільш пріоритетним напрямком керівництво України вважає нині реформування власної інформаційної безпеки за рахунок створення дієвої системи кібербезпеки, розбудова якої потребує розв'язання багатьох завдань як соціального і техногенного, так і, особливо, організаційного характеру.

Найбільш актуальні серед цих завдань такі [26]: чітке визначення функцій суб'єктів забезпечення кібернетичної безпеки та розподіл повноважень між ними; забезпечення належної координації діяльності як загальних суб'єктів забезпечення кібернетичної безпеки, так і відповідних спеціальних суб'єктів; розробка й упровадження найсучасніших підходів, форм і методів забезпечення кібернетичної безпеки, а також застосування дієвих стимулів для залучення до такого роду діяльності фахівців високого рівня кваліфікації.

1.2. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. Процедура обрання раціонального варіанта реагування на кібернетичні втручання і загрози

Із розвитком ІКТ, ІТС та глобальної мережі Інтернет світове співтовариство, отримавши небачені досі можливості в плані обміну інформацією, стало надзвичайно вразливим щодо стороннього кібернетичного впливу [3; 4; 9], а саме щодо *фактично неприхованих спроб впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної і/або спеціальної техніки й відповідного програмного забезпечення — **кібервтручань**, а також інших проявів їхнього дестабілізуючого впливу на той чи інший об'єкт, здійснюваного за рахунок технологічних можливостей інформаційного і кіберпростору, зі створенням небезпеки — так званих **кіберзагроз***, як для цього простору, *так і для свідомості кожної людини*.

Нині з метою уникнення багатозначності тлумачень відповідних термінів інструктивні матеріали Інтерполу поділяють їх на групи, що охоплюють:

- власне комп'ютерні інциденти, які полягають, наприклад, у втручанні в роботу обчислювальних систем, порушенні авторських прав на програмне забезпечення, а також у розкраданні даних і комп'ютерного часу;
- інциденти, пов'язані з комп'ютерами, що супроводжують здебільшого протиправні дії з фінансового шахрайства;
- мережні інциденти, що призводять до укладання незаконних угод.

Під ***інцидентами*** у сфері високих технологій розумітимемо *події, що полягатимуть в реалізації певної загрози та порушенні встановленого рівня безпеки інформаційно-комунікаційних систем* (рис. 1.13). ***Процесом управління інцидентами*** називатимемо *процес реєстрації інформації про стан безпеки та рівноваги ІКС, передавання інформації в пункти її нагромадження, переробки й аналізу, з ухваленням прийняття рішення та формуванням певного керуючого впливу на об'єкт управління*.

Інша класифікація таких дій визначає *сім основних їх груп*, які характеризують передусім способи, що їх використовують зловмисники для здійснення нападу, а саме: перехоплення паролів інших користувачів; «соціальна інже-

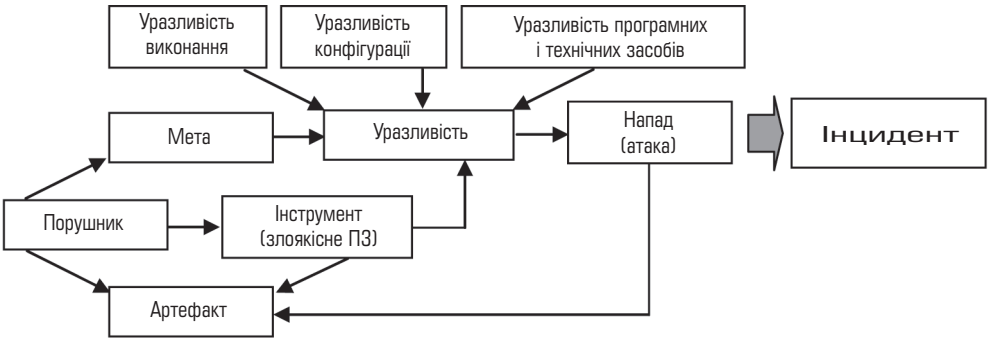


Рис. 1.13. Діаграма виникнення інцидентів у сфері високих технологій

нерія»; використання помилок ПЗ і програмних закладок, а також помилок механізмів ідентифікації користувачів і недосконалості протоколів передавання даних; одержання інформації про користувачів стандартними засобами операційних систем; блокування сервісних функцій системи, що зазнає атаки.

Зауважимо, що інтерес у плані класифікації кібернетичних втручань і загроз становить схема, запропонована Конвенцією Ради Європи 2001 року й спрямована на боротьбу з кіберзлочинністю [9]. У ній йдеться про чотири можливі групи таких дій.

1. *Інциденти, що мають на меті завдати шкоди конфіденційності, цілісності й доступності комп'ютерних даних та систем* і реалізуються через:

• несанкціонований доступ в інформаційне середовище (протиправний навмисний доступ до комп'ютерної системи або її частини, а також до ІР протиборчої сторони, здійснений в обхід систем безпеки);

• втручання в дані (протиправна зміна, ушкодження, вилучення, перекручування або блокування комп'ютерних даних і керуючих команд за допомогою кібератак на інформаційні системи, ресурси та мережі державного і військового управління);

• втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи через розробку та поширення вірусного ПЗ, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби й системи телекомунікацій і зв'язку, на обробку та передавання інформації, на системи захисту ІР, систем і мереж, програмно-математичне забезпечення, протоколи передавання даних, алгоритми адресації та маршрутизації);

• незаконне перехоплення (протиправне навмисне аудіовізуальне і/або електромагнітне перехоплення не призначених для загального доступу комп'ютерних даних, переданих СІТС в обхід заходів безпеки);

• незаконне використання комп'ютерного й телекомунікаційного обладнання або його повне вилучення.

2. *Шахрайство та підробка, пов'язані з використанням комп'ютерів*, а саме:

• підробка документів із застосуванням комп'ютерних засобів (протиправне навмисне внесення, змінювання, вилучення або блокування комп'ютерних даних, що призводить до зниження вірогідності документів);

• шахрайство із застосуванням комп'ютерних засобів (втручання у функціонування комп'ютерної системи з метою навмисного протиправного одержання економічної вигоди).

3. *Інциденти, пов'язані з розміщенням у мережах протиправної інформації* (наприклад, поширенням дитячої порнографії).

4. *Інциденти щодо авторських і суміжних прав*.

Наприклад, у США згідно із законодавством цієї країни до таких дій відносять [3; 4]: несанкціонований доступ до інформації з комп'ютера, використовуваного урядовим відомством, ушкодження або порушення функціонування останнього; шпигунство, шахрайство, загрози, вимагання, шантаж та інші протиправні діяння, вчинені з використанням комп'ютера; торгівля викраденими або підробленими пристроями доступу, які можуть бути використані для одержання грошей (товарів, послуг), комп'ютерними паролями або аналогічною інформацією; навмисне ушкодження майна, устаткування, ліній і систем зв'язку; перехоплення й розголошення повідомлень, переданих по телеграфу, усно або електронним способом; порушення конфіденційності електронної пошти й голосових повідомлень; несанкціоноване одержання або видозміна повідомлень, що зберігаються в пам'яті комп'ютера, а також створення перешкод для санкціонованого доступу до таких повідомлень.

У Великобританії до протиправних дій у сфері ІТ-технологій відносять [9]: навмисний протизаконний доступ до комп'ютера або комп'ютерної інформації, що циркулює в ньому; розголошення персональних даних, виготовлення й поширення порнографічних матеріалів.

У ФРН до таких протиправних дій відносять [9]: неправомірний доступ до комп'ютерної інформації, її несанкціоновану модифікацію, підробку, приховання або використання; руйнування, ушкодження, приведення в непридатність технічних засобів обробки інформації; порушення таємниці телекомунікаційного зв'язку; комп'ютерне шахрайство; незаконне втручання в роботу телекомунікаційних систем.

У Франції протиправними діями у сфері ІТ-технологій, як правило, вважають [9]: перехоплення, розкрадання, використання або розголошення повідомлень, переданих засобами зв'язку; незаконний доступ до автоматизованої системи обробки даних; порушення або перешкоджання нормальній роботі комп'ютерної системи; знищення або модифікацію інформації в автоматизованій інформаційній системі; уведення або зберігання в пам'яті ЕОМ заборонених законом даних; порушення порядку автоматизованої обробки персональних даних; збір і обробку даних у незаконний спосіб; зберігання певних даних понад установлений законом строк; несанкціоноване використання даних; знищення, псування або розкрадання будь-якого документа, техніки, споруди, устаткування, установки, апарата, технічного пристрою або системи автоматизованої обробки даних, а також внесення в них змін; збір або передавання інформації, що міститься в пам'яті ЕОМ чи картотеці, іноземній державі; знищення, розкрадання, вилучення або копіювання даних, що мають характер секретів національної оборони й містяться в пам'яті ЕОМ або картотеках, а також ознайомлення із цими даними сторонніх осіб; терористичні акти, пов'язані з діяннями у сфері інформатики.

Наведений перелік протиправних дій хоча й не є вичерпним, усе ж дає змогу [1; 9]:

• умовно об'єднати зазначені типи дій у *дві категорії* — ***втручання*** і ***загрози***, спрямовані безпосередньо на порушення нормального функціонування ІТС та підімкнених до них комп'ютерів (*тип 1* — за схемою, пропонованою Конвенцією Ради Європи 2001 року), а також «традиційні» протиправні дії (*типи*

2, 3 і 4 — за тією самою схемою), що або пов'язані з комп'ютером (*computer related*), або вчинені за його допомогою (*computer facilitated*);

• дійти висновку, що зазначені та подібні до них дії у кіберпросторі вийшли за межі окремих країн й отримали істотну фінансову підтримку на базі високоякісних комунікацій;

• формалізувати зазначені типи дій за допомогою моделі, яка включатиме в себе три головні етапи — 1) етап вивчення певного об'єкта; 2) етап здійснення нападу на нього; 3) етап приховування слідів цього нападу, а також принаймні по дві стадії в кожному з етапів: перша — стадія інформаційного обміну, а друга — стадія здійснення самого нападу на соціальному (біологічному), інфокомунікаційному та соціотехнічному рівні. Ці стадії, у свою чергу, включатимуть у себе низку операцій: по-перше, обміну даними, рекогносціювання, сканування та складання карти — операцій, характерних для інформаційного обміну, і, по-друге, операцій з одержання доступу, розширення повноважень, крадіжки інформації, зомбування, знищення слідів, створення «чорних ходів» і відмови в обслуговуванні, характерних для стадії здійснення нападу.

Згідно зі сказаним узагальнена модель системи управління інцидентами ІБ набирає вигляду:

$$Model_{IKC}^{INC} = \\ = \left(INC, SEC, CRI, KBS, X, Y, S, DMF, AGT, ARS, TRS, IRS, MST, T, SYN\right),$$

де INC — управління інцидентами (внутрішніми та зовнішніми); SEC — мета; CRI — критерії оцінювання стану безпеки; KBS — база знань про внутрішні та зовнішні інциденти; X — вхідні впливи; Y — реакція на внутрішні та зовнішні інциденти; S — стан системи; DMF — функція ухвалення (реагування), що поділяється на два етапи: на першому ухвалюється рішення про включення елемента ARS до набору TRS, а на другому (згідно з результатом виконання першого етапу) — рішення про включення елемента ARS до набору IRS; AGT — множина програмно-реалізованих мобільних інтелектуальних агентів; ARS — набір ресурсів інформаційної безпеки, які доступні агентам; TRS — тестовий набір ресурсів інформаційної безпеки; IRS — інцидентно-орієнтовані набори ресурсів; MST — стратегія управління інцидентами; T — час; SYN — самоорганізація.

При цьому під ***внутрішнім інцидентом*** розумітимемо такий інцидент, джерелом якого є порушник, безпосередньо пов'язаний із постраждалою стороною (рис. 1.14). Серед найпоширеніших системних подій такого типу можна виокремити *витік конфіденційної інформації*; *неправомірний доступ до інформації*; *вилучення інформації*; *компрометацію інформації*; *саботаж*; *шахрайство за допомогою ІТ*; *аномальну мережну активність*; *аномальне поводження бізнес-додатків*; *використання активів установи в особистих цілях або в шахрайських операціях*.

Під з***овнішнім інцидентом*** — інцидент, джерелом якого є порушник, безпосередньо не пов'язаний із постраждалою стороною. До системних подій такого типу належать *шахрайство в системах електронного документообігу*; *атаки типу «відмова в обслуговуванні» (DoS), у тому числі розподілені (DDoS)*; *перехоплення й підміна трафіку*; *неправомірне використання бренду установи в мережі Інтернет*; *фішинг*; *розміщення конфіденційної (провокаційної) інформації в мережі Інтернет*; *злам або спроба зламу мережних*

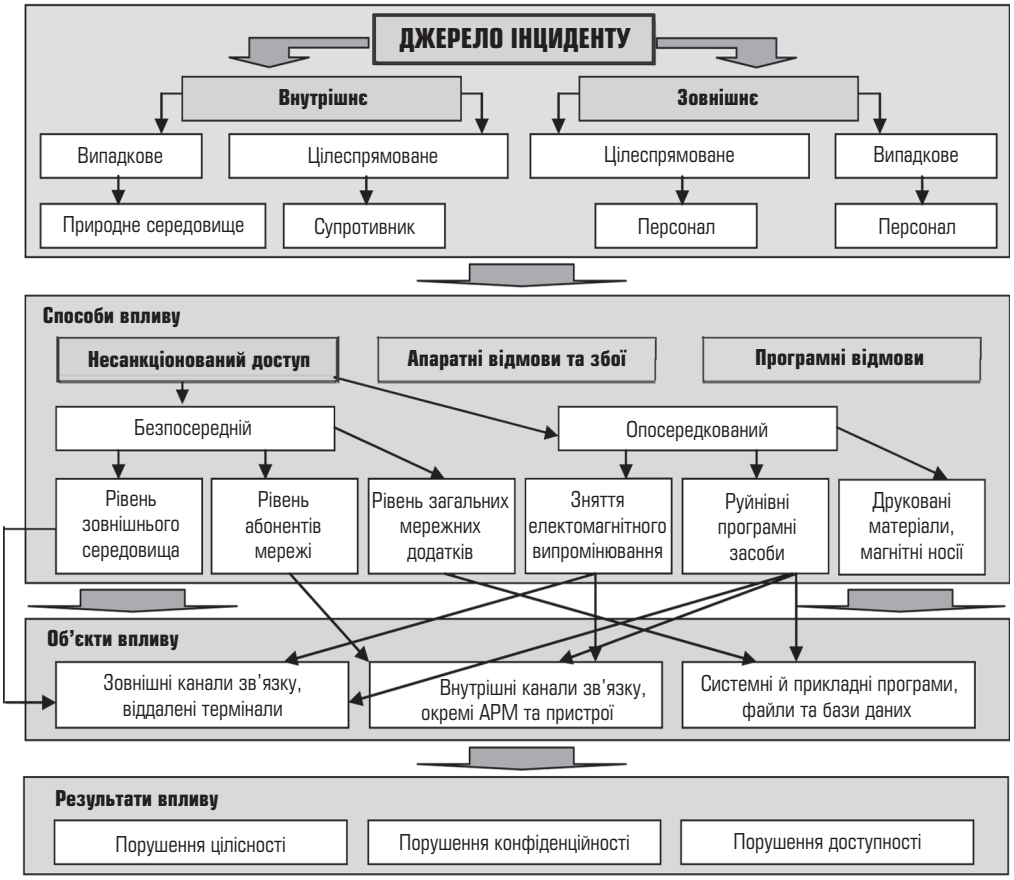


Рис. 1.14. Класифікація джерел інцидентів, а також способів, об'єктів та результатів їхнього впливу

вузлів; *сканування порталу установи або мережі*, *вірусні атаки*; *неправомірний доступ до конфіденційної інформації*; *анонімні листи* (*листи з погрозами*) тощо.

Усі такі джерела згідно з кодифікатором, використовуваним Міжнародною кримінальною поліцією — Інтерполом, мають власний ідентифікатор, який починається з літери Q й може бути використаний для характеристики таких дій:

1) QA — несанкціонований доступ або перехоплення:
   QAH — комп'ютерний абордаж;
   QAI — перехоплення;
   QA1 — крадіжка часу;
   QAZ — інші види несанкціонованого доступу й перехоплення;
2) QD — зміна комп'ютерних даних:
   QDL — логічна бомба;
   QDT — троянський кінь;
   QDV — комп'ютерний вірус;
   QDW— комп'ютерний хробак;
   QDZ — інші види зміни даних;
3) QF — комп'ютерне шахрайство (*computer fraud*):

QFC — шахрайство з банкоматами;
QFF — комп'ютерна підробка;
QFG — шахрайство з ігровими автоматами;
QFM — маніпуляції з програмами вводу/виводу;
QFP — шахрайство з платіжними засобами;
QFT — телефонне шахрайство;
QFZ — інші види комп'ютерного шахрайства;

4) QR — незаконне копіювання («піратство»):
QRG — комп'ютерні ігри;
QRS — інше програмне забезпечення;
QRT — топографія напівпровідникових виробів;
QRZ — інше незаконне копіювання;

5) QS — комп'ютерний саботаж:
QSH — з апаратним забезпеченням;
QSS — із програмним забезпеченням;
QSZ — інші види саботажу;

6) QZ — інші комп'ютерні злочини:
QZB — із використанням комп'ютерних дощок оголошень;
QZE — розкрадання інформації, що становить комерційну таємницю;
QZS — передавання інформації конфіденційного характеру;
QZZ — інші комп'ютерні злочини.

З огляду на неготовність більшості організацій до обробки таких подій, що потенційно загрожують їхньому бізнесу, а також на ускладненість у відновленні нормального функціонування пошкоджених унаслідок атак систем нагально необхідним стає *процес управління інцидентами інформаційної безпеки*, який включає в себе аналіз рівнів ІБ, оцінювання ефективності заходів із забезпечення безпеки, упровадження коригувальних, попереджувальних або інших заходів (рис. 1.15).

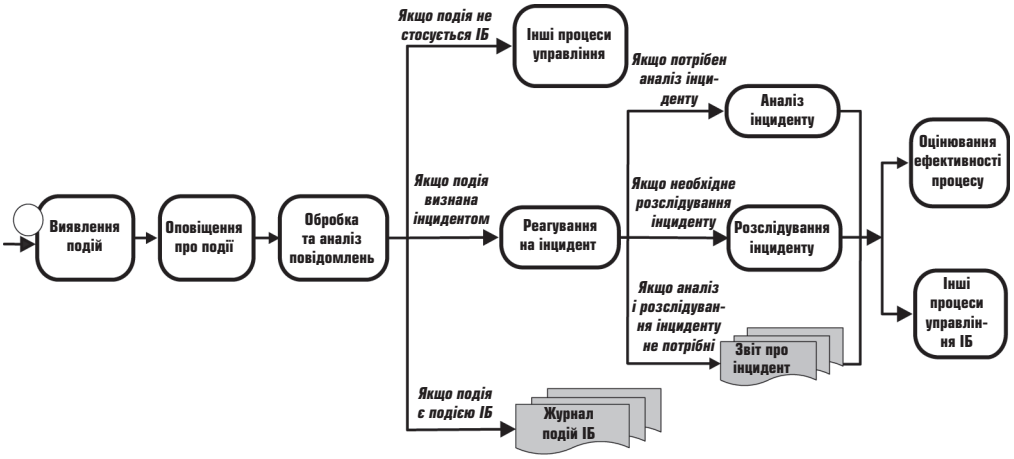


Рис. 1.15. Процес управління інцидентами ІБ

До найбільш небезпечних інцидентів належать [27]:

1) пошукова оптимізація (SEO — *Search Engine Optimization*), яку застосовують зловмисники для поширення шкідливих програм. Використовуючи технології SEO та вразливість ПЗ, зловмисники посилюють позиції своїх попередньо заражених web-сторінок і в такий спосіб спонукають користувачів

зробити запит щодо інтригуючої новини в пошуковій системі, отримати результат, перейти за одним із найбільш верхніх посилань на сторінку зловмисника, запустивши цим самим на своїй ПЕОМ шкідливу програму;

2) експлуатація вразливостей у клієнтському ПЗ, розробленому третьою стороною, наприклад уразливостей так званої нульової доби, що їх застосовують зловмисники для призупинення виконання певних виробничих процесів. Дедалі частіше з цією метою використовуються вразливості в офісних програмах (Word, Excel і PowerPoint) і мультимедіа-програвачах (Real Player, iTunes, QuickTime), а також спеціальні утиліти для перегляду документів (наприклад, Adobe Reader);

3) цільовий фішинг (*Spear Phishing*), що його застосовують зловмисники для того, аби змусити користувача виконати якусь деструктивну дію на кшталт установлення шкідливого ПЗ на сервері компанії. Із цією метою зловмисники надсилають певним працівникам компанії ретельно підготовлені цільові повідомлення, що мають переконати жертву відкрити шкідливе вкладення або перейти за посиланням на сайт, що містить експлойти для зламу програм на боці користувача;

4) перехоплення браузера (*browser hooking*), що його застосовують зловмисники для розміщення на web-сайтах контенту, який містить шкідливі скрипти (сценарії). Відкриваючи такий сайт, користувач фактично запускає на своїй ПЕОМ відповідні скрипти, тобто надає зловмисникові контроль над власним браузером. Перехоплений у такий спосіб контроль над браузером користувача дозволяє зловмисникові використовувати його як відправну точку для подальших атак на інші системи, у тому числі внутрішні ресурси мережі й сервери компанії;

5) масові SQL-ін'єкції, що їх застосовують зловмисники для крадіжки конфіденційних даних з окремих web-додатків і баз даних; зміни вмісту баз даних, які будуть відображатися на web-сайтах; зміни web-контенту й розміщення на сайті шкідливих скриптів для атаки на браузери відвідувачів, а також інших експлойтів, що використовують уразливості ПЗ на боці користувача;

6) атаки на адміністративні web-інтерфейси, що їх застосовують зловмисники для здійснення контролю за певними системами або інфраструктурами (ERP-системами, системами управління HVAC і електропостачанням тощо) за рахунок перехоплення браузера або експлуатації вразливостей ПЗ на боці користувача;

7) атаки на сайти соціальних мереж (Facebook, LinkedIn, Twitter та ін.), що їх застосовують зловмисники для збору критичної інформації про діяльність компанії та технології, використовувані її співробітниками; поширення експлойтів і скриптів із метою перехоплення браузера користувача;

8) атаки типу «передача хеша» (*pass-the-hash*), що їх застосовують зловмисники для одержання доступу в корпоративний домен за рахунок інтегрованих у Windows-системи пакетів для проведення атак (таких, наприклад, як Metasploit і Nmap). При цьому викрадені хеші використовуються зловмисниками для автентифікації замість паролів;

9) злам устаткування, що за рахунок перехоплення інформації, переданої по шинах даних (*bus sniffing*), зламу прошивань, зміни системного часу (*clock glitching*) та інших витончених атак на обладнання забезпечує зловмисникам можливість обійти захисні механізми й одержати ключі шифрування.

Незважаючи на таке розмаїття та приховані можливості, деструктивні інциденти у сфері високих технологій ані в Україні, ані в інших державах світу не набули ще значних масштабів (табл. 1.3) [1; 28; 29], хоча кількість їх неухильно збільшується [1; 28] Зокрема, лише за період з 2002-го по 2010 рік кількість викритих внутрішніх і зовнішніх інцидентів зросла приблизно у 2,5 разу.

Таблиця 1.3

Кількість ІТ-інцидентів, що підлягали розслідуванню в різних країнах світу з грудня 2010-го по квітень 2012 р.

Країна	Усього	Вік зловмисників, років			
		До 18	Від 18 до 28	Старші	Невідомий
США	107	5	24	8	70
Туреччина	32	8	—	—	24
Італія	15	5	10	—	—
Великобританія	16	6	9	1	—
Аргентина	10	—	—	—	10
Іспанія	7	1	—	—	6
Чилі	6	2	4	—	—
Нідерланди	6	1	1	—	4
Колумбія	5	—	—	—	5
Франція	3	1	—	1	1
Греція	3	2	1	—	—
Польща	1	—	1	—	—

Наведемо конкретні приклади таких інцидентів [1; 28–31].

1. *Червень 1982 р.* Через активацію програмного забезпечення, отриманого радянськими розвідниками в Канаді, куди, як з'ясувалося згодом, американці попередньо ввели помилкові дані, було здійснено кібератаку проти сибірського газопроводу. Після одержання команди ззовні програма перевищила режим роботи газопроводу настільки, що він вибухнув.

2. *1995 рік.* Банк «Україна» через проникнення в його мережу було пограбовано на суму майже 4 млн дол.

До речі, аналогічні деструктивні інциденти в Україні трапляються дедалі частіше (рис. 1.16). Найзначніші атаки відбулися 1997 року, коли на кілька годин було заблоковано роботу інтернет-провайдера «Глобал Юкрейн»; 2000 року, коли сталася інформаційна диверсія проти інтернет-провайдера «ukr.net»; лютого 2012 року — масований кібернапад на державні інтернет-ресурси під час виборчої кампанііі.

3. *2009 рік*. Здійснено цілеспрямовану атаку GhostNet із центром управління в Китаї, зорієнтовану на понад 100 країн. Вторгнення відбувалося за допомогою повідомлення електронної пошти, при відкритті якого запускалася шкідлива програма із прикріпленого файла. Після встановлення вірус завантажував хакерський інструментарій Ghost Remote Administration Toolkit для дистанційного управління системами. Управляючий сервер у Китаї потім міг

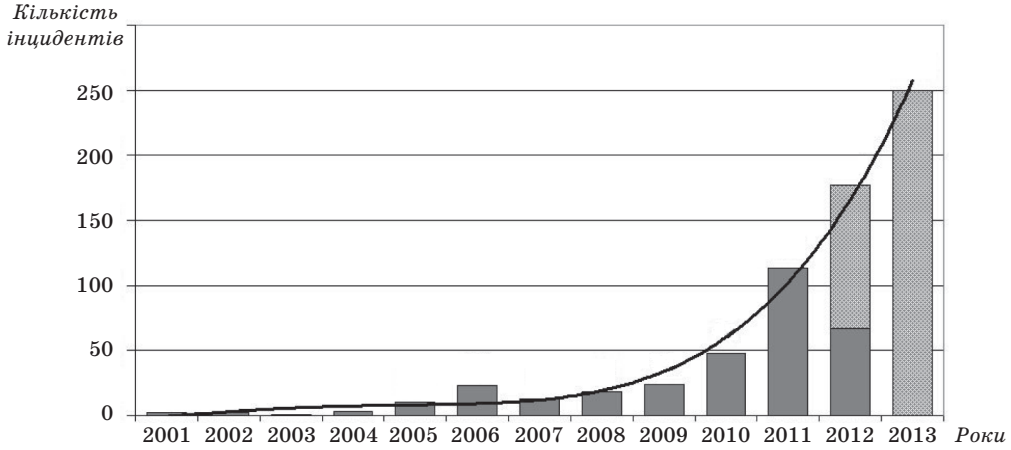


Рис. 1.16. Динаміка деструктивних інцидентів щодо державних інформаційних ресурсів в Україні

надсилати вірусу команди на передавання інформації з комп'ютерів що зазнали атаки. У тому самому 2009 році почалася операція «Аврора», яка, цілком імовірно також виходила з Китаю й мала на меті викрадення інтелектуальної власності й закритої інформації з баз даних високотехнологічних компаній та національних безпекових і оборонних відомств. Атакувальники використовували вразливість класу *use-after-free* в *Internet Explorer*, що уможливлювала псування пам'яті об'єктів HTML. Це дозволяло атакувальнику впровадити сторонній код в область пам'яті, що вивільнялась із вилученням об'єкта. Для цього негайно після вилучення об'єкта на його місці сторонній код створював новий. Атака здійснювалась методом супутного завантаження (*drive-by download*), що відбувалось без відома користувача, у результаті чого його машина зазнавала зараження вірусом.

4. *2010–2012 роки*. Сталися міждержавні інциденти, до яких призвели відомі мережні черв'яки *Duqu*, *Flame* та *Stuxnet*. Останній було розроблено групою фахівців з Ізраїлю та США за участю представників Німеччини й Великобританії. Наслідком його деструктивних дій стало гальмування ядерної програми Ірану. Цьому посприяло виявлення вірусом програмованих логічних контролерів (ПЛК) у автоматизованій системі управління технологічними процесами станції (*Supervisory Control And Data Acquisition*), а також те, що нападникам удалося використати (для впровадження особливого коду в «залізо» ПЕОМ АЕС) чотири невідомі раніше вразливості «нульової доби» («zero-day») у діючих версіях ОС Windows та два дійсні сертифікати від компаній Realtek і JMicron. Саме наявність останніх дала змогу Win32/Stuxnet тривалий час уникати антивірусних радарів (рис. 1.17).

У процесі докладного вивчення Win32/Stuxnet фахівці відомої лабораторії Касперського дійшли невтішного висновку: поява згаданої шкідливої програми фактично знаменувала собою початок нової ери — ери кібервоєн. За висловлюванням Є. Касперського — співзасновника і генерального директора цього наукового осередку, зазначений програмний засіб призначений не стільки «...для викрадення грошей, розсилання спаму або знищення особистих даних...», скільки для «...виведення з ладу заводів та ушкодження промислових систем...».

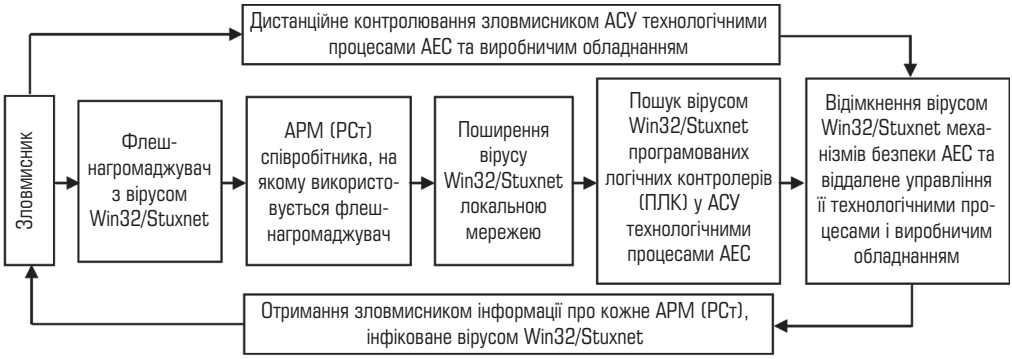


Рис. 1.17. Схема функціонування вірусу Win32/Stuxnet

Що ж до мережного черв'яка Worm.Win32.Flame, виявленого 2012 року фахівцями лабораторії Касперського, то його розробили західні програмісти, як з'ясувалося, виключно з метою ведення кібершпигунства. Основні функції Worm.Win32.Flame такі:

- поширення за допомогою знімних дисків та локальних мереж;
- зараження лише певних ПЕОМ;
- перехоплення мережних пакетів, виявлення мережних ресурсів та збір переліку вразливих паролів;
- сканування диска інфікованої системи щодо наявності визначених розширень та контенту;
- копіювання зображень з екрана користувача в разі активності певних процесів;
- використання мікрофона інфікованої системи для запису звуків із навколишнього середовища;
- передавання інформації на сервери зловмисників;
- використання понад 10 доменів для приймання команд із серверів управління;
- установлення безпечного з'єднання із серверами управління через SSH- та HTTPS-протоколи;
- сумісність з операційними системами Windows XP, Vista та 7.

Характерна відмінність черв'яка Worm.Win32.Flame від інших троянів полягає в наявності прихованого алгоритму дії та широкого спектра «бойових» можливостей (табл. 1.4).

Сьогодні такі та подібні до них дії домінують у геополітичній конкуренції більшості країн світу. Це, у свою чергу, висуває нові завдання до їхніх збройних сил, актуалізуючи проблеми інформаційних і кібервоєн та інформаційного протиборства. Серед головних причин такої ситуації можна назвати:

- відсутність або недосконалість нормативно-правової бази, яка б забороняла застосування інформаційної і кіберзброї та проведення інформаційних і кібероперацій, а також встановлювала б відповідальність протиборчих сторін за здійснення злочинів у інформаційно-телекомунікаційній сфері;
- формування окремими державами власних доктрин і стратегій наступальних і підривних дій в інформаційному та кіберпросторі;
- створення та застосування спеціальних сил і засобів негативного впливу на критично важливу інформаційну і кіберінфраструктуру;

Таблиця 1.4

Можливості троянських вірусних програм Stuxnet, Duqu та Flame

Характеристика програми	Stuxnet	Duqu	Flame
Дата впровадження	Червень-вересень 2012 р.	Вересень 2011 р.	Травень 2012 р.
Призначення	Ураження автоматизованих систем управління атомною інфраструктурою Ірану (АЕС у м. Бушер та завод зі збагачення урану в м. Натанз)	Збір конфіденційної інформації про особливості функціонування стратегічно важливих ядерних та індустріальних об'єктів	Цілеспрямований систематичний збір даних (офісні документи, креслення тощо), можливість модифікації інформації
Географія поширення	Іран, Норвегія, країни Близького Сходу	Близький Схід	
Спосіб поширення	Мережа Інтернет, знімні носії інформації типу USB Flash Drive		
Мови програмування	Асемблер, C, C++	C, програмна архітектура Microsoft Visual C++	C, C++, ША
Обсяг файла	До 0,5 Мбіт	Від 0,06 до 0,23 Мбіт	Понад 20 Мбіт
Розмір програмного коду	Близько 10 тис. рядків	6–8 тис. рядків	750 тис. рядків (базовий модуль — 650 тис. рядків /6 Мбіт; найменший модуль — 70 тис. рядків (170 — зашифровані)
Принцип дії	Ґрунтується на використанні вразливостей (помилок) ОС Microsoft Windows		
Можливість самодублювання і самознищення	Самодублювання	Самодублювання та самознищення	Самознищення
Алгоритм маскування присутності в системі	Використання фальшивих сертифікатів компаній «Realtek Semicon ductof» та «JMicron Technology»	—	Використання дійсних сертифікатів компанії «Microsoft»
Інші особливості	Залучення до розробки значних технічних та фінансових ресурсів		

• проникнення ІТ-технологій в усі сфери державного й громадського життя, побудова на їхній основі систем державного і військового управління;

• розвиток державних проектів і програм у сфері інформатизації (електронний документообіг, міжвідомча електронна взаємодія, універсальні електронні карти), спрямованих на формування інформаційного суспільства.

Сьогодні вже розроблено комплекс захисних заходів, які дозволять користувачеві запобігти деструктивним діям, заблокувати НСД зловмисників до мереж і систем компанії або ж мінімізувати збиток, якого вони можуть завдати. Передусім ідеться про 20 найбільш критичних заходів, рекомендованих американською ІТ-компанією «SANS» [27]. Ці заходи за своєю суттю відповідають заходам із захисту інформації, що в Україні регламентуються системою *нормативних документів із технічного захисту інформації* (*НД ТЗІ*) [9–22].

Заходи із захисту інформації (мереж і систем) від кіберзагроз характеризує табл. 1.5, з якої випливає, що певні заходи реалізуються через упровадження відповідних *функціональних послуг безпеки* (ФПБ). Структуру та семантичне позначення останніх наведено в НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

Щоб адекватно й швидко реагувати на можливі інциденти у сфері високих технологій, доцільно застосовувати так звану *карту кіберзагроз*, що містить ключові елементи, притаманні будь-якій кібератаці, і дозволяє обрати раціональні варіанти дій для захисту від неї. Приклад такої карти наведено в табл. 1.6 на с. 40, яка унаочнює три варіанти атак: 1) викрадення банківських карток та фінансової інформації; 2) APT-атака; 3) пошукова оптимізація (SEO).

Головні передумови успіху при цьому такі:

• використання ліцензійного загального і спеціального (наприклад, антивірусного) ПЗ, що постійно (регулярно) оновлюється;

• застосування політики паролів, блокування облікових записів, компрометації ключів та засобів криптографічного захисту інформації протиборчих сторін;

• «обмеження» прав процесів, ініційованих виконавчими програмами в системі;

• використання можливостей ОС щодо шифрування файлів і папок.

Якщо було зафіксовано порушення кібербезпеки на ОІД, то співробітники служби безпеки компанії (організації, установи) мають вжити таких заходів [9; 32]:

1) ідентифікувати інцидент і переконатися, що він насправді відбувався;

2) локалізувати область ІТ-інфраструктури, задіяної в інциденті;

3) обмежити доступ до об'єктів, задіяних в інциденті;

4) повідомити підрозділ інформбезпеки про факт виникнення інциденту;

5) залучити компетентних фахівців для консультування;

6) створити групу з розслідування інциденту, скласти план робіт зі збору доказів і відновлення систем, а також забезпечити ведення протоколу подій;

7) забезпечити схоронність і належне оформлення доказів, для чого зняти енергозалежну інформацію із системи, яка працює; зібрати в реальному часі інформацію про інцидент; відімкнути від мережі живлення;

8) у присутності третьої незалежної сторони вилучити й опечатати носії інформації з доказовою базою, знявши образи та іншу інформацію для подальшого її аналізу та зберігання. При цьому необхідно:

• оформити протоколом всі операції з носіями інформації;

• задокументувати процес на фото- або відеокамеру;

• подати докладний опис об'єктів, що містять інформацію, даних, які витягаються, а також місць їх зберігання;

• зберегти опечатані об'єкти разом зі складеним протоколом у надійному місці до передачі носіїв на дослідження;

9) після збереження та оформлення речових доказів відновити роботоздатність ІС;

Таблиця 1.5

Заходи із захисту інформації (мереж і систем) від кіберзагроз та їхній зміст

№ з/п	Відповідно до рекомендацій американської IT-компанії «SANS»		Відповідно до вимог НД ТЗІ України
1	2		3
1	Інвентаризація дозволених для підімкнення пристроїв, а також пристроїв, підімкнених не санкціоновано		Реалізація функціонального профілю безпеки (ФПБ) «Автентифікація отримувача» унеможливлює відмову від одержання і забезпечує однозначне встановлення факту одержання певного об'єкта певним користувачем
2	Інвентаризація дозволеного для встановлення ПЗ, а також ПЗ, установленого на ПЕОМ мережі не санкціоновано		Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення потоків інформації, які існують, але не контролюються іншими ФПБ
3	Безпечне настроювання апаратного й програмного забезпечення для серверів, робочих станцій і ноутбуків	*Образи, з яких здійснюється встановлення систем, мають бути попередньо налаштовані для забезпечення необхідного рівня захисту та протестовані*	Реалізація ФПБ «Самотестування» дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ІТС
4	Безпечне настроювання мережних пристроїв	*Налаштовування міжмережних екранів, маршрутизаторів, комутаторів і т. ін.*	Реалізація ФПБ «Самотестування» дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ІТС
5	Захист периметра мережі	*Забезпечуваний міжмережними екранами, проксі, DMZ і системами IPS рівень захисту мережі має бути перевірений сканерами вразливостей*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення потоків інформації, які існують, але не контролюються іншими ФПБ
6	Супровід, моніторинг і аналіз журналів реєстрації подій		Реалізація ФПБ «Реєстрація» дозволяє контролювати небезпечні для ІТС дії. Рівні цієї послуги ранжуються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації та здатності до виявлення потенційних порушень
7	Безпека прикладного ПЗ	*Розроблене й придбане ПЗ має бути протестоване за допомогою автоматизованих засобів аналізу або засобів ручного тестування на проникнення*	Реалізація ФПБ «Самотестування» дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування та цілісність певної множини функцій ІТС
8	Контроль використання адміністративних привілеїв	*Проведення моніторингу використання й відстежування облікових записів, що мають адміністративні привілеї*	Реалізація ФПБ «Розподіл обов'язків» дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні цієї послуги ранжуються на підставі вибірковості керування можливостями користувачів і адміністраторів

Продовження табл. 1.5

1	2		3
9	Контроль доступу на основі принципу «повинен знати»	*Відокремлення критичних даних від менш критичних та забезпечення контролю доступу до них*	Реалізація ФПБ «Адміністративна (довірча) конфіденційність» та «Адміністративна (довірча) цілісність» дозволяє адміністраторові або спеціально авторизованому користувачеві керувати потоками інформації від користувачів до захищених об'єктів. Рівні цієї послуги ранжуються на підставі повноти захисту та вибірковості керування
10	Постійний аналіз уразливостей й їх усунення	*Упровадження ефективних засобів для сканування, які дозволяють порівнювати здобуті результати з результатами попереднього сканування для визначення змін, що відбулися*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення наявних потоків інформації, не контрольованих іншими ФПБ
11	Моніторинг і контроль облікових записів	*Застосовування самостійно розроблених скриптів або спеціалізованих додатків для аналізу вмісту журналів реєстрації подій*	Реалізація ФПБ «Ідентифікація і автентифікація» дозволяє комплексу засобів захисту інформації визначити і перевірити особистість користувача, що намагається одержати доступ до ІТС. Рівні цієї послуги ранжуються залежно від кількості задіяних механізмів автентифікації
12	Захист від шкідливого коду	*Використання адміністративних функцій або корпоративних систем забезпечення безпеки кінцевих точок для перевірки функціонування засобів захисту від шкідливих програм і системи IPS/IDS рівня хосту на всіх ПЕОМ мережі*	—
13	Обмеження та контроль мережних портів, протоколів і служб	*Відімкнення невикористовуваних служб і протоколів, блокування непотрібних для роботи портів, установлення міжмережних екранів рівня хосту для підвищення захисту*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення наявних потоків інформації, не контрольованих іншими ФПБ
14	Захист і контроль безпроводових пристроїв	*Застосовування спеціалізованих IDS. Сканування та моніторинг для виявлення діючих безпроводових мереж*	Реалізація ФПБ «Конфіденційність при обміні» та «Цілісність при обміні» дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, або її модифікації під час їх експорту/імпорту через незахищене середовище
15	Запобігання витоку даних	*Використання рішень DLP для виявлення спроб виведення критичних даних за межі мережі компанії, а також іншої підозрілої активності*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення наявних потоків інформації, не контрольованих іншими ФПБ

Закінчення табл. 1.5

1	2		3
16	Забезпечення безпеки мережі	*Застосовування найкращих практиктичних досягнень у сфері безпеки при проектуванні мережі, а також при настроюванні маршрутизаторів, комутаторів, критичних серверів, міжмережних екранів, компонентів безпеки й груп клієнтських ПЕОМ*	Реалізація ФПБ «Аналіз прихованих каналів» забезпечує виявлення та усунення потоків інформації, не контрольованих іншими ФПБ
17	Тестування на проникнення	*Наслідування дій комп'ютерних зловмисників при визначенні меж і підходів до проведення тестів на проникнення. Використовування відомостей про виявлені недоліки для підвищення безпеки*	Випробування КСЗІ в цілому та комплексу засобів захисту інформації (як складової КСЗІ або як окремого об'єкта експертизи в галузі ТЗІ) — обов'язкові етапи при створенні КСЗІ в ІТС. Вимоги до випробувань визначаються відповідними *критеріями гарантій*
18	Організація реагування на інциденти	*Періодичне проведення навчань і практичне відпрацювання процедур реагування на інциденти на основі певних сценаріїв*	Одна з неодмінних умов створення та функціонування КСЗІ в ІТС — наявність служби захисту інформації в ІТС, на яку покладаються заходи з організації та координації робіт, пов'язаних із захистом інформації в ІТС, підтримання необхідного рівня захищеності інформації та ресурсів ІТС
19	Організація дій із відновлення даних	*Упроваджування надійних і безпечних процедур резервного копіювання важливих даних*	Реалізація ФПБ «Відкочування» уможливлює відмінну операцію або послідовності операцій і повернення (відкочування) захищеного об'єкта до попереднього стану. Рівні цієї послуги ранжуються на підставі множини операцій, для яких забезпечується відкочування
20	Оцінювання наявних навичок щодо безпекиі, проведення необхідних тренінгів	*Оцінювання знань і навичок співробітників із питань безпеки та проведення в разі потреби додаткового навчання*	Одна з функцій служби захисту інформації в ІТС полягає в організації професійної підготовки та підвищення кваліфікації користувачів ІТС із питань захисту інформації, проведення заліків та контрольних перевірок

10) при проведенні дослідження джерел інформації забезпечити незмінність доказів (працювати тільки з копією);

11) у процесі розслідування забезпечити коректну взаємодію із зацікавленими підрозділами та зовнішніми організаціями;

12) закінчивши розслідування, оформити відповідний звіт та скласти рекомендації зі зниження ризиків виникнення аналогічних інцидентів у майбутньому.

Окрім цього слід своєчасно налаштувати ПЗ АРМ (РСт) та програми міжмережного екрана (Firewall) для безпечного доступу до ресурсів мережі Інтернет і ЛОМ, заборонити копіювання та запуск на виконання невідомих програм або програм, отриманих із несертифікованих джерел, обмежувати права доступу користувачів до об'єктів файлової системи та запуску системних програм, керувати розмежуванням доступу.

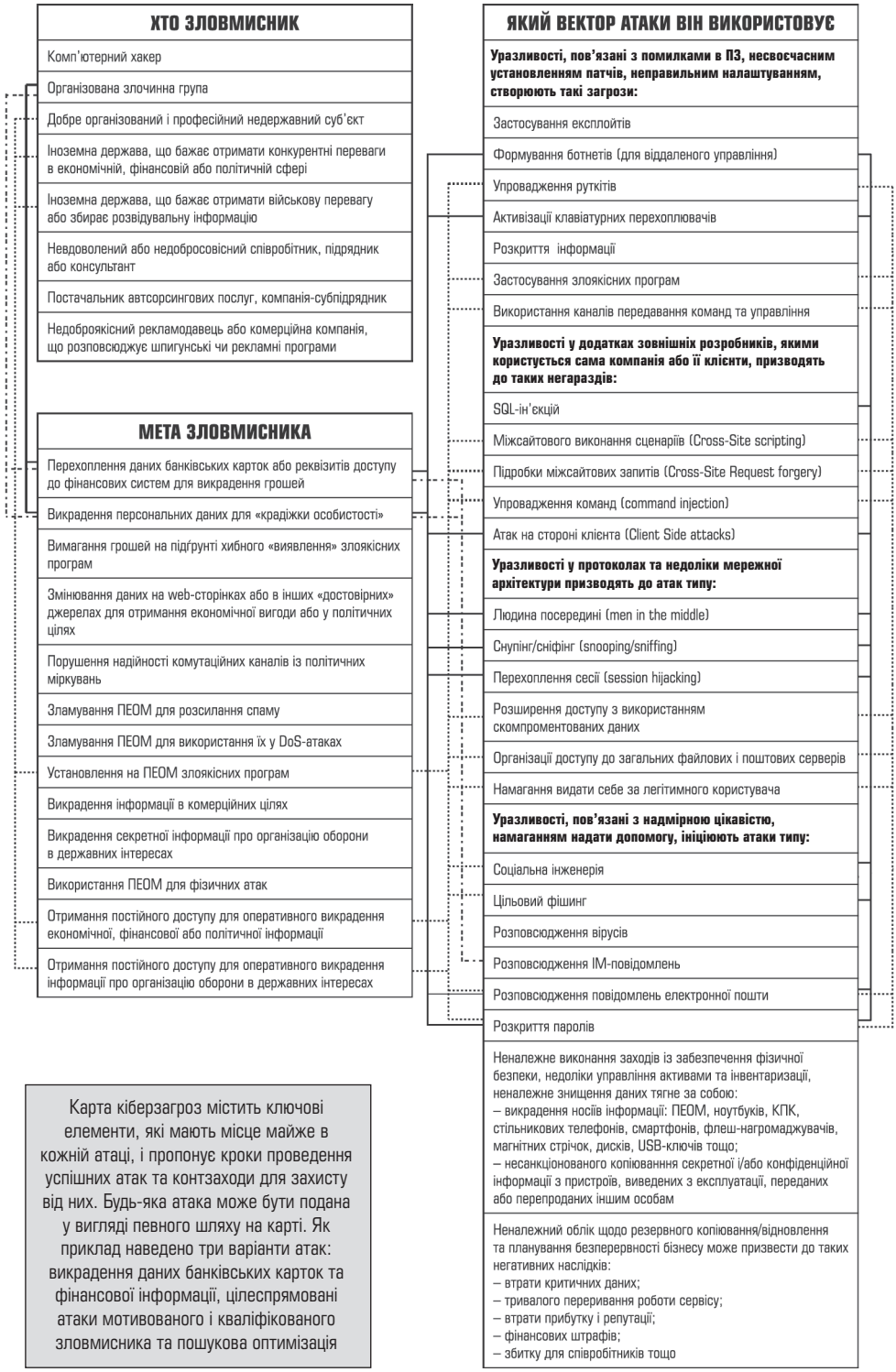
Утім чітких правил поводження при атаках кіберзлочинців поки що не існує. Міжнародна організація зі стандартизації тільки готує новий стандарт ISO 27037. *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*, який стосуватиметься опису й систематизації зібраних доказів під час розслідування комп'ютерних інцидентів.

Пріоритетний напрямок реформування інформаційної безпеки в Україні визначає доктрина, затверджена Указом Президента України від 8 липня 2009 р. № 514/209. Цією доктриною передбачено забезпечення конфіденційності, цілісності та доступності до інформації в державних інформаційних ресурсах завдяки створенню надійної системи захисту людини, суспільства та держави від впливу внутрішніх і зовнішніх, навмисних і/або випадкових кібернетичних втручань і загроз та негайному реагуванню на їх прояви. Останнє поряд із відповідним нормативно-правовим забезпеченням [32] має передбачати низку організаційних та інженерно-технічних заходів. До основних напрямків удосконалення організаційного забезпечення системи кібербезпеки України слід віднести [26]:

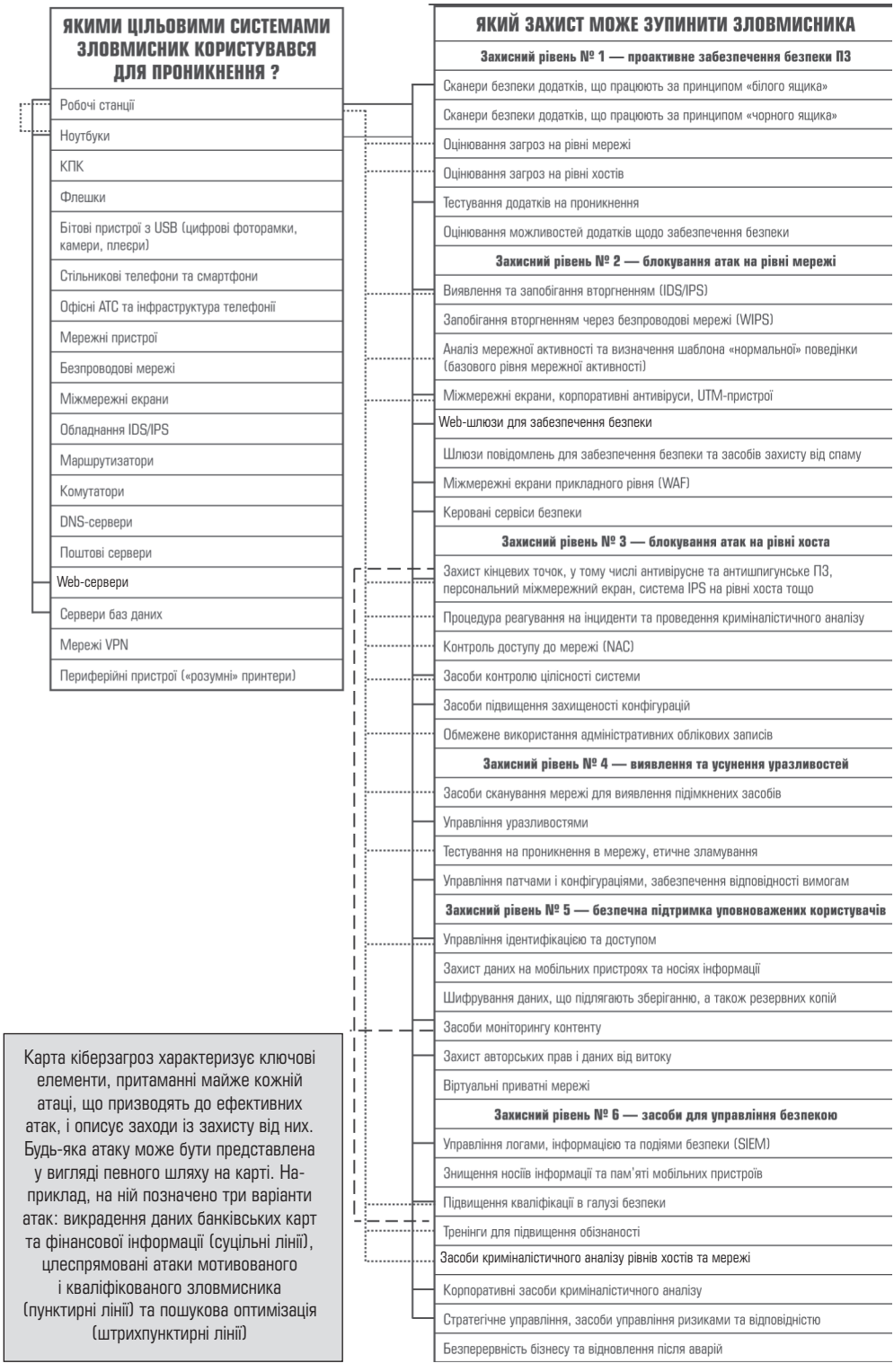
- створення сприятливих зовнішньополітичних умов для подальшого розвитку національного сегмента кіберпростору;
- забезпечення повноправної участі України в загальноєвропейській та регіональних системах кібербезпеки;
- зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби з проявами організованої злочинності та кібертероризму;
- забезпечення максимальної ефективності Збройних сил України в кіберпросторі, їхньої здатності давати адекватну відповідь реальним і потенційним кіберзагрозам;
- посилення державної підтримки розвитку пріоритетних напрямків науки і техніки як основи розвитку високих інформаційних технологій;
- забезпечення необхідних умов для реалізації прав інтелектуальної власності в національному сегменті кіберпростору;
- створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури і ресурсів.

Таблиця 1.6

КАРТА КІБЕРЗАГРОЗ



Карта кіберзагроз містить ключові елементи, які мають місце майже в кожній атаці, і пропонує кроки проведення успішних атак та контзаходи для захисту від них. Будь-яка атака може бути подана у вигляді певного шляху на карті. Як приклад наведено три варіанти атак: викрадення даних банківських карток та фінансової інформації, цілеспрямовані атаки мотивованого і кваліфікованого зловмисника та пошукова оптимізація


ЯКИМИ ЦІЛЬОВИМИ СИСТЕМАМИ ЗЛОВМИСНИК КОРИСТУВАВСЯ ДЛЯ ПРОНИКНЕННЯ ?
Робочі станції
Ноутбуки
КПК
Флешки
Бітові пристрої з USB (цифрові фоторамки, камери, плеєри)
Стільникові телефони та смартфони
Офісні АТС та інфраструктура телефонії
Мережні пристрої
Безпроводові мережі
Міжмережні екрани
Обладнання IDS/IPS
Маршрутизатори
Комутатори
DNS-сервери
Поштові сервери
Web-сервери
Сервери баз даних
Мережі VPN
Периферійні пристрої («розумні» принтери)
ЯКИЙ ЗАХИСТ МОЖЕ ЗУПИНИТИ ЗЛОВМИСНИКА
Захисний рівень № 1 — проактивне забезпечення безпеки ПЗ
Сканери безпеки додатків, що працюють за принципом «білого ящика»
Сканери безпеки додатків, що працюють за принципом «чорного ящика»
Оцінювання загроз на рівні мережі
Оцінювання загроз на рівні хостів
Тестування додатків на проникнення
Оцінювання можливостей додатків щодо забезпечення безпеки
Захисний рівень № 2 — блокування атак на рівні мережі
Виявлення та запобігання вторгненням (IDS/IPS)
Запобігання вторгненням через безпроводові мережі (WIPS)
Аналіз мережної активності та визначення шаблона «нормальної» поведінки (базового рівня мережної активності)
Міжмережні екрани, корпоративні антивіруси, UTM-пристрої
Web-шлюзи для забезпечення безпеки
Шлюзи повідомлень для забезпечення безпеки та засобів захисту від спаму
Міжмережні екрани прикладного рівня (WAF)
Керовані сервіси безпеки
Захисний рівень № 3 — блокування атак на рівні хоста
Захист кінцевих точок, у тому числі антивірусне та антишпигунське ПЗ, персональний міжмережний екран, система IPS на рівні хоста тощо
Процедура реагування на інциденти та проведення криміналістичного аналізу
Контроль доступу до мережі (NAC)
Засоби контролю цілісності системи
Засоби підвищення захищеності конфігурацій
Обмежене використання адміністративних облікових записів
Захисний рівень № 4 — виявлення та усунення уразливостей
Засоби сканування мережі для виявлення підімкнених засобів
Управління уразливостями
Тестування на проникнення в мережу, етичне зламування
Управління патчами і конфігураціями, забезпечення відповідності вимогам
Захисний рівень № 5 — безпечна підтримка уповноважених користувачів
Управління ідентифікацією та доступом
Захист даних на мобільних пристроях та носіях інформації
Шифрування даних, що підлягають зберіганню, а також резервних копій
Засоби моніторингу контенту
Захист авторських прав і даних від витоку
Віртуальні приватні мережі
Захисний рівень № 6 — засоби для управління безпекою
Управління логами, інформацією та подіями безпеки (SIEM)
Знищення носіїв інформації та пам'яті мобільних пристроїв
Підвищення кваліфікації в галузі безпеки
Тренінги для підвищення обізнаності
Засоби криміналістичного аналізу рівнів хостів та мережі
Корпоративні засоби криміналістичного аналізу
Стратегічне управління, засоби управління ризиками та відповідністю
Безперервність бізнесу та відновлення після аварій
Карта кіберзагроз характеризує ключові елементи, притаманні майже кожній атаці, що призводять до ефективних атак, і описує заходи із захисту від них. Будь-яка атаку може бути представлена у вигляді певного шляху на карті. Наприклад, на ній позначено три варіанти атак: викрадення даних банківських карт та фінансової інформації (суцільні лінії), цілеспрямовані атаки мотивованого і кваліфікованого зловмисника (пунктирні лінії) та пошукова оптимізація (штрихпунктирні лінії)

ТОП-9 найбільш небезпечних векторів атак

1	**Пошукова оптимізація (SEO — Search Engine Optimization)**	Спосіб розповсюдження злоякісних програм. Коли відбуваються певні події, інформація про які з'являється в усіх новинах, зловмисники використовують технології SEO, аби підняти позиції своїх попередньо заражених web-сторінок у результатах видачі пошукових систем. Коли користувач зробить у пошуковій системі запит до новини, яка його цікавить, він, отримавши результат, почне рух згідно з одним із верхніх посилань і потрапить на сторінку зловмисника, яка намагатиметься завантажити й запустити на ПЕОМ користувача злоякісну програму завдяки уразливості ПЗ користувача
2	**Експлуатація уразливостей у клієнтському ПЗ, розробленому третьою стороною**	Оскільки операційні системи (ОС) стали значно безпечнішими, зловмисники дедалі частіше переходять до використання уразливостей у сторонньому ПЗ, що працює в ОС, передусім у Word, Exel та Power Point, мультимедіа-програвачах — Real player, QuickTime тощо, а також у спеціальних утилітах для перегляду документів, наприклад Adobe Reader. Доволі часто зловмисники використовують у своїх атаках уразливості «нульової доби», для яких розробник ще не випустив патч, який виправляє недоліки уразливого ПЗ
3	**Цільовий фішинг (Spear phising)**	Зловмисники надсилають певним особам (передусім керівникам) у компанії цільові й реалістичні сценарії (повідомлення), аби спонукати жертву відкрити злоякісне вкладення або перейти за посиланням на сайт, який містить експлойти для зламування програм на боці користувача
4	**Перехоплення браузера (browser hooking)**	Експлуатуючи уразливості, що дозволяють здійснювати міжсайтове виконання сценаріїв на довірених web-сайтах, зловмисники розміщують контент, який містить злоякісні скрипти (сценарії). Коли користувач відкриває такий сайт, браузер на його ПЕОМ запускає ці крипти та надає зловминику контроль над самим браузером користувача. Перехоплений таким чином контроль над браузером користувача дозволяє зловмиснику використати його як точку відліку для подальших атак на інші системи, зокрема на внутрішні ресурси мережі та сервери компанії
5	**Сайти соцмереж як засіб крадіжки інформації та розповсюдження злоякісних програм**	Зловмисники використовують популярні соцмережі типу FaseBook, LinkedIn, Twitter для збору критичної інформації про діяльність компанії. Більш того, вони розповсюджують експлойти та скрипти для перехоплення браузера через сайти соцмереж
6	**Масові SQL-ін'єкції**	Протягом багатьох років атаки, що використовували SQL-ін'єкції, зосереджувались на крадіжці конфіденційних даних в окремих web-додатках та базах даних (БД). Останнім часом зловмисники розширили спектр використання SQL-ін'єкцій за допомогою автоматизованого ПЗ, яке дозволяє одночасно атакувати тисячі web-додатків. Замість викрадення даних сучасні атаки на основі SQL-ін'єкцій найчастіше намагаються змінити вміст БД, які будуть відображатися на web-сайтах, спотворити web-контент, розмістити на сайті злоякісні скрипти для атаки на браузери користувачів, а також інші експлойти, які використовують уразливості ПЗ на боці користувача. Усі ці дії, як правило, виконують для встановлення на ПЕОМ користувача злоякісного ПЗ
7	**Атаки на адміністративні інтерфейси**	Більшість великих корпоративних систем, таких як комплекси забезпечення безпеки кінцевих точок, засобів мережного адміністрування, ERP-системи тощо налаштовуються через адміністративні web-інтерфейси. Виконуючи атаки перехоплення браузера або експлуатуючи уразливості ПЗ на боці користувача, зловмисники все частіше полюють на адміністративні інтерфейси, які можуть забезпечити контроль відповідної системи або інфраструктури
8	**Атаки «передача хешу» (pass the hash) у Windows інтегровано в пакети для проведення атак**	Зловмисники замість паролів використовують техніку «передачі хешу» відносно Windows-систем, аби отримати доступ до корпоративного домена. Нині ці можливості включено в широко використовувані інструменти комп'ютерних атак, такі як Metasploit та Nmap, що значно спрощує проведення широкомасштабних атак із використанням відповідної техніки
9	**Зламування обладнання**	Оскільки захист ПЗ останнім часом значно поліпшився й водночас набули значного поширення «розумні» пристрої (*embedder device*), такі як стільникові телефони, безпроводові маршрутизатори тощо, то кіберзлочинці частіше почали зламувати обладнання. Через перехоплення інформації, що передається шинами даних (*bus sniffing*), зламування прошивок, змінювання системного часу (*clock glitching*) та інші витончені атаки на обладнання зловмисники обминають захисні механізми й отримують ключі шифрування, що допомагає їм при подальших атаках на інфраструктуру компанії-жертви

1.3. Кібератаки та кібертероризм: поняття і визначення. Особливості реалізації атак і заходи з послаблення їхнього деструктивного впливу

Деструктивні інциденти у сфері високих технологій протиборчі сторони ініціюють, як відомо [1], з метою:

• порушення або блокування роботи ІС і мереж стратегічно важливих галузей (об'єктів) інфраструктури, передусім фінансового, енергетичного, промислового, транспортного та військового секторів;

• несанкціонованого отримання інформації із закритих баз даних (баз знань) державних, комерційних та інших установ, її модифікації і/або знищення.

Нині злочинні дії з організації різного роду кібератак (КбА), несанкціонованого доступу (НСД) до чужих сайтів, створення «сайтів-двійників» вийшли за межі окремих країн, причому за темпами зростання значно випереджають решту видів організованої злочинності. Більш того, останніми роками вони отримали істотну фінансову підтримку та високоякісні комунікації, охопивши всі види злочинів, скоєних у ІТ-сфері [1]. Проте й досі немає чіткого визначення відповідних понять, зокрема й такого поняття, як ***кібератака***. З огляду на це проаналізуємо відомі підходи до його тлумачення.

♦ *В. Харченко* зі співавторами визначає КбА як ***заходи, здійснювані для підриву безпеки систем чи реалізації загрози характеристикам безпеки ресурсам ІС через використання їх уразливостей*** [2; 33].

♦ *Д. Дубов* і *М. Ожеван* кваліфікують КбА як ***цілеспрямовані дії, що реалізуються в КбП*** (або за допомогою технічних можливостей цього простору) ***і призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість та психічний стан громадян)*** [2; 34].

♦ *В. Шеломенцев* під КбА розуміє ***процес реалізації програмно-математичних заходів, спрямованих на пошук та використання кібернетичних уразливостей інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем*** [2; 35].

♦ *С. Мельник*, *О. Тихомиров* та *О. Лєнков* розглядають КбА ***як результат використання технічних недоліків механізмів безпеки сучасного кіберпростору з метою дезорганізації роботи його елементів*** [2; 7].

Узагальнюючи сказане, можна сформулювати таке визначення:

кібератака — *сукупність узгоджених щодо мети, змісту та часу дій або заходів* — так званих ***кіберакцій***, *спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності і/або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об'єкта* [1].

Зауважимо, що загальної кількісної оцінки стосовно видів кібератак та методів їх застосування досі немає [1]. Комплексних статистичних досліджень у цьому плані не було. Але ще в далекому 1984 році Фред Коен (F. Cohen) у праці «Computer Viruses: theory and experiments», присвяченій математичним основам вірусної технології, довів: ***із того, що множина всіх можливих злоякісних кодів нескінченна, випливає нескінченність множини самих атак.***

Загальну структуру кібератак унаочнює рис. 1.18.

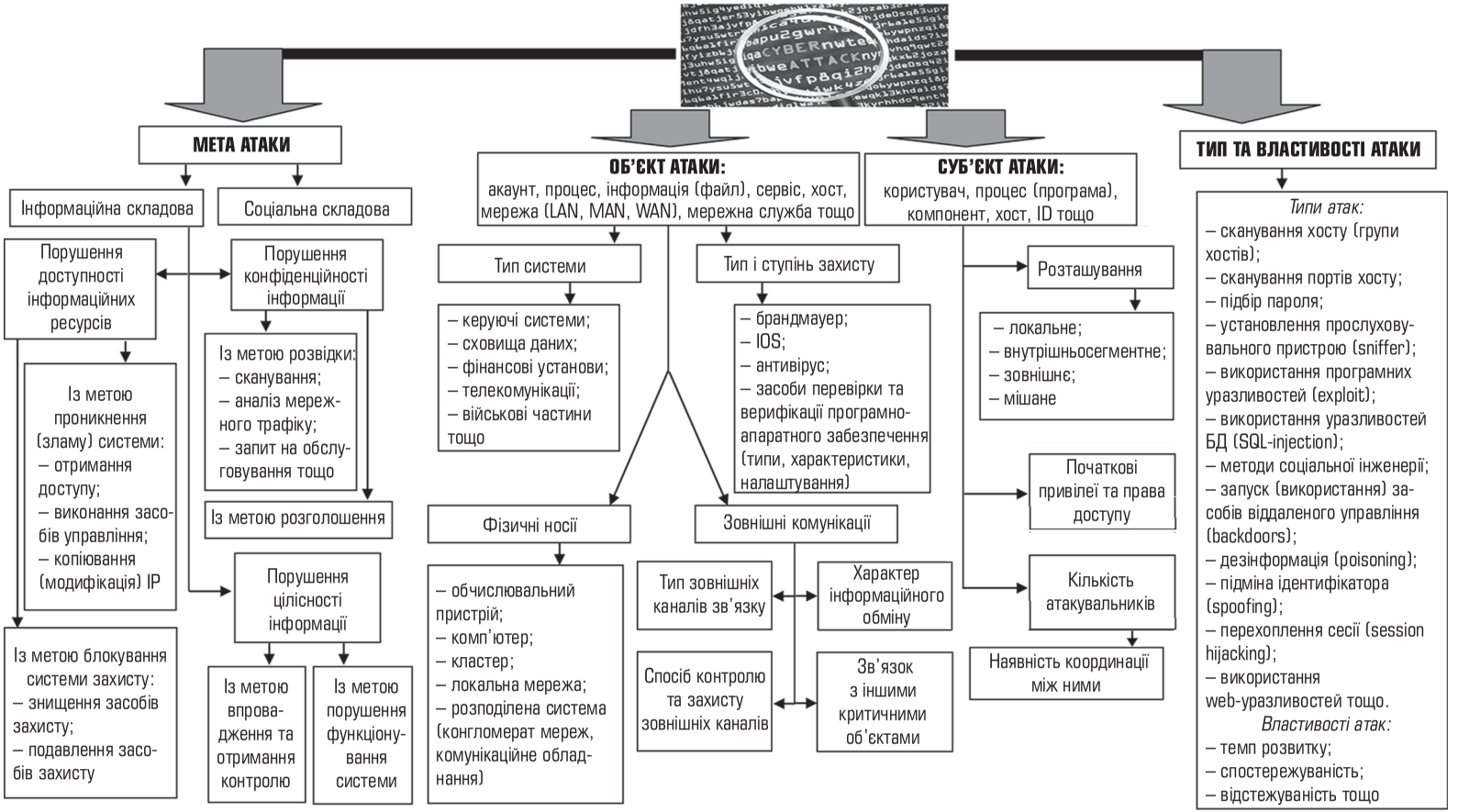


Рис. 1.18. Загальна структура кібернетичної атаки

Характерна особливість кібератак — миттевість їх здійснення (протягом секунд, хвилин).

Класифікують кібератаки за наведеними далі ознаками.

1. *За метою впливу на об'єкт атаки*. Цей вплив може бути спрямований, наприклад, на порушення цілісності (*integrity*) або конфіденційності (*confidentiality*) інформації, її захищеності від несанкціонованого доступу (*authentication*), а також на порушення живучості (*survivability*) системи та надійності (*availability*) її функціонування. Як показує світовий досвід, для розв'язання відповідних завдань використовують методи криптографії в поєднанні з перевіреним і ліцензованим ПЗ, а також надійні інтелектуальні носії важливої інформації (матеріал ключа). При цьому саме ***живучість системи*** — здатність її вчасно виконувати свої функції в умовах фізичного руйнування, часткової втрати ресурсів, відмов і збоїв елементів, несанкціонованого втручання в систему управління — розглядається як головна характеристика, що визначає готовність збройних сил, промисловості, економіки, народного господарства й суспільства в цілому як до ведення війни, так і до ліквідації наслідків терористичних актів, стихійних лих і техногенних катастроф.

2. *За принципом впливу на об'єкт атаки:*

• використання прихованих каналів (шляхів передавання інформації, що дозволяють двом процесам обмінюватися нею у спосіб, який порушує політику безпеки);

• застосування прав суб'єкта системи (користувача, процесу) до об'єкта (файлів даних, каналів зв'язку тощо).

3. *За характером впливу на об'єкт атаки*:

• активний вплив (користувач виконує деякі дії, що виходять за рамки його обов'язків і порушують наявну політику безпеки, наприклад розкриття пароля);

• пасивний вплив (користувач прослуховує лінії зв'язку між двома вузлами мережі).

4. *За способом впливу на об'єкт атаки*, зокрема на систему дозволів (захоплення привілеїв), а також безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв.

5. *За засобами впливу на об'єкт атаки*, що передбачають використання або стандартного ПЗ, або спеціально розроблених програм.

6. *За об'єктом атаки*: напад може здійснюватися на систему в цілому; на дані і програми, що містяться на зовнішніх (дисководи, мережні пристрої, термінали) або внутрішніх (оперативна пам'ять, процесор) пристроях системи, а також у каналах передавання даних; на процеси і підпроцеси системи за участю користувачів. Метою таких атак є або прямий вплив на роботу процесу (його припинення, зміна привілеїв і характеристик), або зворотний вплив (використання зловмисником привілеїв, характеристик тощо іншого процесу у своїх цілях).

7. *За станом об'єкта*: безпосередньо під час атаки нформація в ньому може зберігатися, передаватися або оброблятися. Наприклад, у ході передавання інформації лініями зв'язку між вузлами мережі або всередині вузла можливий доступ до фрагментів переданої інформації через перехоплення пакетів на ретрансляторі мережі або прослуховування з використанням прихованих каналів.

8. *За використовуваною системою захисту*; *за кількістю атакувальників*; *за джерелами атак*; *за розміщенням атакуючого об'єкта відносно атакованого*; *за наявністю зв'язку з атакованим об'єктом*; *за рівнем еталонної моделі OSI об'єкта, на який здійснюється вплив*. При цьому помилки СЗІ можуть бути зумовлені, наприклад, помилками адміністративного управління, помилками в алгоритмах програм, а також у зв'язках між ними, помилками кодування тощо.

Зауважимо, що абсолютна більшість зазначених видів кібератак на практиці не застосовується. Натомість набула поширення класифікація, запропонована компанією Internet Security Systems Inc. Скоротивши кількість можливих категорій кібератак до п'яти, фахівці компанії умовно виокремили з них такі, що мають на меті:

1) сприяти збору інформації (*Information gathering*);

2) сприяти спробам несанкціонованого доступу до інформації (*Unauthorized access attempts*);

3) досягти стану відмови в обслуговуванні (*Denial of service*);

4) імітувати підозрілу активність (*Suspicious activity*);

5) чинити вплив на операційні системи (*System attack*).

Згідно з міркуваннями фахівців компанії, перші чотири категорії охоплюють вилучені (можливо, віддалені) кібератаки, а остання стосується локальних кібератак (вони реалізуються на вузлі, що зазнає атаки). При цьому всі кібератаки можуть бути як автоматизованими, так і неавтоматизованими (рис. 1.19).

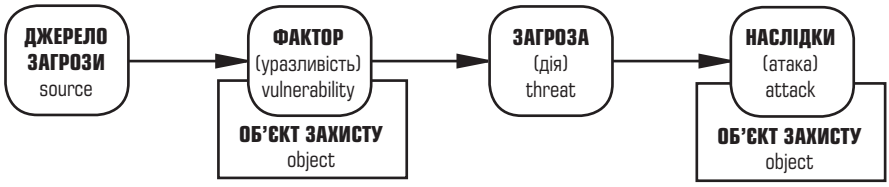


Рис. 1.19. Механізм формування кібератаки

Що ж до *об'єктів* впливу кібератак, то це можуть бути системи і канали зв'язку, канали передачі даних, АРМ (РСт), тобто системи, що взаємодіють з інформаційним середовищем. Суб'єктами кібератак виступають джерела несанкціонованих дій (рис. 1.20), спрямованих на той чи інший об'єкт.

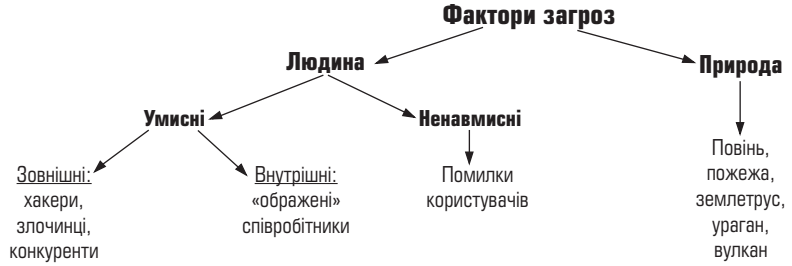


Рис. 1.20. Джерела несанкціонованих дій

Найбільш поширеним видом кібератак, за висновками Ф. Коена та багатьох інших незалежних експертів, є *комп'ютерні віруси*. Утім П. Нойман [36] пропонує розрізняти понад 20 типів кібератак (табл. 1.7).

Таблиця 1.7

Основні типи кібернетичних атак згідно з класифікацією П. Ноймана

Тип атак		Спосіб здійснення	Результат
Зовнішні		Візуальне спостереження	Спостереження за клавіатурою або монітором
		Омана	Уведення в оману операторів або користувачів
		Вилучення сміття	Вилучення інформації зі сміттєвих корзин
Апаратні		Логічне відновлення	Вилучення інформації з викрадених носіїв
		Прослуховування	Перехоплення даних
		Втручання	—
		Фізична атака	Руйнування або ушкодження обладнання, джерел живлення
		Фізичне видалення	Вилучення обладнання або сховищ даних
Маскувальні		Імітування	Використання хибних ідентифікаторів
		Узурпація ліній зв'язку або хостів	—
		Атака з підміною параметрів	—
		Заплутування мереж	Маскування фізичного місця розташування або маршруту
Злоякісні програмні коди		Троянські коні	Впровадження злоякісного коду
		Логічні бомби	Різновид троянських коней
		Черв'яки	Заволодіння розподіленими ресурсами
		Віруси	Прикріплення до програм та розповсюдження
		Обхід	Обхід механізмів безпеки
		Експлуатація уразливостей	—
		Зламування паролів	—
Зловживання	активне	Інкрементальні атаки	Поступова ескалація привілеїв, повільне просування до мети
		Відмова в обслуговуванні	Здійснення масованих атак
	пасивне	Огляд	Випадковий або вибірковий пошук
		Збір та виведення даних	Використання баз даних та аналіз трафіку
		Приховані канали	Використання прихованих каналів або інших способів витоку інформації
	інертне	—	—
	побічне	—	—

Найбільш поширеними способами здійснення кібератак П. Нойман вважає сніфер пакетів та IP-спуфінг, DoS і DDoS атаки, парольні атаки, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки й так звані ін'єкції (табл. 1.8).

Сніфер пакетів — програма, яка використовує мережний інтерфейс, функціонуючи в так званому нерозбірливому (*promiscuous mode*) режимі. Вона перехоплює мережний трафік, призначений для інших вузлів, та здійснює його подальший аналіз (рис. 1.21). Застосування програми дає змогу виявити паразитний, вірусний і закільцьований трафік; виявити в мережі шкідливе та несанкціоноване ПЗ (мережні сканери, флудери, троянські програми тощо); перехопити будь-який призначений для користувача незашифрований, а іноді й зашифрований трафік із метою отримання паролів

Таблиця 1.8

Особливості найпоширеніших кібератак

№ з/п	Тип атаки	Опис впливу
1	Denial of service	Атака з поодинокого джерела. Блокує авторизованим користувачам доступ до того чи іншого комп'ютера-жертви через «переповнення» легального трафіку зовнішніми повідомленнями
2	Distributed denial of service	Скоординована атака відразу з багатьох комп'ютерів. Для її організації комп'ютери, що беруть у ній участь, часто попередньо заражаються спеціальними програмами — черв'яками
3	Exploit tools	Привселюдно доступні засоби проникнення в системи різного рівня складності з метою пошуку в тій чи інший кіберсистемі уразливих місць і одержання доступу до комп'ютера-жертви
4	Logic bombs	Форма саботажу, коли програміст уводить спеціально сконструйований код, що викликає деструктивну роботу виконуваної програми, зокрема її повне припинення
5	Phishing	Створення та подальше використання спеціальних електронних повідомлень і web-сайтів, подібних до легальних і добре відомих користувачам. Має на меті дезорієнтувати користувачів, спонукати їх до розкриття своїх персональних даних
6	Sniffer	Програма, що перехоплює та фільтрує інформаційний трафік, вишукуючи в ньому спеціальну інформацію про користувача, наприклад передані паролі
7	Trojan horse	Комп'ютерна програма, що містить неявні шкідливі коди. Трояни, як правило, маскуються під звичайні програми, якими користувач зазвичай послуговується
8	Virus	Програма, що інфікує комп'ютерні файли включенням до них спеціальних команд. Ці команди виконуються, як правило, при завантаженні інфікованого файла в оперативну пам'ять комп'ютера. На відміну від комп'ютерних черв'яків, розмноження вірусів вимагає втручання (хоча найчастіше й неусвідомленого) людини-користувача
9	Vishing	Різновид фішингу, який використовує дешеві інтернет-технології для передавання звукових (у тому числі голосових) файлів. Дає змогу шахраям створювати власні телефонні «кол-центри» і звідти (від імені легальних користувачів) надсилати потенційним жертвам голосові або електронні повідомлення з проханням виконати певні деструктивні дії
10	War driving	Метод отримання несанкціонованого доступу до комп'ютерних мереж, що використовують ноутбуки. Для проникнення в мережу Інтернет застосовує антени та безпроводові мережні адаптери, що містять контрольовані локатори
11	Worm	Незалежні комп'ютерні програми, поширювані в мережі Інтернет за допомогою копіювання самих себе з одного комп'ютера в інший. На відміну від комп'ютерних вірусів, черв'яки не вимагають для свого розмноження втручання людини
12	Zero-day exploit	Спосіб запобігання кіберзахисту. Загроза реалізується того самого дня, коли громадськість дізнається про наявність у системі безпеки уразливих місць

та іншої інформації; локалізувати несправність мережі або помилку конфігурації мережних агентів.

Щоб знизити загрозу сніфінгу пакетів, доцільно:

• застосовувати такі методи автентифікації, як одноразові паролі типу One-Time Passwords (OTP) і DTP. В інших випадках, наприклад у разі перехоплення електронної пошти, зазначені методи не ефективні;

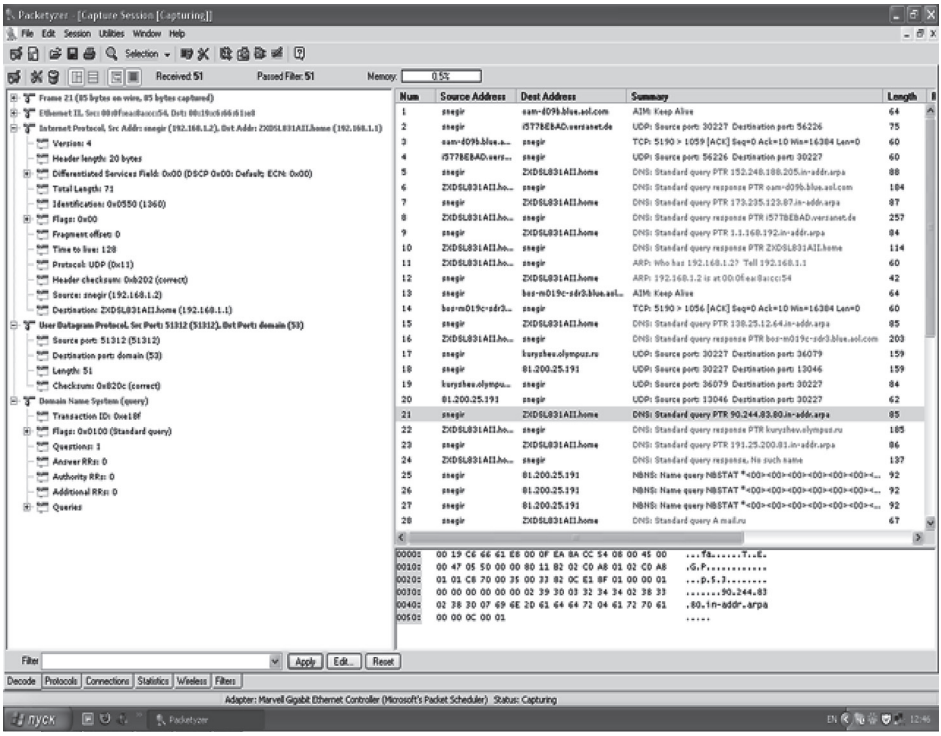


Рис. 1.21. Інтерфейс програми-сніфера Network Chemistry Packetyzer

• створити комутуючу інфраструктуру (у разі використання комутуючого Ethernet-протоколу це дозволить хакерам отримати доступ лише до трафіку, що надходить на порт, до якого вони під'єднані);

• установити антисніфери або ПЗ, яке розпізнає сніфер пакетів, наявний у певній мережі (антисніфери вимірюють час реагування хостів і визначають, чи не доводиться хостам обробляти зайвий трафік);

• створити систему криптографічного захисту. Це найбільш ефективний спосіб боротьби зі сніфером пакетів. Якщо канал зв'язку має криптографічний захист, то хакер перехоплює не повідомлення, а зашифрований текст (тобто незрозумілу послідовність бітів).

IP-спуфінг (*spoof* — обман, містифікація, підроблення) — вид хакерської атаки (рис. 1.22), що передбачає використання чужої IP-адреси, тобто введення в оману системи безпеки (зловмисник, який перебуває всередині корпорації/установи або поза нею, видає себе за санкціонованого користувача). Часто застосовується як складова комплексної атаки. Типовий приклад — DDoS атака, для здійснення якої хакер розміщує відповідну програму за чужою IP-адресою, щоб приховати власну.

Послабити загрозу IP-спуфінгу, а кібератаку перетворити на абсолютно неефективну можна завдяки:

• правильному настроюванню управління доступом (із забороною будь-якого трафіку, що надходить із зовнішньої мережі з вихідною адресою, яка має перебувати всередині власної мережі);

• застосуванню фільтрації RFC 2827 (із забороною будь-якого трафіку, вихідна адреса якого не є однією з IP-адрес певної установи);

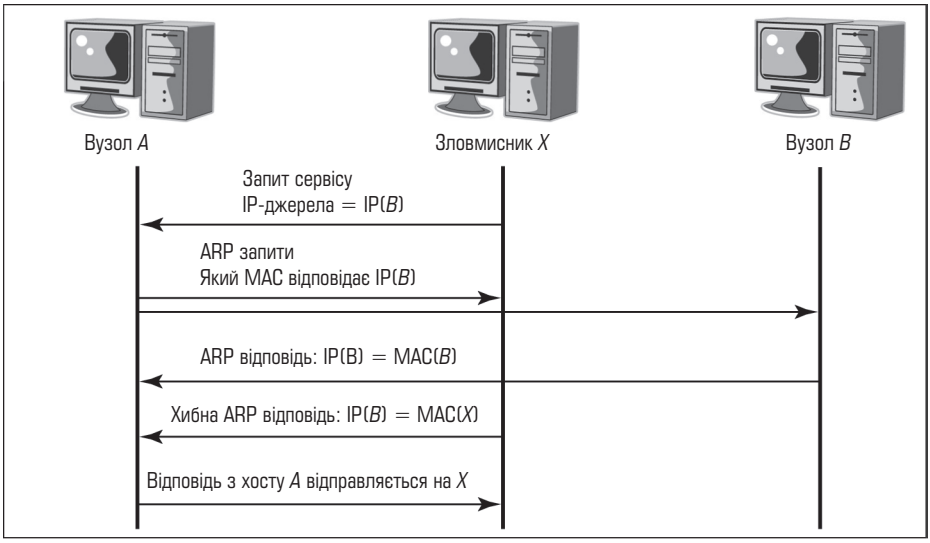


Рис. 1.22. Застосування IP-спуфінгу для отримання несанкціонованого доступу до ресурсів

• упровадженню додаткових заходів автентифікації, таких як створення системи криптографічного захисту.

Відмова в обслуговуванні **(***Denial of Service – DoS***)** — атака на комп'ютерну систему, що має на меті зробити комп'ютерні ресурси/мережу недоступними для користувачів через перевищення припустимих меж функціонування мережі, операційної системи або додатка; підвищення витрат ресурсів процесора та зменшення пропускної здатностіі каналу зв'язку (рис. 1.23). До найвідоміших різновидів DoS атак належать такі: *Flood, ICMP flood, Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco, Stacheldracht, Trinity.*

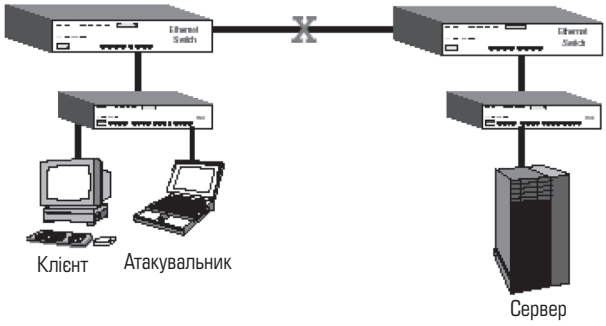


Рис. 1.23. Схема DoS атаки

На думку фахівців, особливо ефективна атака TCP SYN flood, що полягає в надсиланні надзвичайно великої кількості запитів на ініціалізацію TCP-з'єднань із вузлом-мішенню. Останньому через це доводиться витрачати всі свої ресурси на те, аби відстежувати ці частково відкриті з'єднання. Зазначена атака — найвідоміший спосіб переповнення інформаційного каналу SYN-пакетами, унаслідок якого сервер втрачає здатність відповідати на запити користувачів.

Flood («затоплення») та ***ICMP flood*** (*flood ping* — «потік пінгів») — це атаки, під час яких система отримує велику кількість ICMP- (найчастіше) або UDP-пакетів, які не несуть корисної інформації, і так званих ехо-запитів ICMP (пінг системи). У результаті маємо зменшення перепускної смуги каналу, із завантаженням комп'ютерної системи непродуктивними діями щодо аналізу «сміття», яке надійшло, та генеруванням на нього відповідей (ICMP-пакети не аналізуються системою за замовчуванням, а відповіді на них не займають багато CPU-часу).

Identification flood (запит ідентифікації системи) — атака, дуже схожа на ICMP flood. Відрізняється від неї тільки тим, що додатковою умовою її проведення є запит інформації про комп'ютерну систему (TCP порт 113). Оскільки аналіз цих запитів і генерування на них відповідей потребують більше процесорного часу, ніж у разі здійснення пінгів, то така атака вважається більш ефективною.

Ping of Death — атака, що призводить до зависання ОС, включаючи мишу й клавіатуру. Це, як правило, є відповіддю системи на надходження сильно фрагментованого ICMP-пакета великого (64 кбіт) обсягу. Сьогодні майже не використовується.

UDP flood (***User Datagram Protocol***) і ***TCP flood*** — атаки, полягають у відправленні на адресу системи-мішені безлічі пакетів UDP та TCP, що зрештою призводить до «зв'язування» мережних ресурсів. Нині ці атаки вважаються найменш небезпечними, оскільки їх легко виявити завдяки застосуванню при обміні пакетами головного контролера й агентів нешифрованих протоколів TCP і UDP.

Загрозу DoS атак можна послабити за допомогою:

- правильної конфігурації на маршрутизаторах і міжмережних екранах функцій антиспуфінгу (упровадження фільтрації RFC 2827) та функцій, спрямованих проти DoS;
- обмеження обсягу некритичного трафіку (***non-critical traffic*** — визначає ймовірність того, що мережа зв'язку відповідає заданому та узгодженому трафіку), який проходить мережею. Типовим прикладом є обмеження обсягів трафіку ICMP, що використовується тільки з діагностичною метою.

Розподілена DDoS атака (*Distributed Denial of Service*) — це підтип DoS атаки, здійснюваної одночасно з великої кількості IP-адрес (комп'ютерів) на систему об'єкта атаки, аби зробити мережу недоступною для звичайного використання (рис. 1.24). Для цього створюються так звані *ботнети* (інакше бот-мережі, або *зомбі-мережі*) із групи заражених шкідливими програмами комп'ютерів, які одночасно надсилають запити до атакованого ресурсу, (рис. 1.25). У результаті сервер не справляється з навантаженням, і доступ до атакованого ресурсу ускладнюється або взагалі стає неможливий.

Найбільш відомі різновиди DDoS атак такі: *TCP SYN flood* (рис. 1.26), *TCP flood* (рис. 1.27), *SYN flooding, UDP flood, Smurf* та *ICMP flood* атаки. При цьому найнебезпечніші ті програми, що використовують одночасно кілька видів описаних атак, наприклад TFN і TFN2K.

Одна з нових програм для організації DDoS атак — *Stacheldracht* — дозволяє здійснювати всілякі типи атак і генерувати лавини широкомовних пінг-запитів із шифруванням обміну даними між контролерами й агентами. Із погляду інформаційного захисту саме DDoS атаки становлять одну з найскладніших мережних загроз, а отже, пошук ефективних заходів протидії

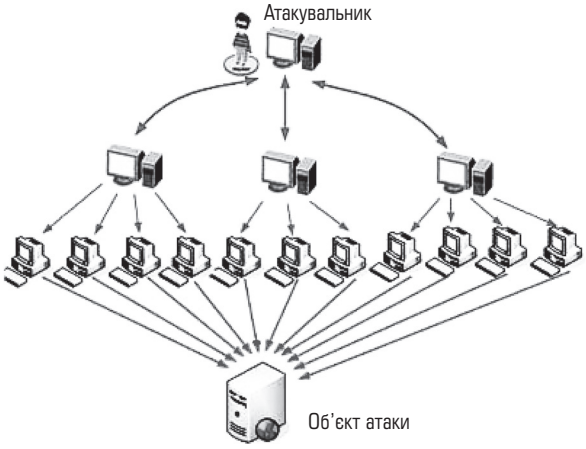


Рис. 1.24. Схема DDoS атаки

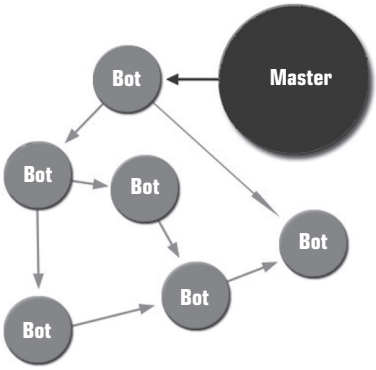


Рис. 1.25. Загальна схема організації бот-мережі

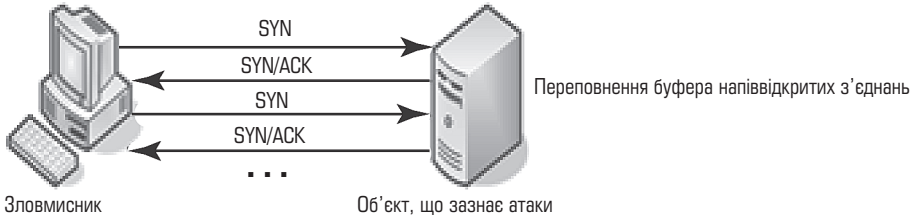


Рис. 1.26. TCP SYN flood атаки

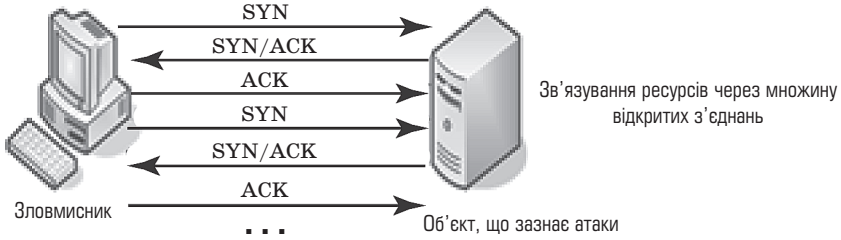


Рис. 1.27. TCP flood атака

їм — складне завдання, особливо, для організацій, діяльність яких безпосередньо пов'язана з інтернетом. Протидія DDoS атакам передбачає:

• профілактику причин, що спонукають тих чи інших осіб організовувати DDoS атаки. Дуже часто атаки здійснюються внаслідок особистої образи або політичних, релігійних розбіжностей;

• розосередження або побудову розподілених і резервних систем, які не припинять обслуговувати користувачів, навіть якщо деякі їхні елементи стануть недоступні;

• фільтрацію трафіку на маршрутизаторах (міжмережні екрани та спеціалізовані antiflood засоби фільтрації — найбільш ефективний, але й найбільш дорогий метод. По змозі їх установлюють якнайближче до джерела flood. Наприклад, програмний засіб ADoS, який є динамічним фільтром TCP-пакетів, здатний блокувати в реальному часі доступ до web-сервера з IP-адрес, що генерують інтенсивний потік HTTP-запитів);

• розміщення (розташування) безпосередньої цілі атаки — доменного імені або IP-адреси подалі від інших ресурсів, які часто зазначають впливу разом із безпосередньою ціллю;

• нарощування ресурсів системи (якщо flood спрямований на вичерпання ресурсів, то найпримітивнішим способом протидії цьому є нарощування власних ресурсів, щоб протиборча сторона не змогла їх вичерпати).

Для викрадення й подальшого передавання інформації третій стороні використовують ***програми-шпигуни*** або так звані ***кіберрозвідники***. Їх поділяють на кілька видів:

• *сканери портів* — збирають інформацію, що передається мережею, через відповідний принтерний, модемний або інший порт комп'ютера (програма Neo Trace);

• *клавіатурні та екранні шпигуни* — збирають все, що вводиться в комп'ютер із клавіатури (програма Hook Dump) або ж, відповідно, копіюють зображення з монітора комп'ютера (програма Ghost spy);

• *модемні та мережні кіберрозвідники* — автоматично записують телефонні розмови в режимі диктофона, програють записи через телефонну лінію або через звукову карту з подальшим надсиланням записів електронною поштою (програми Modem spy, Flexispy, Mobile Spy й Mobistealth) або ж, відповідно, визначають версію ОС, установленої на ПЕОМ, обсяг пам'яті та процесор, здійснюють моніторинг адрес електронної пошти; відстежують масиви інформації, передавані всередині мережі, відвідувані сайти та інформацію з них, а також розділи, які викликають інтерес у користувачів.

Алгоритм реалізації КбА унаочнює рис. 1.28.

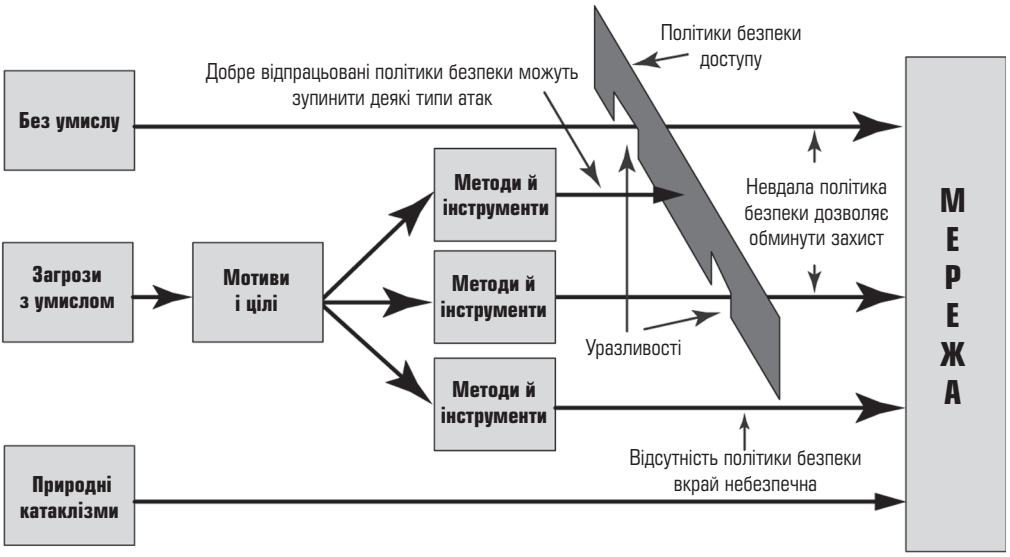


Рис. 1.28. Алгоритм реалізації кібератаки

Останнім часом складність кібератак, а також їхня кількість і частота поступово зростають. Свого апогею вони досягли нині в глобальній мережі Інтернет [37–43], яка з часом почала впливати на розвиток усієї планети та стала незамінним депозитарієм загальнолюдського знання. Сьогодні інтернет може

бути як предметом (метою) злочинних зазіхань, так і середовищем, в якому скоюються правопорушення. За висновками експертів дослідницького інституту *United States Institute for Peace* (*USIP*), саме мережа Інтернет являє собою «... ідеальне середовище для діяльності терористів ...». Адже доступ до цієї глобальної мережі надто легкий. У ній «... надзвичайно легко забезпечити анонімність користувачів ...», вона «... ніким не управляється і не контролюється ...», у ній «... не діють закони та не існує поліції ...» [44].

Підтвердженням такого висновку стали результати досліджень *Institute for Security Technology Studies At Dartmouth College* (США) [45], що мали на меті прогнозування ситуації в мережі Інтернет унаслідок здійснення Сполученими Штатами широкомасштабної антитерористичної кампанії після трагедії 11 вересня 2001 року. У звіті під назвою «Cyber Attacks During The War on Terrorism: A Predictive Analysis», опублікованому 22 вересня 2001 року, фахівці інституту проаналізували політичні конфлікти, що стимулювали зростання кількості атак на ресурси мережі Інтернет. Ішлося, зокрема, про конфлікти між Індією і Пакистаном, Ізраїлем і Палестиною, NATO і Сербією, США і Китаєм. Фахівці інституту констатували, що фізичні атаки на елементи критично важливої інфраструктури провідних країн світу супроводжуються неодмінним зростанням кількості кібератак, передусім на сервери та активне мережне устаткування, під'єднане до цієї глобальної мережі. Представники інституту *System Administrator and Network Security* (США) та Центру із захисту національної інфраструктури при ФБР (США) зробили спільну заяву про те, що здійснення кібератак поступово стає потужним засобом ведення інформаційних воєн між державами, а мережа Інтернет — незамінним «інструментом кіберпланування» [46], яка забезпечує сучасним терористам анонімність, можливість керувати і координувати дії при підготовці та здійсненні терактів. Тобто, згідно із [44–46] та твердженням інших фахівців, тероризм останнім часом зробив якісний крок у своєму розвитку й еволюціонує в напрямку, який можна назвати *мережною війною* (*netwar*). Саме на цьому наголошував директор ЦРУ Леон Панетта, прогнозуючи, що для США «майбутній Пірл-Харбор, швидше за все, буде комп'ютерною атакою». На його думку, цьому не в останню чергу сприятимуть такі чинники (рис. 1.29):

- стрімкий розвиток глобальної мережі Інтернет, що перетворилася на незамінний депозитарій людського знання і вже налічує сотні мільярдів документів, розміщених на десятках мільйонів серверів, охоплюючи кілька мільярдів користувачів;

Рис. 1.29. Фактори, що впливають на інформаційну безпеку

• уможливлення високошвидкісного безпроводового доступу зловмисників до всього спектра наявних і перспективних послуг мережі Інтернет за доступними цінами й у будь-якій точці світу на базі новітніх ІТ-технологій;

• небувале нашестя на світовий ринок злоякісного ПЗ (троянські програми всілякого призначення, вірусні програми для смартфонів, комунікаторів і КПК, численні вірусні програми для операційних систем Linux, Mac OS тощо) і можливість здійснення електронних нападів за допомогою ПЗ;

• поява нових і вдосконалення відомих видів зловживань, таких як фішинг, смс-шахрайство, лже-антивіруси, кібер-шантаж, фальшиве розсилання інформації від «друзів», електронні листи з «цікавими» вкладеннями, створення бот-мереж, у тому числі й для проведення атак на різні сайти.

Зауважимо, що тероризм є постійним супутником людства. Ще в І сторіччі нашої ери в Іудеї діяла секта сикаріїв (*сика* — кинджал або короткий меч), які знищували представників єврейської знаті за співробітництво з римлянами. Представники середньовічної мусульманської секти асошафінів полювали на префектів і каліфів. У ті самі часи політичний терор практикували деякі таємні товариства в Індії та Китаї. На територіях сучасного Ірану, Афганістану й деяких інших країн безмежний жах у своїх супротивників із мусульманської сунітської знаті та правителів викликали ісмаїліти — представники могутньої та гранично закритої секти, що послуговувалася у своїй боротьбі довершеними способами фізичного усунення небажаних осіб. Нині терористичні дії вчиняють не лише проти певних індивідів із політичних міркувань, а й проти цивільних і військових об'єктів, маючи на меті підрив економічної безпеки чи обороноздатності противника. При цьому діяльність сучасних терористів характеризується:

1) відсутністю національних кордонів (терористичні акції останнім часом можуть здійснюватися практично з будь-якого куточка земної кулі);

2) спрямованістю терористичних дій як на цивільні (енергетику, фінансові та урядові електронні системи), так і на військові об'єкти;

3) здатністю ефективно використовувати конфліктні та кризові ситуації у своїх цілях (упровадження в поточну політичну кон'юнктуру проявів інформаційного тероризму).

Такий стан справ призвів до появи принципово нового різновиду терористичних дій у віртуальному просторі — ***кібертероризму*** (***КбТ***). Власне, як термін це поняття в ІТ-лексиконі з'явилось приблизно в середині 1980-х років. Саме тоді один із наукових співробітників США Беррі Колін уперше впровадив його в офіційний обіг. У 1997 році спеціальний агент ФБР М. Полліт визначив цей вид тероризму як «навмисні політично вмотивовані атаки на інформаційні та комп'ютерні системи, комп'ютерні програми й дані, що полягають у застосуванні насильства щодо цивільних цілей із боку субнаціональних груп або таємних агентів». Наприклад, у 1998 році майже половина з 30 терористичних організацій, внесених США до списку «іноземних терористичних організацій», мали власні web-сайти, а 2000 року практично всі терористичні групи виявили свою присутність у мережі Інтернет. Протягом 2003 і 2004 років було виявлено близько сотні сайтів, що обслуговують терористів і їхніх прихильників. Директор Центру захисту національної інфраструктури ФБР США Рональд Дік у доповіді, опублікованій на сайті Федерального бюро розслідувань, характеризує сучасну ситуацію так: «... У світі постала нова форма тероризму — *кібертероризм*, який використовує комп'ютер і мережі зв'язку

для руйнування частин національної інфраструктури та досягнення власних цілей» [47].

Але на порядку денному світового співтовариства проблема КбТ актуалізувалася лише після 2010 року, коли в Іранському Центрі зі збагачення урану було виявлено вірус «Stuxnet», що призвело до виходу з ладу ядерних центрифуг (цей інцидент описано в підрозд. 1.1, с. 32). Якщо раніше питання безпеки в інтернеті зводилися переважно до захисту особистої інформації та банківських даних, то тепер необхідно було думати про захист цілих комп'ютерних систем і секретних баз даних від несанкціонованого проникнення. Розвинені країни на прикладі Ірану побачили, що і їхні внутрішні об'єкти можуть опинитися в небезпеці. Це дало поштовх до активного обговорення форм, яких може набирати *кібертероризм*, пошуку методів боротьби з ним, а також до налагодження міжнародного співробітництва в цій сфері, спрямованого на зниження можливих ризиків.

Згідно з Конвенцією Ради Європи 2001 року щодо кіберзлочинів засобами кібертероризму можуть виступати комп'ютерна система, комп'ютерні дані, послуги ТКС, а також дані трафіку. Збиток від застосування таких засобів може знаходити таке вираження:

1) людські жертви або матеріальні втрати, викликані деструктивним використанням елементів мережної інфраструктури;

2) втрати (у тому числі й загибель людей) від несанкціонованого використання інформації з високим рівнем таємності або мережної інфраструктури керування в життєво важливих (критичних) для держави сферах діяльності;

3) витратами на відновлення керованості мережі, спричинені діями щодо її руйнування або ушкодження;

4) моральний збиток, якого зазнав сам власник мережної інфраструктури та його інформаційний ресурс;

5) усілякі втрати від несанкціонованого використання інформації з високим рівнем таємності.

Утім чіткого визначення поняття «*кібертероризм*» і досі не існує. З огляду на це проаналізуємо відомі підходи до його тлумачення [2].

1. Багато науковців, серед яких *В. Харченко, О. Корченко, О. Довгань, В. Хлань, Ю. Травніков, О. Климчик, М. Девост, Р. Кравченко, Є. Старостіна, Б. Хьютон та Н. Поллард* вважають, що під КбТ необхідно розуміти тільки виключно використання компонентів КбП як засобів або середовища для реалізації терористичних дій (*Instrument*). У відповідних визначеннях присутні всі ознаки традиційного тероризму, реалізованого за допомогою сучасних інформаційних та комунікаційних технологій. Це класичний випадок:

КбТ = ТЕРОРИЗМ + КбП.

2. Інші науковці, такі як *В. Голубєв, М. Політ, Д. Деннінг, В. Пилипчук, О. Дзьобань, Ю. Гаврилов і Л. Смирнов,* стверджують, що КбТ — це дії, пов'язані з використанням елементів КбП як предмета (*Subject*) злочинних зазіхань, які реалізуються через різного роду КбА та мають на меті завдати шкоди конкретним об'єктам критичної інформаційної інфраструктури.

3. У працях *К. Колмена, С. Мельника, О. Тихомирова, О. Федорова та Є. Роговського* чітко відстежується гіпотеза про те, що терористичні угруповання використовують КбП перважно в суміжних цілях (*AdjTarget*) — для встановлення зв'язку із суспільством, здійснення інформаційно-психологіч-

ного впливу, створення пропагандистських сайтів, збирання необхідної для реалізації терактів інформації засобами інтернету.

4. Деякі з відомих авторів, таких як *О. Корченко, Дж. Левіс, Д. Малишенко, К. Керр, С. Гавриш і К. Вілсон* [37; 42; 43; 47] під КбТ розуміють синтез дій, визначених у п. 1 і 2.

На підставі ґрунтовного аналізу відомих визначень КбТ було складено таблицю 1.9, яка дає підстави констатувати, що жодне з цих визначень не задовольняє всі базові критерії.

Таблиця 1.9

Багатокритеріальний аналіз визначень поняття кібертероризму

№ з/п	Автори визначення	Базові критерії		
		Instrument	Subject	Adj Target
1	В. Харченко, О. Корченко та ін.	+	–	–
2	О. Корченко та ін.	+	+	–
3-4	В. Голубєв	–	+	–
5	М. Політ	–	+	–
6	О. Довгань та В. Хлань	+	–	–
7	К. Колмен	–	+	+
8	Національний центр захисту інфраструктури США	+	–	–
9	Д. Деннінг	–	+	–
10	Дж. Левіс	+	+	–
11	Ю. Травніков	+	–	–
12	Націон. конф. державної законотворчості, США	+	–	–
13	О. Климчик та Р. Кравченко	+	–	–
14	Д. Малишенко	+	+	–
15	К. Керр	+	+	–
16	Є. Старостіна	+	–	–
17	С. Гавриш	+	+	–
18	В. Бутузов	+	+	–
19	С. Мельник та О. Тихомиров	–	–	+
20	О. Федоров та ін.	–	+	+
21	В. Пилипчук та О. Дзьобань	–	+	–
22	М. Девост, Б. Хьютон та Н. Поллард	+	–	–
23	Ю. Гаврилов та Л. Смирнов	–	+	–
24	К. Вілсон	+	+	–
25	Є. Роговський	+	–	+

Згідно зі сказаним можна сформулювати таке визначення.

Кібертероризм *— це суспільно небезпечна діяльність, що свідомо здійснюється в кіберпросторі (або з використанням його технічних можливостей) окремими особами або організованими групами з терористичною метою та реалізується ними через заздалегідь спланові й політично вмотивовані кібератаки на ІТС з використанням високих технологій* (рис. 1.30).

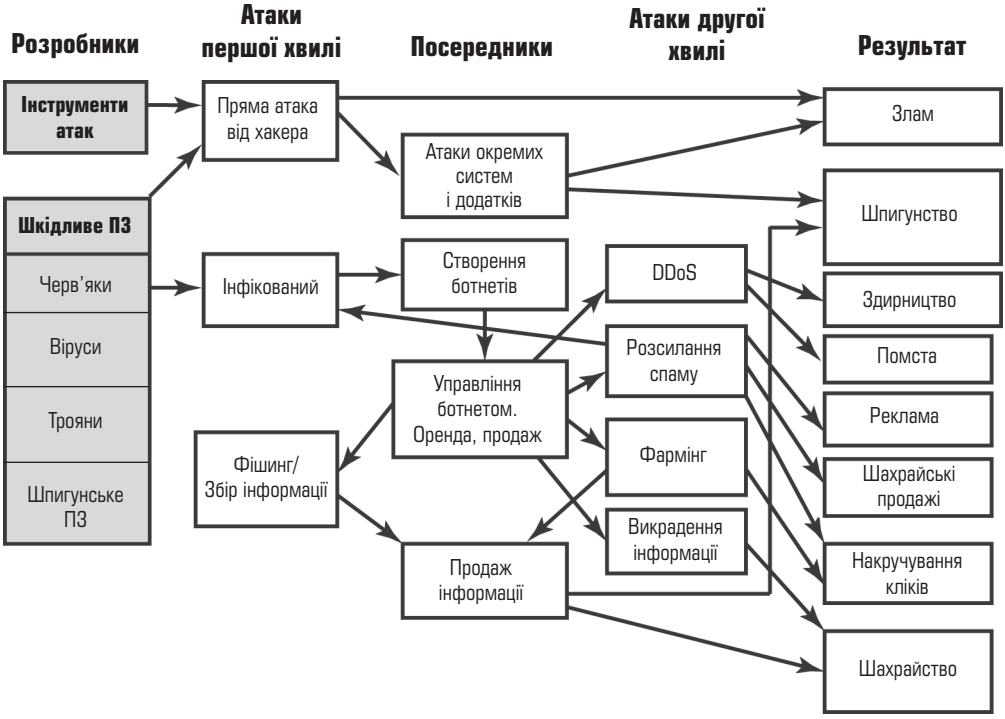


Рис. 1.30. Індустрія сучасного кібертероризму

Спектр впливу КбТ достатньо широкий — від нав'язування хибних рішень або панічних настроїв до проникнення в канали й системи зв'язку та навігації. Результатом таких дій може бути, наприклад, введення хибного IP або порушення цілісності існуючого, дезорганізація роботи критично важливих елементів інформаційної і/або кібернетичної інфраструктури держави, дестабілізація суспільно-політичної обстановки в державі та регіоні, ускладнення міжнародних відносин або інші негативні наслідки, що створюють небезпеку для життя і здоров'я населення. Головні особливості КбТ такі:

- висока ефективність кібератак;
- просторово-часова невизначеність джерела кібератаки та його віддаленість від об'єкта атаки;
- часова невідповідність між власне кібератакою та процесом її підготовки;

можливість організації складних кібератак одночасно на різні ІТС із різних напрямів тощо.

Торкаючись проблем світових загроз, директор ЦРУ США Джордж Тенет свого часу наголошував, що кібертероризм у сьому світі стрімко набуває неочікувано великих масштабів і зрештою стає реальною загрозою для національної безпеки будь-якої держави. За його твердженням, більшість терористичних угруповань на кшталт Hizbollah, HAMAS, the Abu Nidal organization та інших подібних до них структур для підтримання своєї протиправної діяльності спираються на останні досягнення інформаційних технологій і комп'ютерного прогресу — комп'ютерні файли, електронну пошту та шифрування (криптографія, стеганографія). Сьогодні всі відомі терористичні групи публікують власні матеріали щонайменше 40 різними мовами, застосовуючи у своїй діяльності такі прийоми [48; 49]:

• завдання збитків окремим елементам інформаційного та кібернетичного простору;

• руйнування апаратних засобів, мереж електроживлення та елементної бази ІТС, а також наведення завад за допомогою спеціальних програм, біологічних і хімічних засобів;

• крадіжку або знищення суспільно значущих інформаційних, програмних і технічних ресурсів інформаційного та кіберпростору через подолання їхніх систем захисту, упровадження вірусів та різного роду закладок;

• вплив на програмне забезпечення та інформацію з метою спотворення або модифікації;

• розкриття із загрозою опублікування (або власне саме опублікування) закритої інформації про функціонування інформаційної інфраструктури держави, про суспільно значущі військові інформаційні системи, коди шифрування та принципи роботи шифрувальних систем;

• захоплення каналів ЗМІ з метою поширення дезінформації, чуток, демонстрації сили терористичної організації та оголошення нею своїх вимог;

• знищення або активне пригнічення ліній зв'язку, штучне перевантаження вузлів комутації;

• проведення інформаційних і психологічних операцій.

Як найбільш характерний приклад «продуктивної роботи» кібертерористів мжна згадати так званий кіберджихад, до якого причетні хакери Пакистану та Індії, що ведуть боротьбу за Кашмір [44; 50]. Пакистанські хакери зламують web-сайти індійських державних установ. У свою чергу, індійська хакерська група (*Indian Snakes*) із метою «віртуальної помсти» поширює мережний черв'як «Yaha-Q». Головне завдання цього вірусу полягає у здійсненні DDoS атак на деякі пакистанські ресурси, серед яких — інтернет-провайдери, сайт фондової біржі в Карачі та урядові ресурси. Ще один не менш виразний приклад являло собою протистояння ізраїльських і палестинських хакерів [44; 51–54]. У жовтні 2000 року, після припинення мирних переговорів, вони брали участь у ряді спрямованих один проти одного кібератак, що мали різний характер: від простої зміни змісту сторінок до скоординованого нападу з метою захоплення повноважень адміністратора системи. Так, 6 жовтня 2000 року було уражено 40 ізраїльських сайтів і принаймні 15 палестинських. Програмний засіб проведення розподілених атак із відмовою в обслуговуванні став головним інструментом, що його використовували ізраїльтяни. Пропалестинські хакери руйнували будь-який тип ізраїльських сайтів, змінюючи їхній зміст повідомленнями під рубрикою «За вільну Палестину». Організація «Hezbollah» взагалі виробила цілу стратегію завдання збитків ізраїльському уряду, його військовим і діловим колам [54]. Ішлося про дестабілізацію урядових органів Ізраїлю, руйнування фінансових інститутів, а також знищення в комп'ютерній мережі даних про сотні угод і фінансових операцій.

Наслідки боротьби хакерів Пакистану та Індії, Ізраїлю та Палестини з усією очевидністю свідчать про безсумнівну уразливість будь-якої держави від різних проявів кібертероризму. Передусім це пояснюється тим, що зазначений різновид кіберзагроз не має державних кордонів, а його потенційні представники здатні однаковою мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі. Отже, як бачимо, сучасний тероризм еволюціонує в напрямку мережної війни.

Нині тероризм у мережі Інтернет взагалі вийшов на якісно новий рівень — здійснення кібератак під неформальною егідою та за фінансування провідних держав світу. Ці атаки спрямовуються, наприклад, проти політичних режимів окремих країн або мають на меті збір персональних даних громадян. Нещодавно, переважно завдяки світовим ЗМІ, стало відомо про існування програми секретних служб Великобританії — Центру урядового зв'язку (UK Government Communications HeadQuarters) під кодовою назвою «Tempora», а також програми Агентства національної безпеки (АНБ) США «Prism», що її ініціювали президенти Дж. Буш і Б. Обама. Зазначені програми спрямовані на стеження за громадянами будь-яких країн світу за допомогою мережі Інтернет. Так, програма британських спецслужб «Tempora» передбачала збір, щоденну обробку та передачу в США близько 20 петабайт інформації через 46 трансатлантичних ліній. До речі, усі архіви інтернету за станом на кінець 2012 року становили 10 петабайт даних. Факт стеження за іноземними громадянами в рамках програми «Prism» визнав навіть глава національної розвідки АНБ США Джеймс Клеппер. Адже відповідно до «Prism» найбільші світові інтернет-компанії (Google Inc., Microsoft Corporation, Facebook Inc., Apple Inc., Yahoo, AOL Inc., розроблювачі сервісів Skype, Youtube, PalTalk) надають без рішення суду спецслужбам США доступ до своїх серверів, які зберігають дані користувачів. Ідеться про вилучення конфіденційної інформації з аудіо- і відео-чатів, фотографій, електронних листів, відправлених файлів документів, логінів зв'язку, історій пошуку, особистих даних учасників соціальних мереж. Окрім того, американські спецслужби мають змогу відстежувати трансакції за кредитними картками та електронним листуванням, отримувати інформацію про підмкнення користувачів до тих чи інших сайтів, а також дані мобільного зв'язку. Поряд з інтернет-корпораціями у програмі «Prism» задіяно й такого відомого виробника комп'ютерної техніки, як американську компанію «Dell». При цьому АНБ США використовує програму інтелектуального аналізу даних «Bovndtess informant», призначену для систематизації даних про країни, в яких ведеться «електронне стеження». Завдяки цій програмі було створено цифрову карту із зазначенням країн — об'єктів для електронної розвідки. Судячи з цієї карти, найактивніше спецслужби діють у тому ж таки Ірані, Пакистані та Йорданії.

Кібертероризм як головна складова кіберзлочинності посідає не останнє місце й серед низки загроз національній безпеці та інтересам України. За даними соціологічних опитувань на його поширення нині активно впливають:

1) високий потенціал і професійний рівень українських програмістів, послугами яких охоче користуються навіть такі флагмани програмної індустрії, як «Майкрософт»;

2) здатність молоді швидко опановувати технічні новинки, про які ще вчора вони не мали жодного уявлення;

3) темпи комп'ютеризації (кількість комп'ютерів в Україні щорічно подвоюється) та стрімке збільшення кількості інтернет-користувачів (з 500 тис. у 2000 році до 5 млн 800 тис. — у 2005-му).

При цьому до основних чинників, що формують джерела таких загроз, вітчизняні експерти відносять:

• недостатню увагу з боку державних органів до проблем інформатизації, незважаючи на потенційну економічну рентабельність національного інтернет-сегмента;

• відсутність належної державної фінансової підтримки фундаментальних і прикладних вітчизняних досліджень у сфері запобігання та боротьби з кіберзлочинністю;

• відставання вітчизняного законодавства в інформаційній галузі від розвинених країн світу в умовах спільного існування у єдиному інформаційному просторі;

• недостатню пропускну здатність і надійність каналів зв'язку, комунікаційного обладнання;

• відсутність ефективної політики безпеки комп'ютерних мереж і необхідних програмно-технічних засобів для обмеження доступу до конфіденційної інформації в базах даних;

• розширення можливостей для негативного інформаційного впливу на людину, суспільство та державу за допомогою нових комп'ютерно-телекомунікаційних засобів і технологій, що постійно розвиваються.

• перехоплення електронної пошти, паролів і файлів за допомогою легкодоступних для зацікавлених користувачів програмно-технічних засобів.

За таких умов напрямком для керівництва України є організація взаємодії та координації зусиль правоохоронних органів, спецслужб і судових органів, передусім СБ та Служби зовнішньої розвідки (СЗР) України, ДССЗЗІ та МВС України, які мають на меті забезпечення безпеки національного інформаційного простору, здійснення заходів із кіберзахисту власної ІТ-інфраструктури, а також активну протидію внутрішнім і зовнішнім кібернетичним загрозам. І все ж протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем та мереж, а також порушенню функціонування об'єктів нападу (інформації, що циркулює та обробляється в ІТС, баз даних та програмного забезпечення, призначеного для обробки зібраної інформації тощо) на тлі інтенсифікації діяльності кіберзлочинців з дня на день стає все важче. Істотно поліпшити ситуацію заважають такі чинники:

• складність організації захисту міжмережної взаємодії;

• наявність помилок у загальному та спеціальному ПЗ, ОС та утилітах, що відкрито розповсюджуються мережею;

• неправильне чи помилкове адміністрування систем;

• відсутність адекватного захисту даних у більшості із сучасних мережних протоколів;

• наявність помилок у конфігурації систем і засобів забезпечення безпеки, а іноді й повне ігнорування необхідності їх упровадження.

Саме цим пояснюється ефективність кібератак, майже кожна з яких досягає очікуваного результату, та надзвичайна актуальність завдань щодо їх виявлення, та запобігання відповідним негативним наслідкам. Головні кроки, що сприятимуть виконанню таких завдань, полягатимуть у вивченні слабких місць прикладних програм за даними корпорацій Bugtrad (http://www.securityfocus.com) і CERT (http://www.cert.com), застосуванні крім системного адміністрування систем розпізнавання атак (IDS-технологій) додаткового ПЗ, що дасть змогу відстежувати всі пакети, які проходять через певний мережний інтерфейс, аналізувати спеціальні аналітичні додатки із застосуванням лог-файлів операційних систем та мережних лог-файлів, використовувати евристичні механізми захисту та антивірусні програми.

Питання для самоконтролю

1. Дайте визначення понять ***інформаційний простір*** *і* ***кібернетичний простір****. Назвіть основних дійових осіб кіберпростору.*

2. Що таке кіберборотьба? Які основні особливості її притаманні?

3. Дайте визначення поняття ***інформаційна безпека****. Назвіть основні чинники, які на неї негативно впливають, та методи, завдяки яким цьому можна запобігти.*

4. Дайте визначення поняття ***кібернетична безпека****. Назвіть істотні ознаки, які його характеризують.*

5. Які документи регламентують діяльність із забезпечення інформаційної та кібернетичної безпеки в Україні? Наведіть приклади внеску в реалізацію цих процесів державних підрозділів спецпризначення.

6. За якими принципами мають розвиватися взаємовідносини між Україною та НАТО у сфері інформаційної та кібернетичної безпеки? Назвіть основні напрямки співробітництва Україна–НАТО у сфері кіберзахисту.

7. Чим зумовлюються намагання України створити дієздатну систему інформаційної і кібербезпеки?

8. Дайте визначення понять ***кібервтручання*** *і* ***кіберзагроза****.*

9. Що слід розуміти під поняттям ***інциденту*** *у сфері високих технологій? Розкрийте сутність процесу управління інцидентами.*

10. Як класифікує інциденти у сфері високих технологій Рада Європи? Який зміст у це поняття вкладають такі провідні країни світу, як США, Німеччина, Франція, Великобританія?

11. Опишіть модель системи управління інцидентами та розкрийте сутність її складових.

12. Дайте визначення внутрішнього і зовнішнього інциденту. Наведіть приклади таких інцидентів класифікації згідно з кодифікатором Інтерполу.

13. Які з вдомих інцидентів становлять нині найбільшу небезпеку?

14. Наведіть приклади деструктивних інцидентів у сфері високих технологій. Розкрийте відмітні риси мережних черв'яків Stuxnet, Duqu та Flame.

15. Назвіть найбільш критичні заходи захисту інформації від кіберзагроз.

16. У чому полягають спільні та відмінні особливості заходів захисту IP від стороннього кібервпливу, пропонованих компанією SANS (США) та НД ТЗІ України?

17. Перелічіть основні кроки, які мають бути дотримані співробітниками служб безпеки в разі фіксації порушень інформаційної та кібернетичної безпеки.

18. Дайте визначення поняття ***кібератака****. Наведіть приклади його тлумачення різними категоріями дослідників.*

19. За якими основними ознаками кібератаки можуть бути класифіковані?

20. Назвіть основні типи кібератак за класифікацією П. Ноймана.

20 Що таке сніфер пакетів? Які заходи сприятимуть зниженню загрози сніфінгу?

21. Що таке IP-спуфінг? Завдяки чому можна послабити загрозу IP-спуфінгу?

22. Що таке DoS та DDoS атаки? Назвіть найбільш відомі їх різновиди. За рахунок чого можна послабити загрози від DoS та DDoS атак?

23. Наведіть приклад алгоритму реалізації кібератак.

24. Дайте визначення поняття ***кібертероризм****. Наведіть приклади його тлумачення різними категоріями дослідників.*

25. Назвіть основні риси кібертероризму. Що сприяє сучасним терористам у веденні їх протиправної діяльності та забезпечує їм успіх?

26. Назвіть головні прийоми, якими користуються сучасні кібертерористи у процесі своєї протиправної діяльності.

27. Які чинники впливають на поширення кібертероризму в Україні?

РОЗДІЛ 2

СОЦІОТЕХНІЧНА БЕЗПЕКА: ПРОБЛЕМНІ АСПЕКТИ

2.1. Особливості захисту сучасної інфосфери в умовах стороннього кібернетичного впливу

Розвиток подій на міжнародній арені наприкінці XX та на початку XXI сторіччя показує: незважаючи на потужні зусилля світової спільноти щодо врегулювання міждержавних конфліктів мирним шляхом, кількість і гострота збройних протистоянь з року в рік не знижуються. Більш того, останнім часом вони вирують не лише у традиційних сферах збройних суперечок, таких як земля, море і повітря, а й поступово просуваються в новітні простори — інформаційний та кібернетичний [54; 55]. Про важливість оволодіння ситуацією в цих ареалах свідчить:

1) створення більшістю країн світу, як зазначалося в розд. 1, спеціальних структур, призначених для ведення ***інформаційного протиборства*** (рис. 2.1) — *закономірного об'єктивного процесу у стосунках між протиборчими сторонами, спрямованого на досягнення ними цілей власної державної політики в мирний та воєнний час, за рахунок комплексного впливу на систему державного і військового управління супротивної сторони та на її військово-політичне керівництво, а також захисту своїх інформаційних об'єктів від аналогічного впливу та розгортання* ***кіберборотьби*** [56];

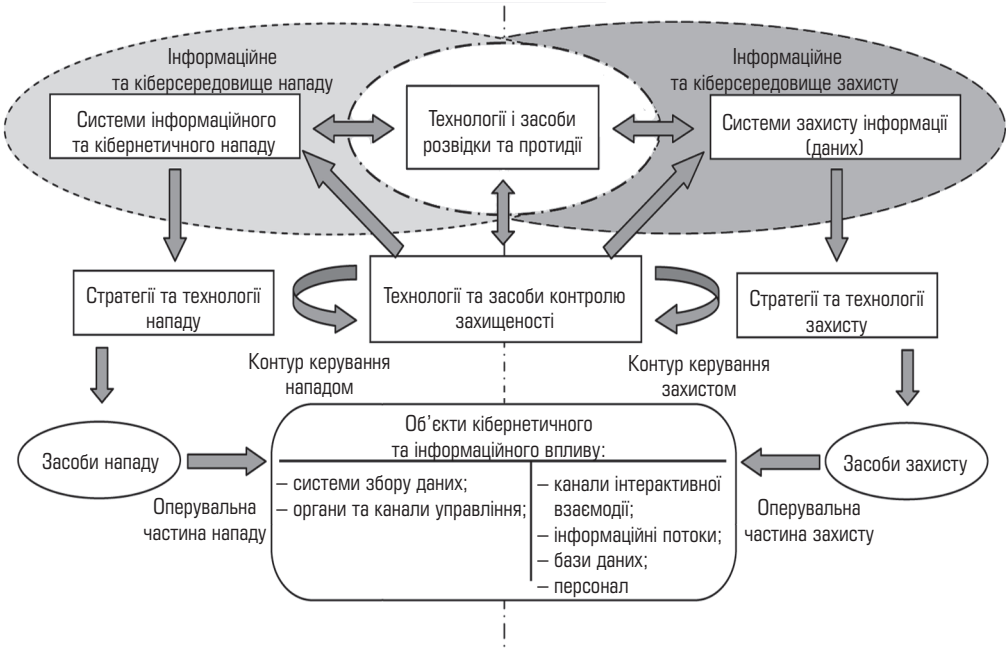


Рис. 2.1. Концептуальна схема інформаційного протиборства

2) змінювання ставлення цих країн до власної ***інформаційної*** та, як наслідок, ***кібернетичної безпеки***.

До основних зон впливу протиборчих сторін при цьому належать соціальна, когнітивна, інформаційна та фізична сфери відповідного суспільства (рис. 2.2), а як головні форми інформаційного протиборства виступають інформаційний і кібернетичний тероризм, інформаційна та кібернетична злочинність у поєднанні із заходами, спрямованими на забезпечення власної інформаційної та кібернетичної безпеки (рис. 2.3).

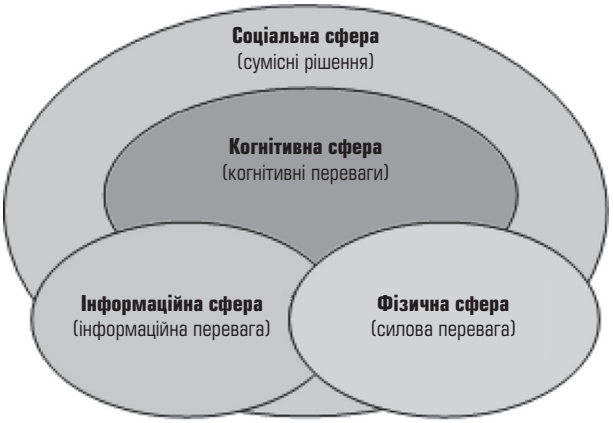


Рис. 2.2. Сфери впливу інформаційного протиборства

Рис. 2.3. Основні форми інформаційного протиборства

Останнім часом такі дії домінують у геополітичній конкуренції більшості країн світу, а це у свою чергу, зумовлює нові завдання їхніх збройних сил і виводить на перший план проблеми ***інформаційних воєн*** — *інформаційного протиборства, що охоплює весь інформаційний простір конфліктуючих сторін і може набирати форм дипломатичної, економічної та збройної боротьби* (рис. 2.4).

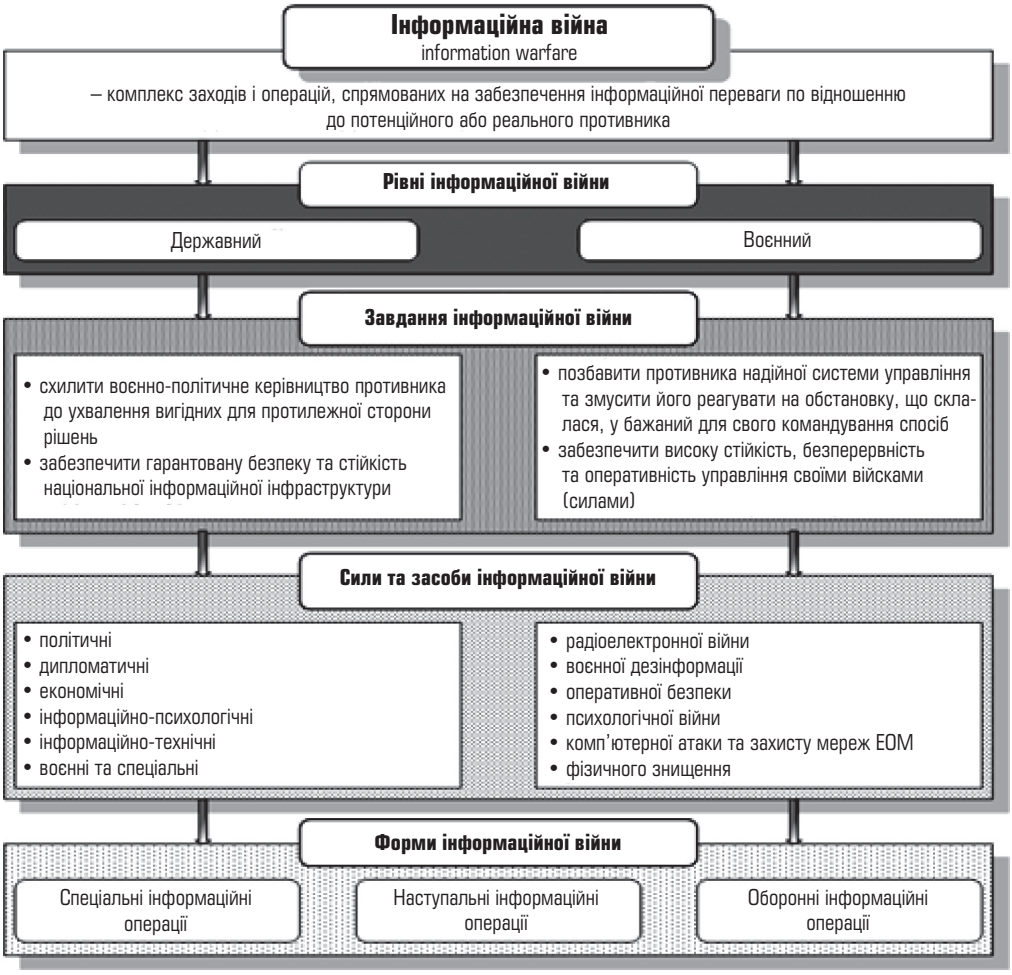


Рис. 2.4. Рівні та форми інформаційної війни

Здебільшого інформаційні війни розгортаються у вигляді ***кібервоєн*** — *активного протистояння між державами, політичними групами, соціальними утвореннями, приватними і комерційними установами та іншими державними і позадержавними суб'єктами. Таке протистояння має на меті заподіяння шкоди один одному в ІТ-сфері за рахунок проведення як оборонних* (*захист власних ІТС від деструктивного впливу*), *так і наступальних* (*установлення контролю над ІТС протиборчої сторони*) *дій* [1; 56].

Розглянемо причини такої ситуації. Усі вони так чи інакше пов'язані з відсутністю чи недосконалістю нормативно-правової бази, яка мала б передбачити:

1) заборону застосування ***інформаційної зброї*** — *різновиду зброї, що являє собою сукупність засобів інформаційного впливу, призначених для завдання протиборчими сторонами в процесі інформаційного протиборства збитку елементам інформаційної інфраструктури один одного* (рис. 2.5).

Передусім ідеться про ***кіберзброю*** (табл. 2.1) — *спеціальні атакувальні та оборонні засоби ураження, що дають можливість цілеспрямовано змінювати, знищувати, копіювати і блокувати інформацію, долати системи захисту,*

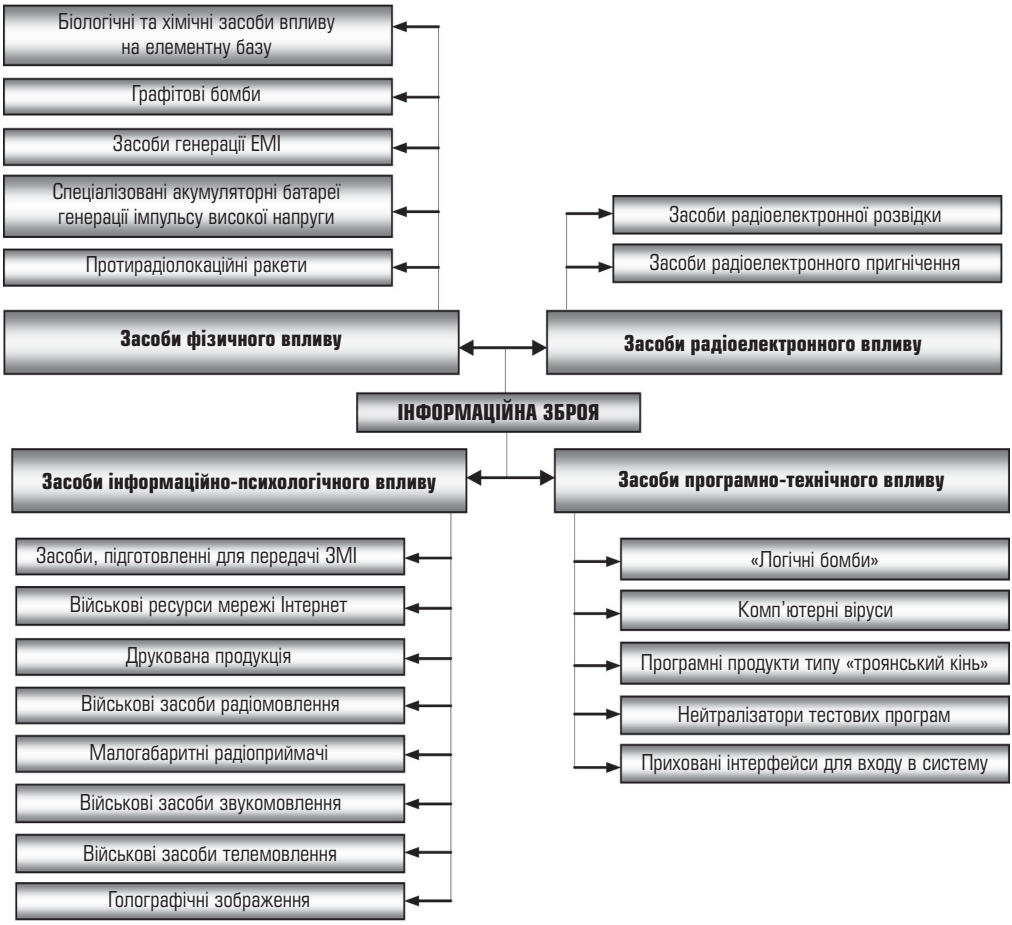


Рис. 2.5. Засоби передавання (доставляння) та застосування інформаційної зброї

обмежувати доступ законних користувачів, порушувати функціонування носіїв інформації для дезорганізації роботи технічних засобів IT-систем і *мереж*, перевага яких порівняно з іншими видами зброї забезпечується за рахунок:

- універсальності (незалежність від кліматичних і географічних особливостей місцевості ведення військових дій);
- прихованості (можливість приховати свої наміри нападати на супротивника);
- економічної ефективності (невеликі витрати);
- застосовності для розв'язання широкого кола завдань (можна застосовувати на будь-яких етапах війни, та щодо різних суб'єктів);
- масштабності застосування (можливе здійснення впливу на стаціонарні і мобільні елементи системи наземного, морського, повітряного та космічного базування);
- наявності ефекту «ланцюгової реакції» (вплив на окремий елемент системи може призвести до виведення з ладу інших елементів, сегментів і системи в цілому);

Таблиця 2.1

Загальна характеристика основних видів наступальної і оборонної кіберзброї (НОКЗ)

Основні види НОКЗ за способом реалізації впливу на ІТС	Засоби реалізації	Класифікаційні ознаки	Типи	Призначення, властивості та функціональні особливості
Алгоритмічна	Існуючі уразливості математичних алгоритмів ПЗ	За способом дій	Експлойти (англ. *exploit* — експлуатувати, розроблювати	Несанкціонований доступ до інформаційних ресурсів через використання «недокументованих» можливостей ПЗ
Програмна	Комп'ютерні віруси	За об'єктом впливу	Завантажувальні	Ураження завантажувальних секторів оперативної пам'яті
			Файлові	Зараження файлової системи в разі запуску програми, яка містить вірус
			Макровіруси	Здійснення транзиту даних до конкретних несанкціонованих адресатів
		За способом зараження	Резидентні	Залишають свою резидентну частину (носій вірусу в оперативній пам'яті після завершення виконання програми)
			Нерезидентні	Не залишають резидентної частини. Активні протягом обмеженого проміжку часу
		За принципом маскування	Поліморфні	Властивість змінювати свою структуру
			Віруси-невидимки	Використовують спеціальні алгоритми, які дозволяють маскувати свою присутність в системі
		За деструктивними можливостями	Із деструктивними функціями	Властивість до самодублювання
			Безпекові	Спрямованість на конкретні програми
	Засоби несанкціонованого доступу	Те саме	Несертифіковане ПЗ	Подолання систем захисту інформації та проникнення до інформаційних систем; вплив на протоколи передавання даних, алгоритми адресації та маршрутизації
	Програмні закладки	За функціями	Троянські програми	Виконання несанкціонованих дій, таких як обхід контролю доступу; знищення, блокування, модифікація або копіювання даних; порушення штатного режиму функціонування системи
			Логічні бомби	Здійснення зловмисних дій, наприклад за умов збігу певних обставин або у визначений момент часу
			Логічні люки	Отримання привілейованої функції доступу до систем за рахунок помилок ПЗ
			Програмні пастки	Опосередкований вплив на функціонування системи через використання помилок програмного забезпечення
			Програмні черв'яки	Маскуються під системні засоби пошуку вільних інформаційних ресурсів

Закінчення табл. 2.1

Основні види НОКЗ за способом реалізації впливу на ІТС	**Засоби реалізації**	**Класифікаційні ознаки**	**Типи**	**Призначення, властивості та функціональні особливості**
Програмна	Програмні закладки	За метою створення	Дослідники	Виявлення уразливих місць в системах
			Перехоплювачі	Несанкціоноване вилучення та отримання даних
			Руйнівники	Спотворення та знищення кодів програм
			Активні завади	Порушення нормального режиму функціонування конкретної програми або операційної системи
		За способом доставляння до системи	Асоційовані з програмно-апаратним середовищем	Упровадження у BIOS та активізація при завантаженні системи
			Асоційовані з програмами первинного завантаження	Активізація при завантаженні активних розділів дискового простору (MasterBoot- та RecordBoot-секторів)
			Асоційовані із завантаженням ОС	Упровадження при завантаженні системи та ініціалізації драйверів
			Асоційовані з прикладним ПЗ	Вбудовані в програми тестування, утиліти та драйвери
			Модулі, що містять код закладки	Упровадження в завантажувальні пакетні файли типу *.bat
			Модулі-імітатори	Закладки, що маскуються під програмні засоби оптимізаційного призначення (архіватори, оптимізатори реєстру)
			Замасковані під програмні засоби	Закладки, що маскуються під програмні засоби ігрового та розважального призначення
Апаратна	Апаратні закладки, вбудовані у комплектуючі частини електронно-обчислювальної техніки та периферійного обладнання	Те саме	Те саме	Закладки, що маскуються під звичайні пристрої мікроелектроніки, призначені для збору, обробки та передавання інформації

• складності здійснення міжнародного контролю за розробкою та застосуванням (може бути надійно прихована від розвідок інших держав, різних міжнародних організацій, їхніх контролюючих органів);

2) заборону проведення ***інформаційних операцій*** — *сукупності узгоджених та взаємозв'язаних за метою, завданнями, місцем і часом інформаційних акцій, ударів та заходів, що проводяться як послідовно, так і одночасно за єдиним задумом та планом для забезпечення національних інтересів в одній обраній сфері життєдіяльності держави*, а також ***кібероперацій*** — *сукупності узгоджених за часом, глибиною і завданнями порівняно короткочасних кібератак, спрямованих на певну кількість об'єктів впливу протиборчої сторони з метою одержання несанкціонованого доступу до IP цих об'єктів, порушення роботи їхніх IT-систем і мереж або взагалі повного виведення обраних об'єктів із ладу* (основні методи проведення таких атак ілюструє табл. 2.2);

Таблиця 2.2

Характеристика кібератак, стратегічних та спеціальних кібероперацій

Рівень завдань	Основні методи проведення
Тактичний	♦ Ускладнення чи вибіркове призупинення діяльності телекомпаній, операторів стільникового зв'язку, інтернет-провайдерів, відомчих локальних обчислювальних мереж тощо. ♦ Тимчасове призупинення, дезорганізація чи ускладнення діяльності систем управління транспортом, енерго- й газопостачанням. ♦ Вибіркове призупинення та порушення діяльності систем управління об'єктами критичної інфраструктури. (включаючи банківську сферу) підприємств атомної, хімічної, нафтопереробної промисловості
Стратегічний	♦ Розкриття державних кодів та шифрів, перехоплення та дешифрування листування вищих посадових осіб держави. ♦ Несанкціонований доступ до державних баз даних, в яких обробляється інформація з обмеженим доступом, розкрадання, навмисне викривлення або знищення інформації в базах даних органів державної влади. ♦ Знищення баз даних операторів стільникового зв'язку, інтернет-провадерів, відомчих комп'ютерних мереж, систем централізованого управління енерго- і газопостачанням, зв'язком. ♦ Завдання програмної чи апаратної шкоди комп'ютерним системам на атомних електростанціях, підприємствах хімічної, нафто- і газопереробної галузей тощо
Спеціальний	♦ Несанкціонований доступ до систем управління стратегічною зброєю та імітація примусового запуску окремих елементів ракетної чи іншої зброї. ♦ Блокування систем управління військами, передавання у війська хибних наказів та директив. ♦ Дезорганізація космічного угруповання протиборчої сторони, ураження систем управління й орієнтації супутників різного призначення, переведення їх на нестабільні орбіти. ♦ Блокування запуску стратегічних ракет, зміна їхнього польотного завдання та навіть перенацілювання на інші об'єкти в суміжних країнах тощо

3) встановлення відповідальності протиборчих сторін за здійснення злочинів у ***інформаційній сфері,*** яка являє собою *сукупність суб'єктів, котрі беруть участь в інформаційній взаємодії, та інформації, призначеної для використання цими суб'єктами, а також технологій, що забезпечують зазначену взаємодію, уможливлюючи обробку, зберігання та обмін інформацією між суб'єктами* (рис. 2.6).

Рис. 2.6. Структура інформаційної сфери

На ситуацію в інформаційній сфері дедалі більше впливають ще й такі чинникі:

• формування окремими державами власних доктрин і стратегій наступальних і підривних дій в інформаційному та кібернетичному просторах;

• створення та застосування спеціальних сил і засобів негативного впливу на критично важливу інформаційну та кібернетичну інфраструктуру;

• проникнення ІТ-технологій в усі сфери державного й громадського життя, побудова на їхній основі систем державного та військового управління;

• розвиток державних проектів і програм у сфері інформатизації (електронний документообіг, міжвідомча електронна взаємодія, універсальні електронні карти), спрямованих на формування інформаційного суспільства.

З огляду на сказане забезпечення інформаційного суверенітету будь-якої держави світу, зокрема й України (згідно із Законами України «Про основи національної безпеки України» та «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки»), можливе лише за умови розгортання ***власних систем кібернетичної безпеки*** [9] з одночасним підвищенням рівня координації діяльності державних органів щодо виявлення, оцінювання та прогнозування загроз інфосфері, запобігання таким загрозам і забезпечення ліквідації їх наслідків, а також здійснення міжнародного співробітництва з цих питань.

Конкретні кроки в напрямку розв'язання цих завдань мають здійснюватись поетапно (рис. 2.7).

У процесі формування державної системи кібербезпеки необхідно:

по-перше, удосконалювати методи, засоби та способи отримання суспільно значущої інформації з відкритих, відносно відкритих і закритих електронних джерел; оцінювати рівень захищеності власних ІТ-систем і мереж від впливу внутрішніх і зовнішніх кібернетичних втручань і загроз;

по-друге, формувати власні системи захисту національної інфосфери від стороннього кібервпливу та вдосконалювати чинну нормативно-правову базу;

по-третє, забезпечувати автоматизацію процесів пошуку й збору інформації (ІРМ, відомостей, даних і знань) із відкритих і відносно відкритих джерел та її добування із закритих електронних джерел, а також нагромадження й оброблення такої інформації в поєднанні з обміном нею.

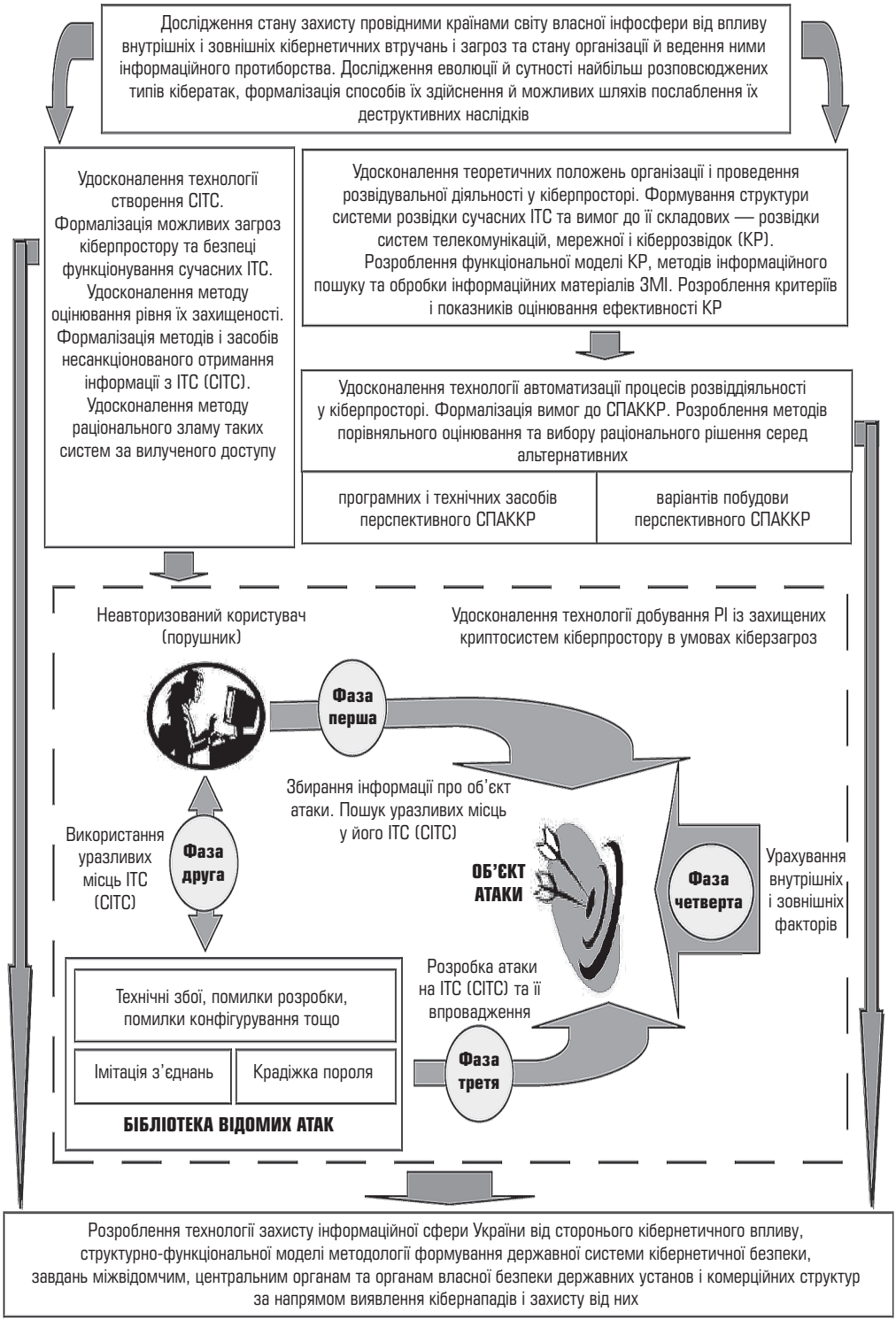


Рис. 2.7. Методологія формування державної системи кібернетичної безпеки

Світовий досвід щодо побудови ІТС та їхніх підсистем показує, що ключовим елементом тут виступають моделі ***системи захисту інформації*** (рис. 2.8), а математичним забезпеченням — моделі процесів кібернападу (КбН) і кіберзахисту (КбЗ) від стороннього кібервпливу (рис. 2.9).

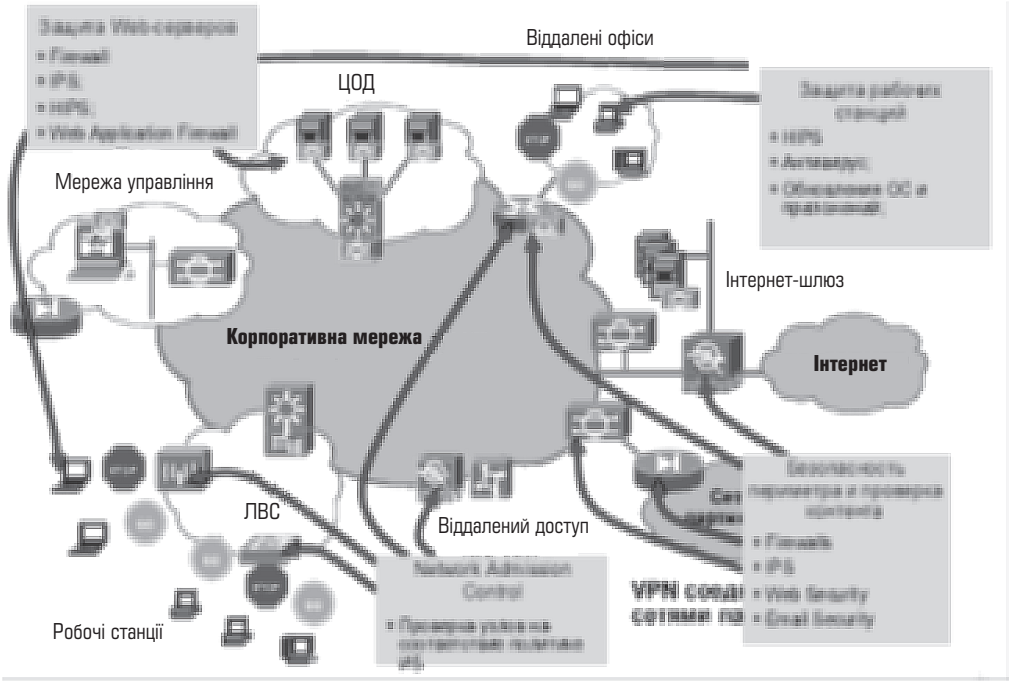


Рис. 2.8. Модель системи захисту інформації в ІТС

Згідно з відомими публікаціями зарубіжних науковців [57], ідеться про моделі:

- дискреційного доступу (п'ятивимірна модель Хартсона, модель на основі матриці доступу, модель Харисона—Рузо—Ульмана (модель HRU), модель типізованої матриці доступу (модель TAM), теоретико-графову модель TAKE-GRANT);
- мандатного доступу (модель Белла—Лападули, модель Low-WaterMark);
- тематичного доступу (модель на основі тематичної решітки, модель тематико-ієрархічного розмежування доступу);
- рольового доступу (модель MMS Лендвера і Мак- Ліна);
- автоматні та теоретико-ймовірнісні (модель Гогена—Месигера (GM-модель));
- захисту від загроз відмов в обслуговуванні (модель розподілення ресурсів Мілена (MPP));
- контролю цілісності (модель Біба, модель Кларка—Вілсона).

Для побудови зазначених моделей використовується математичний інструментарій [1; 57], в основу якого покладено *теоретичний*, *емпіричний* та *теоретико-емпіричний* підходи.

Теоретичний підхід ґрунтується передусім на методах теорії підтримання та ухвалення рішень, теорії графів, теорії ймовірностей, теорії мереж Петрі та напівмарковських процесів. Моделі КбН і КбЗ, розроблені на зазна-

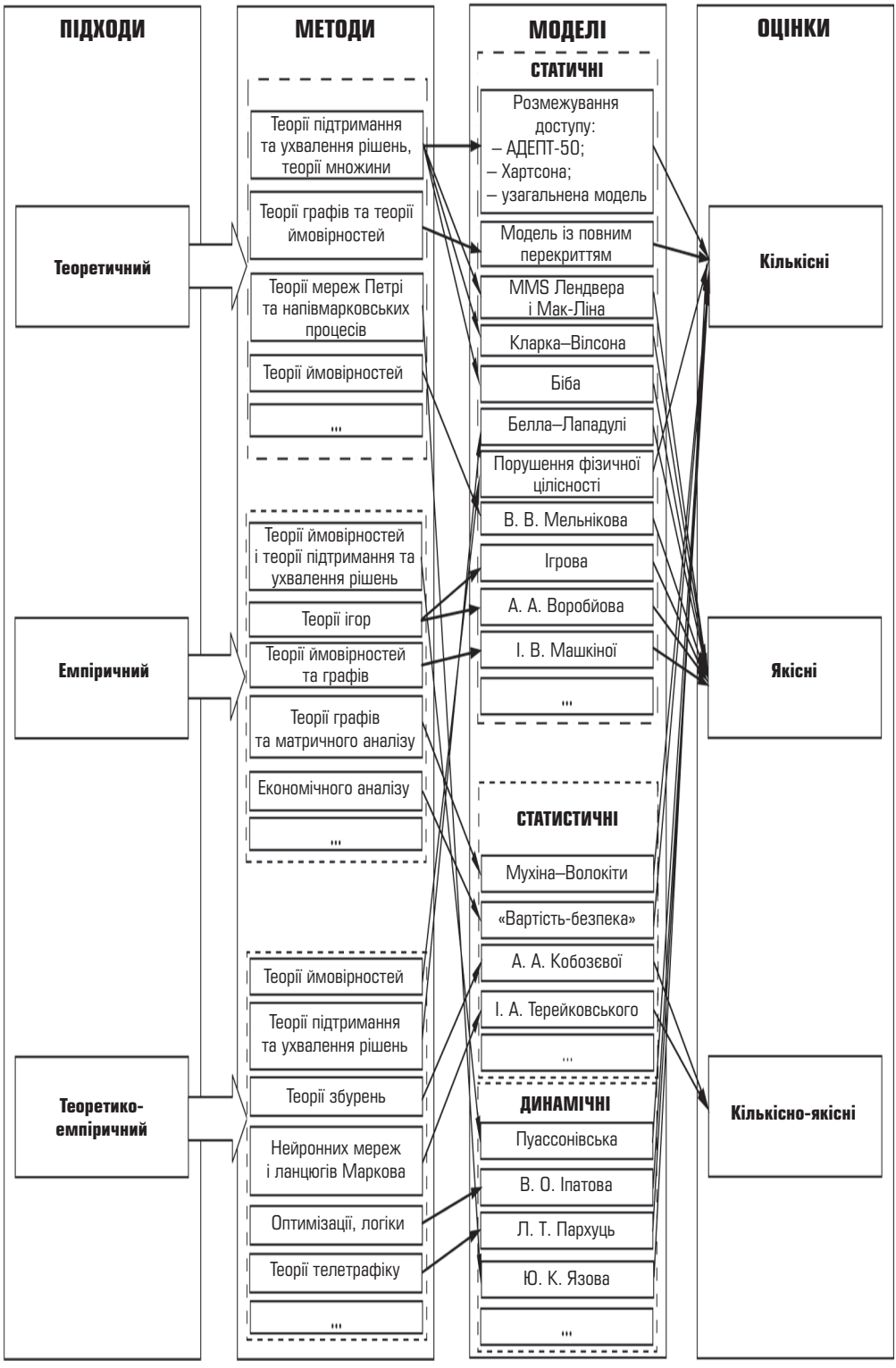


Рис. 2.9. Методи та моделі процесів кібернападу і кіберзахисту

ченій базі, *дають змогу отримати передусім якісні оцінки* рівня захищеності (РЗ). Науково-методичний базис ***емпіричного підходу*** становлять методи теорії ймовірностей, теорії підтримання та ухвалення рішень, теорії ігор, мереж Петрі, теорії графів та матричного аналізу, економічного аналізу тощо. Статичні, стохастичні та динамічні моделі, розроблені на основі емпіричного підходу, *дозволяють отримувати як суто якісні, так і суто кількісні показники оцінювання РЗ*. Синтез теоретичного та емпіричного підходів — ***теоретико-імпіричний підхід*** спирається на групу відповідних математичних методів. Особливість цього підходу полягає у використанні найширшого математичного інструментарію: методів теорії збурень, нейронних мереж та ланцюгів Маркова, методів теорії логіки та оптимізації, теорії трафіку тощо. При цьому побудовані моделі, на базі теоретико-емпіричного підходу, *дозволяють отримувати не лише кількісні, а й кількісно-якісні оцінки РЗ*.

Особливої уваги, а іноді й докорінних змін при підготовці та проведенні інформаційних і кібернетичних воєн сучасності й найближчого майбутнього потребують погляди на ***систему розвідувального забезпечення*** всіх супровідних заходів. Передусім це зумовлюється появою нових комунікаційних можливостей та постійно зростаючим інформаційним ресурсом, що зрештою призводить до примноження потенційно придатних джерел для такого прогресивного виду розвідки, як ***розвідка ІТ-систем*** (рис. 2.10). Зазначена розвідка включає в себе *комплекс заходів, спрямованих на систематичний і цілеспрямований пошук, збір та добування з автоматизованих ІТС (СІТС), комп'ютерних мереж і систем зв'язку цивільного і/або військового призначення інформації щодо протиборчої сторони (конкурента), вивчення й обробку цієї інформації, а також формування на її базі уявлення про реальні і/або потенційні джерела стороннього кібернетичного впливу* [1; 58; 59].

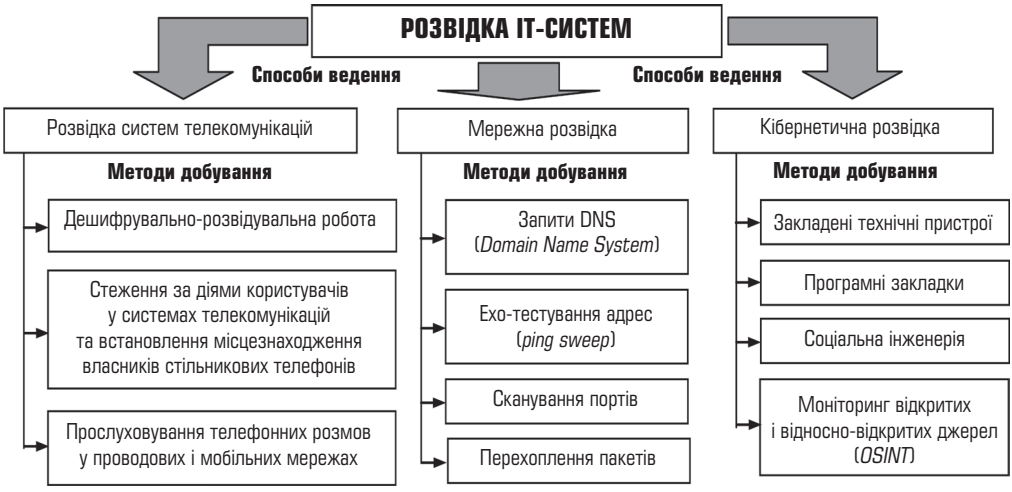


Рис. 2.10. Способи та методи ведення розвідки ІТ-систем

Розвідка ІТС відрізняється від інших видів розвідувальної діяльності механізмами (способами), а також силами й засобами, використовуваними насамперед з метою добування розвідувальної інформації (РІ). У цьому контексті під ***силами розвідки*** слід розуміти підрозділи (особовий склад), задіяні в процесі добування, аналітичної обробки та зберігання інформації, а під ***засобами***

розвідки — спеціальну техніку (у тому числі й бойову), пристрої, спорядження, тобто все те, за допомогою чого особовий склад виконує завдання розвідки ІТС. Поняття РІ включає в себе інформаційні й розвідувальні матеріали й відомості, що надійшли від засобів різних видів розвідки або з будь-яких відкритих, відносно відкритих і закритих джерел.

Зауважимо, що ***відносно відкритими*** називають електронні ресурси, які вимагають реєстрації для подальшої роботи в них (форуми, більшість мережних сервісів тощо) або осіб, котрі спілкуються за допомогою соціальних мереж, чатів, засобів швидкого обміну повідомленнями або електронною поштою, а ***відкритими*** — ресурси, які можна отримати офіційним шляхом без залучення органів добування та без жодних порушень норм міжнародного права і національного законодавства.

До відкритих належать, як правило, такі ресурси:

• *засоби комунікації* — інформаційні агентства, друковані ЗМІ (газети, журнали тощо), аудіовізуальні ЗМІ (радіо, телебачення), електронні ЗМІ, інформаційні ресурси мережі Інтернет;

• *суспільна інформація* — урядові повідомлення, фінансові плани, демографічні дані, законотворчі акти, матеріали прес-конференцій, промови, презентації, результати опитувань;

• *наукові та професійні дані* — академічні дослідження, НДДКР, матеріали наукових конференцій, семінарів та круглих столів, наукові публікації;

• *геоінформаційні матеріали* — карти, атласи, географічні відомості щодо визначених об'єктів;

• *електронні on-line системи для масового споживача* (*consumer on-line market*), інформаційні системи, реалізовані у вигляді інтернет-сервера (наприклад, інформаційна служба *Business Intelligence and Data Warehouse*), *професійні бази даних*.

Розглянемо головні способи ведення розвідки ІТС.

Розвідка систем телекомунікацій — *комплекс заходів, спрямованих на систематичний та цілеспрямований пошук і добування інформації про об'єкти розвідки із систем передавання, випромінювання і/або приймання знаків, сигналів, письмового тексту, зображень, звуків і повідомлень будь-якого роду, а також на їх подальше вивчення та обробку.*

Мережна розвідка — *комплекс заходів, спрямованих на систематичний та цілеспрямований пошук і добування інформації про ІТС об'єкта розвідки, їхні ресурси, засоби захисту, пристрої та ПЗ, що в них використовується, уразливі місця та межі проникнення, а також на подальше вивчення цих даних та їх обробку.*

Кібернетична розвідка — *комплекс заходів, спрямованих на систематичний та цілеспрямований пошук і добування інформації про об'єкти розвідки за допомогою засобів ЕОТ і ПЗ із ресурсів ІТС з їх подальшим нагромадженням, верифікацією та аналітичною обробкою, а також на оцінювання згідно з отриманою інформацією можливих загроз (ризиків) власному кіберпростору, виявлення ознак цих загроз та прогнозування їх можливого прояву, зокрема планування та здійснення при потребі впливу на кіберпростір ворогуючої сторони.*

Зазначені види розвідувальної діяльності характеризуються різним рівнем можливостей щодо розвідки кібервтручань і кіберзагроз, використовуючи той чи інший набір способів і методів.

Наприклад, розвідувальні органи більшості країн світу використовують у своїй повсякденній діяльності здебільшого:

• методи ***дешифрувально-розвідувальної роботи (ДРР)*** та ***соціальної інженерії (СІ)*** — *комплекс заходів, спрямованих на одержання неавторизованим користувачем НСД до інформації про призначення, структуру, установлені права доступу, систему захисту, реєстраційні імена й паролі, а також до іншої конфіденційної інформації про об'єкт атаки (особу чи групу осіб) завдяки слабкості, некомпетентності, непрофесіоналізму або недбалості цього об'єкта та керованості з боку зовнішніх впливів;*

• методи ***моніторингу відкритих і відносно-відкритих джерел (МВВВД)*** — *процес постійного збору із зазначених джерел широкого спектра інформації про одне й те саме явище, подію чи об'єкт розвідки, супроводжений її обробкою та приведенням у структуровану й логічно обґрунтовану систему просторово-часових, причинно-наслідкових та інших залежностей, необхідних для підготовки оперативних і виважених рішень за визначеною тематикою*, що притаманні відповідно розвідці систем телекомунікацій та кібернетичній розвідці.

Серед згаданих методів особливої ваги набувають методи *соціальної інженерії*, або ***соціального інжинірингу (СІ)***. Їх застосування завдяки домінуванню людського чинника в умовах стрімкого розвитку мережі Інтернет дає змогу чинити опір таким відомим технологіям безпеки, як міжмережні екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережних атак тощо.

Останнім часом фахівці в усьому світі впроваджують ці методи самостійно, без застосування технічних засобів [60], а також використовують їх як інструмент під час планування та проведення інших видів атак на об'єкт розвідки.

Як показує практика, методи ДРР, СІ та МВВВД забезпечують несуперечливі результати, які, за висновками експертів, здебільшого доповнюють один одного. На підтвердження згадаємо досвід діяльності структурних підрозділів спецпризначення, зокрема відповідних навчань і тренувань, що, за оцінками вітчизняних і західних фахівців, дозволяє стверджувати: сьогодні такими, наприклад, силами й засобами, як ДРР, вдається добувати про об'єкти розвідки від 5 до 8% інформації (матеріалів, відомостей, даних та знань). Натомість методи МВВВД і СІ забезпечують отримання від 35 до 95% розвідувальних даних, що нерідко становлять найвищу державну таємницю.

Що ж до інших методів розвідки ІТС, то їх світова розвідувальна спільнота розглядає як надзвичайно ризиковані. Адже вони передбачають цифрове проникнення в мережі й комп'ютери, які перебувають на балансі інших держав, корпорацій чи приватного сектору, а отже, і взаємодію з певними організаційними структурами та механізмами збору РІ. Легітимність застосування цих методів може бути визначена лише після фахового аналізу правових, технічних, організаційно-штатних та інших особливостей кожного з них на предмет відповідності чинному вітчизняному законодавству та, особливо, міждержавним угодам.

Зауважимо, що функціонування високотехнологічних галузей промисловості, Збройних сил загалом, і, зокрема, сил та засобів розвідки характеризується на сучасному етапі розвитку інформаційного суспільства постійним зростанням обсягів інформації, яка циркулює в мережі Інтернет, жорстким дефіцитом часу на її пошук, збір, добування, первинну обробку,

нагромадження, систематизацію за певними класифікаційними ознаками з подальшим аналізом, синтезом, узагальненням і доведенням до споживачів. Особливо виразно критичність часового чинника постає тоді, коли йдеться про перетворення інформації в синтезовані пропозиції для розроблення та ухвалення тих чи інших рішень. Саме тому набуває дедалі більшої ваги завдання щодо ***автоматизації всіх етапів зазначених процесів*** [61–63]. Це, у свою чергу, потребує впровадження в діяльність державних структур сучасної системи інформаційного забезпечення, що має задовольняти низку вимог стосовно:

- якості (стислості і чіткості формулювань, своєчасності надходження);
- цілеспрямованості (задоволення конкретних потреб);
- точності та вірогідності (правильного добору початкових матеріалів і відомостей, безперервності їх збору, нагромадження та оброблення, оптимальності систематизації інформації, а також її доведення до споживача/передавання).

У підрозділах спеціального призначення (ПСП) України, що являють собою комплекси з великою кількістю повсякденно пов'язаних між собою структурних одиниць, саме точність і вірогідність інформаційного забезпечення виступають головними чинниками їх надійного й ефективного функціонування. Високий рівень інформаційного забезпечення можливий, у свою чергу, лише з упровадженням сучасної ЕОТ і новітніх ІТ-технологій у всі процеси діяльності таких структур, із неодмінним оснащенням їх сучасними програмними та програмно-апаратними засобами. Один із можливих підходів до розв'язання цього завдання полягає у створенні та розгортанні за певними напрямками підпорядкування ***уніфікованих спеціальних програмно-апаратних комплексів розвідки, передусім кіберрозвідки*** (***СПАКР***), що мають відповідати вимогам до систем підтримки ухвалення рішень, включаючи в себе систему організаційно-технічних засобів і заходів, призначених для забезпечення автоматизації процесів розвіддіяльності в кіберпросторі, зокрема математично-аналітичного розв'язання нагальних управлінських завдань. Зазначені комплекси сприяють мінімізації витрат часу, необхідного для роботи з інформаційними та розвідувальними даними й документами, а також для оцінювання на їх підставі можливих загроз власному кіберпростору, виявлення відповідних ознак і прогнозування подальшого перебігу подій, із надійним захистом власних масивів розвідувальної інформації та процесів інформаційного обміну між підсистемами й компонентами СПАККР зі здійсненням, при потребі, кібернетичних атак (нападів) на кіберпростір протилежної сторони.

Із функціонального погляду перспективний СПАККР — це система, що має такі характерні ознаки:

а) вона складається з низки взаємозалежних підсистем і їхніх компонентів, зорієнтованих на розв'язання певного комплексу завдань (рис. 2.11);

б) створюється на базі розширюваної мережі клієнт-серверної архітектури з використанням професійної термінальної клієнтської частини;

в) оснащується сучасними програмними й технічними засобами.

При цьому ***головними підсистемами*** СПАККР мають бути підсистеми добування інформації з відкритих і відносно відкритих джерел, інформаційно-аналітичної роботи, планування та управління силами й засобами, комплексного захисту інформації в системі, тобто ***функціональні підсистеми*** основного призначення, а також ***підсистеми обслуговування***, одним з елементів

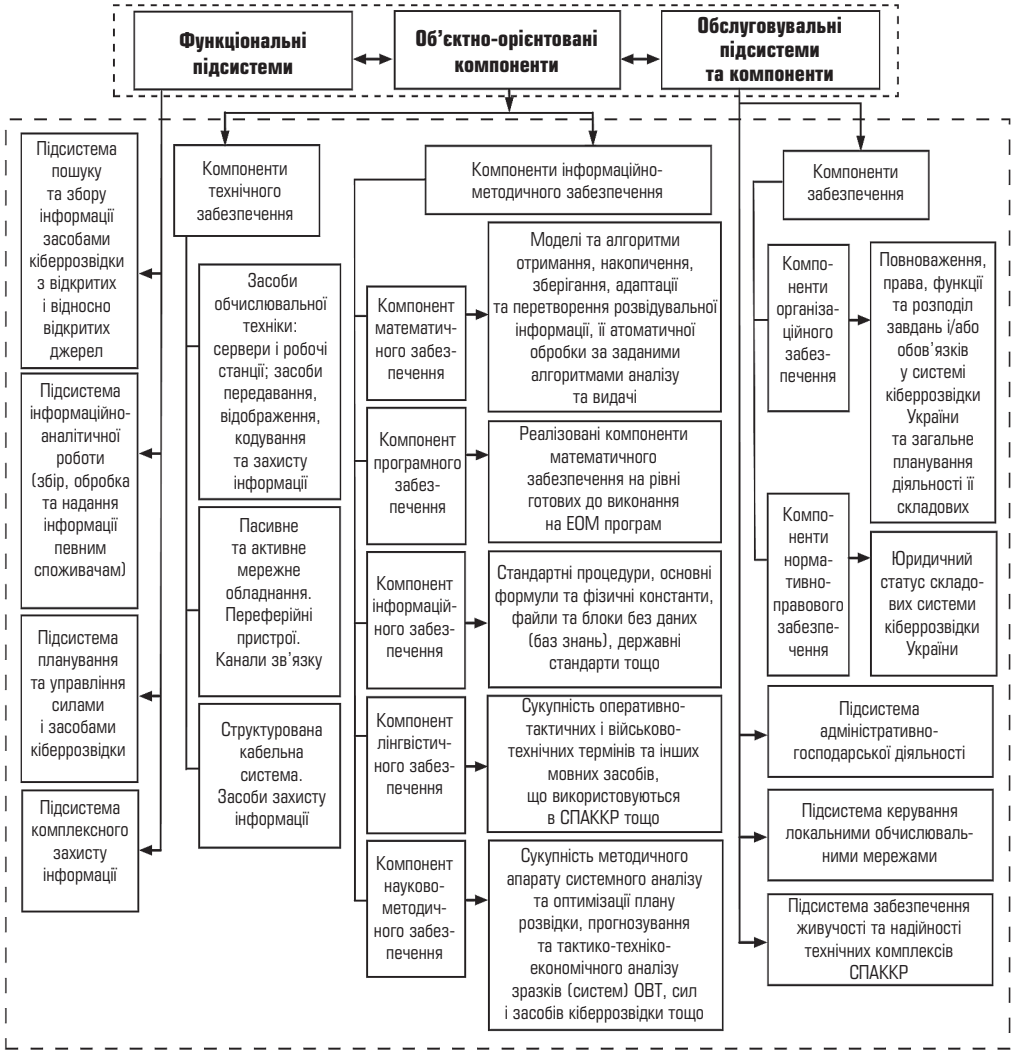


Рис. 2.11. Взаємозв'язок підсистем та компонентів перспективного СПККР

яких має бути, наприклад, блок системного адміністрування (забезпечує вибірковий доступ користувачів до інформації та БД, а також дієздатність СПЗ і ЗПЗ АРМ комплексу).

Варто наголосити, що серед дієвих засобів профілактики, протидії та боротьби з найрізноманітнішими кібернетичними втручаннями й загрозами незаперечну перевагу має розвідка ІТ-систем. Значного підвищення її результативності вдається досягати активізацією зусиль, срямованих на здійснення *розвідки систем телекомунікацій* (*РСТ*), *мережної розвідки* (*МР*) і *кіберрозвідки* (*КР*). Саме КР завдяки раціональному поєднанню чотирьох основних процедур — пошуку, збору, обробки та подання інформації в інтересах певних сил — слід розглядати як головний, найбільш потужний спосіб ведення розвідувальної діяльності у відкритих і відносно відкритих електронних джерелах. Коли ж ідеться про добування інформації із закритих електронних дже-

рел (використання уразливостей у тих чи інших криптографічних алгоритмах і/або протоколах, застосування сучасних криптографічних методів захисту інформації та проведення криптоаналітичних атак) тільки РСТ може забезпечити очікувані результати.

Як уже зазначалося, здійснення розвідувальної діяльності на сучасному етапі розвитку ІКТ та ІТС неможливе без автоматизації заходів із пошуку, збору і/або добування інформації про об'єкт розвідки, її подальшої обробки, аналізу і синтезу. Такій автоматизації сприяє і надалі сприятиме створення згідно з певними напрямками підпорядкування спеціальних програмно-апаратних комплексів, таких, скажімо, як СПАККР. Загалом підвищення продуктивності, відмовостійкості, сумісності, розширюваності, масштабованості та ефективності існуючих і перспективних систем обробки даних, а також їх інформаційної та кібербезпеки неможливе без розгортання спеціальних ІТ-систем.

2.2. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки

В епоху глобальної інтенсифікації інформаційних процесів і їх проникнення в усі сфери (соціальну, політичну, економічну) діяльності людини, коли практично кожній людині доводиться виконувати різні завдання, взаємодіючи з численними елементами ІТ-інфраструктури, залежність кожного індивіда від інформаційних систем і мереж та його уразливість щодо стороннього кібернетичного впливу постійно зростають. Зрештою травмується психіка людини, а це, у свою чергу, може спонукати її до розголошення інформації з обмеженим доступом (ІзОД). Саме тому соціальні інженери в пошуках об'єктів своїх атак беруть до уваги передусім психологічний стан причетних до них осіб. У сучасних організаціях (установах, компаніях) потенційними жертвами таких зловмисників можуть бути адміністратори, начальники, користувачі та навіть більш чи менш знайомі будь-кого зі згаданих категорій осіб. Вони можуть мати різні права досту до ІР або не мати жодних таких прав. Особистісно-професійні характеристики осіб, що приваблюють атакувальників і можуть стати джерелом витоку ІзОД, якою вони володіють, а також можливі дії соціальних інженерів ілюструє рис. 2.12.

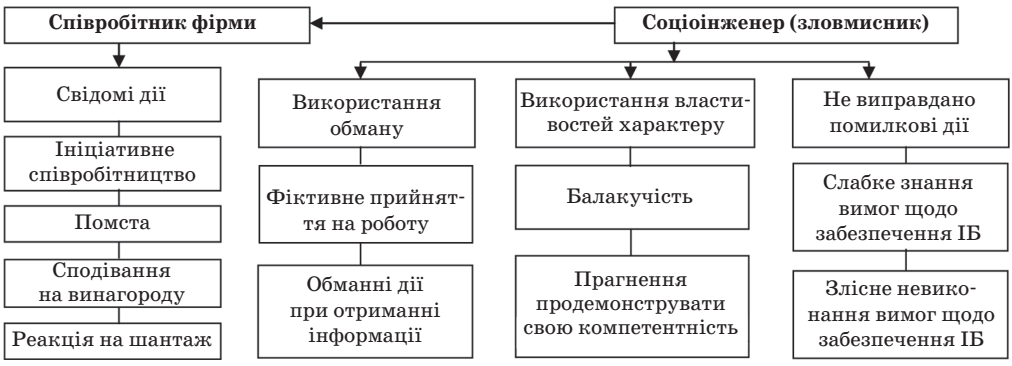


Рис. 2.12. Особистісно-професійні характеристики причетних до ІзОД осіб та дії зловмисників, що сприяють реалізації загроз інформаційній і кібернетичній безпеці

Проілюструємо ступінь (із трьох можливих: *1* — низький; *2* — середній; *3* — високий) отримання доступу соціального інженера з рівнем підготовки *новачок*, *аматор* і *професіонал* до різних засобів застосування, на різних рівнях взаємовідносин та до різних категорій персоналу організації (табл. 2.3). При цьому дії такої особи ґрунтуються передусім на особливостях аргументації (так званих когнітивних упередженнях), згідно з якою людина ухвалює те чи інше рішення.

Зауважимо, що всі засоби впливу на людину, до яких вдається зловмисник — соціальний інженер, передбачають введення цієї людини в оману, аби змусити її вчинити певну дію, необхідну зловмисникові.

Таблиця 2.3

Імовірність отримання несанкціонованого доступу різних рівнів до ІзОД через персонал наявних категорій

Клас атаки	Підготовленість зловмисника		
	Новачок	Аматор	Професіонал
Засоби застосування			
Телефон	*3*	*3*	*3*
Електронна пошта	*2*	*3*	*3*
Звичайна пошта	*1*	*3*	*3*
Розмова в інтернеті	*3*	*3*	*3*
Особиста зустріч	*1*	*2*	*3*
Рівень спілкування (відносини)			
Офіційний	*2*	*3*	*3*
Товариський	*3*	*3*	*3*
Дружній	*1*	*2*	*3*
Ступінь доступу			
Адміністратор	*1*	*2*	*3*
Начальник	*1*	*2*	*3*
Користувач	*3*	*3*	*3*
Знайомий	*2*	*3*	*3*

Для досягнення поставленої мети зловмисник використовує ту чи іншу тактику, наприклад:

- видає себе за іншу особу;
- відвертає увагу потенційної жертви;
- нагнітає психологічну напругу тощо.

При цьому зловмисник, послуговуючись відомостями про симпатії жертви, її страхи, реактивність і довіру вводить у дію ще й психологічні важелі:

- входження в певну роль (соціальний інженер звичайно демонструє кілька характерних ознак тієї ролі, яку він на себе взяв);
- примушення жертви відігравати певну роль (соціальний інженер часто змушує свою мішень виконувати незвичну роль, наприклад поводитися надто агресивно або, навпаки, співчутливо);
- збивання жертви з думки (соціальні інженери намагаються вступити в контакт із мішенями, коли ті перебувають у роздумах, аби нав'язати їм власну програму дій);

• досягнення із жертвою моменту згоди (соціальні інженери створюють таку ситуацію поетапно, роблячи цілу серію запитів, що позитивно налаштовують жертву);

• формування в жертви бажання допомогти (люди відчувають позитивні емоції, коли допомагають іншим).

Незважаючи на те, що співробітники фірми (організації, установи) можуть стати джерелом загрози, її керівництво часто відмовляється це визнавати. Існує кілька пояснень такого поводження:

• довіра керівництва до співробітників, що спирається на особисті симпатії;

• упевненість керівництва в порядності і відданості співробітників;

• упевненість керівництва в силі впливу корпоративної етики.

А проте факти розголошення ІзОД мають місце практично в кожній фірмі (організації, установі). Причини можуть бути такі:

• прагнення людини до самоствердження, популярності й слави;

• невідповідність адміністративних заходів із покарання за розголошення ІзОД збитку, що його завдає така дія;

• випадкове розголошення ІзОД у бесідах з іншими особами чи спілкуванні із засобами масової інформації;

• прагнення співробітників до фінансової вигоди;

• відсутність служби безпеки компанії;

• безконтрольне використання інформаційних і копіювальних засобів на фірмі, установлення недозволеного програмного забезпечення;

• психологічні конфлікти між співробітниками, а також між співробітниками й керівництвом.

На мотивацію людини щодо розголошення ІзОД можуть впливати також і певні надзвичайні ситуації (НС) соціального характеру (рис. 2.13)

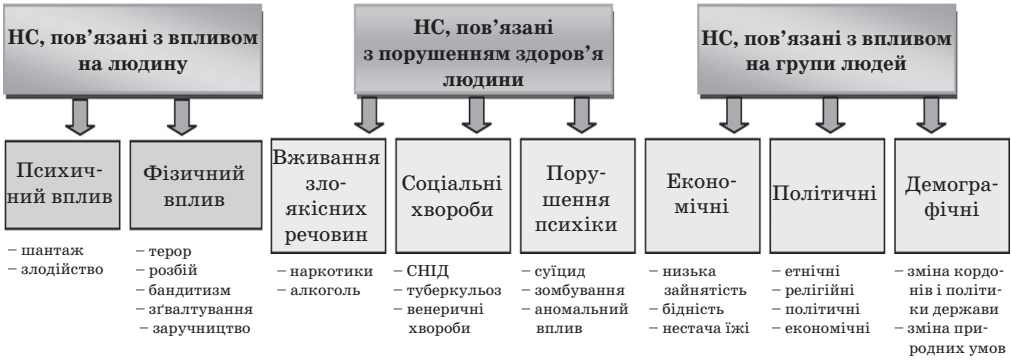


Рис. 2.13. Надзвичайні ситуації соціального характеру

Що ж до лояльності співробітників, то на неї можуть впливати такі чинники [64]:

1) матеріальна винагорода;

2) цікава робота;

3) кар'єрні перспективи;

4) перспективи професійного зростання;

5) репутація компанії;

6) психологічна атмосфера в колективі;

7) умови роботи;

8) корпоративна культура;

9) особистість начальника;

10) поводження начальника.

Із наведеного переліку мотиваційних чинників на перші місця претендують такі, як заробітна плата, цікава робота, кар'єрні перспективи, перспективи професійного зростання, репутація компанії. Варто згадати, що заробітна плата посідає високе друге місце у п'ятиступеневій ієрархічній градації мотивацій американського соціолога А. Маслоу [65–66], поступаючись лише чинникам біологічного виживання людини (повітря, питво, іжа, світло). Доволі високе (шосте) місце психологічного клімату в колективі, образно кажучи, завершує перелік головних мотиваційних механізмів. Саме простір між першою і шостою незадоволеними мотиваціями дає поживу для негативного прояву людського фактора: нелояльності й зрадництва інтересів фірми (організації, установи).

Отже, схоронність ІзОД на 80% залежить від правильного добору, розміщення та виховання кадрів, персоналу, відданого фірмі (організації, установі) [67–68]. Єдино правильний шлях, який дозволить запобігти розголошенню ІзОД,— це ретельний добір персоналу з неодмінним обмеженням його доступу до такої інформації. Для цього керівництво фірми (організації, установи) має виробити певний алгоритм прийняття на роботу, що включає в себе такі кроки:

1) аналіз робочого місця (оцінювання наявних інформаційних, фінансових і людських ресурсів; складання портрета ідеального співробітника, характеристики якого повністю відповідають вимогам даного робочого місця; визначення майбутніх перспектив компанії та формування програми їх реалізації);

2) добір майбутніх співробітників за критеріями освіти, комунікабельності, досвіду, уміння ухвалювати рішення в екстремальних ситуаціях тощо;

3) проведення попередньої бесіди з добору кадрів та заповнення бланка заяви;

4) перевірка рекомендацій і зобов'язань перед іншими фірмами;

5) ухвалення остаточного рішення.

Надалі керівництво фірми (організації, установи) має унеможливлювати розголос ІзОД за рахунок:

• підписання угоди про нерозголошення ІзОД при прийнятті співробітника на роботу (психологічно це діє дуже добре: більшість людей не схильні порушувати підписані домовленості);

• відстеження взаємин у колективі, із виявленням незадоволених і скривджених співробітників, які можуть здійснити розголошення ІзОД із принципових міркувань;

• застосування системи відеоспостереження;

• формування ради із забезпеченням безпеки, до складу якої мають входити представники кожного відділу;

• матеріального стимулювання співробітників, що працюють із ІзОД;

• проведення заходів, що підвищують лояльність співробітників;

• доведення до відома громадськості всіх фактів розголошення ІзОД співробітниками як усередині фірми (організації, установи), так і на зовнішньому ринку;

• проведення комплексної перевірки співробітника, що звільняється. Пропонування йому не залишати фірму (організацію, установу), обійнявши посаду консультанта або ставши одним з акціонерів.

Водночас керівництво фірми (організації, установи), не обмежуючись зазначеними діями, має вживати реальних заходів із захисту ІзОД: забезпечувати умови захисту й безпеки; здійснювати планування дій, спрямованих на забезпечення безпеки; розв'язувати питаня із забезпечення безпеки, не чекаючи того моменту, коли щось небажане станется. Неуважність керівництва до потреб підлеглих, до міжособистісних конфліктів може призвести до розголосу ІзОД. Аби уникнити таких дій, керівництво має дбати про підвищення продуктивності праці та прибутків, помітне поліпшення життєвого рівня співробітників, створення позитивного психологічного клімату в колективі, формування у співробітників почуття причетності до спільної справи, а також про мінімізацію плинності кадрів і негативних проявів людського фактора в системі забезпечення комплексної безпеки.

2.3. Соціальні мережі: особливості, основні поняття та визначення. Моніторинг соціальних мереж — цілі та способи реалізації

Останнім часом мережа Інтернет перетворилась на справжню зброю в руках незадоволених споживачів і співробітників, за допомогою якої вони успішно атакують фірми (організації, утанови), їхню продукцію та керівництво. Розміщення в мережі негативної інформації може здійснюватися в різний спосіб:

1) створенням спеціалізованих сайтів (*consumer opinion sites*), де споживачі висловлюють невдоволення щодо певного виду продукції або послуг;

2) поширенням «електронних пліток» й іншої невірогідної інформації;

3) створенням різних груп у соціальних мережах, блогах, форумах.

Під ***соціальною мережею*** в цьому сенсі розуміють *множину дійових осіб (акторів) (точок, вершин, агентів — індивідів і організацій), які можуть взаємодіяти один з одним*. Така мережа, являючи собою результат розвитку інформаційних технологій, становить частину соціальної структури суспільства. Водночас соціальна мережа як цікавий соціотехнічний об'єкт відбиває наявні зв'язки між дійовими особами (різноманітні соціальні контакти) в термінах вузлів і сполучних ланок, починаючи з випадкових знайомств і закінчуючи тісними родинними узами. Вузли отожнюються з акторами в мережах, а зв'язки відповідають стосункам між акторами.

Виокремлимо три важливі види соцмереж (рис. 2.14) [69]:

1) *комерційні*, орієнтовані на дохід;

2) *мережі практиків*, орієнтовані на навчання;

3) *«нова парадигма»*, орієнтовані на соціально-значущі проекти.

Рис. 2.14. Процес розвитку соцмереж

З формального погляду соціальні мережі зручно подавати графоаналітичними моделями виду $G(N, E)$ (рис. 2.15) [70], застосовуючи для їх подальшого аналізу розвинені ймовірнісно-реляційні та реляційно-алгебраїчні моделі. Наприклад, у наведеному на рис. 2.15 графі $G(N, E)$ маємо скінчену множину $N = \overline{1,n}$ вершин, роль яких відіграють програмно-технічні пристрої H (хости) та користувачі інформаційної системи A (агенти); E — множина ребер, що відбивають взаємодію кожного агента A з хостом H та зв'язки між пристроями й між користувачами.

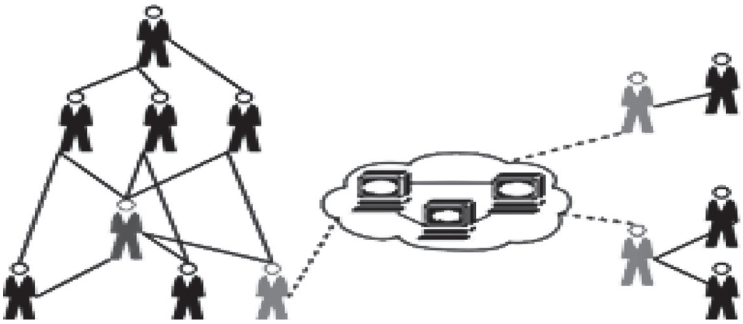


Рис. 2.15. Приклад відображення схеми зв'язків у соціальних мережах

На поводження агентів можуть впливати такі чинники (рис. 2.16):

• індивідуальний — внутрішня схильність (перевага) агента щодо вибору тієї чи іншої дії за відсутності будь-якого зовнішнього впливу;

• соціальний — обумовлений взаємодією (взаємовпливом) з іншими агентами;

• адміністративний — результат впливу на актора з боку керівного органу (центру).

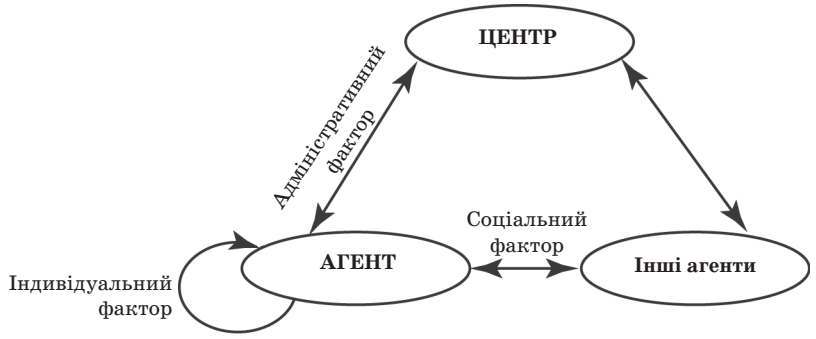
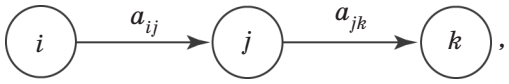


Рис. 2.16. Фактори, що впливають на актора у соцмережі

Агенти, які зазнають впливу описаних факторів, називаються *залежними* (від одного чи кількох факторів). Агенти, які не перебувають під впливом перелічених щойно факторів, називаються *незалежними*. Наприклад, агент, виділений згущеним тоном на (рис. 2.15), має найбільше зв'язків усередині своєї соціальної мережі, тобто виступає як лідер або керівник групи (організації). Агенти, позначені світлим тоном, мають зв'язки з іншими

соціальними групами і можуть відігравати роль передавачів інформації між мережами. Їхній вплив один на одного можна зобразити в такий спосіб:



де k-й користувач побічно впливає на i-го (хоча i-й може навіть не здогадуватись про існування k-го).

Моделям користувачів ІС, асоційованим із вершинами графа, наведеного на рис. 2.15, можна поставити у відповідність такі атрибути (позначки) [71; 72]:

- множину пристроїв, до яких у даного користувача є доступ, зокрема й до конфіденційної інформації, що зберігається на цих пристроях;
- права доступу користувача до конфіденційної інформації;
- посаду користувача;
- права доступу користувача до контрольованих зон;
- профіль уразливостей користувача, що включає в себе рівень їх вираженості.

Із моделями хостів (програмно-технічних пристроїв) ІС, асоційованих із вершинами описаного графа (див. рис. 2.15), можна зіставити такі атрибути (позначки):

- критичні документи, що зберігаються на пристроях;
- програмно-технічні характеристики пристроїв;
- місцезнаходження хостів відносно контрольованих зон інформаційної системи.

Реляційно-алгебраїчна модель на додачу до результатів, отриманих на базі графо-аналітичної моделі, дозволяє аналізувати захищеність користувачів ІС від соціотехнічних атак. Ця модель включає в себе такі елементи: I — критичну інформацію, що циркулює в системі; H — хости, що характеризуються програмно-технічним наповненням і зв'язками; A — користувачів, що характеризуються відповідним профілем уразливості; U — атакувальні дії зловмисників; R — ресурси зловмисників. У зазначеній моделі оцінюванню можуть підлягати декартові добутки виду $U \times A$, $H \times A$ і $A \times I$, на яких задано відношення та ймовірнісні оцінки переходів.

Імовірнісно-реляційна модель, на відміну від реляційно-алгебраїчної, враховує стохастичний характер успішності соціоінженерного атакувального впливу зловмисника на користувачів ІС. У рамках цієї моделі профіль уразливостей користувача містить рівні вираженості цих уразливостей і формалізується як тривимірний масив. Залежно від рівня вираженості уразливостей користувача його відповідні реакції на соціоінженерні атакувальні впливи зловмисника мають різну ймовірність p_{ijk} , де k — конкретний користувач ІС; i — конкретна уразливість цього користувача; j— конкретний соціоінженерний атакувальний вплив зловмисника, спрямований на певну уразливість користувача.

Соціальна мережа — це складний соціотехнічний об'єкт, що з погляду кібернетики являє собою *велику систему*. Характерні ознаки соцмережі такі [73]:

1) наявність власних міркувань агентів;

2) змінювання думки під впливом інших членів соцмережі;

3) різна значущість думок (впливовості, довіри) одних агентів для інших;

4) різний ступінь здатності агентів підпадати під вплив (конформізм, стійкість думок);

5) існування побічного впливу в мережі соцконтактів, зменшення побічного впливу зі збільшенням відстані;

6) існування лідерів міркувань (агентів із максимальним впливом), формалізація індексів впливу;

7) існування порогу чутливості до змін навколишнього середовища;

8) локалізація груп (за інтересами, за світоглядними особливостями;

9) наявність специфічних соціальних норм;

10) урахування факторів соціальної кореляції (спільних для груп агентів);

11) існування зовнішніх факторів впливу (реклама, маркетингові акції) та зовнішніх агентів (засоби масової інформації, виробники товарів тощо);

12) наявність стадій — характерних етапів динаміки думок соцмережі (наприклад, процесу дифузії інновацій);

13) лавиноподібні ефекти (каскади);

14) вплив структурних властивостей соцмереж на динаміку думок:

• чим більше в агента зв'язків, тим більше в нього можливостей впливу через власне оточення на всю мережу, а водночас тим вищий ступінь уразливості від чужого впливу;

• чим вища щільність зв'язків активних агентів-сусідів, тим більша ймовірність змінювання стану зв'язаного з ними агента (ефект кластеризації);

• чим більше проміжне значення агента, тим, з одного боку, більша його участь у поширенні міркування/інформації з однієї частини мережі в іншу, а з другого — тим менший його вплив на агента-сусіда;

15) активність (цілеспрямованість поведінки) агентів;

16) можливість утворення угруповань, коаліцій;

17) неповна або асиметрична інформованість агентів, ухвалення ними рішень в умовах невизначеності;

18) нетривіальна взаємна інформованість агентів;

19) ігрова взаємодія агентів;

20) оптимізація інформаційних впливів;

21) інформаційне управління в соціальних мережах.

Сфери застосування та напрямки розвитку класичних соціальних мереж ілюструє табл. 2.4 [74].

Таблиця 2.4

Сфери застосування та напрямки розвитку соціальних мереж

Сфера застосування	Можливість	Тренд	Приклад	Примітка
Суспільна	Реальна	Мережа партійного об'єднання	—	Дезінтегрованість
Освітня	Деделі зростаюча	Підтримка дистанційного навчання	Мережа творчих учителів – www.IT-N.ru	АПК і ППРО за підтримки MicroSoft
Науково-технічна	Необмежена	Мережі професійних співтовариств	Медична мережа www.wurman.ru	Миколаєнко Євген Іванович
Ділова	Реальна	Мережі практиків	Мережа автолюбителів	www.Avto.ru
Культурна	Потенційна	Взаємопроникнення	Соціальна мережа художників	*www.algonet.ru/?ID = 637620*

Під ***віртуальною*** (*онлайновою*) ***соціальною мережею*** розуміють соціальну структуру інтернет-середовища, вузли якої ототожнюються з організаціями або окремими людьми, а зв'язки між ними унаочнюють відповідну взаємодію (політичну, корпоративну, службову, сімейну, дружню, за інтересами тощо). Інтернет забезпечує зростання інтенсивності інтелектуальної взаємодії на кілька порядків, появу нових якостей за рахунок емерджентних властивостей (*emergence* — незвідність властивостей системи до властивостей окремих її елементів) складної соціотехнічної системи. При цьому соціальне співтовариство, що діє в інтернет-середовищі, на відміну від класичної соціальної групи, такої, скажімо, як група вчених, інженерів, лікарів, піддається оперативному вивченню, вимірюванню та класифікації.

Віртуальна мережа, що забезпечує розвиток системотехнічного підходу, розглядається сьогодні з позицій суспільної мети та корисності, соціальної значущості та можливостей впливу на суспільство. Її характерні особливості — це топологія, розмаїтість, поширеність, складність, стійкість, а також наявність групової динаміки в поводженні. Організація внутрішньомережної міжособистісної взаємодії з комунікаційного погляду дає кількісну оцінку потужності такого об'єднання (за принципом «багато з багатьма») у вигляді 2^N, де N — кількість учасників мережі. Натомість у класичній трансляційній мережі, де поширення інформації забезпечується за широкомовним принципом від «одного до багатьох», потужність пропорційна до кількості точок (учасників). Соціальна орієнтованість мережних об'єднань сприяє розвитку її емерджентних властивостей, зокрема виникненню «ефектів бджолиного рою», що мають такі характерні ознаки:

- відсутність централізованого управління;
- самостійність субодиниць;
- висока здатність субодиниць до під'єднання;
- павутинна (нелінійна) зумовленість впливу.

У своєму розвитку віртуальні соціальні мережі проходять низку типових етапів:

- ***етап становлення***, коли спостерігається приплив енергії, генерованої людською цікавістю, ностальгією та бажанням знайти старих і нових знайомих;
- ***етап стабільності***, коли процеси, що відбуваються усередині мережі, стають ізоенергетичними;
- ***етап стагнації***, коли цікавість до соціальної мережі поступово спадає.

Корисну інформацію для пояснення цих процесів дає графік стрімкого зростання кількості користувачів соціальної мережі Facebook з поступовим її зменшенням (рис. 2.17) [75; 78]. Спільна особливість — поетапність розвитку проекту. У перші дні приросту користувачів немає, а далі йде «спалах розголосу», на зміну якому приходить деякий спад — «площина тих, хто сумнівається». Ці особи залучилися завдяки розголосу або за компанію, але невдовзі втратили інтерес до соціально-мережного життя. Після цього спостерігається планомірне зростання кількості учасників мережі до її «насичення». Наступна зона припадає на період стабільної роботи, за яким неминуче йде вмирання проекту із заміною його новим, більш модним, технологічним, актуальним. Особливий інтерес для дослідника становлять етап «сплеску розголосу» і зона зростання кількості прихильників проекту — тих, хто не піддався зовнішнім збуренням, а навпаки, діяв під керуючим впливом влас-

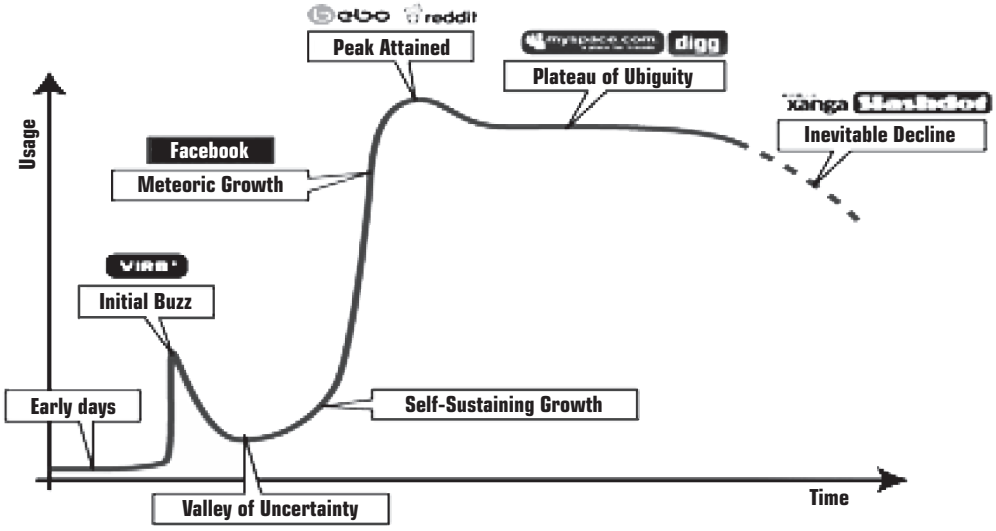
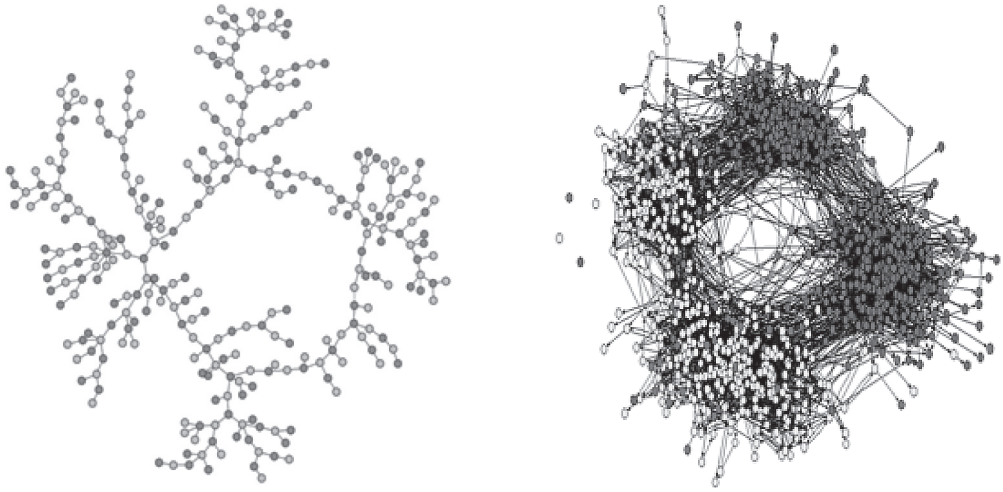


Рис. 2.17. Графік зростання кількості користувачів

ників проекту й, можливо, що більш цікаво, згідно з внутрішніми процесами самоорганізації та формування груп.

Віртуальні соцмережі [76] можуть бути найрізноманітніші — залежно від причин і цілей їх виникнення. Наприклад, соціальна мережа друзів в університеті схожа на гніздо (рис. 2.18, *а*), а соціальна мережа знайомств має зовсім інший вигляд (рис. 2.18, *б*).



а *б*

Рис. 2.18. Граф соцмережі університету (*а*) та соцмережі знайомств (*б*)

Здебільшого соціальні мережі мають комерційну, професійну та суспільну орієнтацію. Рейтинг найбільш популярних із них унаочнює діаграма, наведена на рис. 2.19.

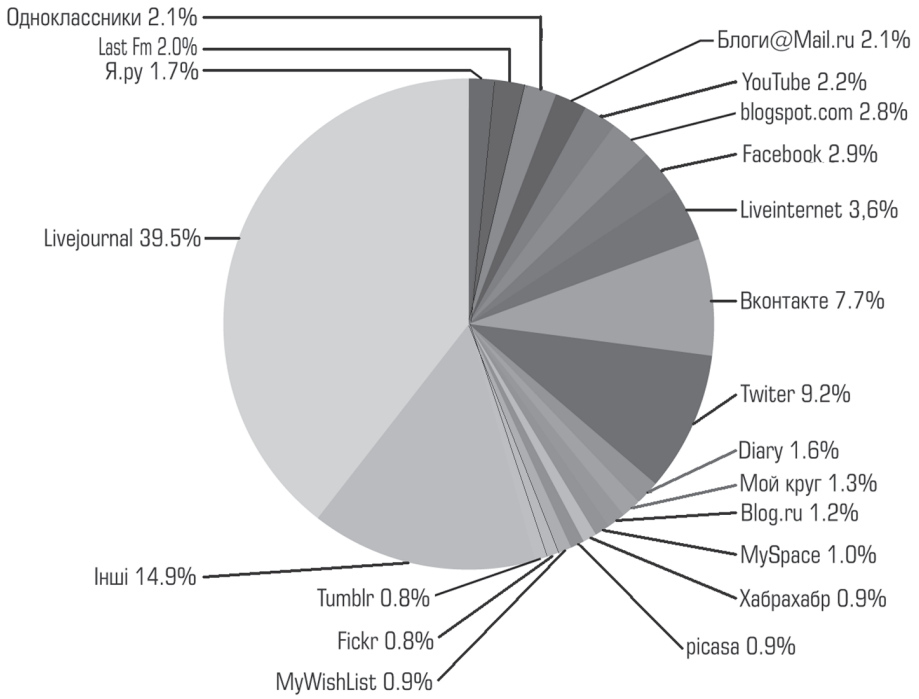


Рис. 2.19. Рейтинг популярності соціальних мереж

Віртуальні соцмережі стартували 1995 року з порталу у США **Classmates.com** («Одноклассники» — його російський аналог). Проект став початком буму соцмереж протягом 2003–2004 років, коли було запущено LinkedIn (для ділових контактів), MySpace и Facebook (для самовираження особистості). Нині на підґрунті таких соцмереж, як **Facebook** і **Twitter,** почали формуватися локальні соціопростори (рис. 2.20) [77–79].

Як показало дослідження, проведене Globalwebindex, лідерство серед соціальних мереж сьогодні, як і раніше, належить Facebook. На друге місце вийшла соціальна мережа Google+, що обігнала YouTube і Twitter. П'яте місце посідає соціальна мережа «None of the Above» — «Проти всіх». Далі підряд ідуть вісім китайських соцмереж. Між ними в середину потрапила ділова соціальна мережа LinkedIn, вона очолює другу двадцятку. Російська соціальна мережа «Вконтакте» посідає 21-ше місце. «Одноклассники» розмістилися на передостанньому місці. На 16-му місці опинилася соціальна мережа знайомств Badoo.com [80].

Дослідники з GlobalWebIndex визнали, що Twitter — соціальна платформа світу, що зростає найвищими темпами. Друге місце — за користувальницькою базою Facebook і Google+. «Вконтакте», «Одноклассники» і Pinterest перебувають у першій десятці.

Для складання рейтингу (рис. 2.20) підраховувалися активні (ті, хто хоча б раз за останній місяць відвідували мережу) користувачі з 31 країни світу. За твердженням дослідників, ці дані релевантні для 90% дорослого інтернет-населення земної кулі. Повністю першу десятку формують такі мережі: Twitter, Facebook, Google+, «Вконтакте», Sonico (Мексика), LinkedIn, Mig33 (Індонезія), Pinterest, «Одноклассники», 51.com (Китай).

Рис. 2.20. Провідні соціальні мережі в різних країнах світу

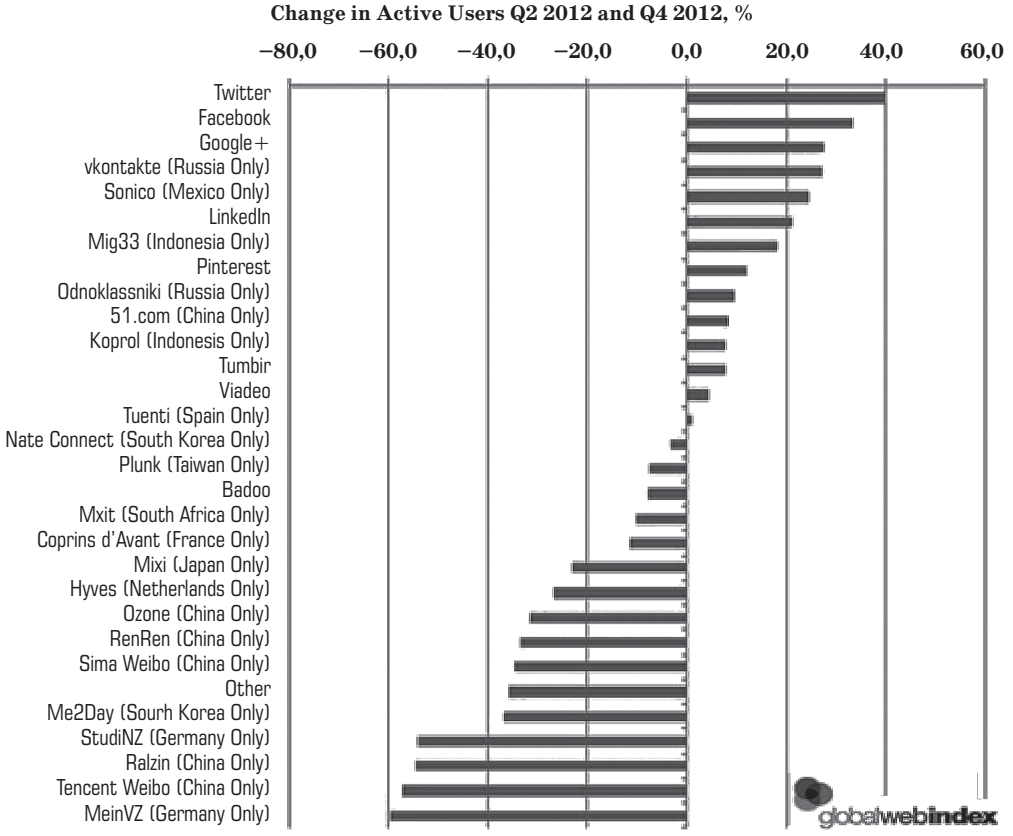


Рис. 2.21. Рейтинг соцмереж за темпами зростання користувальницької бази

В Україні найбільшою популярності в користувачів набула соцмережа Connect.ua. Ще кілька років тому вона об'єднала в собі понад 760 тис. осіб (вузлів), що становило 1,65% населення України. При цьому утворилося більш як 10 млн зв'язків. Відповідний граф зображено на рис. 2.22, де для наочності сильніші зв'язки розміщено в центрі графа, а більш слабкі — по його периметру.

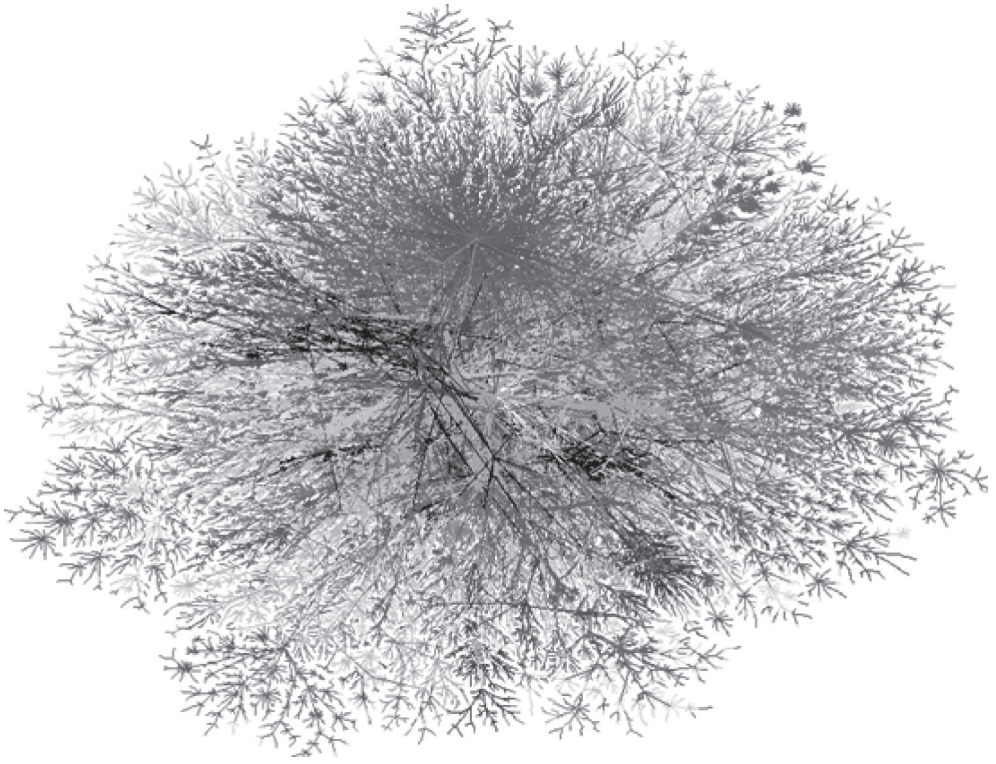


Рис. 2.22. Граф соціальної мережі Коннект

У той час виникла й одна з перших українських політичних соціальних мереж *Politiko.com.ua*. Вона поєднала політиків, експертів, журналістів, лідерів партій і виборців України, посівши друге місце. На третьому місці розташувалось співтовариство *Profeo*. До його складу ввійшли професіонали, що опікуються налагодженням ділових і особистих контактів, розвитком фахівців, підвищенням їхнього професійного рівня. *Profeo.ua* — універсальна платформа для розвитку професіоналів майбутнього. Четверте місце на той час посідала соцмережа *Tuse.ua,* відіграючи роль незамінного засобу спілкування. На п'яте місце потрапив інтерактивний портал *rybalka.com* із питань риболовлі та мисливства, де вміщувались також GPS карти рік і озер України, фотозвіти про риболовлю й полювання. Наступні п'ять місць розподілилися так: [77]

Autovisio.com.ua — актуальна інформація про автомобільні новини;
Prweb.com.ua — осередок журналістів і піарників.
People.ukrhome.net — соціальна мережа jiteli.net;
Science-community.org — сайт для вчених;
Cafe.beeline.ua — соціальна мережа, призначена для абонентів Beeline.

Регулярне відстежування (моніторинг) інформації в цих та інших подібних до них соціальних мережах дозволяє відповідним дійовим особам оцінювати ефективність своєї діяльності, заздалегідь виявляти й розв'язувати можливі ризики, а також мінімізувати негативні наслідки їх реалізації. Отже, під ***моніторингом соціальних мереж (SMM)*** будемо розуміти *спеціально організоване систематичне спостереження за станом соціальних мереж, за перебігом явищ і процесів, що відбуваються у відповідних середовищах, здійснюване з метою їх оцінювання, контролю та прогнозування*. Проведенням SMM окрім спеціальних компаній опікуються як стражі порядку (ЦРУ в США та МВС в Україні), так і роботодавці, використовуючи при цьому безліч стартапів. Лідирують серед них такі:

1. Сервіс Trendrr [80], що дає змогу:

• чітко фіксувати кількість завантажень додатків для Facebook;

• підтримувати велику кількість відео sharing сайтів, з'ясовуючи, яку кількість відео з тим чи іншим тегом було переглянуто);

• вести web-статистику сайтів з даними від Compete, Netcraft Site Rank і Quantcast.

2. Сервіс Trackur [81], що уможливлює відстежування потоків інформації, пов'язаної з багатьма онлайновими проектами (сервіс збирає всі типи інформації, відображаючи її в максимально зручному вигляді);

3. Сервіс Sentiment Metrics [82], що дозволяє аналізувати й обробляти дані, подаючи їх у доступному й зрозумілому вигляді. SentimentMetrics — система, що містить інформацію про бренд, яка надходить із різних блогів, форумів, прес-релізів.

Зауважимо, що моніторинг соціальних мереж в інтернеті через величезний потік інформації не може здійснюватися вручну. Процес відбувається автоматизовано, з використанням спеціальних онлайнових сервісів або програмного забезпечення — як платного, так і безплатного. Сервіс фіксує появу на будь-якому сайті згадування назви даної компанії, імен ключових фігур і конкурентів, посилання на сайт цієї компанії, а також ключових слів, важливих для даної індустрії й, зрештою, надсилає менеджерові відповідне повідомлення.

Нині розрізняють такі види моніторингу соціальних мереж:

• *регулярний моніторинг* — постійне відстежування інформації, що з'являється в соціальних мережах, яке допомагає зрозуміти тенденції зміни думок, особливості реагування на ту чи іншу інформацію, а отже, і скоригувати власну інформаційну політику;

• *первинний моніторинг* — процес, здійснюваний компаніями, які лише починають використовувати нові інтернет-медіа у своїй комунікаційній діяльності. Він дозволяє визначати «гарячі теми», місця присутності цільової аудиторії та лідерів думок, що допоможе закласти основи комунікаційної стратегії компанії в інтернет-середовищі;

• *конкурентний моніторинг* — сукупність дій, спрямованих на відстежування становища конкурентів у мережі й коливань їхньої активності, а також на промоцію власної компанії;

• *репутаційний моніторинг* — процес, що охоплює, як правило, період не менш як 6 місяців і дозволяє визначити імідж компанії та її продукції, що сформувався в інтернет-середовищі, передусім в очах споживачів.

Починати моніторинг потрібно з аналізу ключових слів (назва компанії, продукту, сервісу, послуги, назва компанії-конкурента тощо), що дадуть

поштовх до відповідних пошуків в інтернеті, необхідних для налагодження моніторингу сервісів або програм. Далі слід визначити майданчики (сайти, блоги), які стосуються потрібної індустрії. І, нарешті, слід попрацювати з негативними хостами, особливо якщо їхні посилання належать до топ 20 пошукових результатів за важливими ключовими словами, намагаючись усунути негативну інформацію і водночас налагодити контакти з власниками потрібних сайтів. При цьому варто пам'ятати, що офіційність, підготовленість відповідей і коментарів не спрацьовують у соціальному інтернеті, де спілкування людини з людиною забезпечується в рамках єдиних, багатокористувальницьких web-платформ, де головне правило — індивідуальний підхід до кожного. Ці платформи дали змогу користувачам спілкуватися з друзями, читати новини, дивитися фільми, слухати музику, брати участь в обговореннях, створювати співтовариства тощо.

Подальші дослідження соцмереж мають зосереджуватися на таких позиціях (рис. 2.23):

- формування математичних моделей топології мережі Інтернет та механізмів поширення в ній інформації;
- формуванні математичних моделей управління семантичним простором;
- розробка систем прихованого контролю інтернет-ресурсів;
- розробка моделей псі-впливу тощо.

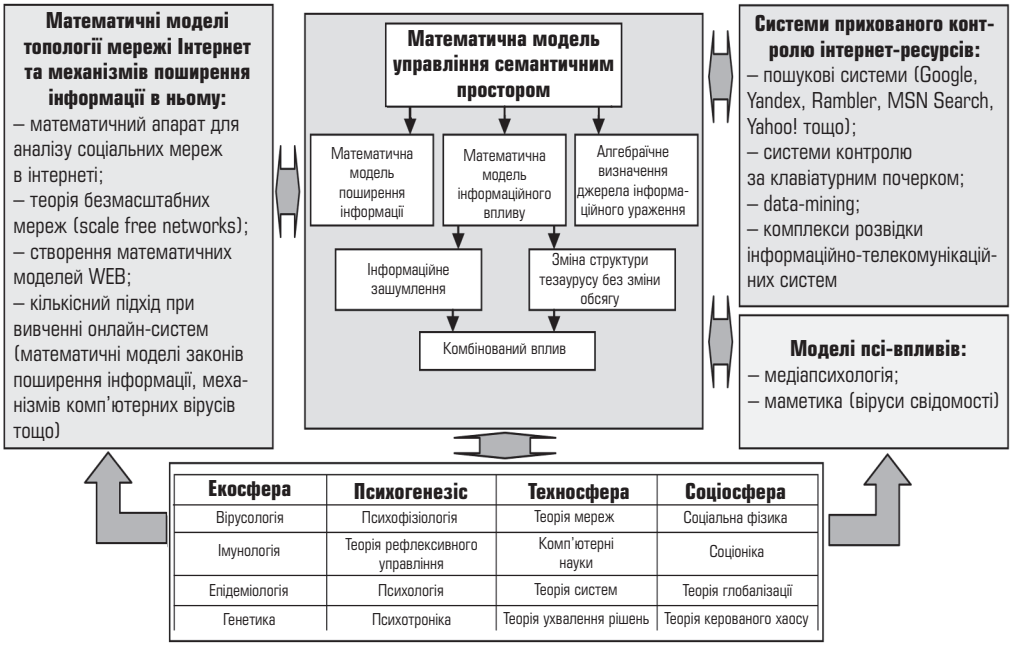


Рис. 2.23. Напрямки дослідження соціальних мереж

При цьому слід пам'ятати, що постійний моніторинг мережі Інтернет, блогосфери й форумів — перший крок у протидії інформаційному нападу, який сприяє значному зниженню витрат на протидію інформаційним атакам.

2.4. Поняття соціотехнічної системи та її властивостей. Системний підхід як загальнометодологічний принцип створення складних соціотехнічних систем

Загалом під ***системою*** слід розуміти *цілісність взаємопов'язаних елементів та взаємозв'язків між ними, яким притаманні певні властивості, мета, цілі та функції* [83–86]. Систему, як правило, характеризує структура, що відбиває взаємодію між її елементами і випливає з властивостей останніх або оточення, а також функціонал, який регламентує відношення між певним елементом системи і системою в цілому та визначає можливість керувати нею. Якщо в системах існують не самі лише однобічні причинно-наслідкові залежності, то говорять про ***комплексні***, або, як їх ще називають, ***складні системи***. Основні властивості складних систем такі [87]:

• *інтегративність* — властивість, що визначає фактори, які утворюють і зберігають систему;

• *комунікативність* — ступінь зв'язку із зовнішнім середовищем;

• *рівновага* — здатність зберігати деякий стан за відсутності збурень;

• *стійкість* — здатність системи повертатись до попереднього стану після того, як її було з нього виведено;

• *адаптація* — здатність системи до цілеспрямованого пристосування.

Ці властивості визначаються як зворотними зв'язками системи, так і особливостями окремих її елементів.

У множині складних систем використовують соціальні, технічні, ергатичні, технологічні, економічні, організаційні та управлінські системи. Наприклад, еволюційний розвиток ***соціальних систем*** можна зобразити схемою, поданою на рис. 2.24.

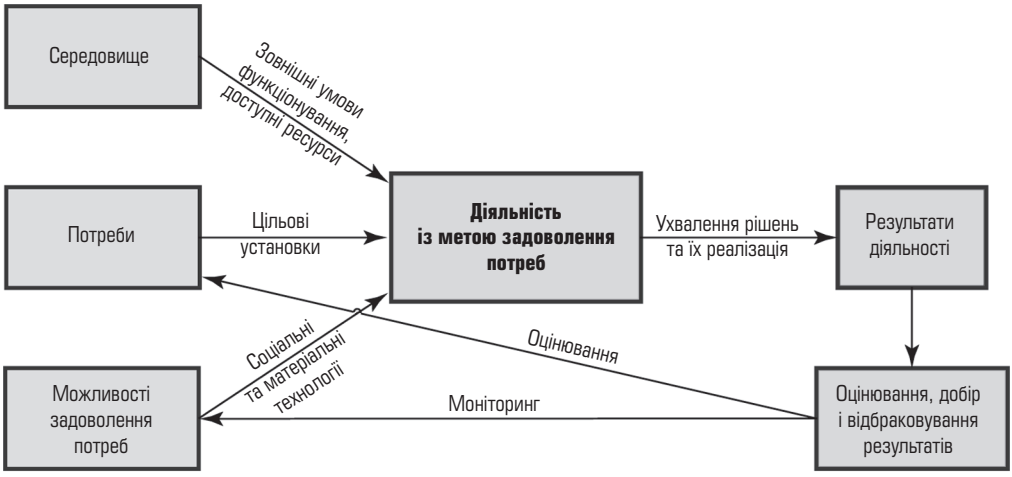


Рис. 2.24. Еволюційний розвиток соціальних систем

Зазначені системи включають у себе ті елементи «людського фактора», які впливають на кожного окремого індивіда та на групи людей, зокрема у плані їхнього ставлення до роботи, на організаційну культуру, на керівництво та управління в цілому.

Складні ***технічні системи*** являють собою *матеріальні системи, які за певними алгоритмами, але без участі людини розв'язують заздалегідь ви-*

значені завдання. Вони містять такі змінювані залежно від технології роботи характеристики: коли і де має виконуватися кожне завдання; в який спосіб воно має виконуватися; який взаємозв'язок між виконуваними завданнями.

Складні ***ергатичні,*** або ***соціотехнічні системи*** — *це системи, складовою яких є людина-оператор, знання, уміння, настрої, ціннісні переваги й ставлення до виконуваних обов'язків якої у взаємодії з технічним пристроєм у процесі, наприклад, виробництва матеріальних цінностей, управління певними процесами, обробки інформації тощо сприяють підвищенню ефективності розв'язання відповідних завдань або поліпшенню їх результативності* (рис. 2.25).

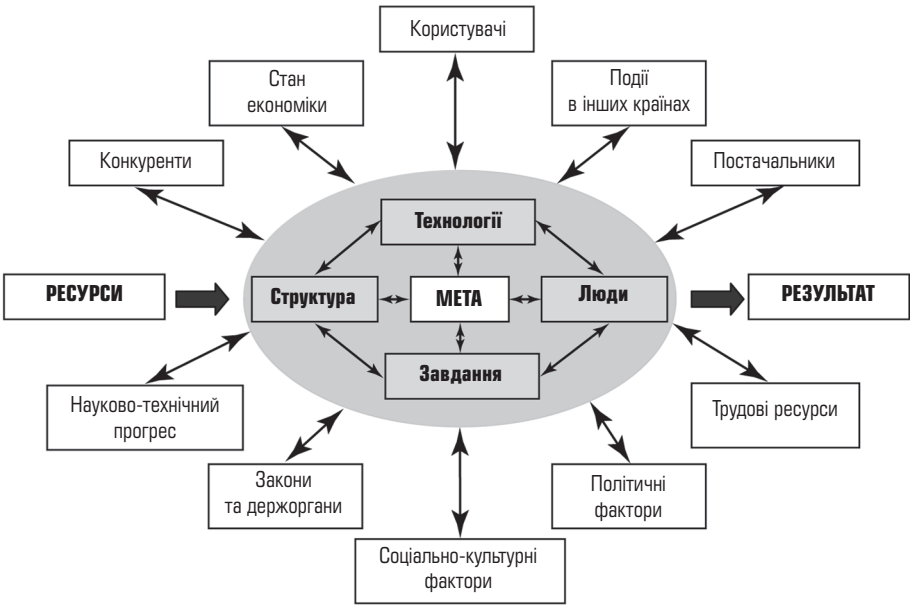


Рис. 2.25. Структурно-логічна схема соціотехнічної системи

Розробники концепції соціотехнічних систем — англійські вчені Е. Тріст та К. Бемфорт (Тевістокський інститут суспільних відносин), які досліджували процеси механізації добування вугілля у Великобританії. Їхні пошуки завершилися встановленням взаємозв'язку та взаємної зумовленості обох частин цілісної системи — *технічної*, що включає в себе інструменти й обладнання, та *соціальної*, утворюваної сукупністю людей, відношень між ними й сформованих інституціональних установок.

Головні характеристики ***соціотехнічної системи*** такі:

1) організаційна філософія, що базується на розумінні працівниками своїх цілей і призначення підприємства, на їхній постійній готовності поділити з адміністрацією всю повноту відповідальності за результати господарської діяльності;

2) організаційна структура управління, що забезпечує рядовим робітникам та службовцям реальні права щодо участі в керуванні;

3) новий підхід до розробки робочих місць і визначення ролі виконавця в процесі ухвалення управлінських рішень;

4) нова схема розміщення обладнання, яка має відповідати потребам перспективної форми організації праці, забезпечуючи прискорене проходження матеріальних потоків на виробництві;

5) нові форми й методи підготовки та перепідготовки кадрів, що спираються на гнучку кадрову політику, спрямовану на гарантування зайнятості;

6) нові критерії в оцінюванні економічної ефективності використання сучасних технологій та здійснення капіталовкладень у розвиток виробництва.

Як один із найбільш відомих загальнометодологічних принципів створення складних соціотехнічних систем використовується ***системний підхід*** [88–91] — *напрямок методології наукового пізнання, в основу якого покладено розгляд кожного явища (процесу, об'єкта) як певної системи* (рис. 2.26). Методологічні принципи й теоретичні положення системного підходу дають змогу:

• розглядати об'єкт дослідження як цілісну систему, відносно відокремлену від зовнішнього середовища і водночас пов'язану з ним, тобто вивчати цей об'єкт у тісному зв'язку й взаємодії з іншими об'єктами;

• відстежувати зміни, що відбуваються в системі внаслідок зміни окремих її ланок;

• вивчати специфічні системні якості;

• доходити обґрунтованих висновків щодо закономірностей розвитку системи;

• визначати оптимальний режим її функціонування.

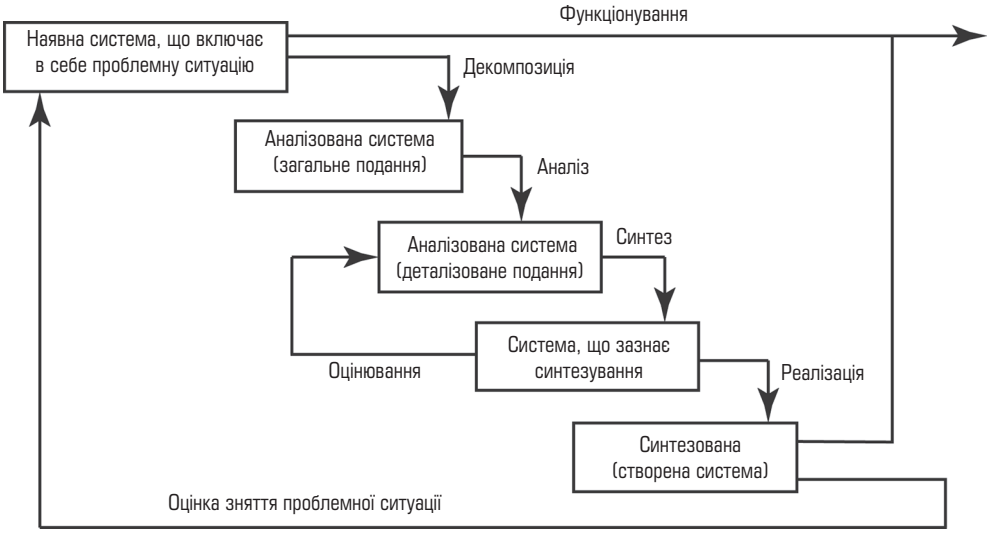


Рис. 2.26. Системний підхід розв'язання проблемної ситуації

Основні етапи реалізації системного підходу:

• формування проблеми;

• виокремлення цілі або сукупності цілей;

• визначення альтернативних засобів, за допомогою яких можна досягти поставлених цілей;

• визначення ресурсів, необхідних при використанні кожної системи;

• побудова математичної моделі, тобто формалізованих залежностей між цілями та альтернативними засобами їх досягнення;

• визначення критеріїв вибору найкращої альтернативи.

***Основні принципи системного підходу*:**

• *принцип системності,* або *єдності* — розгляд і вивчення об'єктів дослідженя як цілісних систем. Передбачає розгляд системи, з одного боку, як цілого, а з другого — сукупності компонентів (елементів, підсистем, системотвірних відношень);

• *принцип кінцевої мети* — зведення до абсолютного пріоритету кінцевої або глобальної мети (основної функції, основного призначення тощо);

• *принцип зв'язності* — кожний компонент системи розглядається разом із його зв'язками з оточенням;

• *принцип модульності* — здебільшого в системі є сенс реалізувати декомпозицію на складові різного ступеня загальності, розглядаючи її як сукупність певних модулів і зв'язків між ними;

• *принцип ієрархічності пізнання* — найчастіше в системі доцільно реалізувати ієрархічну побудову і/або впорядкувати її складові за важливістю. Принцип вимагає трирівневого вивчення об'єкта: рівень 1 — вивчення самого об'єкта («власний» рівень); рівень 2 — вивчення цього об'єкта як елемента більш складної системи («зовнішній» рівень); рівень 3 — вивчення цього об'єкта відповідно до його складових («нижчий» рівень);

• *принцип функціональності* — спільний розгляд структури і функцій об'єкта з огляду на пріоритет функцій над структурою. На практиці принцип функціональності означає, зокрема, що в разі надання системі нових функцій корисно переглянути її структуру, а не намагатися реалізувати нову функцію в старій схемі реалізації системи;

• *принцип розвитку* — має закладатися при побудові штучних систем як здатність до вдосконалення, розвитку системи за умови збереження якісних особливостей. Межі розширення функцій і модернізації повинні передусім чітко усвідомити творці штучної системи, оскільки існують доцільні межі її універсальності. Можливості для розвитку закладаються через надання системі властивостей до самонавчання, самоорганізації, штучного інтелекту;

• *принцип децентралізації* — в управлінні системою співвідношення між централізацією та децентралізацією визначається призначенням та метою системи. При цьому ступінь централізації має бути мінімальний, що забезпечить досягнення остаточної мети;

• *принцип невизначеності* — дуже часто ми працюємо з системою, про яку далеко не все знаємо й не все розуміємо в її поведінці. Тому невизначеності та випадковості доводиться брати до уваги при визначенні стратегії і тактики розвитку системи;

• *принцип формалізації* — системний підхід має на меті здобуття кількісних характеристик, створення методів, що звужують неоднозначність понять, визначень, оцінок тощо;

• *принцип інтеграції* — спрямованість системного підходу на вивчення інтегративних властивостей і закономірностей системи, розкриття базисних механізмів формування єдиного цілого.

Як головні інструменти системного підходу використовують ***системний аналіз*** і ***синтез***. Аналіз і синтез — загальнонаукові методи, без яких не може обійтися жодний акт наукового дослідження, являють собою протилежно

спрямовані (аналіз — від цілого до частини, синтез — від частин до цілого) і водночас нерозривно пов'язані між собою способи пізнання [90; 91].

Системний аналіз *— це методологія дослідження таких властивостей і відношень в об'єктах, які важко піддаються спостереженню та розумінню в разі подання цих об'єктів у вигляді окремих складових елементів, ознак, а натомість припускають поглиблене вивчення як цілеспрямовані системи, що постають з їхніми характерними властивостями та взаємними відношеннями, що розглядаються як відношення між цілями та засобами їх реалізації.*

Системний аналіз успадкував шість основних етапів системного підходу (рис. 2.27). Від інших методів дослідження він відрізняється такими особливостями:

- враховує принципову складність об'єкта дослідження (ОД);
- бере до уваги розгалужені та стійкі взаємні зв'язки його з оточенням;
- ураховує неможливість спостереження ряду властивостей об'єкта та навколишнього середовища;
- реальні явища, їхні властивості та зв'язки з оточенням трансформуються далі в абстрактні категорії теорії систем;
- на базі відомих властивостей складних систем дозволяє виявити нові конкретні властивості та взаємні зв'язки конкретного ОД;
- передбачає визначення (відшукання чи конструювання) об'єкта, з яким надалі оперуватиме;
- орієнтується не на розв'язання «правильно сформульованих» задач, а на відшукання правильної постановки задачі та вибір відповідних методів її розв'язування.

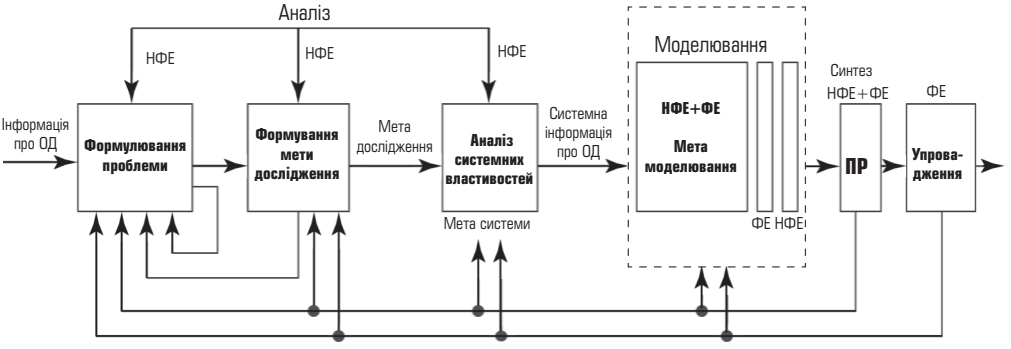


Рис. 2.27. Взаємозв'язок основних етапів системного аналізу

Головне в системному аналізі — знайти спосіб, в який складну проблему можна перетворити на простішу, причому це стосується проблеми, складної не тільки для розв'язання, а й навіть для розуміння. Зрештою зазначену проблему потрібно перетворити в послідовність задач, які можна розв'язати відомими вже методами. Системний аналіз неодмінно конкретний, оскільки завжди має справу з певною проблемою, цілком певним об'єктом дослідження, а отже, і продуктивний тоді, коли застосовується до розв'язування завдань певного типу. Він, як правило, спрямований на розв'язання складних слабко структурованих проблем, в яких переважають якісні, маловідомі і невизначені аспекти, зумовлені:

- недостатньо чітким розумінням проблеми;

• складністю класифікації поставлених проблем, а через це вибором неадекватних засобів їх розв'язування;

• хибною оцінкою сутності проблем (близькі, добре знайомі, але другорядні проблеми затуляють великі, але віддалені);

• неправильною оцінкою значущості проблем через вузькопрофесійний підхід до них;

• складність постановки проблем на віддалену перспективу;

• змішуванням цілей, яких необхідно досягти, із засобами їх досягнення.

Мета застосування системного аналізу до конкретної проблеми (події) полягає в підвищенні ступеня обґрунтованості знайденого розв'язання. Саме завдяки системному аналізу вдається виокремити такі ознаки даної події, згідно з якими можна було б здійснити об'єднання, систематизацію фактів, розмістивши їх у певному (хронологічному, функціональному, структурному) порядку, що в той чи інший спосіб характеризує важливі аспекти розвитку досліджуваної події. На базі системного аналізу встановлюються протилежні властивості, тенденції перебігу події, що відбивають певні суперечності й дозволяють розкрити внутрішні рушії розвитку події.

Потреба в застосуванні системного аналізу постає, коли:

• формулюється (визначається) нова проблема, а її розв'язання вимагає координації поставлених цілей із множиною засобів їх досягнення;

• сформульована проблема має розгалужені зв'язки, що призводять до віддалених наслідків у різних галузях, а отже, ухвалення остаточного рішення в таких випадках змушує враховувати сукупну його ефективність та повні витрати на його реалізацію;

• для досягнення взаємозв'язаного комплексу цілей існують варіанти розв'язання проблеми, які важко порівняти;

• створюються нові складні системи або відбувається вдосконалення (модернізація) існуючих, а важливі рішення мають ухвалюватися на достатньо віддалену перспективу за наявності невизначеності та ризику.

Для забезпечення ефективності системного аналізу потрібно:

• застосовувати його в тих випадках, для яких він призначений;

• відчувати потребу в його проведенні, чітко уявляючи мету й призначення такого аналізу;

• відповідально ставитися до системного аналізу з боку як аналітиків, так і замовника;

• мати достатньо інформації, досвіду, ідей та уявлень про предмет дослідження;

• відображати в результатах системного аналізу справжній стан справ і реальні шляхи розв'язання проблем, а не позірні «обґрунтування» суб'єктивних рішень;

• мати відповідні ресурси (кваліфікованих експертів, обладнання, грошові кошти);

• ураховувати в роботі можливий вплив сторонніх другорядних факторів (прогноз наукових відкриттів, винаходів, політичної ситуації).

Як невід'ємна складова системного аналізу виступає ***моделювання*** — *процес, що включає в себе дослідження реальної соціотехнічної системи* (рис. 2.28), *побудову моделі* (об'єкта, подібного до свого прототипу, що завдяки цієї подібності відіграє роль засобу опису, пояснення та прогнозування його поведінки) *цієї системи, дослідження її властивостей та перенесення здобутих відомостей на модельовану систему.*

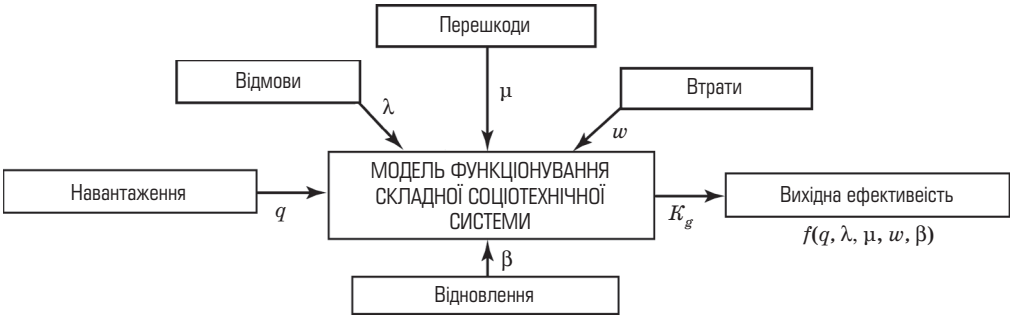


Рис. 2.28. Процес моделювання складної соціотехнічної системи, що має такі показники надійності: q — параметри потоку навантажень; λ — параметри потоку відмов; μ — параметри перешкод; w — параметри втрат; β — параметри відновлень; K_g — коефіцієнт готовності

Математична модель соціотехнічної системи (СТС) у такому разі має створюватися на принципах функціонального об'єднання моделей елементів і підсистем у єдиний комплекс програмно реалізованих алгоритмів, які забезпечують імітацію відповідних процесів для будь-яких вхідних умов і поточних станів.

Нині існує чимало різноманітних методологій і методів опису складних соціотехнічних систем. Найбільш відомі серед них — методи специфікації систем, що базуються на теоріях відношень і графів, відбиваючи структуру тієї чи іншої досліджуваної системи. З огляду на сказане під час опису СТС розглядають здебільшого *функціональні, технічні, організаційні*, *документальні*, *алгоритмічні*, *програмні*, *інформаційні* види структури зазначених систем (рис. 2.29).

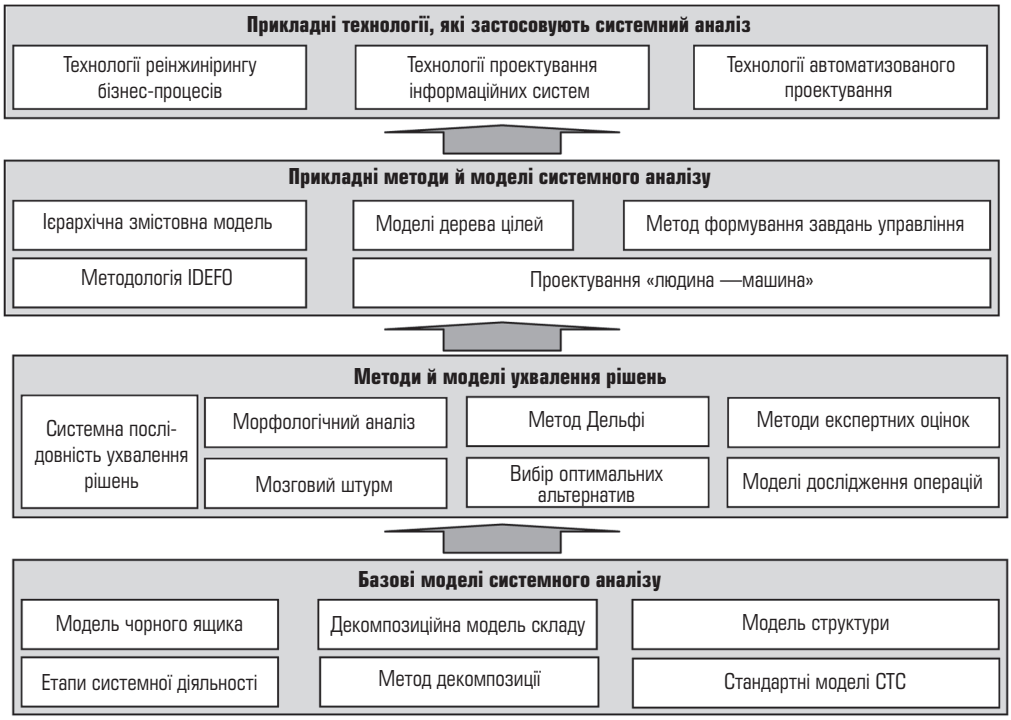


Рис. 2.29. Класифікація моделей і методів системного аналізу

Структура СТС залежить від типів використовуваних елементів і зв'язків між ними (табл. 2.5).

Таблиця 2.5

Види структури СТС, елементи цих систем та зв'язки між ними

Вид структури	Елементи структури	Зв'язки між елементами структур
Функціональна	Функції, завдання, процедури	Інформаційні
Технічна	Пристрої, компоненти й комплекси	Лінії та канали зв'язку
Організаційна	Колективи людей і окремих виконавців	Інформаційні, супідрядності та взаємодії
Документальна	Документи	Взаємодії, вхідності та супідрядності
Алгоритмічна	Алгоритми	Інформаційні
Програмна	Програмні модулі й вироби	Керівні
Інформаційна	Форми існування та подання інформації в системі	Операції перетворення інформації в системі

Зауважимо, що альтернативу зазначеним методам може становити методологія сім'ї IDEF. За їх допомогою можна ефективно відображати й аналізувати моделі діяльності широкого спектра складних систем у різних аспектах. При цьому широту й глибину відстежування процесів у системі визначатиме сам розроблювач.

Методологія сім'ї IDEF має такі переваги:

- простота в освоєнні;
- забезпечення специфікацій, графічно доступних для огляду;
- придатність для відображення різних взаємозалежних і необхідних для проектування аспектів побудови системи;
- уможливлення покрокового уточнення специфікацій;
- незалежність від прикладної області системи.

Нині до складу сім'ї IDEF можна віднести:

- по-перше, методологію (стандарт) IDEF0 функціонального моделювання. За допомогою наочної графічної мови IDEF0 досліджувана система постає перед розроблювачами й аналітиками у вигляді набору взаємозалежних функцій (функціональних блоків — у термінах IDEF0). Як правило, моделювання засобами IDEF0 є першим етапом вивчення будь-якої системи;
- по-друге, методологію IDEF1 моделювання інформаційних потоків усередині системи, що дає змогу відображати й аналізувати структуру та взаємозв'язки інформаційних потоків;
- по-третє, методологію IDEF2 динамічного моделювання розвитку систем. Через достатньо серйозні складнощі аналізу динамічних систем від цього стандарту практично відмовилися, і його розвиток призупинився вже на початковому етапі. Проте існують алгоритми та відповідні комп'ютерні реалізації, що дозволяють перетворювати набір статичних діаграм IDEF0 у динамічні моделі, побудовані на базі *забарвлених мереж Петрі* (*CPN — Color Petri Nets*);
- по-четверте, методологію IDEF3 документування процесів, що відбуваються в системі. За допомогою IDEF3 описують сценарій і послідовність операцій для кожного процесу. IDEF3 має прямий взаємозв'язок з методологією IDEF0 — кожна функція (функціональний блок) може бути подана у вигляді певного процесу засобами IDEF3;

• по-п'яте, методологію IDEF4 побудови об'єктно-орієнтованих систем. Засоби IDEF4 дають змогу унаочнювати структуру об'єктів і головні принципи їхньої взаємодії, тим самим дозволяючи аналізувати й оптимізувати складні об'єктно-орієнтовані системи;

• по-шосте, методологію IDEF5 онтологічного дослідження складних систем. За допомогою методології IDEF5 онтологія системи може бути описана з використанням певного словника термінів і правил, на підставі яких можна сформулювати вірогідні твердження про стан розглядуваної системи в деякий момент часу. На основі цих тверджень формулюються висновки про подальший розвиток системи й здійснюється її оптимізація.

Таким чином, у рамках методології сім'ї IDEF будь-яка складна соціотехнічна система може бути специфікована, як правило, у вигляді трьох моделей: *функціональної*, *інформаційної* та *динамічної*. Ці моделі відбивають відповідно функції описуваної системи, інформаційні взаємозв'язки всередині системи та динаміку роботи системи.

У ***функціональній моделі*** система подається у вигляді ієрархії функцій (процесів, рішень, діянь). Щодо кожної з функцій вказано, які об'єкти надходять на її входи, а які виробляються на її виходах; зазначено керуючі впливи та механізми реалізації функції. Функціональна модель системи має розкривати такі її особливості:

• що являє собою система в цілому;

• яка декомпозиція функцій у системі;

• що перетворює функції системи та що є результатом їх виконання;

• що керує виконанням функцій;

• що необхідно для виконання функцій (які механізми);

• як пов'язані між собою функції та об'єкти.

Послідовно з'ясовуючи перелічені характеристики системи, можна побудувати функціональну модель будь-якої складної соціотехнічної системи.

Для інформаційних об'єктів функціональної моделі може бути побудована ***інформаційна модель***, що описує відношення між елементами системи у вигляді структур даних (склад та взаємозв'язки).

У спрощеному вигляді таку модель будують за три кроки:

крок 1 — визначення типів сутностей;

крок 2 — визначення типів зв'язків між сутностями;

крок 3 — визначення ключових (і не ключових) атрибутів сутностей, за якими розрізняються їхні екземпляри в межах кожного типу сутностей.

Інформаційна модель включає всебе опис форм існування та подання інформації в системі, а також операцій з її перетворення.

Сучасні СТС забезпечують великий спектр форм подання інформації та методів її перетворення, зокрема переведення з однієї форми в іншу залежно від характеру виконуваних завдань. Наприклад, подання інформації можливе у формі формалізованих і неформалізованих текстів природною мовою, формалізованих і неформалізованих графічних зображень, реляційних відношень, аудіоповідомлень, відеозображень тощо. Опис форм подання інформації в цілому визначає характер взаємодії людини-оператора з інформаційною моделлю, а також структуру останньої.

Динамічна модель відбиває часові характеристики системи, а також послідовність взаємодії функцій у часі. Отже, вона описує інформаційні процеси

(динаміку функціонування), оперуючи такими поняттями, як *стан системи*, *події*, *перехід із одного стану в інший*, *умови переходу*, *послідовність подій*.

Динамічну модель будують за чотири кроки:

крок 1 — визначення діянь, на які витрачається час;

крок 2 — визначення черг, що виникають в очікуванні обслуговування;

крок 3 — визначення ресурсів, необхідних для виконання діянь;

крок 4 — задання статистичних параметрів моделі, її входів і виходів.

Отже, зазначена сукупність моделей уможливлює опис як існуючої, так і майбутньої соціотехнічної системи.

Системний синтез — процес установлення зв'язків між виділеними елементами та ознаками з подальшим відтворенням їх у контексті досліджуваної події з відповідними істотними ознаками й відношеннями. Необхідна передумова проведення такого синтезу — здатність дослідника відстежувати об'єкт у динаміці, установлюючи зв'язки між його теперешнім, минулим і майбутнім станами. Саме ці категорії відбивають часову структуру способу пізнання, готовність дослідника розглядати систему в процесі її розвитку.

Основна функція синтезу полягає в установленні зв'язків між фактами та об'єднанні їх у класи (групи, підгрупи тощо) згідно з виокремленими ознаками. Синтез дає змогу встановлювати зв'язки між спостережуваними фактами, явищами й подіями, розкривати причини їх настання та можливі функціональні залежності, з'ясовуючи послідовність етапів, ступенів, тенденцій розвитку досліджуваної системи.

Синтез систем (складних проектів і програм) *поділяють на чотири етапи:*

1) вибір методу синтезу та розробка математичної моделі оптимізації, що являє собою сукупність математичної моделі функціонування системи та моделі, яка реалізує вибраний метод оптимізації засобами комп'ютерного моделювання;

2) розробка технічного завдання на програмування та налагодження;

3) перевірка адекватності моделі;

4) здійснення синтезу, коригування та реалізація здобутих результатів.

У процесі системного синтезу використовують три методи: ***аналітичний, імітаційний*** та ***евристичний***.

1. *Аналітичний метод* полягає в тому, що задача подається сторого математично, а далі на базі цього подання реалізується засобами ЕОМ.

2. *Імітаційний метод* сприяє отриманню статистичних даних про найбільш доцільні напрямки оптимізації системи залежно від змін у її функціонуванні. Загалом імітаційний синтез можна розглядати в двох аспектах:

• по-перше, як експериментальне визначення статистичних характеристик випадкового процесу за допомогою машинного експерименту, що дуже часто включає в себе оптимізацію;

• по-друге, як синтез за допомогою варіаційних розрахунків.

Що ж до імітаційного моделювання то його виконують у такий спосіб: методом варіантних розрахунків; методом статистичних випробувань; методом на основі множини досяжності.

3. *Евристичний метод* застосовується для синтезу систем, які не підлягають строгій математичній формалізації чи комп'ютерному моделюванню.

Зазначені методи системного синтезу поєднують суто математичні та неформальні методи, достатньо строгі способи дослідження формалізованих

моделей з експериментом та евристичними прийомами. При цьому аналітичний та імітаційний методи базуються здебільшого на відомих методах оптимізації. Наприклад, залежно від типу моделі (статична або динамічна) задачу оптимального синтезу доцільно розв'язувати методом математичного програмування або варіаційним методом.

Розглянемо один із різновидів складних соціотехнічних систем, при створенні яких повною мірою реалізується теорія системного підходу. Ідеться про ***інформаційно-телекомунікаційні системи***, що являють собою сукупність *інформаційних* і *телекомунікаційних* систем.

Інформаційні системи включають у себе різноманітні *організаційно-технічні системи, в яких реалізовано технології обробки інформації з використанням технічних і програмних засобів, спрямовані на вироблення тих чи інших управлінських рішень.*

Телекомунікаційні системи *постають на базі технічних і програмних засобів, призначених для забезпечення обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в деякий інший спосіб, причому у процесі обробки інформації, призначеної для задоволення певних інформаційних потреб, діють ці системи як єдине ціле, орієнтуючись на виконання певних спеціальних функцій і завдань.*

За рахунок упровадження та реалізації новітніх ***ІКТ*** — *сукупності методів і засобів функціональних, змістовних і забезпечувальних компонентів інформаційно-комунікаційної структури, які завдяки поєднанню їх засобами ЕОТ підтримують процеси циркуляції та переробки інформації, визначають хід її використання, впливаючи, зокрема, на надійність і оперативність перебігу процесів планування, управління, структуризації й постановки інформаційних завдань*, — у сучасних ІТС організовується і ведеться робота за напрямками [92–97]:

- виявлення інформаційних потреб та добору джерел інформації;
- збору інформації, її введення та виведення;
- опрацювання інформації, оцінювання її повноти та значущості;
- подання інформації у зручному для користувачів вигляді та організації належного зворотного зв'язку;
- використання інформації для оцінювання тенденцій, розробки прогнозів, оцінювання альтернатив рішень і дій, вироблення стратегій тощо.

Згідно зі сказаним мета створення будь-якої ІТС полягає в тому, аби в найстисліші терміни створити систему обробки інформації, яка, маючи задані споживчі якості, а саме: *продуктивність, відмовостійкість, сумісність, розширюваність, масштабованість і ефективність*, — характеризуватиметься властивостями:

1) *загальності і абстрактності* — як окремі системи розглядаються предмети, явища природи, різні процеси;

2) *множинності* — кожна сукупність елементів, яка може бути підмножиною різних систем, вирізняється певними системотвірними властивостями та конкретними відношеннями між своїми елементами;

3) *цілісності* — система поводиться як єдине ціле;

4) *емерджентності* — наявність у системі властивостей, які не можуть бути отримані із властивостей її елементів. Відомо, що досліджувана система формується деякою множиною елементів, кожний з яких сам може бути

складною системою. Елементи та їхні властивості істотно визначаються всією системою. У свою чергу, система визначається властивостями елементів, але не зводиться до їхньої формальної суми. Вона має деякі нові характерні властивості, притаманні лише системі в цілому. Тому для отримання властивостей системи необхідно аналізувати відношення між її елементами;

5) *еквіпотенційності* — кожна система є підсистемою вищого рівня і водночас вона є системою зі своїми елементами та зв'язками. Відомо, що досліджувана складна система будується з елементів завдяки існуванню зв'язків між ними. Сукупність усіх зв'язків та їхній певний порядок визначають структурну організацію системи, яка може мати ряд рівнів і специфічних «зрізів», що перебувають у відношеннях субординації та координації між собою. В організації таких систем важливу зроль відіграють прямі і зворотні зв'язки, а також структури, що забезпечують процес управління;

6) *синергізму* — ефективність функціонування кожної системи вища за сумарну ефективність ізольованого функціонування її елементів. Відомо, що кожний елемент системи та система в цілому певним чином виявляють себе, впливаючи на інші елементи і на всю систему, а також на зовнішнє середовище, тобто виконують деякі функції. Ці функції закономірно пов'язані зі структурою системи та зовнішнім впливом на неї. Установивши зв'язки між структурою та функціями, між «входами» та «виходами» системи, можна докорінно змінити її стан.

Модель складної ІТС, що поєднує соціальну та технічну складові, урівноважувані між собою за рахунок так званих модераторів (ролей у системі кожного працівника, цілей узгодження мотивації працівників із технічними можливостями системи, умінь працівників та їхніх здібностей з покладеними на них функціями) зображено на рис. 2.30.

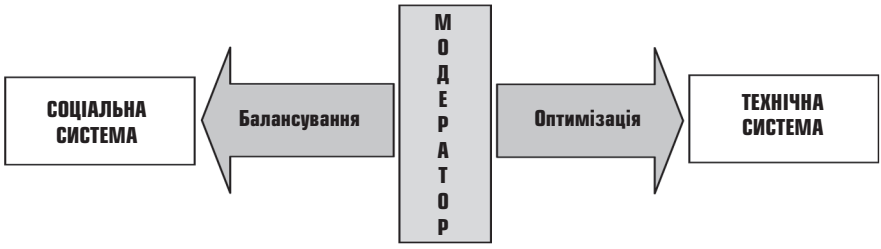


Рис. 2.30. Соціотехнічна модель складної ІТ-системи

Моделі ІТС складаються з *підсистем* і *компонентів*.

***Підсистеми** деякої глобальної ІТС являють собою виділені за деякими ознаками частини цієї системи, що виконують завдання з приймання і передавання даних від інших підсистем і компонентів, а також із їх обробки й зберігання.*

До найбільш визначених підсистем глобальної ІТС належать [92–97]:

- ***телефонні мережі**, призначені для передавання мовної інформації*;
- ***радіомережі**, призначені для передавання мовної інформації і даних*;
- ***комп'ютерні мережі**, призначені для передавання даних у будь-якій формі*;
- ***телевізійні мережі**, призначені для передавання мовної інформації та відеоінформації.*

Провідна роль зазначених мереж у сучасному інформаційному суспільстві визначається такими взаємозалежними чинниками:

1) потребою держав світу в отриманні найрізноманітнішого економічного, наукового, культурного та іншого інформаційного ресурсу;

2) рівнем телефонізації держав світу, розвиненістю та інтегрованістю в міжнародні мережі їхніх власних систем електрозв'язку;

3) ступенем комп'ютеризації (загальною кількістю комп'ютерів та їхньою щільністю в розрахунку на 1000 мешканців) держав світу, а також рівнем застосування комунікаційного обладнання — комутаторів, маршрутизаторів, шлюзів;

4) наявністю в державах світу досить розгалуженої системи загальнодоступних баз даних і різних довідкових служб;

5) злиттям (конвергенцією) технологій радіо, телефонних та інших ІТ-мереж.

Усі згадані вище мережі мають доволі складну структуру й на сучасному етапі розвитку ІТ-технологій здатні об'єднувати не тільки системи управління, зв'язку та обчислювальної техніки, й бойові платформи, зокрема носії засобів вогневого ураження. Складовими таких мереж можуть бути засоби розвідки, контррозвідки та спостереження, системи інформаційного забезпечення операцій, дипломатичних заходів та соціальних процесів.

Під ***компонентами ІТС*** — технічним, інформаційно-методичним, організаційним, нормативно-правовим тощо — розуміють [92–97] *елементи засобів забезпечення, що виконують певні програмно-технічні функції в тій чи іншій підсистемі ІТС*. При цьому, наприклад, *технічний компонент* може включати до свого складу пристрої для прийому, передачі, обробки і зберігання інформації. *Інформаційно-методичний компонент* об'єднує, як правило, низку споріднених компонент лінгвістичного, математичного, програмного, інформаційного та інших видів забезпечення. У свою чергу, *компонент лінгвістичного забезпечення* має містити термінологічні словники, правила формалізації даних і засоби діалогової взаємодії посадових осіб із технічними і програмними засобами СІТС, а *компонент математичного забезпечення* — загальне та спеціальне математичне забезпечення (математичні методи, моделі/процедури та алгоритми).

Компонент програмного забезпечення має включати в себе:

- загальне програмне забезпечення (ЗПЗ) — операційні системи (ОС) автоматизованих робочих місць (АРМ) користувачів та локальної обчислювальної мережі (ЛОМ); програми, що реалізують математичні моделі (процедури) та алгоритми;
- спеціальне програмне забезпечення (СПЗ) — програмно-апаратні засоби, що дозволять розв'язувати специфічні завдання управління, які не можуть бути розв'язані на базі програм загального програмного забезпечення;
- програмну документацію.

Компонент власне інформаційного забезпечення утворюється з комплексу спеціалізованих системних програм, призначених для пошуку, збору, добування та обміну інформацією. До його складу входять відомості про користувачів, систему форм і шаблонів електронних документів, системні та інші журнали, необхідні для відстежування етапів функціонування системи та здійснення відповідного контролю інших компонентів і сервісів.

Організаційний і нормативно-правовий компоненти містять базу даних нормативно-правових актів законодавства України; методичний апарат організації та ведення роботи; розподіл повноважень, прав, завдань і обов'язків; режимні правила та обмеження згідно з чинним законодавством.

Структурно ІТС в цілому та її функціональні підсистеми охоплюють технічні засоби; інформаційні канали; навколишнє середовище та обслуговувальний персонал. До *обслуговувального персоналу* належать усі особи, котрі в будь-який спосіб пов'язані з існуючою ІТС (оператори, адміністратори, техніки тощо). Під *навколишнім середовищем* розуміються будинки, службові приміщення, шахти, де перебувають елементи ІТС, тощо. *Інформаційні канали* в цьому разі являють собою систему взаємозв'язаних елементів інформаційного середовища. У результаті їхньої взаємодії створюються поля, що переносять інформаційний ресурс і забезпечують його передавання в середовищі поширення в заданому напрямі. Під *середовищем поширення* тут розуміється, як правило, частина простору, де відбувається переміщення інформації. Це середовище визначається набором фізичних параметрів, головними з яких є часові і частотні характеристики, а також характеристики перепускної здатності та параметри навантаження.

Сучасний системний підхід до створення складних ІТС ґрунтується на одно- чи багатокритеріальному оцінюванні альтернатив. Найбільш відомий варіант системного аналізу полягає в ***однокритеріальному оцінюванні*** за показниками вартості та ефективності (критерій *К* «ефективність-вартість»). При цьому вибір раціональної ІТС (раціонального зразка ОВТ, раціонального проекту) здійснюється за *максимумом цільової функції при заданій вартості*. Як *цільову функцію* беруть *критерій ефективності використання коштів*, *витрачених*, *наприклад, на розробку нового* (*проведення модернізації існуючого*) *зразка* (*системи*) *ОВТ*. Суть цього критерію полягає у визначенні того, який бойовий (потенційний) ефект очікується від даного зразка в конкретних умовах застосування, за конкретних витрат на його розробку та серійне виробництво: $K = E/C$, де E — показник ефективності зразка озброєння; C — показник вартості зразка озброєння, що забезпечує задану ефективність.

Що ж до методів ***багатокритеріального оцінювання альтернатив***, то вони більш універсальні. Усю множину таких методів можна розбити на такі групи: *прямі методи* (метод зваженої суми оцінок критеріїв, метод «дерева рішень»); *методи компенсації*; *методи порогів непорівнянності*; *аксіоматичні методи та людино-машинні методи*. При застосуванні більшості з них постають дві основні проблеми: по-перше, як знайти оцінки за окремими критеріями; по-друге, як об'єднати ці оцінки в загальну оцінку корисності альтернативи.

Для формування багатокритеріальної оцінки складної ІТС (СІТС) використовується розглянута далі система показників [1].

1. *Коефіцієнт результативності* $K_{\text{р}}$, що визначає розмір внеску (ефекту) СІТС у результативність певних завдань. Визначається через продуктивність ІТС, тобто швидкість виконання нею регламентованих дій. У загальному випадку

$$K_{\text{р}} = \sum_{n=1}^{H_0} P_n B_n \Pi \Big/ \sum_{n=1}^{H_0} P_n B_n, \qquad (2.1)$$

де P_n — імовірність появи, а B_n — коефіцієнт важливості інформації n-ї категорії; П — продуктивність СІТС за певний період часу; H_0 — загальна кількість упроваджених категорій важливості.

2. *Коефіцієнт ефективності* $K_е$, дорівнює відношенню ефекту застосування СІТС до витрат на його досягнення.

3. *Коефіцієнт новизни* $K_н$, числове значення якого характеризує ступінь використання нових ідей і технічних вирішень при проведенні модернізації (оновлення) СІТС, тобто відносний рівень підвищення результативності, який можуть забезпечити на момент початку модернізації нові ідеї та нові технічні рішення:

$$K_н = K_{р.н} K_{о.р} K_{с.вп} , \qquad (2.2)$$

де $K_{р.н}$ — показник рівня новизни ідей; $K_{о.р}$ — показник обсягу реалізації нових ідей; $K_{с.вп}$ — показник ступеня впливу нових ідей і технічних новацій на результативність зразка техніки. Значення показників $K_{р.н}$, $K_{о.р}$ та $K_{с.вп}$ визначають експертним оцінюванням.

4. *Коефіцієнт перспективності* $K_{п,}$ що характеризує рівень морального старіння елементів СІТС на момент завершення їх розробки, тобто рівень результативності, очікуваний на зазначений момент за рахунок нових ідей і технологічних новацій. Значення $K_п$ визначається експертним оцінюванням.

5. *Коефіцієнт технологічності* $K_т$, що визначає науково-технічний рівень технології проектування та виробництва СІТС на момент початку цієї системи. Практично визначає потенційний рівень результативності попереднього покоління техніки як відправну точку для розробки нового або оновлювання існуючого. Значення $K_т$ визначається експертним оцінюванням.

6. *Коефіцієнт технічного (воєнно-технічного) ризику* $K_{в.т.р}$, що визначає міру небажаних наслідків у разі невдалої реалізації заданих тактико-технічних вимог (ТТВ) і дорівнює ймовірності невиконання ТТВ:

$$K_{в.т.р} = 1 - P_{к.р} , \qquad (2.3)$$

де $P_{к.р}$ — імовірність того, що здобуте значення коефіцієнта результативності міститься в припустимих межах. Значення $P_{к.р}$ визначається експертним оцінюванням, а верхня і нижня припустимі межі задаються в технічному завданні (ТЗ).

7. *Коефіцієнт технологічного ризику* $K_{т.р}$, визначає міру небажаних наслідків при завершенні розробки нового або модернізації існуючої СІТС у визначені терміни і дорівнює ймовірності того, що реалізована тривалість $T_р$ розробки (оновлення) системи вийде за припустимі межі:

$$K_{т.р} = 1 - P_{т.р} , \qquad (2.4)$$

де $P_{т.р}$ — імовірність того, що значення $T_р$ містяться в заданих згідно з ТЗ межах. Значення $P_{т.р}$ визначається експертним оцінюванням.

Наведену систему показників у загальному вигляді можна подати так:

$$K = \left\{ K_k \,\middle|\, k = \overline{1, kk} \right\}, \qquad (2.5)$$

де k — порядковий номер показника; kk — загальна кількість показників, використовуваних у кожній конкретній експертизі.

Питання для самоконтролю

1. Дайте визначення поняття «інформаційне протиборство». Назвіть його основні форми та сфери впливу.

2. Дайте визначення понять «інформаційна війна» та «кібервійна». Що впливає на виникнення інформаційних і кібервоєн?

3. Дайте визначення понять «інформаційна зброя» та «кіберзброя». Чим зумовлюється перевага цих видів зброї над усіма іншими видами зброї?

4. Дайте визначення понять «інфосфера», «інформаційна операція» та «кібероперація».

5. Назвіть напрямки діяльності зі створення дієвої системи кібербезпеки.

6. Що відіграє роль базису для розробки моделей кібернападу і кіберзахисту? Наведіть приклади найбільш відомих таких моделей.

7. У чому має полягати реорганізація підсистеми добування інформації при підготовці та проведенні воєн майбутнього?

8. Дайте визначення поняття «розвідка інформаційно-телекомунікаційних систем» а також понять, пов'язаних з основними способами її ведення: розвідкою систем телекомунікацій, мережною та кібернетичною розвідкою.

9. Поясніть значення термінів «відкриті джерела» та «відносно відкриті джерела».

10. Дайте визначення методів розвідки інформаційно-телекомунікаційних систем і мереж: соціальної інженерії та моніторингу відкритих і відносно відкритих джерел.

11. Які вимоги має задовольняти система інформаційного забезпечення кібернетичної безпеки? Перелічіть основні вимоги до програмно-апаратних комплексів кіберрозвідки.

12. Назвіть основні особистісно-професійні характеристики поведінки працівників і дій користувачів, що сприятимуть реалізації загроз інформаційної та кібернетичної безпеки.

13. Які тактики та інструменти може використовувати соціальний інженер для отримання доступу до ІР-конкурента?

14. Що може впливати на розголошення в організації ІзОД? Перелічіть фактори, які можуть впливати на лояльність працівників, а також на процес прийняття нових співробітників на роботу.

15. Дайте визначення поняття «соціальна мережа». Назвіть найбільш відомі класи соцмереж. Чим регламентується поведінка агентів у мережі?

16. Назвіть основні відмітні особливості реляційно-алгебраїчних та імовірнісно-реляційних моделей соціальних мереж.

17. Назвіть характерні закономірності соцмереж та головні етапи їх життєвого циклу.

18. Що слід розуміти під моніторингом соціальних мереж? Назвіть основні його різновиди.

19. Дайте визначення поняття «система». Назвіть основні властивості системи.

20. Дайте визначення складних технічних і соціотехнічних систем. Назвіть основні їхні характеристики

21. Розкрийте сутність системного підходу до створення складних соціотехнічних систем. Назвіть основні принципи та етапи системного підходу.

22. У чому полягають основні інструменти системного підходу? Дайте відповідні визначення.

23. Чим системний аналіз відрізняється від інших методів дослідження складних соціотехнічних систем?

24. Що є невід'ємною складовою системного аналізу? Дайте визначення цього процесу.

25. Дайте визначення поняття «системний синтез». Розкрийте сутність його основних етапів.

26. Якими методами забезпечується системний синтез?

27. Дайте визначення поняття «інформаційно-телекомунікаційна система». Назвіть головні складові та характерні властивості таких систем.

28. Наведіть приклад моделі складної ІТС. Дайте визначення понять «підсистема ІТС» та «компонент ІТС» .

29. Якими чинниками зумовлюється провідна роль ІТС у розвитку інформаційного суспільства?

30. Який критерій є визначальним при виборі раціональної ІТС із сукупності наявних альтернатив?

31. Перелічіть показники, використовувані для багатокритеріального оцінювання ІТС. Розкрийте сутність цих показників.

РОЗДІЛ 3

МЕТОДИ І ЗАСОБИ СОЦІАЛЬНОГО ІНЖИНІРИНГУ

Глибинні зміни у ставленні більшості країн світу, зокрема й України, до власної інформаційної, а отже, і кібернетичної безпеки спонукають приділяти дедалі більшу увагу розробленню рекомендацій стосовно коротко- та довгострокових пріоритетів трансформації безпекового сектору за напрямками пошуку й збору інформації з відкритих і відносно відкритих джерел, а також добування її із закритих електронних джерел, переймаючись водночас питаннями захисту власного інформаційного ресурсу від стороннього кібервпливу. Розв'язанню зазначених проблем у певних аспектах присвячено чимало публікацій зарубіжних і вітчизняних авторів, таких як В. В. Домарєв, Дж. Козіол [98], М. Кузнєцов [99], Кр. Касперськи [100], К. Митник, І. Симдянов. Проте й досі бракує результатів комплексних досліджень процесів розвідувальної діяльності в ІТ-середовищі, способів і методів її здійснення передусім щодо поведінки в цьому просторі так званого когнітивного базису — звичайних користувачів, професійних шпигунів і/або хакерів (порушників) [101]. Саме тому викладення основних понять і особливостей соціального інжинірингу як одного з дієвих методів розвідки ІТС слід розглядати як завдання першочергової ваги.

3.1. Соціальна інженерія як метод розвідки складних соціальних і соціотехнічних систем: основні аспекти, поняття та визначення

Розвідка ІТС, структуру якої унаочнює наведений на с. 75 рис. 2.10, характеризується специфічними механізмами — способами і методами, а також силами і засобами, задіяними у процесах збору і/або добування інформації [59; 102]. Головні способи її ведення — *розвідка систем телекомунікацій* (*РСТ*), *мережна розвідка* (*МР*) та *кіберрозвідка* (*КР*). Ці види розвідки, як зазначалося в розд. 2, мають на меті систематичний пошук, збір і/або добування:

- інформації про об'єкти розвідки в ІТ-системах її передавання, випромінювання і приймання та в захищених криптосистемах — засобами РСТ, а також у відкритих і відносно відкритих електронних джерелах — засобами КР;
- даних про ресурси, засоби захисту, пристрої та програмне забезпечення (ПЗ), використовуване в ІТС об'єкта розвідки, їхні уразливі місця та межі проникнення — інформації, що далі підлягає обліку, верифікації, вивченню та аналітичній обробці.

Зауважимо, що за допомогою РСТ і МР протиборчим сторонам вдається добувати відповідно близько 5–8 і 7% інформації одна про одну. Незрівнянно більших результатів досягають, використовуючи КР. Саме кіберрозвідка забезпечує від 35 до 95% найціннішої інформації про об'єкти розвідки, яка нерідко стосується найбільших військових і державних таємниць. Кіберрозвідка ІТС, залежно від важливості та специфіки покладених на неї завдань, наявних ресурсів і способів пошуку й збору інформації [59], використовує різні інстру-

менти (рис. 3.1). Згідно з цим можна виокремити *технічний* і *програмний методи* її ведення, *методи так званої соціальної інженерії* (*СІ*), а також *метод, що передбачає моніторинг відкритих і відносно відкритих електронних джерел* (аналог відомої OSINT розвідки).

Рис. 3.1. Головні підходи до здійснення кіберрозвідки

Оскільки за умов стрімкого розвитку мережі Інтернет на противагу відомим технологіям забезпечення безпеки (міжмережні екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережних атак тощо) особливо ефективно постає людський чинник, то західні і вітчизняні фахівці [98–103; 109–119] розглядають СІ як один із найперспективніших підходів до розвідки ІТС. Ідеться передусім про те, що неавторизований користувач (хакер, порушник) отримує інформацію про призначення, структуру, установлені права доступу, систему захисту, реєстраційні імена й паролі, а також іншу конфіденційну інформацію про об'єкт атаки (розвідки) через несанкціонований доступ до інтернет-ресурсів, використовуючи для цього слабкість чи некомпетентність, непрофесіоналізм чи недбалість людини (групи людей), а також вдаючись до керування її діями.

Зрештою СІ має на меті змусити об'єкт атаки до певних дій, які їй не вигідні, але необхідні атакувальникові.

Інформаційні джерела для діяльності соціоінженера включають у себе:

- соціальні закладки (*social bookmarking*), які утворюють список закладок чи популярних web-сайтів і використовуються для пошуку користувачів зі спільними інтересами (*Delicious*);
- соціальні каталоги (*social cataloging*), зрієнтовані на наукову сферу для роботи з базами даних, цитатами з наукових статей (*Academic Search Premier, LexisNexis, Academic University, CiteULike, Connotea*);
- соціальні бібліотеки, які містять посилання на книги, аудіозаписи із системою рейтингів (discogs.com, IMDb.com);
- соціальні мережі web-майстрів, які містять посилання на пости, звернення тощо, часто мають рейтинги або рекомендації;
- багатокористувальницькі мережні ігри (*Massively Multiplayer Online Games*), які імітують віртуальні світи з різними системами переможців і переможених (*World of Warcraft*);
- геосоціальні мережі, які містять дані про геолокації, наприклад GPS для визначення місцезнаходження користувача;
- професійні соцмережі для пошуку роботи, розвитку ділових зв'язків (*LinkedIn, MarketingPeople* тощо);
- вікові та гендерні соцмережі для відповідних користувачів.

Для пошуку та збирання інформації про об'єкт атаки соціоінженери користуються, як правило, механізмами претекстингу, фішингу, бейтингу тощо.

Наприклад, ***претекстинг*** — це дії, до яких під час атаки, здійснюваної зазвичай по телефону або з використанням Skype, вдається порушник за заздалегідь сформованим сценарієм, маючи на меті ввійти в довіру до жертви.

Здебільшого зловмисник видає себе за якусь третю особу чи особу, яка потребує допомоги. Найкраща стратегія — використання спочатку невеликих запитів і згадування імен реальних людей, переважно керівного складу, з тієї організації, яка цікавить зловмисника. У процесі розмови він вдає, що потребує допомоги (більшість людей готові виконати невеликі завдання, що їх вони не сприймають як підозрілі запити). Установивши довірчий контакт, зловмисник може висловити прохання про щось більш істотне, маючи великі шанси на успіх.

Цей прийом особливо ефективний щодо нетехнічних користувачів, які можуть володіти цінною інформацією.

Фішинг (дослівно — риболовля) являє собою атаку, яку порушник здійснює через e-mail, аби спонукати потенційну жертву до розголошення певної конфіденційної інформації про себе (логін, паролі тощо) під приводом її «перевірки».

Мета більшості фішингових листів — змусити користувача натиснути деякі клавіші, аби зафіксувати послідовність його дій, або ж установити шкідливе програмне забезпечення як частину більш широкомасштабної спроби проникнення (рис. 3.2). Ключ до успішної кампанії фішингу — персоналізація [106–108]. Модифікація під конкретного користувача електронного повідомлення, нібито отриманого з надійного джерела, підвищує ймовірність того, що користувач прочитає пошту або навіть виконає дії згідно з рекомендаціями, поданими в повідомленні.

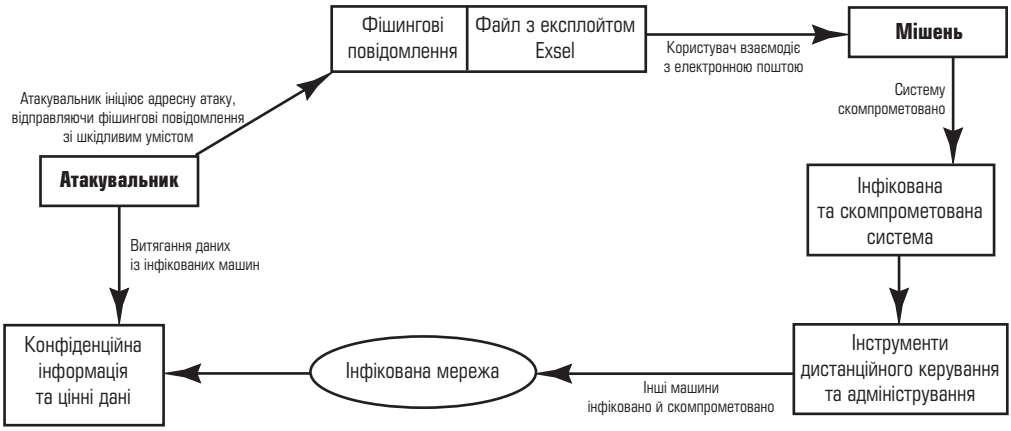


Рис. 3.2. Адресна атака з фішинговим повідомленням

За оцінками фахівців, понад 70% фішингових атак у соцмережах досягають своєї мети. Фішинг стрімко набирає обертів. Що ж до оцінок збитку, то вони хоч і різнятся, усе ж дають величезні цифри. Так, згідно з відомостями компанії «Gartner», у 2008 році жертви фішерів втратили 2,4 млрд дол. США, 2009 року збиток становив 2,8, а 2010-го — 3,2 млрд дол. США (табл. 3.1).

Таблиця 3.1

Економічні показники атак масованого і цільового фішингу на типову установу

Показник	Масований фішинг	Цільовий фішинг
Витрати на проведення	2 000$	10 000$
Загальна кількість надісланих повідомлень	**1 000 000**	1 000
Частка заблокованих повідомлень	**99%**	**99%**
Частка відкритих повідомлень	**3%**	**70%**
Частка повідомлень із використаними посиланнями	**5%**	**50%**
Частка успіху	**50%**	**50%**
Дохід від однієї жертви	2 000$	8 000$
Загальний прибуток	14 000$	150 000$

Зауважимо, що стосовно окремої установи економіка цільового фішингу може бути набагато більш виграшна. Незважаючи на те, що витрати на проведення такої операції значно вищі (за оцінками Cisco SIO, майже в п'ять разів) ніж у разі масованого фішингу, причому вищий може бути як дохід, так і прибуток. Тут визначальну роль відіграють якість отримання адрес і орендованого ботнету, а також вартість засобів генерування повідомлень електронної пошти, придбаного злоякісного ПЗ і створеного сайту. Істотний внесок належить і вартості засобів управління установою, базової інфраструктури обробки замовлень, послуг провайдерів із реалізації та вивчення даних користувачів.

Бейтинг — запуск злоякісного ПЗ, наприклад троянських програм (бекдорів, руткітів, кейлогерів, клікерів та проксі-троянів) як відповідні на поданий електронною поштою або через інфікований CD (флеш-нагромаджувач) запит порушника.

Злоякісне ПЗ, створюване з використанням широкого класу технологій, поступово стає дедалі серйознішою проблемою. Таке ПЗ може мати на меті:

- закачування або скачування файлів;
- копіювання помилкових посилань, що ведуть на підроблені web-сайти, чати чи інші сайти з реєстрацією;
- створення перешкод роботі користувача;
- викрадення даних, що становлять цінність або таємницю, зокрема інформації для автентифікації, для НСД до ресурсів;
- поширення інших шкідливих програм, таких як віруси;
- знищення даних (стирання або переписування даних на диску, ушкодження файлів) і обладнання, виведення з ладу комп'ютерних систем і мереж;
- збір адрес електронної пошти й використання їх для розсилання спаму;
- шпигування за користувачем і таємне повідомлення третім особам тих чи інших відомостей;
- реєстрація натискань клавіш із подальшою крадіжкою інформації такого роду, як паролі й номери кредитних карток;
- дезактивація або створення перешкод роботі антивірусних програм і фаєрволу.

Поетапну дію злоякісного ПЗ унаочнює рис. 3.3.

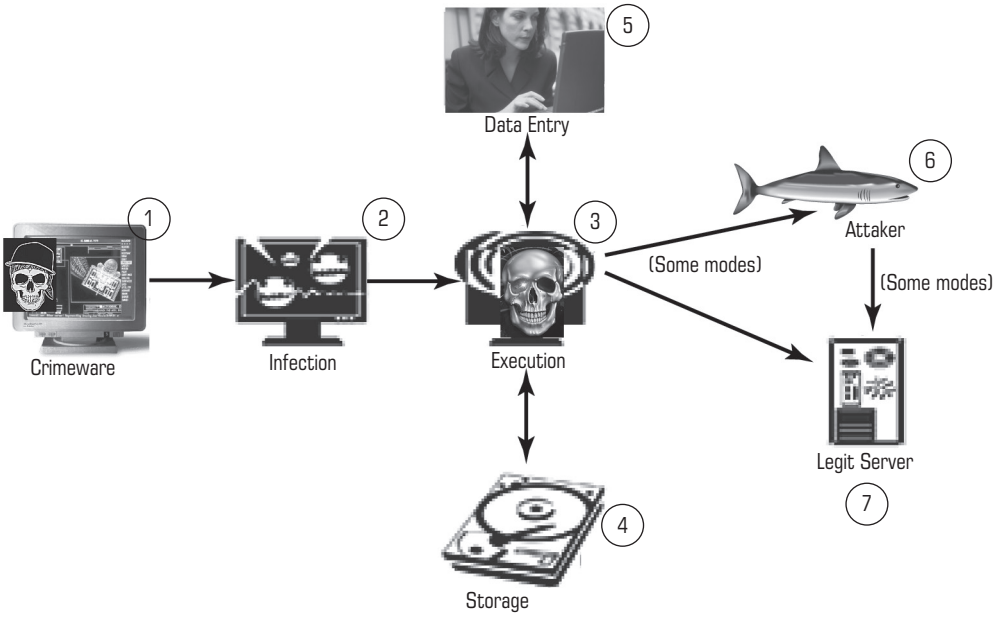


Рис. 3.3. Структурно-логічна схема організації бейтинг-атак

Eman 1 — поширення злоякісного ПЗ засобами соціального інжинірингу; *eman 2* — інфікування ПЕОМ; *eman 3* — запуск злоякісного ПЗ через проведення одноразової атаки або за рахунок реконфігурування системи (упровадження руткітів); *eman 4* —сканування пам'яті системи на наявність у ній конфіденційних даних; *eman 5* — крадіжка конфіденційних даних із пам'яті системи; *eman 6* — пересилання конфіденційних даних за визначеною адресою; *eman 7* — отримання сервером конфіденційних даних або від злоякісного ПЗ, або від атакувальника.

Поширення злоякісного ПЗ ґрунтується переважно на заходах зі створення соціальних пасток і здійснюється спеціально для отримання фінансової вигоди.

QUI PRO QUO — несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи.

Цей вид атаки передбачає дзвінок соціального інженера в організацію по корпоративному (внутрішньому) телефону. Здебільшого соціальний інженер представляється співробітником технічної підтримки, який здійснює опитування щодо виникнення технічних проблем. Під час «розв'язання» технічних проблем соціальний інженер «спонукає» користувача до введення команд, які дадуть змогу соціальному інженерові запустити або встановити шкідливе ПЗ на його комп'ютер.

Як приклади застосування таких підходів можна згадати троянський proxy-сервер «Mitglieder« та ICQ-черв'як «Bizex», що з'явилися 2004 року [100; 104]. Перший із них проникав до комп'ютера-жертви через уразливість у Microsoft Internet Explorer, яка дозволяла встановити і запустити proxy-сервер на зараженій машині без відома користувача. Після зараження відкривався порт, що використовувався для розсилання спаму. Зрештою заражені машини утворювали мережу машин-зомбі (ботнет), які підлягали дистанційному

керуванню. Для поширення ICQ-черв'яка «Bizex» порушники використовували масове несанкціоноване розсилання повідомлення «http://www.jokeworld.biz/index.html:)) LOL». Отримавши його, об'єкт атаки, який нічого не підозрював, відкривав зазначену сторінку. Далі, якщо використовувався браузер Internet Explorer із незакритою уразливістю, на комп'ютер завантажувалися файли черв'яка, а в деяких випадках і супутнього йому троянa. Після встановлення в систему «Bizex» закривав запущеного ICQ-клієнта і, підімкнувшись до сервера ICQ з даними зараженого користувача, розсилав спам за знайденими на комп'ютері списками контактів. Одночасно відбувалася крадіжка конфіденційної інформації — банківських даних, логінів і паролів тощо. Алгоритм дій порушників базувався при цьому на особливостях ухвалення рішень звичайними користувачами, професійними шпигунами і/або хакерами, яких у західних інформаційних джерелах називають *когнітивним базисом* [59].

Ще один із механізмів, використовуваних порушниками для отримання спеціальної інформації з ІТС, полягає у ***створенні підставних профілів***. Відомий приклад такої дії — створення Томасом Райаном з Provide Security підставного профілю молодої симпатичної дівчини 25 років, яка за легендою була фахівцем з 10-річним стажем роботи у сфері безпеки, закінчила престижний коледж у Нью-Хемпширі й мала вчений ступінь. Від імені свого віртуала Томас через популярні соціальні сервіси Facebook, LinkedIn і Twitter відправив запити щодо включення в коло друзів 300 чоловікам і жінкам із середовища військових, співробітників сек'юриті-компаній і державних чиновників. Згодом віртуальну дівчину стали запрошувати на конференції з питань безпеки, а великі компанії типу Google і Lockheed Martin взагалі висловили бажання найняти її на роботу. Через деякий час після початку активного життя її почали з власної ініціативи включати в коло друзів інші люди — колеги тих, кому «спеціалістка у сфері безпеки» нав'язала своє спілкування першою. У такий спосіб Томас Райан отримав доступ до великого обсягу особистої інформації (персональних даних), фотографій, а також розкрив зв'язки спілкування багатьох фахівців, що становили для нього певний інтерес.

Але, як з'ясувалося, СІ не вичерпується одними лише соціальними мережами. Свідченням цього став конкурс, проведений на одній з конференцій Defcon. Під час цього конкурсу всім охочим було запропоновано за один дзвінок тривалістю 25 хв добути максимум інформації, що сприяла б організації успішної кібератаки. Один із учасників конкурсу зумів за допомогою всього двох телефонних дзвінків ввести в оману співробітника технічної підтримки компанії British Petroleum та змусити його видати інформацію, яка допомогла організувати кібератаку на цю фірму. Серед отриманих ним відомостей були дані про те, які моделі ноутбуків використовують співробітники British Petroleum, а також які операційні системи, браузери, антивіруси й програми для організації VPN установлено на їхніх комп'ютерах. Окрім того, переможець змусив співробітника British Petroleum відвідати сайт Social-Engineer.org, завдяки чому заробив ще кілька додаткових балів.

Варто зазначити, що хакери отримували нагоду проникнути до ІТС об'єкта розвідки за результатами вивчення вмісту сміттєвих ящиків, як це було, наприклад, у Нью-Йоркській телефонній компанії, або завдяки виявленню слабких місць у системі мережної безпеки. Одним з таких місць у мережі банку BABank (США) виявилось закриття порту технічного обслуговування паролем, що його встановив виробник [101]. У результаті хакери отримали всі пра-

ва доступу до системи. Згодом, використавши на поштовому сервері застарілу версію Unix, хакери встановили над цим сервером контроль, налагодивши взаємодію з іншими серверами на адміністративному рівні.

На підтвердження можливостей СІ компанія Check Point Software Technologies — розробник ПЗ, призначеного для забезпечення ІБ, у 2011 році провела дослідження під назвою «Ризики соціальної інженерії в контексті інформаційної безпеки», яке мало на меті збирання даних щодо впливу соціальної інженерії на бізнес [105]. Її фахівці у ході опитування 853 ІТ-професіоналів і спеціалістів з інформаційної безпеки, які представляли провідні компанії США, Великобританії, Канади, Австралії, Нової Зеландії та Німеччини, з'ясували таке:

• по-перше, близько 86% усіх опитаних ІТ-професіоналів та 97% спеціалістів з ІБ добре усвідомлюють ризики, пов'язані з людським фактором;

• по-друге, 43% опитаних визнали, що в певні моменту часу бізнес-структури, які вони представляли, зазнали цільових атак методом СІ, кожна з яких потенційній жертві обійшлася близько 25–100 тис. дол. При цьому майже 70% усіх порушень, пов'язаних з безпекою інформації, здійснили саме співробітники цих структур;

• по-третє, майже третину з досліджених бізнес-структур було атаковано 25 і більше разів і лише 16% з опитаних респондентів заявили, що СІ їх не турбує.

За результатами опитування (рис. 3.4) також з'ясувалось [105], що головною мотивацією соціальних злочинців є фінансові вигоди (51% досліджених структур) та помста (14%), а основними методами їх роботи є розсилання фішингових листів (47% респондентів), вплив через соціальні мережі (39%), а також через незахищені мобільні пристрої (12%).

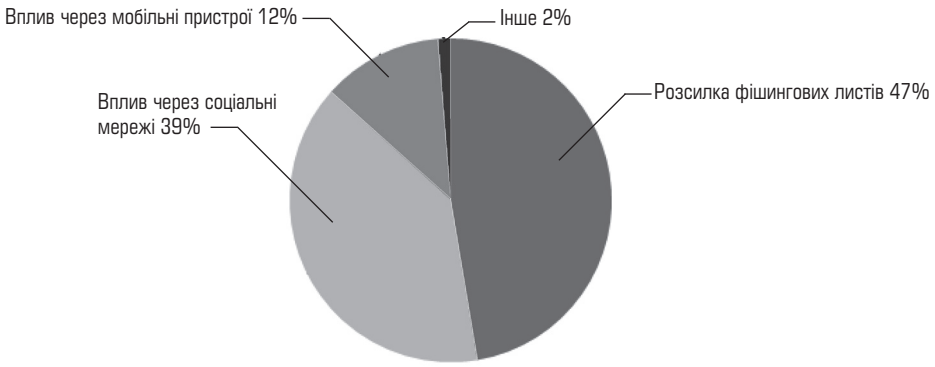


Рис. 3.4. Джерела проектування соціальних загроз

Найбільш сприйнятливими щодо таких дій на думку опитаних, є нові співробітники (60%), підрядники (44%) та виконавчі помічники (38%). При цьому 40% респондентів усю відповідальність за можливі витоки покладають саме на персонал (рис. 3.5). Щоб зменшити ризик впливу на нього методами СІ, значна (26%) частина учасників дослідження засвідчила, що вони регулярно проводять відповідні тренінги для персоналу або планують розроблення відповідної програми (19%), тоді як 34% респондентів констатували, що взагалі не приділяють уваги підготовці персоналу для запобігання збиткам від застосування методів СІ.

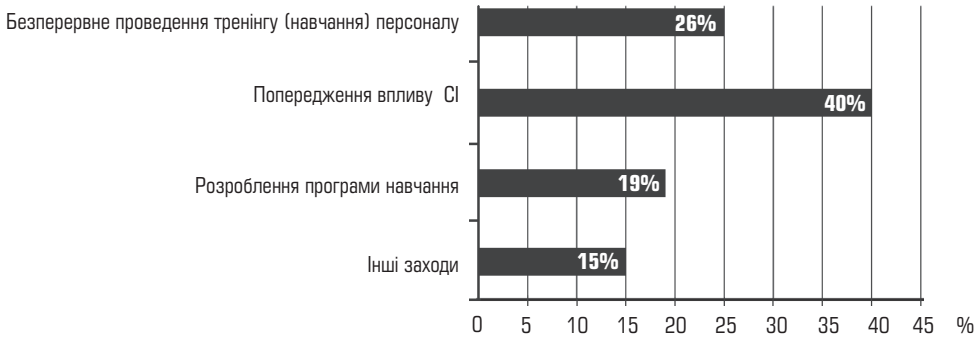


Рис. 3.5. Результати реагування на соціальні атаки

Для захисту користувачів від СІ фахівці компанії рекомендували застосовувати як організаційні (на рівні установи, організації), так і програмно-технічні засоби [60; 105].

До ***організаційних засобів забезпечення захисту інформації*** нині належать *організаційно-технічні* (підготовка приміщень з ПЕОМ, прокладання кабельної системи з урахуванням вимог щодо обмеження доступу тощо) та *організаційно-правові* (вимоги національного законодавства тощо) засоби. Їхня перевага зумовлюється можливістю розв'язання різних проблем, простотою реалізації та необмеженими можливостями модифікації і розвитку. Головний недолік — висока залежність від суб'єктивних факторів.

До ***технічних (апаратних) засобів*** належать різні за типом пристрої, які або заважають фізичному проникненню на об'єкт розвідки (захисна сигналізація тощо), або виявляють і перекривають потенційні канали витоку інформації (генератори шуму, мережні фільтри, сканувальні радіоприймачі тощо). Їхні переваги зумовлюються надійністю, незалежністю від суб'єктивних факторів та високою стійкістю до модифікації. Основним недоліком, як правило, є вартісний аспект.

До ***програмних засобів*** належать програми для ідентифікації користувачів, контролю доступу, шифрування інформації, вилучення тимчасових файлів тощо. Їхні переваги полягають в універсальності, гнучкості, надійності, здатності до модифікації та розвитку. Недоліки зумовлюються обмеженою функціональністю мережі, використанням частини ресурсів файл-сервера та автоматизованих робочих місць (робочих станцій), чутливістю до випадкових і спланованих змін, можливою залежністю від типів ПЕОМ тощо.

3.2. Методи соціального інжинірингу

Технологіями СІ людство в тій чи іншій формі користувалось із давніхдавен. Так, «нічні демони» в Японії, або ніндзя, вельми активно використовували властивості людського розуму поряд із гіпнотичним впливом. У Римській імперії вшановували людей, які вміли ввести співрозмовника в оману та впевнити його у правоті того, чого не могло бути. Прикриваючись високими посадами своїх покровителів й виступаючи від їхнього імені, вони, використовуючи вигідні аргументи, підлещування або завуальовану дезінформацію, вели дипломатичні переговори, розв'язуючи певні питання не тільки особистого, а й державного рівня. СІ завжди була головною зброєю і в середовищі шпигунів (розвідників). Наприклад, агенти КДБ СРСР та ЦРУ США вміли,

видаючи себе за іншу особу, вивідати державні таємниці. Тобто в усі часи підтверджувалася давня істина: найслабкіша ланка системи безпеки — людина.

У сучасному розумінні поняття СІ з'явилось досить недавно. Уперше його ввів Кевін Митник, який стверджував, що набагато простіше довідатись про чийсь пароль для доступу, ніж зламувати всю систему цілком. Враховуючи, що нині понад 70% усіх порушень, пов'язаних із безпекою інформації, здійснюються саме завдяки тонкощам людського фактору (рис. 3.6), К. Митник запропонував застосовувати можливості соціального інжинірингу з метою (рис. 3.7):

• збору довідкової інформації про об'єкт атаки (розвідки), а саме з'ясування інтересів та особливостей поведінки потенційної жертви, чатів і форумів, якими вона користується, а також імен, під якими вона з'являється у мережі Інтернет, через ведення діалогу з нею або з її оточенням у службах обміну миттєвими повідомленнями (messenger), наприклад ICQ;

• отримання закритої (конфіденційної) інформації про об'єкт атаки (розвідки) або інформації, що становить для порушника певний інтерес, наприклад номери телефонів потенційної жертви, адресу її реєстрації/проживання, реальне ім'я та прізвище тощо, через установлення контакту з нею і/або уведення її в оману;

• отримання інформації про об'єкт атаки (розвідки), необхідної для забезпечення НСД до системи, а саме пароля, яким користується потенційна жертва, серії й номера її паспорта та інших відомостей про неї через входження в довіру до обраної жертви;

• примушення об'єкта атаки (розвідки) до дій, необхідних порушникові, через нав'язування такому об'єкту нової моделі поведінки.

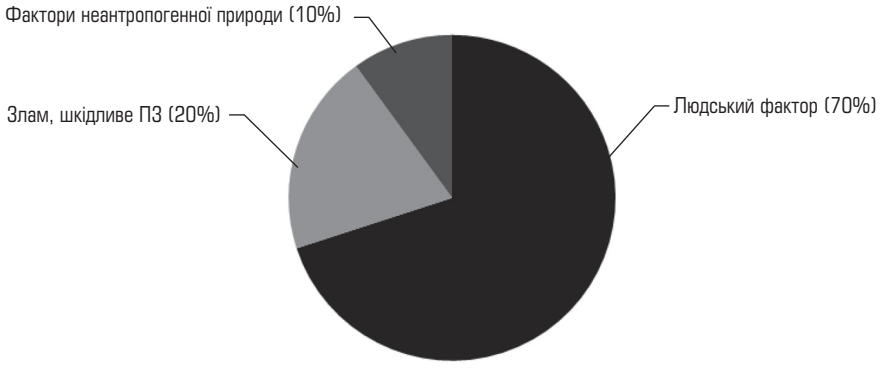


Рис. 3.6. Кругова діаграма, що ілюструє відсоткове співвідношення загроз інформаційній та кібербезпеці

З огляду на можливі прояви безвідповідальності або недбалості (співробітник цілеспрямовано або випадково може вчинити деякі дії з компрометації інформації), на наявність у певної частини співробітників корисливих інтересів (співробітник намагатиметься цілеспрямовано перебороти систему захисту для доступу до інформації підприємства, яка є закритою), прагнення самоствердитись (співробітник затіває свого роду гру «користувач проти системи». І хоча наміри самі по собі можуть бути нешкідливі, усе це неминуче призведе до порушення самої практики безпеки.

Отже, сучасні техніки СІ, спираючись на такі чинники, як стреси й психологічні взаємовпливи в колективах (зокрема, через необхідність виконання

Рис. 3.7. Основні сфери застосування СІ

співробітником вимог режиму таємності, тобто дій згідно з певним обмеженням його власної волі) та плинність кадрів (унаслідок переманювання конкурентами талановитих співробітників підприємства, до того ж обізнаних у секретах) спрямовуються на таких осіб:

• співробітників, які безпосередньо причетні до діяльності компанії (установи, підприємства): керівників і начальників відділів, персоналу відділу кадрів, секретарів та персональних помічників;

• нових і тимчасових співробітників, які виявляють незадоволення роботою в компанії (установі) або звільняються.

При цьому соціоінженери (неавторизовані користувачі) застосовують методи, які за ознаковим принципом (рис. 3.8) доцільно згрупувати так: *методи за взаємодією з політикою безпеки* та *дистанційністю; за ініціалізацією та маніпулюванням; за порушенням характеристик безпеки; за реляційними ознаками; за ступенем важкості; за типом джерела та за типом доступу*. Зазначені методи можуть практикуватись як самостійно, без залучення технічних засобів [112], так і бути інструментом у плануванні або проведенні інших видів атак на об'єкт розвідки із застосуванням закладених пристроїв і/або програмних закладок.

При цьому за ***взаємодією з політикою безпеки*** методи соціальної інженерії (МСІ) можуть бути *постполітизаційними* та *деполітизаційними*.

Постполітизаційні МСІ базуються на використанні недоліків у вже існуючій політиці безпеки. Наприклад, це можуть бути такі недоліки: неправильно побудовані правила розмежування доступу; використання програмних і апаратних засобів із недостатнім рівнем захищеності; прорахунки у блокуванні каналів витоку інформації з обмеженим доступом; заборона видачі імен та телефонів персоналу джерелу (яке здійснює запит), вірогідно не ідентифікованому.

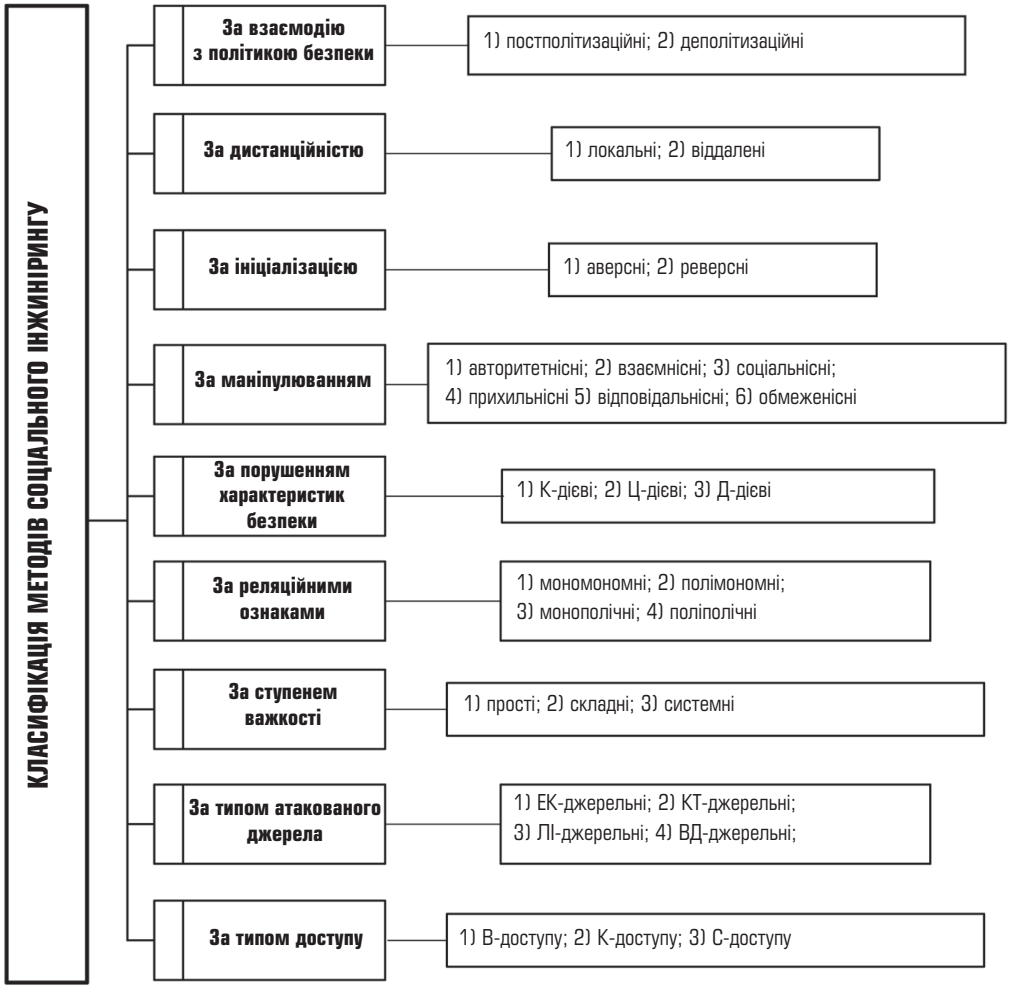


Рис. 3.8. Узагальнена класифікація МСІ

Деполітизаційні атаки спираються на помилки й недбалість, яких припустилися виконавці, реалізуючи заходи із забезпечення здійснюваної в організації політики безпеки. Це пов'язано здебільшого з людським чинником, що активізується в разі адміністративної підтримки, коректності виконання функцій захисту, своєчасності реагування на нештатні ситуації (тобто коли створюються умови, не описані в політиці безпеки, і працівники реагують на них у непередбачуваний спосіб). Прикладом нештатної ситуації може бути неадекватна реакція персоналу на прохання найвищого керівництва компанії отримати секретну інформацію.

За ***дистанційністю*** МСІ поділяються на *локальні* та *віддалені*.

Локальні МСІ реалізуються через безпосереднє індивідуальне спілкування соціотехніка з атакованим. Наприклад, коли останній є службовцем компанії, а соціотехнік шляхом прямого контакту представляється як співробітник, постачальник або працівник партнерської компанії, людиною зі служби підтримки тощо та просить про допомогу.

Віддалені МСІ поділяються на Т- та МТ-віддалені. Такі МСІ реалізуються за допомогою засобів комунікації (телефон, факс, електронна пошта, віртуальна комп`ютерна мережа тощо).

Т-віддалені МСІ базуються на використанні телефону, що є найбільш поширеним засобом у проведенні соціотехнічних атак. Володіючи навичками маніпулювання основними рисами людської натури, атакувальник може добувати потрібну йому інформацію, видаючи себе за іншу особу, якщо йому вдалося переконати в цьому атакованого (це особливо дієвий метод у великих корпораціях, де знати всіх співробітників та відстежувати прийом нових достатньо складно). Соціотехніки звертають особливу увагу на те, як створити досконале психологічне середовище для атаки. Незалежно від застосовуваного методу основна мета — переконати людину, від якої очікується розкриття інформації, у тому, що соціотехнік і є такий суб'єкт, якому можна довірити відповідну інформацію. Для цього використовуються маскарадингові технології [109]. Наприклад, соціотехнік може представитися або співробітником віддаленого офісу і просити локального доступу до пошти, або новим співробітником, що просить про допомогу, постачальником чи розробником ПЗ, який пропонує його оновлення.

МТ-віддалені МСІ базуються на використанні мережних технологій, наприклад електронної пошти, широкого спектра вірусного та інших шкідливих видів ПЗ, інтернет-ресурсів. У разі використання електронної пошти жертві може бути відправлено запит або прохання про виконання певної дії від імені керівництва, співробітників, знайомих тощо. Прикладом такого типу атак може бути відправлення запиту до відділу фінансів щодо надання керівництву місячного звіту, який потрібно відіслати на запропоновану соціотехніком електронну поштову скриньку. Інший випадок МТ-віддаленого МСІ — відправлення разом із листом або прикладним ПЗ вірусів чи шкідливого ПЗ, або адреси інтернет-ресурсу на них. Це можна здійснити, відправивши вкладення до листа на електронну поштову скриньку, прикріпивши шкідливе ПЗ до завантажуваної програми. Соціотехнік може надіслати атакованому лист із повідомленням про винайдення нової корисної утиліти, отримати яку можна, звернувшись на певну адресу, причому саме за цією адресою атакувальник розміщує шкідливу програму або вірус. Атакувальник може також відправити тільки адреси інтернет-ресурсу на відомі джерела з дуже схожою, але відмінною від справжньої адресою, створивши в такий спосіб графічний інтерфейс. Тоді жертва, не підозрюючи нічого лихого, може зареєструватись, залишивши свій ідентифікатор, пароль чи адресу електронної поштової скриньки, або спробувати ввійти як уже зареєстрований користувач. Соціотехнік може здійснити МТ-віддалену атаку за допомогою фальшивого pop-up вікна (небажане вікно, яке з'являється під час роботи з інтернет-ресурсами), де можуть бути розміщені корисні, на перший погляд, а насправді небезпечні адреси інтернет-ресурсів, форми для додаткової реєстрації, вікна завантаження шкідливого ПЗ під виглядом корисних додатків.

За ***способом ініціалізації*** МСІ поділяються на *аверсні* і *реверсні*.

Аверсними (прямими) називають МСІ, при яких соціотехнік звертається до атакованого зі своєю проблемою, переконуючи його в своїй авторизованості, і прохає про допомогу. Аверсні соціотехнічні атаки можуть також досягати мети з використанням шкідливого ПЗ, а також неуважності атакованого. Наприклад, зловмисник може представитись адміністратором комп'ютерного

відділу, зателефонувавши на вихідних додому одному зі службовців, який виконує розробку важливого проекту, та зробити повідомлення (ніби на знак ввічливості) про несправність локальної мережі та можливості її відновлення тільки через деякий час. А оскільки (і соціотехнік це знає) терміни закінчення проекту стислі, то атакований на відповідний запит погоджується видати свій ідентифікатор і пароль для швидкого відновлення потрібних файлів.

Реверсні (зворотні) МСІ полягають у тому, що соціотехнік створює ситуацію, в якій атакований стикається з певною проблемою і звертається до атакувальника по допомогу в її розв'язанні. Інша форма реверсної соціальної інженерії полягає в переспрямуванні дій на атакувальника, тобто об'єкт атаки (соціотехнік) розпізнає атаку і використовує різні методи (психологічні прийоми) для отримання максимально можливої інформації про атакувальника.

Наприклад, представившись працівником технічної допомоги провайдера (компанії, що надає послуги з доступу до мережі Інтернет), соціотехнік може повідомити своїй потенційній жертві про можливі вже найближчим часом проблеми з доступом до глобальної мережі і дати свій номер телефону, за яким потрібно звернутися, аби швидко усунути проблему (у цьому прикладі жертвою зловмисника є новий співробітник або особа, що перебуває у філії компанії, де немає адміністратора). Після цього атакувальник телефонує провайдеру, та представляючись начальником компанії, просить відімкнути доступ згаданої філії через невідкладні ремонтні роботи в офісі. Зловмиснокові залишається тільки чекати, коли жертва залетефонує в надії отримати допомогу. Після такого дзвінка зловмисник може сам приїхати туди, де перебуває жертва, і отримати бажаний доступ до робочої станції.

За ***способом маніпулювання особливостями людської натури*** МСІ поділяються на 1) *авторитетнісні*; 2) *прихильнісні*; 3) *взаємнісні*; 4) *відповідальнісні*; 5) *соціальнісні*; 6) *обмежувальнісні*, які назвемо відповідно *АВ-*, *ПР-*, *ВМ-*, *ВП-*, *СЦ-* та *ОБ*-маніпулюванням. Такі ознаки було визначено узагальненням результатів соціальних досліджень щодо впливів (маніпуляцій) на людей, які дали змогу виокремити *шість характерних рис* людської натури, які можна використовувати для отримання потрібної інформації.

Методи ***АВ-маніпулювання*** ґрунтуються на тому, що люди схильні прислужитися (задовольнити запит) особі, яка має авторитет (владу). Наприклад, соціотехнік отримує необхідні дані, якщо атакований сприймає його як авторитетне чи компетентне джерело. Аби створити таке враження, соціотехнік може задіяти маскарадні технології, стверджуючи, що телефонує керівництво, представник правоохоронних органів тощо.

В основу методів ***ПР-маніпулювання*** покладено вміння зловмисника викликати в атакованого прихильність до себе. Адже люди зазвичай задовольняють запит суб`єкта, який справляє приємне враження, має споріднені інтереси, спільні проблеми тощо. Саме тому зловмисник, перш ніж з'ясувати необхідні йому питання, вивчає інтереси атакованого, подаючи їх як свої власні, або називає спільних знайомих, земляків тощо.

Методи ***ВМ-маніпулювання*** спираються на схильність людини машинально надавати інформацію у відповідь на певні дії, що викликали в неї розчулення (через бажання віддячити). Це може бути порада, допомога тощо. Прийом цей особливо ефективний тоді, коли його застосування — повна несподіванка для атакованого. Найефективніший шлях до завоювання взаємності, що

сприяє розголошенню потрібної зловмисникові інформації, — прислужитися жертві, аби вона почувалася зобов'язаною своєму благодійникові. Наприклад, представившись співробітником департаменту інформатизації, повідомити, що деякі комп'ютери компанії інфіковано новим особливо небезпечним вірусом [109], який не вдається виявити відомими досі засобами, і при цьому негайно запропонувати розв'язання зазначеної проблеми. Далі (на свою користь) соціотехнік просить атакованого протестувати нову утиліту, що дозволяє користувачу змінити паролі.

Методи ***ВП-маніпулювання*** ґрунтуються на тому, що людина схильна виконувати обіцяне, аби не втратити довіри тих, хто має з нею справу. Наприклад, соціотехнік радить новому відповідальному співробітникові (згідно з підписаною ним угодою) ознайомитися з процедурами і правилами політики безпеки, виконання яких необхідне для коректного користування ресурсами інформаційних систем компанії. Після обговорення кількох положень безпеки соціотехнік запитує пароль співробітника (на підтвердження його готовності виконувати угоду), аби перевірити, наскільки піддається вгадуванню, і подає рекомендації щодо формування пароля надалі. Атакований, потрапляє в пастку, не бажаючи діяти всупереч політиці безпеки, суті якої він ще не збагнув.

Методи ***СЦ-маніпулювання*** використовують належність атакованої особи до певної авторизованої (соціальної) групи, дії більшості представників якої ця особа вважає істиною в останній інстанції. Наприклад, соціотехнік видає себе за перевіряючого зі служби безпеки і називає імена інших людей із відділу атакованого, які вже пройшли відповідну процедуру перевірки. Жертва, повіривши цьому, готова відповідати на всі запитання зловмисника, зокрема й щодо власного ідентифікатора і пароля.

Методи ***ОБ-маніпулювання*** ґрунтуються на готовності жертви скуштувати «безкоштовного сиру». Наприклад, соціотехнік розсилає електронні листи з повідомленням про те, що всі, хто до кінця тижня зареєструються на новому розважальному сайті, отримають безкоштовно електронний альбом того чи іншого популярного виконавця. У процесі такої реєстрації безтурботна жертва зазначає свій ідентифікатор, пароль, електронну пошту тощо. А як відомо, люди часто, щоб не забувати паролів та ідентифікаторів, використовують однакові в усіх системах. Скориставшись цим, соціотехнік може отримати доступ до службових або приватних інформаційних ресурсів атакованого.

Атака, під час якої експлуатуються різні риси людської натури, належить до комбінованого типу. Наприклад, АВВД-маніпулювання спирається на авторитетність та відповідальність особистості.

За ознаками, що стосуються ***порушень характеристик безпеки***, МСІ поділяються на *К-*, *Ц-* та *Д-діяві*.

К-діяві методи спрямовані на порушення такої характеристики безпеки, як *конфіденційність*. Наприклад, унаслідок відповідних дій соціотехніка його здобутком стає конфіденційна інформація, незважаючи на заборону доступу до неї.

Приклад 3.1. Розроблення К-діявої атаки, спрямованої на отримання доступу до важливої документації організації (установи).

Етап 1. На відповідному сайті знаходимо ім'я директора компанії, номер телефону його приймальні, а також номер телефону служби підтримки. Зателефонувавши в цю службу і запропонувавши послуги з надання інтернету, дізнаємося, який провайдер обслуговує компанію.

Етап 2. Зробивши дзвінок до служби підтримки вдруге, уже від імені провайдера з огляду на невідкладну справу дізнаємося номер телефону та ім'я чергового адміністратора

Етап 3. Оскільки компанія велика і рядовий адміністратор може не знати особисто директора, дзвонимо за наданим службою підтримки телефоном і від імені директора скаржимося черговому адміністраторові на низьку продуктивність праці секретарки, а через це просимо заблокувати доступ із комп'ютера секретарки до розважальних сервісів (youtube, соцмережі). Потім телефонуємо у приймальню директора і від імені мережного адміністратора просимо перевірити в секретарки роботоздатність інтернету, перейшовши на сайт youtube.com або vk.com. Оскільки обидва сайти заблоковано, повідомляємо: якийсь новий вірус вразив усю мережу компанії, а тому потрібно негайно зробити резервну копію цінних документів. Секретарка, керуючись почуттям відповідальності, береться допомагати. Оскільки вірус вразив і засоби віддаленого доступу, пояснюємо їй, де скачати і як установити TeemViewer. Після цього просимо вказати, де міститься цінна інформація і через TeemViewer завантажуємо її на доступний нам файлообмінник.

Рекомендації щодо захисту від К-дієвих атак.

1. Бухгалтери, секретарки та інший рядовий персонал не повинен мати повноважень на встановлення будь-якого ПЗ на своїх робочих місцях.

2. У разі виявлення несправностей у ПК або мережі дії користувачів мають бути чітко регламентовані.

3. У кожній організації має реалізовуватись чітка ієрархічна модель видання наказів (директор → керівник відділу → працівник) за умови неухильного виконання суворих правил щодо роботи з цінними документами.

Ц-дієві методи мають на меті порушити цілісність інформації. Наприклад, такого ефекту вдається досягти, якщо соціотехнік у той чи інший спосіб зміг замінити блоки коду нового програмного продукту.

Приклад 3.2. Розроблення Ц-дієвої атаки, спрямованої на отримання електронної пошти та паролю менеджера компанії.

Етап 1. На сайті компанії соціотехнік знаходить номер телефону служби підтримки. Дзвонить туди, пропонуючи свої послуги з певного питання, наголошуючи на їх особливій вигідності. Йому радять звернутися до менеджера компанії. Зрештою соціотехнік отримує електронну пошту менеджера, щоб надіслати йому всі умови надання послуги.

Етап 2. За отриманою електронною адресою соціотехнік здійснює пошук акаунтів жертви в різноманітних соцмережах. За змістом знайденої там інформації доходить висновку про характерні звички чи вподобання жертви.

Етап 3. На електронну пошту жертви соціотехнік надсилає листа, в якому йдеться про розробку надсучасного браузера, інтегрованого з безліччю функцій, що відповідають уподобанням жертви (це може бути інтегрована панель для прослуховування улюбленої радіостанції чи забезпечення інтеграції із соцмережами).

Соціотехнік пропонує взяти участь у тестуванні бета-версії браузера та отримати абсолютно безкоштовну ліцензію. Авторизація браузера відбувається за електронною адресою, із неминучим запитом на введення пароля. Уведений пароль передається по інтернету, аби стати надбанням соціотехніка, а встановлення браузера закінчується помилкою. Після цього, як правило, користувач швидко забуває про інцидент.

Рекомендації щодо захисту від Ц-дієвих атак.

1. Не можна встановлювати ПЗ із ненадійних джерел.

2. Неприпустимо вводити будь-які авторизаційні дані, якщо немає підтвердження надійності ресурсу чи ПЗ.

3. Для робочих і особистих потреб слід неодмінно мати дві різні електронні адреси. У разі найменшої підозри щодо можливості інциденту необхідно відразу змінити пароль до електронної пошти.

Д-дієві методи мають на меті порушити доступність інформації, наприклад досягти відмови мережного сервера, скориставшись ідентифікатором та паролем адміністратора безпеки, які вдалося роздобути.

Приклад 3.3. Розроблення Д-дієвої атаки, спрямованої на блокування доступу до бухгалтерської інформаційної бази 1С.

Етап 1. На сайті установи соціотехнік знаходить номер телефону її менеджера. Дзвонить йому, пропонуючи свої послуги з упровадження бази 1С. Дізнається, що потенційну жертву вже обслуговує в цьому плані інша компанія. Поміж словом вивідує її.

Етап 2. Подзвонивши до компанії — постачальника послуг 1С, зловмисник під виглядом потенційного користувача дізнається, як звуть директора, і з'ясовує, що кожний клієнт цієї компанії-постачальника має закріпленого за ним працівника.

Під час другого дзвінка до компанії-постачальника соціотехнік каже, що знайомі рекомендували йому певного працівника цієї компанії, який забезпечує високий рівень обслуговування, але він не може пригадати ім'я цієї людини. Зрештою зловмисник дізнається, як звуть працівника, що обслуговує потенційну жертву.

Етап 3. Удаючи із себе працівника компанії-постачальника, соціотехнік повідомляє, що його візит зумовлено потребою в оновленні конфігурації, необхідної для нормального функціонування 1С, додаючи, що з'явився замість свого колеги, який захворів. Від головного бухгалтера він отримує пароль до ІБ із адміністративними правами. Для «оновлення» блокує доступ до бази, і під час своєї «роботи» змінює у всіх облікових записах бази пароль. Насамкінець повідомляє, що доступ до бази було заблоковано, а тепер усе гаразд, і доступ найближчим часом відновиться. Після цього соціотехнік спокійно залишає компанію.

Рекомендації щодо захисту від Д-дієвих атак.

1. У разі будь-яких неочікуваних змін у складі обслуговувального персоналу слід неодмінно з'ясувати їх легітимність, звернувшись до відповідної компанії.

2. Після виконання технічного обслуговування необхідно пересвідчитись, що роботоздатність пошкодженої системи відновлено. За перебігом роботи працівника зі сфери технічного обслуговування потрібно уважно стежити.

3. Слід переконатись у легальності встановлюваного оновлення.

Атаки, унаслідок яких порушуються різні характеристики безпеки, належать до комбінованого типу. Саме так можна можна класифікувати КЦД-дії, що порушують *конфіденційність*, *цілісність* і *доступність* інформації.

За ***реляційними ознаками*** МСІ поділяються на *моно-* і *полімономні*, *моно-* і *поліполічні*.

Мономономні МСІ передбачають здійснення атаки, спрямованої з боку *одного атакувальника* на *одного атакованого*. Наприклад, здійснення дзвінка до тієї чи іншої особи із запитом щодо отримання потрібної інформації.

Полімономні МСІ, на відміну від мономономних, передбачають участь *двох чи більшої кількості атакувальників* за наявності *одного атакованого*. Це може бути, наприклад, відправлення електронної пошти від кількох соціотехніків (які, скажімо, видають себе за знайомих жертви) на адресу однієї особи. При цьому атакованого спробують переконати відкрити надану адресу інтернет-ресурсу, де його може спіткати неприємність завантажити шкідливе ПЗ.

Монополічні МСІ спрямовуються від *одного атакувальника* на *двох чи більшу кількість атакованих*. Наприклад, тут може йтися про отримання інформації, якої не може надати одна особа, побоюючись викриття. Тоді соціотехнік може телефонувати в різні дні різним особам для отримання потрібних йому даних.

Поліполічні МСІ поєднують у собі *полімономні* та *монополічні* технології. Відповідна атака реалізується спрямованими діями від двох чи більшої кількості атакувальників до двох чи більшої кількості атакованих. Група соціотехніків зможе швидше отримати потрібну їм інформацію від кількох осіб, аніж це було б у разі застосування трьох попередніх технологій, виокремлених за реляційними ознаками.

За ***ступенем складності*** МСІ поділяють на *прості*, *складні* та *системні*.

Прості МСІ реалізуються в кілька кроків. Наприклад, щоб дізнатись імена службовців того чи іншого відділу на підприємстві, соціотехнік може скористатися наявними інформаційними ресурсами компанії (наприклад, web-сайтом). Знайшовши номер телефону служби підтримки та зателефонувавши туди, соціотехнік може зробити запит щодо потрібної йому інформації.

Складні МСІ передбачають комбінування нескладних алгоритмів для отримання шуканої інформації. Наприклад, аби роздобути паролі користувачів, зловмисник може діяти так: з'ясувавши, чиї паролі потрібні, тобто встановивши імена відповідних осіб, він знаходить джерела потрібної інформації, а далі намагається отримати пароль у той чи інший відомий спосіб.

Системні МСІ реалізуються згідно з надзвичайно складним алгоритмом (розгалуженим, зі зворотними зв`язками та циклічними процесами). Тут ідеться про отримання інформації, яку неможливо роздобути інакше (коди нових продуктів ПЗ, відомості, необхідні для доступу до серверів систем безпеки).

За ***типом атакованого джерела*** МСІ поділяються на *ЕК-*, *ЛГ-*, *КН-* і *ВП-джерельні*, причому тип джерела визначається рівнем поінформованості атакованого.

ЕК-джерельні атаки розраховано на експерта, чиї професійні знання та контакти (як ділові, так і ті, що не стосуються роботи) забезпечують високу ерудицію в питанні, яке цікавить соціотехніка. Експерт може не лише видати базові матеріали, а й вивести на невідомі джерела інформації. Загальна надійність отримуваних у такий спосіб даних здебільшого дуже висока.

ЛГ-джерельні атаки орієнтуються на легковажну особу, здатну розголошувати мимохідь доступну їй інформацію, що може становити високу цінність. Утім із такого джерела можна почерпнути нісенітницю, зокрема й будь-яку навмисну дезінформацію.

КН-джерельні атаки спрямовуються на осіб (контактерів), які так чи інакше спілкуються (або колись спілкувалися) з об'єктом (особою, групою осіб, організацією), що становить інтерес для соціотехніка. Здебільшого це випадкові ділові партнери, родичі та знайомі, працівники сервісу і т. ін. Контактери здатні не тільки повідомляти різні факти, а й сприяти в наближенні до об'єкта або й брати участь у вилученні в нього потрібної інформації.

ВП-джерельні атаки передбачають використання випадкового індивіда, котрий не розглядається як потенційний інформатор, але є носієм важливої інформації. З огляду на випадковість спілкування з такою особою і непередбачуваність її повідінки соціотехніки не покладаються на таке джерело, хоча й намагаються використати його повною мірою.

Якщо під час атаки задіяно різні види атакованих джерел, то вона належить до типу комбінованих. Наприклад, ЕККН-джерельна атака пов'язана з експертом та контактером.

За ***типом доступу до інформації*** виокремлюють методи *В*-, *К*- та *С*-доступу.

Методи ***В-доступу*** стосуються інформації, що міститься у відкритих джерелах (друковані періодичні видання, інтернет-ресурси, засоби масової інформації, база даних тієї чи іншої служби підтримки тощо.

Методи ***К-доступу*** зорієнтовано на конфіденційну інформацію, тобто не секретну, але таку, доступ до якої контролюють певні особи, що несуть за неї відповідальність. Це, наприклад, імена, номери телефонів, поштові адреси, посади і т. ін.

Методи ***С-доступу*** мають на меті здобуття інформації із грифом секретності, привілеї доступу до якої має обмежене коло довірених осіб (секретні коди доступу, новітні розробки, секретні матеріали тощо).

Якщо соціотехнічна атака поєднує в собі спроби отримання доступу до різних типів інформації, то йдеться про комбінований метод нападу, коли поряд із переліченими раніше прийомами вводиться в дію певна сукупність засобів і «параметрів оточення». Прикладом може бути атака ВК-доступу, зорієнтована як на відкриту, так і на конфіденційну інформацію.

З огляду на сказане множину всіляких кібератак із залученням соціальної складової можна поділити на три категорії за такими характерними ознаками:

1) *засобами здійснення* — використання при спілкуванні телефону, електронної пошти, інтернету (у реальному часі), звичайної пошти або особистої харизми в ході зустрічі;

2) *рівнем стосунків з об'єктом розвідки* — офіційний, товариський чи дружній;

3) *ступенем доступу об'єкта до ІКС* — високий в адміністратора, середній у начальника, низький у користувача.

Отже, соціотехнік має у своєму розпорядженні чимало методів, що дадуть йому змогу:

- провести пошук необхідної інформації у відкритих джерелах;
- отримати пароль або коди доступу до потрібної системи;
- надіслати потенційній жертві шкідливе безплатне ПЗ або патч для встановлення чи вірус троян на додаток до електронного листа;
- не знехтувати вмістом сміттєвих контейнерів компанії як джерелом непересічної інформації;

• відвідати компанію, виступивши як клієнт, співробітник постачальника або виробник загального і спеціального ПЗ, представник партнерської компанії або законодавчого органу;

• проникнути в компанію під виглядом нового керівника або співробітника, представника обслуговувального персоналу, знайомого чи родича;

• зробити псевдопомилкові дзвінки в компанію або до її співробітників, представившись довіреною людиною або співробітником, аби роздобути необхідну інформацію;

• налагодити персональні стосунки зі співробітниками компанії;

• працевлаштуватись у компанію — потенційну жертву атаки.

3.3. Алгоритм соціотехнічної атаки: етапи проведення, супутні уразливості та основні ризики

Як уже зазначалося, головна мета соціотехнічних атак — отримати несанкціонований доступ до захищених ІКС (паролі, персональні дані тощо). Для цього неавторизовані користувачі діють згідно з наведеною на рис. 3.9 схемою Шейнова [120].

Рис. 3.9. Алгоритм дій порушників методом соціальної інженерії

Щоб реалізувати схему Шейнова, порушник має:

1) визначити мету операції, з'ясувавши, якого роду інформація становить об'єкт полювання і де вона міститься;

2) зібрати інформацію про об'єкт розвідки, що дасть змогу вивчити його психологію (джерелом інформації може бути практично все: результати аналізу трафіку, пошти, навіть касових чеків. Під «об'єктом» розуміється жертва, на яку націлено атаку неавторизованого користувача);

3) розробити план дій, провести моральну підготовку та тренування (опрацювати сценарій, зіставити кожне його слово з психологічною моделлю потенційної жертви);

4) виявити найбільш привабливі мішені впливу;

5) створити умови, необхідні для здійснення впливу соціального інженера на об'єкт розвідки, тобто змусити жертву до дій, потрібних зловмиснокові. Наприклад, ключем до маніпулювання може стати гостра потреба потенційної жертви в грошах, про що соціальному інженерові вдалося дізнатися на етапі збору інформації. Заходи СІ мають активізувати атакованого до невідкладних дій щодо роздобування грошей;

6) сформувати звіт і подати його замовникові.

Узагальнений алгоритм соціотехнічної атаки, спрямованої на реалізацію 2-го етапу схеми Шейнова, наведено на рис. 3.10. Тут дії соціотехніків подано одновимірним масивом Д[i], який позначає необхідну додаткову інформацію ($i = \overline{1,n}$, де n — кількість додаткової інформації).

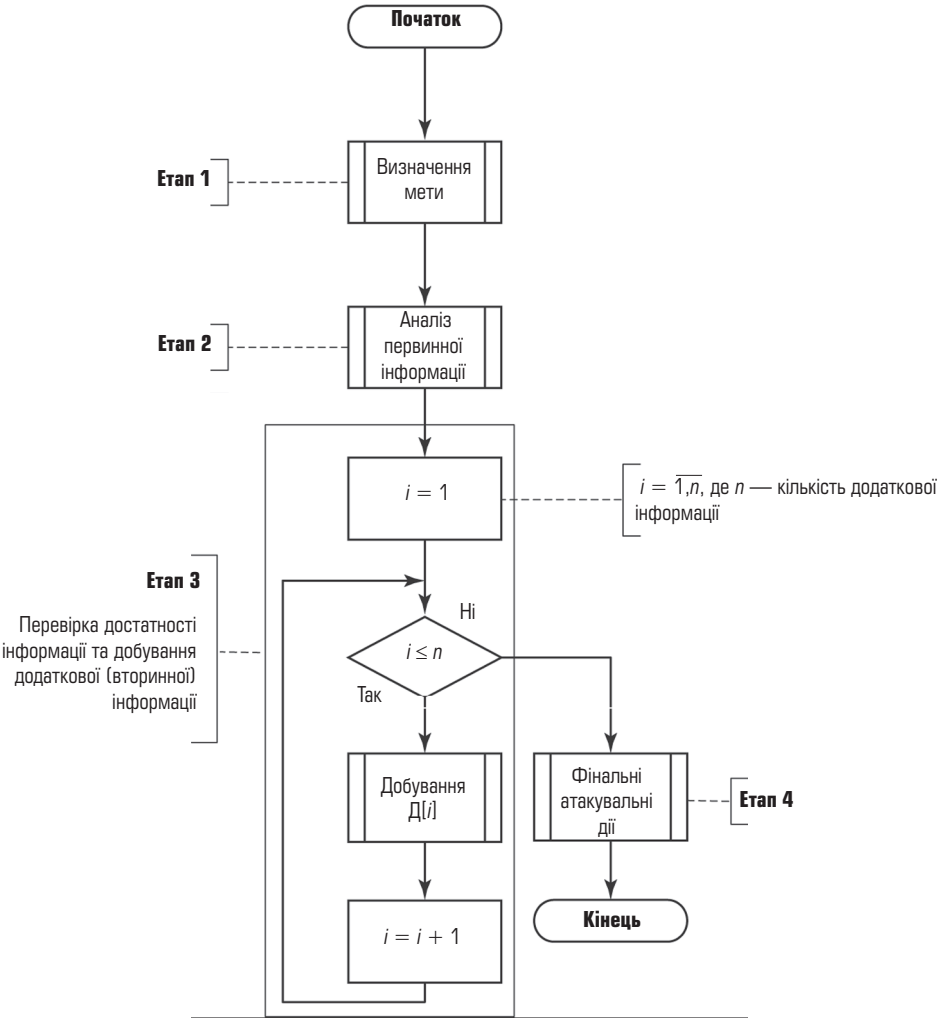


Рис. 3.10. Узагальнений алгоритм соціотехнічної атаки

Алгоритм передбачає неодмінне виконання таких етапів [121; 122] (Додаток В):

Етап 1. Визначення мети.

Етап 2. Аналіз джерел, з яких можна добути інформацію, потрібну на початковому етапі. Насамперед розглядаються відкриті джерела, доступ до яких необмежений.

Етап 3. Перевірка достатності добутої інформації для здійснення атаки. Якщо постає потреба в додаткових даних, то соціотехнік визначає кроки, спрямовані на добування потрібної інформації. У протилежному випадку соціотехнік переходить до наступного етапу.

Етап 4. Фінальні атакувальні дії.

Природно, що при проведенні будь-якої атаки з використанням соціального інжинірингу (коли нападник видає себе за іншу особу; відвертає увагу жертви; нагнітає психологічну напругу тощо) так само, як і здійснення будь-яких інших кібератак, одним із неодмінних атрибутів є класифікація ступеня доступу до інформації в разі успішно проведеної атаки. Цей ступінь залежить від рівня підготовленості соціального інженера, а також від того, хто виступає в ролі жертви (див. табл. 2.3). Надалі, коли розроблено сценарій атаки, соціоінженери використовують такі основні компоненти ПЗ, як повідомлення. Адже кожне з них, у свою чергу, поряд з інформаційним наповненням містить певні відомості про відправника, а також посилання на злоякісне ПЗ і засіб доставляння (електронна пошта, служба миттєвих повідомлень і/або однорангові мережі).

Приклад 3.4. Розроблення соціотехнічної атаки, спрямованої на отримання кредитної картки та номера мобільного телефону начальника проекту нової продукції фірми *A* для фірми-конкурента *B*.

З урахуванням наведених у табл. 2.3 обмежень алгоритм здійснення такої атаки засобами MCI можна подати схемою (рис. 3.11), що включає в себе розглянуті далі етапи.

Етап 1. Визначення номера кредитної картки та мобільного телефону начальника проекту нової продукції фірми *A* для фірми-конкурента *B*.

Етап 2. Пошук шляхів виходу на сайт компанії *C*, де міститься телефон служби підтримки (довідкової служби). Із цією метою представники фірми *B* обрали компанію *C*, оскільки потенційна жертва — постійний її клієнт.

Етап 3. З'ясовування номера телефону та імені потрібного службовця відділу клієнтів. Для цього соціотехнік має бути обізнаний із процедурою видачі інформації про клієнтів. Зателефонувавши до служби підтримки компанії *C*, соціотехнік представляється клієнтом, повідомляє про викрадення кредитної картки в особи, яка є клієнтом фірми *C*, здійснюючи при цьому запит щодо потрібної йому інформації (які дані і в який спосіб надає клієнт та чи надійно вони зберігаються). На цей запит соціотехнік отримує таку відповідь: кожний клієнт має власний порядковий номер, а його персональні дані, номери контактних телефонів, кредитних карток тощо надійно зберігаються в базі компанії. Утім тим часом соціотехнік дізнається про те, куди потрібно зателефонувати та як зробити запит щодо номера кредитної картки і мобільного телефону начальника проекту нової продукції компанії *C*, аби не викликати підозри. І все ж для здійснення атаки соціотехнік має себе якось ідентифікувати. Знаючи структуру компанії *C* (інформація з відповідного сайту), він вибирає регіональне відділення в іншому місті. Телефонуючи у службу підтримки, соціотехнік дізнається ім'я та телефон працівника відділу рахунків.

Етап 4. Фінальним кроком є дзвінок у відділ клієнтів компанії *C*. Соціотехнік представляється службовцем відділу клієнтів регіонального відділення, називаючи відповідне ім'я. Далі повідомляє, що його комп'ютер інфіковано вірусом, а через це в даний момент не можна відкрити базу, щоб задовольнити запити серйозного клієнта. Після чого просить надати йому потрібну інформацію, називаючи лише ім'я клієнта [122].

Як бачимо, головні ризики в разі успішної реалізації соціотехнічної атаки, спрямованої на отримання номерів кредитної картки та мобільного теле-

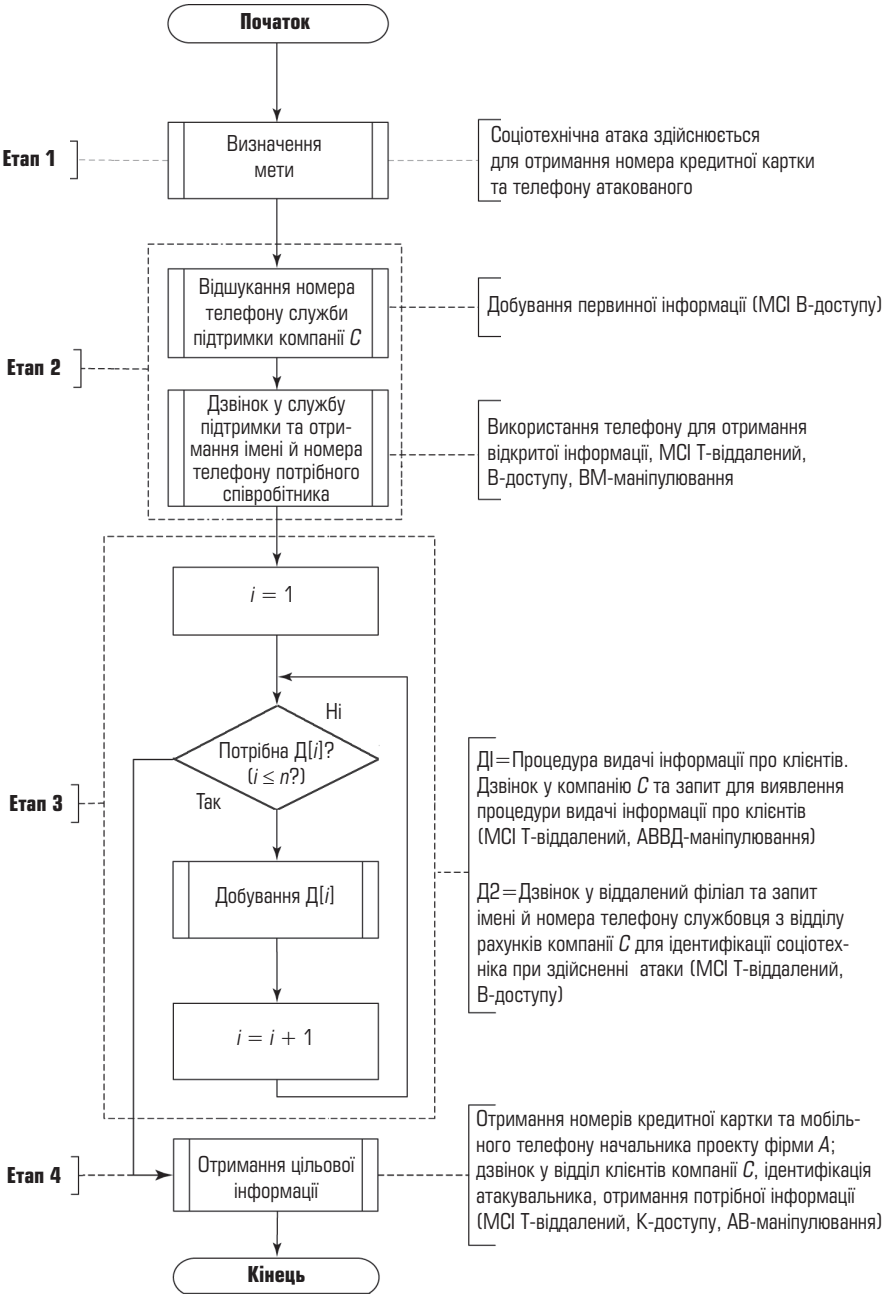


Рис. 3.11. Приклад алгоритму здійснення соціотехнічної атаки

фону начальника проекту з виготовлення нової продукції фірми *A* в інтересах фірми-конкурента *B* можуть бути такі [4–6]: витік конфіденційної інформації (ВКІ); завдання збитку репутації організації (ЗЗРО); зниження працездатності організації (ЗПО); перевитрата ресурсів (ПрР) та фінансові втрати (ФВ). На результат такої атаки можуть суттєво вплинути уразливості, що характеризує табл. 3.2 [123].

Таблиця 3.2

Уразливості корпоративної мережі, що сприяють проведенню атак неавторизованими користувачами

Напрям атаки	Нинішній стан справ	Коментар
	Мережні атаки	
Електронна пошта	На комп'ютерах усіх співробітників установлено програму Microsoft Outlook	У кожного співробітника свій електронний ящик, чим унеможливлюється контроль за вхідною поштою
Інтернет	Співробітники використовують інтернет у виробничих і особистих цілях	Користування інтернетом в особистих цілях заважає контролювати дії співробітників
Плинні додатки	—	На сучасний момент жодні технічні засоби захисту від плинних додатків в організації не використовуються
Служба миттєвого обміну повідомленнями	Прийняті в організації методи роботи припускають неконтрольоване використання систем миттєвого обміну повідомленнями	—
	Телефонні атаки	
Корпоративна телефонна станція	Телефони використовуються без визначника внутрішніх і зовнішніх номерів	—
Служба підтримки	У цей час функції служби підтримки безсистемно виконує технічний відділ	Процеси надання послуг підтримки мають набути системності
	Пошук інформації в смітті	
Внутрішнє сміття	Кожне відділення позбувається власного сміття самостійно	—
Зовнішнє сміття	Сміттєві контейнери розташовуються на території організації. Вивіз сміття здійснюється в певний день тижня	—
	Особистісні підходи	
Безпека офісів	Усі офіси залишаються незамкненими протягом усього робочого дня	—
Співробітники, що працюють удома	Письмові стандарти забезпечення безпеки систем співробітників, що працюють удома, відсутні	—
	Інші напрями атак і уразливості, специфічні для компанії	
Підрядники, що працюють на об'єктах	—	Немає жодної інформації про співробітників компанії та не здійснюється щодо них політика безпеки

Використовуючи табл. 3.2, можна визначити вимоги щодо здійснення політики безпеки, а також типів і рівнів ризику для фірми *A* (табл. 3.3) [124; 125].

Соціотехнічну атаку, розглянуту в табл. 3.3, можна класифікувати як деполітизаційну, Т-віддалену, аверсну, АВВМ-маніпульовану, К-дієву, монополічну, складну та ЕК-джерельну атаку ВК-доступу.

Таблиця 3.3

Форма для визначення можливих вимог щодо забезпечення безпеки та оцінювання факторів ризику

Напрям атаки	Вимоги щодо здійснення політики безпеки	Тип ризику	Рівень ризику	Дія
	Викласти головні положення ПБ щодо захисту від загроз, які спираються на методи соціального інжинірингу, у письмовій формі			
	Внести пункт про необхідність дотримання ПБ у стандартний контракт зі співробітником			
	Внести пункт про необхідність дотримання ПБ у стандартний контракт із підрядником			
Мережні атаки				
Електронна пошта	Прийняти ПБ, що регламентує дії співробітників при отриманні вкладень конкретних типів	ВКІ ЗЗРО ФВ	**3-й**	Розроблено ПБ щодо використання електронної пошти, створено єдиний поштовий клієнт-сервер
Плинні додатки	Включити в політику використання інтернету явні вказівки стосовно того, що варто робити з появою плинних діалогових вікон	ВКІ ПрР ФВ	**3-й**	Розроблено політику використання комп'ютерів
Інтернет	Прийняти ПБ, що регламентує використання інтернету	ВКІ ЗПО ПрР ФВ	**4-й**	Розроблено політику використання інтернету
Служба миттєвого обміну повідомленнями	Прийняти політику, що визначає підтримувані й припустимі клієнтські програми миттєвого обміну повідомленнями	ВКІ ЗПО	**2-й**	Розроблено правила щодо роботи зі службами миттєвих повідомлень
Телефонні атаки				
Корпоративна телефонна станція	Прийняти політику керування обслуговуванням корпоративної телефонної станції	ВКІ ФВ	**2-й**	Розроблено політику роботи під час телефонних переговорів
Служба підтримки	Прийняти політику, що регламентує надання доступу до даних	ВКІ ПрР	**2-й**	Розроблено політику управління доступом
Пошук інформації у смітті				
Паперове сміття	Прийняти політику утилізації паперового сміття	ВКІ ЗЗРО ФВ	**3-й**	Розроблено інформаційну ПБ
Електронне сміття	Прийняти політику утилізації електронного сміття	ВКІ ЗЗРО ФВ	**3-й**	Розроблено інформаційну ПБ
Особистісні підходи				
Фізична безпека	Прийняти політику роботи з відвідувачами	ВКІ ФВ	**2-й**	Розроблено ПБ роботи з відвідувачами
Безпека офісів	Прийняти політику управління ідентифікаторами й паролями користувачів	ВКІ ЗЗРО ФВ	**3-й**	Розроблено ПБ ідентифікації та автентифікації
Співробітники, що працюють поза об'єктом	Прийняти політику використання мобільних комп'ютерів поза організацією	ВКІ ЗЗРО ФВ	**3-й**	Розроблено ПБ щодо роботи поза організацією
Інші напрями атак і уразливості, специфічні для організації				
Підрядники, що працюють на об'єктах організації	Прийняти політику перевірки співробітників сторонніх організацій	ВКІ ЗЗРО ТР ФВ	**4-й**	Підписано угоду про нерозголошення відомостей

3.4. Загрози соціального інжинірингу

Останнім часом при організації та проведенні атак соціоінженери застосовують такі інструменти (канали) нападу [126; 127]:

- електронну пошту (e-mail);
- телефонний зв'язок;
- аналіз сміття;
- особистісні підходи;
- реверсивну соціальну інженерію.

Завдяки відносній анонімності інтернету соціоінженерам удається вийти на об'єкт атаки й скористатися його системними ресурсами.

3.4.1. Загрози з використанням електронної пошти (e-mail)

Техніку застосування електронної пошти для розповсюдження фішинг-повідомлень із деструктивним інформаційним наповненням уперше було докладно описано 1987 року, а сам термін «фішинг-атака» з'явився 2 січня 1996 року в новинній групі «alt.online-service.America-Online» мережі «Usenet». Сьогодні це, мабуть, найпопулярніша схема соціального інжинірингу, реалізовуючи яку, соціоінженери вдаються до атак:

- типу «людина посередині» (Man-in-the-middle);
- із використанням крос-сайтових сценаріїв (Cross-site Scripting);
- із підміною URL та інші.

Одними з перших можливості фішингу наприкінці минулого століття реалізували розробники вірусів «Melissa» та «LoveLetter». Віруси через e-mail надсилали користувачам власні копії з ознакою важливого повідомлення певного змісту. Потрібні адреси вибирались з адресної книги інфікованої ПЕОМ.

Механізм імітації при використанні e-mail та ІМ ілюструє рис. 3.12, де зловмисник (на рисунку найбільш затінений), виступаючи в ролі відомого своїм потенційним жертвам користувача, надсилає їм електронну пошту або ІМ-повідомлення. Адже налаштованість на знайомого кореспондента послаблює користувальницьку пильність і захищеність. У результаті дій так званих *phishing kit* — утиліт, які дозволяють дуже швидко створювати фішинг-сайти, інфікуються, як правило, усі ПЕОМ, власники яких зацікавились цим повідомленням.

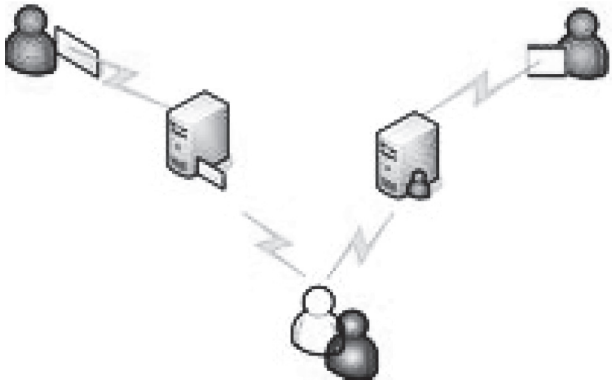


Рис. 3.12. Структурно-логічна схема дій зловмисника з використанням можливостей e-mail і служби миттєвих повідомлень (ІМ)

Уже майже 10 років тому активність фішингу була дуже висока. За даними звіту компанії APWG (Anti-Phishing Work Group), уже тоді щомісяця вдавалося виявляти понад 20 000 фішингових розсилань та близько 12 000 фішерських web-сайтів. Наприклад, лише в першому півріччі 2006 року фішери відправили 157 тис. унікальних листів, що на 81% перевищило їхню кількість, зафіксовану у другому півріччі 2005 року. На сучасному етапі розвитку IT-індустрії без цього вже не обходиться жодний витік персональних даних. Фішингові розсилання (рис. 3.13) із відомостями, що викликають тривогу (наприклад, містять загрози щодо закриття банківських рахунків), пропонують неправдоподібно привабливі угоди, благають про пожертвування (наприклад, від імені благодійних організацій), обіцяють великі грошові вигоди з мінімальними зусиллями, насправді являють собою підготовчі кроки для нападу на клієнтів банків і електронних платіжних систем. Здобиччю фішерів дедалі частіше стають користувачі соціальних мереж.

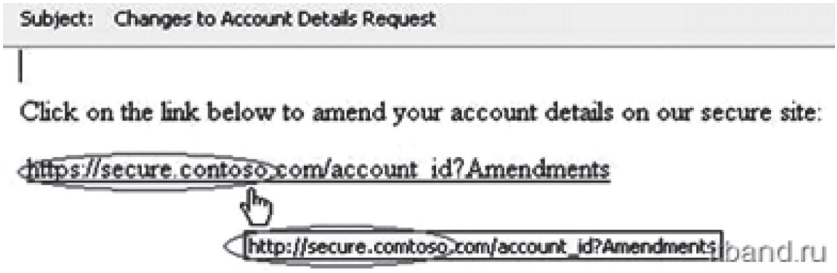


Рис. 3.13. Web-сторінка e-mail фішинг-повідомлення

Зауважимо, що на рис. 3.13 подано зовні припустиме посилання на сайт управління облікового запису Contoso. Утім при уважному розгляді можна знайти такі суперечності:

а) із тексту повідомлення (використовуючи https) бачимо, що сайт безпечний. Проте на екрані показано, що сайт фактично використовує http;

б) назва компанії в пошті — «Contoso», а в посиланні — «Comtoso».

Камуфляж, використовуваний у таких випадках, надає електронній пошті більш правдоподібного вигляду. У листі часто міститься пряме посилання на сайт, який за зовнішнім виглядом неможливо відрізнити від справжнього (рис. 3.14). При цьому кожний фішинг-лист маскується під запит про користувальницьку інформацію, що нібито має полегшити користувачеві встановлення відновлення або забезпечити додаткове обслуговування (рис. 3.15).

Вийшовши на такий сайт користувач може надати зловмисникам цінну інформацію, яка, наприклад, дозволить їм отримати доступ до акаунтів і банківських рахунків.

Головні правила, які має виконувати користувач, аби не стати жертвою фішингової атаки:

- не відкривати підозрілих посилань, отриманих навіть у повідомленнях від знайомих людей;
- не встановлювати й не запускати ігри та додатки, рекламовані у спам-розсиланнях;
- за жодних обставин не вводити логин і пароль від свого облікового запису в «У контакті» на сайтах, URL яких відрізняється від vkontakte.ru;
- використовувати сучасне антивірусне програмне забезпечення.

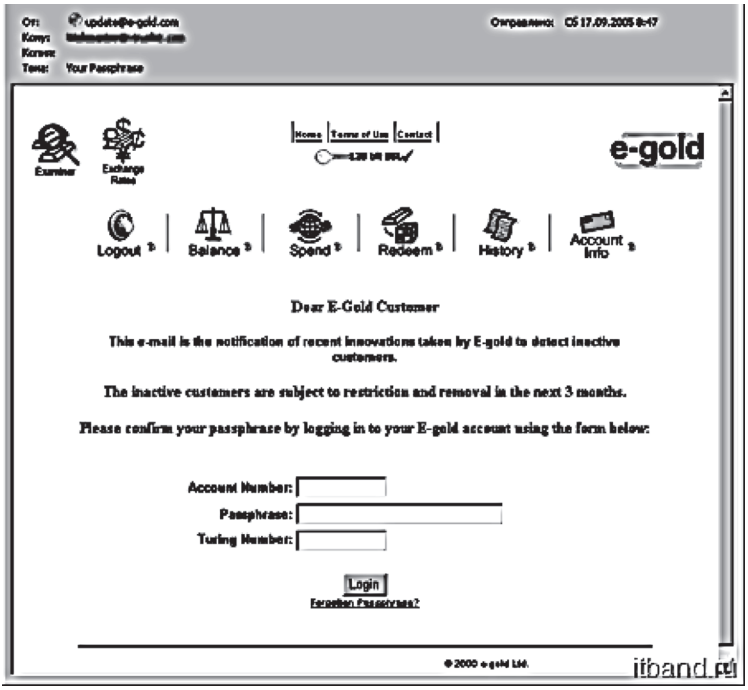


Рис. 3.14. Зразок фішингового листа підробленою mail-адресою відправника

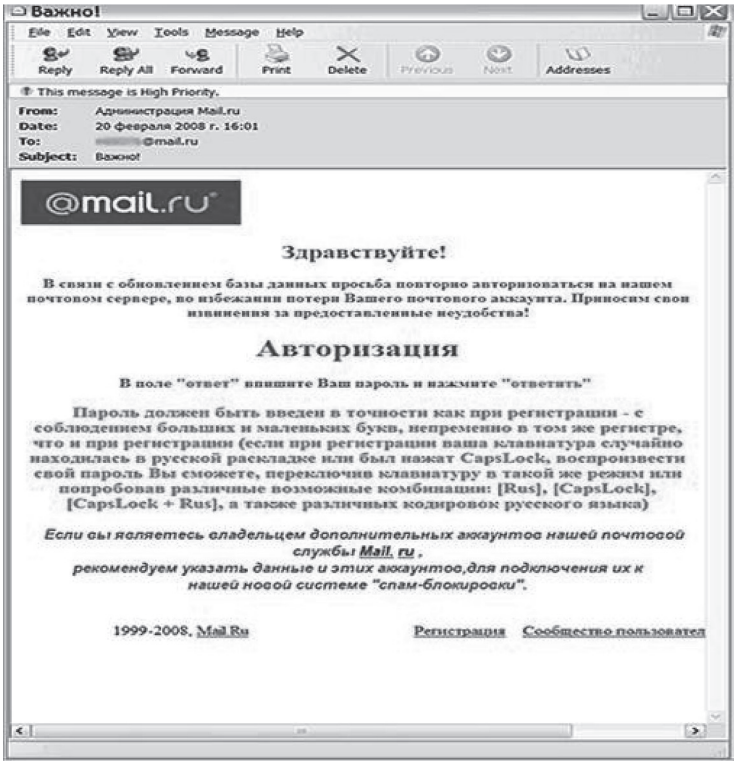


Рис. 3.15. Зразок фішингового листа користувачам пошти Mail.ru

У липні 2006 року з'явився новий різновид фішингу, який відразу було названо ***вішингом***. Атака спирається на використання системи попередньо записаних голосових повідомлень, мета яких — відтворити «офіційні дзвінки» від банківських та інших IVR (*Interactive Voice Response*) систем. Принцип дії таких атак унаочнює рис. 3.16. Потенційна жертва отримує зазвичай запит (найчастіше через фішинг електронної пошти) про необхідність зв'язку з банком для підтвердження або відновлення якоїсь інформації. При цьому система вимагає автентифікації користувача за допомогою введення PIN-коду або пароля.

Рис. 3.16. Принцип дії IVR систем

Основна різниця між фішингом і вішингом така: у разі вішингу в повідомленні міститься прохання подзвонити на певний міський номер. При цьому зачитується повідомлення, в якому потенційну жертву просять повідомити свої конфіденційні дані. Власників такого номера знайти непросто, оскільки з розвитком IP-телефонії дзвінок на міський номер може бути автоматично переспрямований у будь-яку точку земної кулі.

Відповідно до інформації від Secure Computing шахраї конфігурують автонабирач номера (war dialler) що функціонує в певному регіоні, і при відповіді на дзвінок відбувається таке:

- автовідповідач попереджає споживача, що з його картою чиняться шахрайські дії, і дає інструкцію — передзвонити за певним номером негайно;
- коли за цим номером здійснено дзвінок, на іншому кінці проводу відповідає типово комп'ютерний голос, який повідомляє, що абонент має пройти звірення даних і ввести 16-цифровий номер карти з клавіатури телефону;
- тільки-но номер уведено, вішер стає власником всієї необхідної інформації (номер телефону, повне ім'я, адреса);
- далі, використовуючи цей дзвінок, можна зібрати й додаткову інформацію, таку як PIN-код, термін дії карти, дата народження, номер банківського рахунку тощо.

Поряд із дуже небезпечними фішинговими та вішинговими атаками в мережі існує ще серйозніша загроза — ***фармінг*** (*pharming*) — перенапрямлення жертви за помилковою (хибною) адресою. Для цього може використовуватися деяка навігаційна структура, скажимо файл hosts, система доменних імен (*domain name system — DNS*). Механізм фармінгу має багато спільного зі стандартним вірусним інфікуванням. Жертва відкриває поштове послання або відвідує якийсь web-сервер, на якому виконується скрипт-вірус. При цьому спотворюється файл hosts. У результаті жертва потрапляє на один із помилкових сайтів.

Механізмів захисту від фармінгу й досі просто не існує.

Ще один різновид фішинг-атак — ***spear-phishing*** (вилов риби за допомогою списа/дротика). Це вузько спрямовані й скоординовані атаки на організацію або конкретного користувача з метою одержання критично важливих даних. У цьому разі зловмисник здійснює більш правдоподібний обман, максимально наближаючись до цільової групи й використовуючи для маскування внутрішню інформацію компанії. Така атака вимагає більшого знання адресата, але вона може бути й більш успішною.

Для того щоб класифікувати напади й визначити ризики в компанії, доцільно використовувати матрицю векторів нападу, цілей нападу та описів останніх (табл. 3.4).

Таблиця 3.4

Інтерактивні поштові напади (e-mail)

Мета нападу	Опис	Спрямованість
Викрадення інформації, що належить компанії	Хакер відіграє роль внутрішнього користувача, щоб отримати інформацію компанії	Конфіденційна інформація. Ділова довіра
Викрадення фінансової інформації	Хакер використовує фішиг, вішинг, фармінг або spear-phishing, щоб запросити конфіденційну інформацію (наприклад, подробиці облікового запису)	Гроші. Конфіденційна інформація
Завантаження mailware	Хакер в обманний спосіб досягає відкриття гіперпосилання або вкладення, унаслідок чого інфікує мережі компанії	Доступність
Завантаження хакерського ПЗ	Хакер, досягнувши в обманний спосіб відкриття гіперпосилання або відкриття вкладення, завантажує шкідливе ПЗ	Атака на ресурси. Доступність. Гроші

Щоб якомога ефективніше протидіяти хакерським нападам на базі соціальної інженерії, потрібно з недовірою ставитись до будь-чого несподіваного у своїй поштовій скриньці. Для впровадження такого самого підходу в організації необхідно формувати політику безпеки, спираючись на посібник з питань поводження з електронною поштою, який торкається, зокрема, використання вкладень у документах; гіперпосилань у документах; запитів про персонал чи інформації про внутрішні справи компанії; запитів про персонал або інформації про зовнішню політику компанії.

Приклад 3.5. Плинні додатки та діалогові вікна.

Більшість співробітників компанії переглядає інтернет із особистих мотивів. При цьому вони наражаються на небезпеку контакту зі зловмисниками,

що спираються на соціальну інженерію. Хоча зловмисники можуть і не мати на меті нападу на якусь конкретну компанію, усе ж не виключено, що вони через персонал отримають доступ до її ресурсів. Одна з най популярніших цілей полягає в тому, аби впровадити поштовий сервер у межах певної комп'ютерної мережі. Тоді через нього зловмисник зможе почати фішинг або інші поштові напади (табл. 3.5) на будь-які сторонні компанії чи на фізичних осіб.

Таблиця 3.5

Онлайн-атака за допомогою плинного додатка та діалогового вікна

Мета нападу	Опис дій	Спрямованість
Викрадення персональної інформації	Хакер запитує персональну інформацію співробітника	Конфіденційна інформація. Гроші
Завантаження mailware	Хакер, маючи на меті інфікувати мережі компанії, хитрощами спонукає користувача відкрити гіперпосилання чи вкладення	Доступність
Завантаження хакерського ПЗ	Хакер обманює користувача, і той під впливом цього зловмисника відкриває гіперпосилання чи вкладення, завантажуючи тим часом інфіковане ПЗ	Атака на ресурси. Доступність. Гроші

Існують два найпростіші методи спровокувати користувача, аби він зреагував на посилання в діалоговому вікні. Йому можна надіслати або попередження щодо певної проблеми, котре не викликає жодної підозри, або прикладне повідомлення про ті чи інші помилки з пропозиціями стосовно додаткових послуг (наприклад, може йтися про безплатне завантаження, яке нібито змусить комп'ютер отримувача цієї інформації працювати швидше).

Захист користувачів від плинних додатків полягає насамперед у розумінні того, що це суцільне шахрайство і що за жодних обставин не можна натискати посилання на плинних вікнах, не порадившись, наприклад, із персоналом служби підтримки. У свою чергу, зазначений персонал має відповідно ставитися до звернень користувачів по допомогу, особливо коли труднощі виникають під час перегляду інтернету. Така взаємна довіра має формуватись на базі неухильно здійснюваної політики безпеки щодо роботи в мережі Інтернет.

Приклад 3.6. Instant Messaging.

Миттєве передавання повідомлень (IM) — порівняно новий сервіс, що створює надзвичайно сприятливе середовище для нападів із використанням соціальної інженерії. Саме безпосередність і дружній інтерфейс IM перетворюють його на ідеальний засіб для нападів. Адже користувачі сприймають цю службу як звичайний телефон, не пов'язуючи її з потенційними загрозами ПЗ. Основні атаки з використанням IM — це гіперпосилання на malware і розсилання злоякісного ПЗ (табл. 3.6). Результативності таких нападів сприяє невимушеність IM, що разом з опцією надання прізвиська значно розширюють можливості атакувальників.

Щоб не відмовлятись від зручного, хоча й ризикованого сервісу IM, необхідно включити IM безпеку в політику безпеки компанії, передбачивши неухильне виконання таких п'яти правил:

1) уведення стандарту на єдину IM платформу;

2) визначення параметрів настроювання безпеки розгортання;

Таблиця 3.6

Напади з використанням ІМ передавання повідомлень

Мета нападу	Опис дій	Спрямованість
Запит про конфіденційну інформацію компанії	Хакер, виконуючи роль колеги, використовує ІМ імітацію, аби зробити запит щодо ділової інформації	Конфіденційна інформація. Довіра
Завантаження malware	Хакер, аби інфікувати мережі компанії, спонукає користувача до відкриття гіперпосилання чи вкладення, і в такий спосіб досягає поставленої мети	Доступність
Завантаження хакерського ПЗ	Хакер уводіть користувача в оману, і той, відкриваючи під впливом зловмисника гіперпосилання чи вкладення, завантажує хакерське ПЗ	Атака на ресурси. Доступність. Гроші

3) застереження користувачів щодо небезпеки, прихованої в настроюванні за замовчуванням;

4) установлення стандартів пароля;

5) упровадження в практику посібника з використання ІМ.

Приклад 3.7. Зламування поштової скриньки.

Найбільш уразливе місце в комп'ютері — cookies файли. Найпростіший спосіб їх викрасти – скопіювати собі на флешку. Як це зробити в умовах, коли користувач постійно стежить за власною ЕОМ?

Можна написати простий VBS скритп, що копіюватиме ці файли, і поставити його на автозавантаження. Скрипт разом із фільмами, музикою або іграми необхідно записати на флешку та підкинути потенційній жертві, яка при спробі прочитати інформацію з флеш-пам'яті негайно запустить і скрипт:

```
[autorun]
open = потрібний скрипт.vbs
```

Для зламування поштової скриньки можна задіяти також і кейлогери — програми, що записують всі натискання клавіш. Дії зловмисника в цьому разі такі самі, як і в попередньому випадку. Тільки в автозавантаження прописується не скрипт, а кейлогер. Жертва вставляє флешку в комп'ютер — кейлогер запускається. Через певний час жертва вирішить перевірити нову пошту й уведе логін із паролем, які негайно буде надіслано зловмисникові.

3.4.2. Загрози при використанні телефонного зв'язку

Телефон також пропонує унікальний спосіб нападу для хакерів. Ідеться про можливість зламу телефонного зв'язку, здійснюваного за IP-протоколом (VoIP). Відповідні дії становлять головну загрозу для компанії, причому VoIP-імітація стає настільки ж поширеним явищем, як і введення в оману за допомогою e-mail та ІМ.

У процесі організації й проведення мовленєвих (*phreaking*) атак діють, як правило, так:

- просять надати певну інформацію, імітуючи законного користувача, щоб або звернутися до телефонної системи безпосередньо, або отримати вилучений доступ до комп'ютерних систем;
- отримують доступ до «вільного» використання телефону;
- отримують доступ до системи комунікацій.

Найбільш природний підхід хакера — симулювання ролі телефонного інженера (3.17).

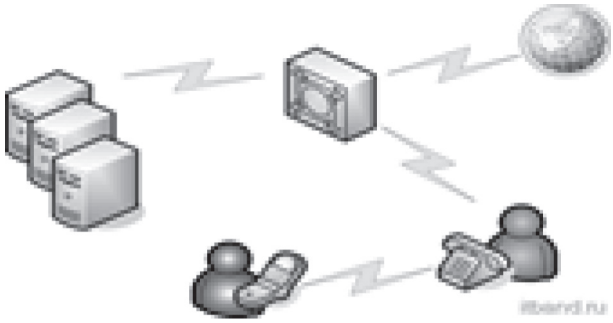


Рис. 3.17. Схема атаки на офісну АТС

Запити про інформацію або доступ по телефону — порівняно не ризикована форма атаки. Якщо в адресата виникає певна підозра або він відмовляється виконувати запит, то хакер може просто покласти трубку. Але такі атаки більш складні, аніж ті, коли хакер просто дзвонить у компанію, прохаючи надати ідентифікатор чи пароль користувача. Зазвичай діє сценарій, коли перш ніж мимохідь відбувається запит про особисту чи ділову інформацію, лунає прохання або пропозиція щодо якоїсь довідки (табл. 3.7).

Таблиця 3.7

Телефонні напади

Мета нападу	Опис дій	Спрямованість
Запит інформації компанії	Хакер виконує роль законного користувача, аби отримати конфіденційну інформацію	Конфіденційна інформація. Ділова довіра
Телефонний запит інформації	Хакер прикидається телефонним майстром, щоб отримати доступ до офісної АТС і далі здійснювати зовнішні запити	Ресурси. Гроші
Звернутися до комп'ютерних систем, скориставшись офісною АТС	Хакер зламує комп'ютерні системи, використовуючи офісну АТС, і захоплює інформацію або починає керувати нею, аби зрештою інфікувати malware	

Зловмисник діє за таким алгоритмом:

1) вибирає об'єкт нападу за телефонною книгою, відшукуючи компанію, де є телефон секретаря;

2) здійснює дзвінок секретареві й з'ясовує ім'я особи, з якою можна проконсультуватися з приводу тих чи інших проблем, пов'язаних із роботою системи;

3) здійснює дзвінок деякій іншій людині, чий номер телефону є в книзі і яка, за його припущенням, має доступ до системи;

4) представляється (зрозуміло, під псевдонімом) як помічник тієї особи, ім'я якої він розвідав під час першого дзвінка, повідомляючи, що з огляду на переінсталяцію системи адміністратор дав завдання замінити паролі всім користувачам;

5) дізнається ім'я входу та колишній пароль, повідомляючи новий пароль.

Якщо доступ до системи відбувається за допомогою телефонних ліній, то зв'язується із секретарем, повідомляючи, що не вдається додзвонитися до системи, і просить назвати правильний номер телефону.

Приклад 3.8.

Адміністратор, як відомо, доволі часто стикається із ситуацією, коли користувач, який довго «не входив» у систему, не пам'ятає нічого зі службової інформації, необхідної для такого входження (окрім свого «імені»). У таких випадках користувач може зловживати телефонним правом.

Змоделюємо такий випадок на прикладі UNIX-системи.

Дзвінок адміністраторові.

Хакер: Здрастуйте, ви адміністратор?

Адміністратор: Так.

Х.: Вибачте, що відриваю вас від справ. Не могли б ви мені допомогти?

А.: У чому річ?

Х.: Я не можу у своєму каталозі виконати команду ls.

А.: В якому каталозі?

Х.: /home/anatoly.

А.: Зараз подивлюся. (Заходить у цей каталог і набирає команду ls, що успішно виконується, засвідчуючи наявність нормальних прав на каталог).

А.: У вас усе має працювати!

Х.: Хммм... Зачекайте. О! А тепер працює. Дивно...

А.: Отже, усе гаразд.

Х.: Дуже вам вдячний. Ще раз вибачаюся, що відірвав віс від справ.

А.: Немає за що. Бувайте.

Кінець розмови.

Начебто нічого особливого. Але що ж відбулося насправді?

У каталозі /home/anatoly серед численних інших файлів був змінений варіант програми *ls*. Саме його адміністратор і запустив. Утім при виконанні цього файла адміністратор мав усі права на систему, а через це кожна із запущених ним програм отримала необмежені можливості робити будь-що. Зрештою, що ще (окрім можливості демонструвати список файлів у каталозі) було в цьому файлі, тепер тільки зломщикові й відомо.

У разі використання телефонного зв'язку зі злочинними намірами головна складність постає, коли потенційна жертва нападу знає справжній голос того, ким представився зловмисник. Останньому доводиться імітувати чужий голос, що дуже важко.

3.4.3. Аналіз сміття

Незаконний аналіз сміття — надзвичайно плідна з погляду зловмисників діяльність. Зокрема ділові паперові відходи стають безцінною поживою для тих хакерів, які використовують СІ, видаючи себе за співробітників тієї чи іншої компанії.

На величезну небезпеку наражається й компанія в який не діють суворі правила утилізації використаних цифрових носіїв — жорстких дисків, компакт-дисків, які можуть стати джерелом усіх видів інформації про діяльність такої компанії (табл. 3.8). Через це політика безпеки кожної компанії має спиратися на положення про управління життєвим циклом носіїв, аж до процедури руйнування або стирання.

Як бачимо, персонал компанії має усвідомити неприпустимість безконтрольного поводження зі сміттям, тим більш, що атаку на нього не можна

Таблиця 3.8

Атаки на сміття

Мета нападу	Опис дій	Спрямованість
Паперові відходи в зовнішніх урнах	Хакер бере зі смітника папірці, що можуть стати джерелом надважливої інформації	Конфіденційна інформація. Атака на довіру
Паперові відходи у внутрішніх урнах	Хакер порпається у внутрішніх офісних урнах, нехтуючи всі рекомдації щодо захисту інформації	Конфіденційна інформація. Атака на довіру
Електронні відходи цифрових носіїв	Хакер отримує інформацію з викинутих електронних носіїв, а також краде самі носії	Конфіденційна інформація. Атака на довіру. Ресурси

вважати правопорушенням. Отже, необхідно ретельно знищувати як паперові відходи, так і електронні носії. Щоб налагодити цю справу, необхідно:

1) розробити процедури знищення сміття й так розмістити відповідні ємності, аби забезпечити їх повну недоступність;

2) управляти внутрішніми відходами. Політика безпеки часто обминає цю проблему, оскільки передбачається, що кожний, хто отримує доступ до ресурсів компанії, має заслуговувати на довіру;

3) визначити категорії інформації, а також спосіб, в який персонал має з нею поводитись. Відповідні категорії можуть формуватися за таким принципом:

- конфіденційна інформація (необхідно знищувати всі папери, що мають цей шифр, у спеціальних знищувачах паперу — шредерах);
- приватна інформація (усі папери, що мають цей шифр, також мають знищуватися у спеціальних знищувачах паперу);
- відомча інформацію (усі папери, що мають цей шифр, зазнають обробки перед викиданням у загальнодоступні урни);
- публічна (загальнодоступна) інформація (такі папери можна кидати в будь-яку урну або використовувати як чернетки).

3.4.4. Особистісні підходи

Для хакера найпростіший спосіб отримати потрібну йому інформацію — звернутися з відповідним проханням безпосередньо до наміченої особи. Цей підхід, хоча він може здаватися грубим, усе ж становить основу шахрайства. Існують чотири різновиди такого підходу:

1) *залякування* (може йтися про уособлення повноважень, що має спонукати жертву нападу до виконання запиту);

2) *переконання* (найбільш звичні форми переконання передбачають застосування лестощів);

3) *використання* довірливих стосунків (потребує підготовчого періоду, протягом якого мають скластися відповідні стосунки);

4) *допомога* (хакер пропонує допомогу потенційній жертві, аби змусити її оприлюднити особисту інформацію).

Вочевидь, завоювати ***довіру*** — одна з головних цілей хакера. Щоб захиститися від ***залякування***, потрібно звільнитися від панічного остраху припуститися помилки. Якщо нормальне поводження керівника з підлеглими — увічливість, то успіх залякування зменшується. ***Переконання*** завжди було важливим чинником людської поведінки. Самої лише надсуворої інструк-

ції стосовно того, що персонал повинен і не повинен робити, завжди замало. Налагоджена атмосфера розуміння в компанії та гнучка політика паролів — найкращі гарантії захищеності. Утім для більшості компаній середнього розміру головну загрозу становлять ***«колеги»***. Штат відділу кадрів має виявляти особливу пильність, наймаючи контрактний персонал. У разі, коли хакер, який послуговується засобами соціальної інженерії, улаштовується на постійну роботу в компанії, то найбільш надійний захист — це повне розуміння з боку персоналу здійснюваної в компанії політики безпеки. Нарешті, атаки ***«допомога»*** можна уникнути, налагодивши в компанії ефективну сервісну підтримку. Внутрішній помічник хакера часто виникає через втрату довіри до надаваних послуг служби підтримки компанії. Аби реалізувати будь-який із зазначених підходів хакери мають вийти на віртуальний або на менш поширений, але більш ефективний особистий контакт із наміченим адресатом.

Сьогодні існують такі види віртуального контакту (табл. 3.9):

- за допомогою електронного поштового повідомлення;
- за допомогою повідомлення, що спливає у вікні браузера.

Таблиця 3.9

Фізичні напади

Мета нападу	Опис дій	Очікувана здобич
Викрадення ідентифікатора мобільного користувача	Хакер спостерігає за законним користувачем, що набирає ім'я та пароль для входу в систему	Конфіденційна інформація
Викрадення ідентифікатора домашнього користувача	Хакер вдає із себе IT для отримання доступу до домашнього комп'ютера працівника й запитує користувальницький ідентифікатор і пароль, щоб перевірити успіх відновлення	Конфіденційна інформація
Прямий мережний контакт через домашню мережу працівника	Хакер звертається до мережі компанії через домашню мережу працівника, удаючи із себе інженера підтримки	Конфіденційна інформація. Ділова довіра. Ділова доступність. Ресурси. Гроші
Зовнішній доступ до домашньої мережі працівника	Хакер отримує доступ до широкосмугового інтернет-каналу через незабезпечену домашню мережу	Ресурси
Несупроводжуваний доступ до офісу компанії	Хакер отримує доступ під виглядом авторизованого користувача компанії	Конфіденційна інформація. Ділова довіра. Ділова доступність. Ресурси. Гроші
Установлення контакту з особою в офісі компанії	Хакер звертається до особи, з якою налагоджено контакт, аби мати змогу використовувати комп'ютерне обладнання чи паперові ресурси	Конфіденційна інформація. Ділова довіра. Ділова доступність. Ресурси. Гроші

Завдяки обсягу отримуваної пошти та використанню «троянців» процедури віртуального контакту лишаються найбільш привабливими, незважаючи на мінімально можливий при цьому успіх.

Щоб запобігти атакам, побудованим на особистісному підході, необхідно:

- визначити в політиці безпеки компанії, що служба підтримки — єдина інстанція, куди потрібно звертатись із проблемами;

• гарантувати, що служба підтримки має ефективний механізм реагування на звернення в межах установленого рівня обслуговування;

• регулярно перевіряти виконання сервісних робіт, аби мати певність, що користувачі на належному рівні отримують відповіді на свої запити.

3.4.5. Реверсивна соціальна інженерія (reverse social engineering)

Зворотна соціальна інженерія (ЗСІ) описує ситуацію, в якій адресат — представник персоналу звертається до хакера по допомогу в усуненні своїх проблем і пропонує хакерові ту інформацію, яку він має намір продати (рис. 3.18). Цьому, як правило, передує дрібна диверсія, у ході якої хакер (можливо інженер компанії) ініціює збій у роботі комп'ютера, підімкненого до мережі. Розрахунок на те, щоб користувач уявляв собі масштаб аварії не таким уже й значним, але при цьому усунути збій власними силами він не зміг. Далі вже справа соціальної техніки: як правило, десь поблизу (наприклад, у списку ICQ контактів) постає «добрий знайомий» когось зі співробітників, який має потрібні знання, або виникає оголошення щодо розташованого неподалік «центру комп'ютерної швидкої допомоги», або з'являється повідомлення про вигідну акцію з підвищення користувальницької грамотності. Головне, що все виконується швидко й дешево (а то й безплатно), без неодмінного оповіщення колег і топ-менеджерів про ганебну IT-безграмотність конкретного працівника.

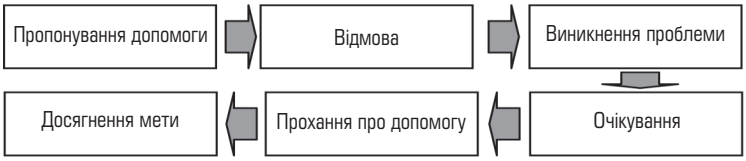


Рис. 3.18. Метод зворотної СІ

Такий сценарій може здатися малоймовірним, хоча насамперед він здійснюється дедалі частіше. Вочевидь, дрібний збій вдається оперативно усунути, і співробітник компанії буде щасливий, поновивши спілкування зі своїм комп'ютером. Що ж до хакера, то він отримав чудову нагоду вдосконалити свою майстерність у пошуку нових жертв.

В основу соціального інжинірингу покладено такі механізми (табл. 3.10):

• створення ситуації, що змушує людину звернутися по допомогу;

• рекламування своїх послуг та надання допомоги;

• випередження спроб інших осіб надати відповідну допомогу.

Розробка заходів щодо захисту від атак СІ — завдання надзвичайно складне. Його не можна розв'язати лише технічними методами. Для побудови системи протидії таким атакам варто залучати професійних консультантів, не покладаючись на власні зусилля. При цьому варто брати до уваги особливості тактики вторгнення, дотримуючись рекомендованих стратегій запобігання їх реалізації (табл. 3.11).

Використання класичних систем запобігання витоку інформації дає особливо високий ефект у разі негайного виявлення та блокування спроб компрометації чутливих даних. Засоби контролю знімних носіїв і зовнішніх пристроїв допоможуть захистити інтелектуальну власність організації, якщо хтось із її співробітників став випадковою жертвою підкинутого пристрою із привабливим умістом.

Таблиця 3.10

Зворотна соціальна інженерія

Мета нападу	Опис дій	Спрямованість
Викрадення ідентифікаційних даних	Хакер отримує користувальницький ідентифікатор і пароль уповноваженого користувача	Конфіденційна інформація; гроші. Ділова довіра та ділова доступність
Викрадення інформації	Хакер використовує ідентифікатор уповноваженого користувача та пароль, щоб отримати доступ до файлів компанії	Конфіденційна інформація; гроші; ресурси. Ділова довіра та ділова доступність
Завантаження malware	Хакер обманює користувача, привертаючи його увагу до небезпечного гіперпосилання або вкладення в e-mail. Коли завантаження закінчено, імітована проблема зникає а користувач не припиняє працювати, не усвідомлюючи, що він припустився порушень захисту, завантаживши malware-програму. У такий спосіб відбувається інфікування мережі компанії	Ділова доступність та ділова довіра
Завантаження хакерського ПЗ	Хакер, привернувши увагу своєї жертви до шкідливого гіперпосилання чи вкладення в e-mail, отримує доступ до ресурсів компанії	Ресурси; гроші. Ділова довіра

Проте найбільш дієвим заходом буде впровадження програми навчання з питань інформаційної безпеки. Зокрема, співробітники компанії мають чітко усмідовлювати, що її електронну пошту призначено передусім для ведення бізнесу. Цим самим вдається мінізувати потрапляння службових адрес електронної пошти в мережу Інтернет. Співробітники мають бути особливо обережні, коли їм доводиться стикатися із вкладеннями з незнайомих джерел. Компанія, у свою чергу, має здійснювати політику безпеки щодо використання соціальних мереж, яка передбачає заборону чи обмеження стосовно інформації, котру співробітники можуть розміщувати на своїх особистих сторінках. Адже сайти соціальних мереж — надзвичайно ефективний інструмент соціального інжинірингу. Регламентування даних про компанію, розташовуваних співробітниками на сайтах соціальних мереж, сприятиме підвищенню рівня загальної інформаційної безпеки компанії.

Питання для самоконтролю

1. На що спрямовано перспективні способи і методи розвідки ІТС? Дайте визначення та наведіть приклади ефективності розвідки систем телекомунікацій, мережної та кібернетичної розвідки.

2. Дайте визначення соціальної інженерії як одного з найбільш перспективних методів кіберрозвідки. До яких інтернет-ресурсів забезпечується доступ завдяки застосуванню засобів СІ?

3. Розкрийте сутність соціальної інженерії. Які риси характеру людини сприяють роботі соціального інженера?

4. Якими механізмами користуються зловмисники, здійснюючи соціальний інжиніринг? Стисло розкрийте сутність цих механізмів.

Таблиця 3.11

Стандартні тактики вторгнення та стратегії щодо запобігання відповідним впливам

Сфера ризику	Тактика хакера	Стратегія запобігання
Телефон (допомоги)	Уособлення та переконання	Повна заборона видавати паролі чи іншу конфіденційну інформацію по телефону
Проникнення в будівлю	Неавторизований фізичний доступ	Сувора перевірка ідентифікаційних карт, навчання службовців і наявність повноцінної служби охорони
Офіс	Підглядання через плече	Не набирайте паролі за будь-чиєї присутності (а якщо доводиться робити це, дійте якомога швидше)
Телефон (допомоги)	Уособлення в разі дзвінка на телефон допомоги	Усі співробітники повинні мати PIN для використання телефону допомоги
Офіс	Блукання по коридорах у пошуках відчиненого офісу	Необхідно, щоб усіх гостей хтось супроводжував
Комп'ютерна кімната/телефонний вузол	Спроба отримати доступ, вилучити устаткування і/або встановити пристрої для перехоплення секретних даних	Комп'ютерні (телефонні) кімнати мають бути весь час зачинені за умови регулярного оновлення опису обладнання
Телефон та АТС	Дзвінки за рахунок компанії	Контроль за міжміськими і міжнародними дзвінками, відстеження дзвінків, заборона на переадресацію
Контейнери та корзини для сміття	Порпання у сміттєзбірнях	Увесь мотлох має зосереджуватись у захищених місцях, важливі дані слід знищувати, перш ніж викидати відповідні носії
Внутрішня мережа та мережа Інтернет	Створення та впровадження троянських коней для викрадення паролів тощо	Безперервне інформування персоналу про системні та мережені зміни, навчання з питань використання паролів
Офіс	Викрадення важливих документів	Конфіденційні документи з відповідними позначками слід зберігати в недоступних місцях
Стан психіки наміченої жертви	Уособлення і переконання	Підтримання достатнього рівня компетентності персоналу за допомогою регулярного інформування та навчання

5. Перелічить основні заходи та засоби організаційного, програмного та технічного забезпечення захисту інформації.

6. За рахунок чого можна зменшити наслідки соціальної інженерії на рівні програмного забезпечення?

7. Що сприятиме підвищенню результативності роботи соціального інженера?

8. Назвіть основні сфери застосування технологій СІ. Наведіть приклади.

9. Наведіть узагальнену класифікацію методів СІ. Розкрийте сутність методів СІ, що спираються на взаємодії з політикою безпеки.

10. Розкрийте сутність локальних і віддалених, аверсних і реверсних методів СІ, а також найбільш поширених прийомів маніпулювання у процесі соціального інжинірингу.

11. На які групи поділяються методи СІ за порушенням характеристик безпеки та реляційними ознаками, за ступенем складності, типом джерела та типом доступу?

12. Назвіть категорії кібератак із використанням соціальної інженерії. Які проблеми дасть змогу розв'язати їх реалізація?

13. Опишіть алгоритм дій зловмисників методом соціальної інженерії. Наведіть приклади.

14. Що може вплинути на успіх у реалізації соціотехнічної атаки?

15. Розкрийте на прикладах результативність К-, Д- та Ц-дієвих атак. Наведіть рекомендації щодо захисту від таких атак.

16. Якими інструментами користується соціальний інженер при організації та проведенні соціотехнічних атак?

17. Поясніть сутність використання електронної пошти як інструмента соціальної інженерії.

18. Назвіть спільні та відмінні риси фішингових і вішингових атак. У чому полягає механізм фармінгу? Наведіть приклади.

19. Поясніть сутність використання телефонного зв'язку як інструмента соціальної інженерії. Наведіть приклади.

20. Поясніть сутність використання незаконного аналізу сміття як інструмента соціальної інженерії. Наведіть приклади.

21. Які особистісні підходи використовують соціальні інженери для отримання інформації від працівників фірми-конкурента?

22. Назвіть головні переваги та недоліки реверсивної соціальної інженерії. Які чинники покладено в її основу?

23. Назвіть основні прийоми запобігання реалізації стандартної тактики вторгнення.

РОЗДІЛ 4

ЗАХИСТ ІНФОРМАЦІЇ ВІД СОЦІОТЕХНІЧНИХ АТАК

За своїм правовим режимом інформація поділяється на *конфіденційну* і *таємну*. Згідно із законом України «Про інформацію» ***конфіденційна інформація*** — це відомості, які перебувають у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. ***Таємна інформація*** — це інформація, що містить відомості, які становлять державну та іншу передбачену законом (банківську, комерційну, службову, професійну, адвокатську) таємницю, розголошення якої завдає шкоди особі, суспільству і державі.

У свою чергу, *конфіденційна інформація* може бути така, що або становить власність держави, або не належить державі. Саме конфіденційна інформація, а точніше право власника на її захист є однією з меж реалізації права на інформацію. При цьому засоби, призначені для захисту інформації можна поділити на два типи:

- *пасивні* — фізичні (інженерні), технічні та програмні засоби;
- *активні* — джерела безперебійного живлення, шумогенератори, скремблери, програмно-апаратні засоби маскування інформації.

4.1. Канали несанкціонованого доступу до інформації

Канали несанкціонованого отримання інформації (КНОІ) — це такі дестабілізуючі фактори, під впливом яких особи чи процеси, котрі не мають на це законних повноважень, можуть отримати або створити небезпеку щодо отримання інформації, яка підлягає захисту. Об'єктивна необхідність формування *повної множини потенційно можливих КНОІ* постає так само, як і в разі *причин порушення цілісності інформації* (*ППЦІ*). Проте труднощі, з якими доводиться стикатися при формуванні повної множини КНОІ, значно більші, ніж у разі ППЦІ. Річ у тім, що несанкціоноване отримання інформації пов'язане переважно зі зловмисними діями, які надто важко піддаються структуризації. З огляду на сказане формування якомога повнішої множини КНОІ доцільно здійснювати або *за критерієм, що відбиває* ***зв'язок*** *зі станом інформації, яка підлягає захисту*, або *за критерієм, що характеризує* ***ступінь взаємодії*** *зловмисника з елементами цієї інформації*. За першим критерієм можна розрізнити дві ситуації: безвідносно до обробки (несанкціоноване отримання інформації можливе й тоді, коли вона не перебуває у процесі обробки, а просто зберігається), і в процесі безпосередньої її обробки.

Для повної структуризації другого критерію виокремимо такі його значення [178]:

перше — зазіхання на інформацію без доступу до неї (тобто непряме отримання інформації);

друге — зазіхання з доступом, але без зміни стану чи змісту інформації;

третє — зазіхання з доступом і зі зміною змісту чи стану інформації.

Класифікаційну структуру КНОІ унаочнює табл. 4.1. Повнота поданої класифікаційної структури гарантується тим, що обрані критерії класифікації охоплюють усі потенційно можливі варіанти взаємодії зловмисника з інформацією, а структуризація значень критеріїв здійснюється за методом поділу цілого на частини.

Отже, усю множину потенційно можливих КНОІ можна розбити на шість класів [178].

Таблиця 4.1

Класифікаційна структура КНОІ

Ознака класифікації		Зв'язок зі станом інформації, що підлягає захисту	
		Безвідносно до обробки інформації А-канали	**Виявляються в процесі обробки В-канали**
Без доступу	К-канали	**1-й клас АК-канали**	**2-й клас ВК-канали**
Із доступом	Без зміни П-канали	**3-й клас АП-канали**	**4-й клас ВП-канали**
	Зі зміною Пі-канали	**5-й клас АПі-канали**	**6-й клас ВПі-канали**

Наступний крок у розв'язанні цієї задачі — обґрунтування більш повного переліку КНОІ в межах кожного з шести класів.

КНОІ 1-го класу — канали, що не пов'язані з обробкою інформації і виникають без доступу зловмисника до інформації:

1) розкрадання носіїв на заводах, де відбувається їх ремонт;
2) підслуховування розмов осіб, що причетні до інформації;
3) провокування на розмову осіб, що причетні до інформації;
4) використання зловмисником візуальних засобів;
5) використання зловмисником оптичних засобів;
6) використання зловмисником акустичних засобів.

КНОІ 2-го класу — канали, що виникають у процесі обробки інформації без доступу зловмисника до неї:

1) електромагнітне випромінювання пристроїв відображення;
2) електромагнітне випромінювання процесорів;
3) електромагнітне випромінювання зовнішніх запам'ятовувальних пристроїв;
4) електромагнітне випромінювання апаратури зв'язку;
5) електромагнітне випромінювання ліній зв'язку;
6) електромагнітне випромінювання допоміжної апаратури;
7) електромагнітне випромінювання пристроїв введення;
8) електромагнітне випромінювання пристроїв підготовки даних;
9) паразитне наведення в комунікаціях електропостачання;
10) паразитне наведення в системах водопостачання і каналізації;
11) паразитне наведення в мережах теплопостачання і вентиляції;
12) паразитне наведення в шинах заземлення;
13) паразитне наведення в колах газифікації;
14) паразитне наведення в колах радіофікації;
15) паразитне наведення в колах телефонізації;
16) паразитне наведення в мережах живлення по колу 50 Гц;
17) паразитне наведення в мережах живлення по колу 400 Гц;

18) підімкнення генератора завад;

19) підімкнення реєструвальної апаратури;

20) огляд відходів виробництва, що потрапляють за межі контрольованої зони.

КНОІ 3-го класу — канали, що виникають безвідносно до обробки інформації з доступом зловмисника до неї, але без зміни інформації:

1) копіювання бланків із вихідними даними;

2) копіювання першоносіїв;

3) копіювання магнітних носіїв;

4) копіювання пристроїв відображення інформації;

5) копіювання вихідних документів;

6) копіювання інших документів;

7) розкрадання виробничих відходів.

КНОІ 4-го класу — канали, що виникають у процесі обробки інформації з доступом зловмисника до неї, але без зміни останньої:

1) запам'ятовування інформації на бланках із вихідними даними;

2) запам'ятовування інформації з пристроїв відображення;

3) запам'ятовування інформації на вихідних документах;

4) запам'ятовування службових даних;

5) копіювання у процесі обробки;

6) виготовлення дублікатів масивів і вихідних документів;

7) копіювання роздруківки масивів;

8) використання програмних пасток;

9) маскування під зареєстрованого користувача;

10) використання недоліків операційних систем;

11) використання недоліків мов програмування;

12) використання інфікованості програмного забезпечення «вірусом».

КНОІ 5-го класу — канали, що виникають безвідносно до обробки інформації з доступом зловмисника до неї і зі зміною останньої:

1) підміна бланків;

2) підміна магнітних носіїв;

3) підміна вихідних документів;

4) підміна апаратури;

5) підміна елементів програми;

6) підміна елементів баз даних;

7) розкрадання бланків із вихідними даними;

8) розкрадання магнітних носіїв;

9) розкрадання вихідних документів;

10) розкрадання інших документів;

11) упровадження в програми блоків типу «троянський кінь», «бомба» тощо;

12) читання залишкової інформації в ОЗП після виконання санкціонованих запитів.

КНОІ 6-го класу — канали, що виникають у процесі обробки інформації з доступом зловмисника до неї та її застосуванням:

1) незаконне підімкнення до апаратури;

2) незаконне підімкнення до ліній зв'язку;

3) зняття інформації на шинах живлення пристроїв відображення;

4) зняття інформації на шинах живлення процесорів;

5) зняття інформації на шинах живлення апаратури зв'язку;

6) зняття інформації на шинах живлення ліній зв'язку;

7) зняття інформації на шинах живлення друкувальних пристроїв;

8) зняття інформації на шинах живлення зовнішніх запам'ятовувальних пристроїв;

9) зняття інформації на шинах живлення допоміжної апаратури.

4.2. Методи та засоби протидії соціотехнічним атакам і захисту від них: переваги та недоліки

При побудові узагальненої класифікації методів протидії соціотехнічним атакам необхідно враховувати чинники *комплексності*, *системності*, *уніфікованості* та *безперервності*. Головним чинником як за ефективністю захисту, так і за ресурсовитратами в кожній зі сфер безпеки є ***комплексність***. Комплексний захист від соціотехнічних атак ефективний лише в разі застосування ***системного підходу*** [103; 109; 115; 128], який, у свою чергу, спирається на принципи:

• *законності* — додержанні повної відповідності заходів, планованих до реалізації в галузі забезпечення інформаційної і кібербезпеки, чинному законодавству;

• *невизначеності*, зумовленої непередбачуваністю поведінки зловмисника (адже невідомо, хто, коли, де і в який спосіб може порушити безпеку об'єкта захисту);

• *неможливості створення ідеальної системи захисту*, що випливає з принципу невизначеності й зумовлюється обмеженістю ресурсів засобів захисту;

• *мінімального ризику й мінімального збитку* — положень, які випливають із неможливості створення ідеальної системи захисту і змушують враховувати конкретні умови існування об'єкта захисту для кожного моменту часу;

• *безпечного часу*, тобто врахування як абсолютного часу (протягом якого необхідно зберігати об'єкти захисту), так і часу відносного (від моменту виявлення злочинних дій до моменту досягнення мети зловмисником);

• «*захисту всіх від усіх*» — організації захисних заходів проти всіляких форм загроз для ОІД, нагальна потреба в якій випливає з принципу невизначеності;

• *персональної відповідальності* (ідеться про персональну відповідальність кожного співробітника ОІД за дотримання режиму безпеки в рамках своїх повноважень, функціональних обов'язків і чинних інструкцій);

• *обмеження повноважень* (ідеться про обмеження повноважень суб'єкта щодо ознайомлення з інформацією, до якої він не має доступу, а також введення заборони доступу до об'єктів і зон, перебування в яких не пов'язане з родом його діяльності);

• *взаємодії й співробітництва* — налагодження клімату довіри між співробітниками, відповідальними за інформаційну та кібернетичну безпеку, і рештою персоналу, а також співпраці з усіма зацікавленими організаціями й особами;

• *комплексності та індивідуальності*, що передбачає доцільність проведення комплексних, взаємозалежних і взаємозамінюваних заходів для забезпечення безпеки об'єкта захисту, реалізовуваних з урахуванням конкретних умов;

• *послідовних рубежів безпеки* — якомога більш раннього оповіщення про кібернапад на об'єкт захисту чи інші несприятливі події, аби служби безпеки мали змогу вчасно визначити причину тривоги й організувати ефективні заходи з протидії злочинним впливам;

• *рівноміцності й рівнопотужності рубежів захисту* — відсутності незахищених ділянок у рубежах захисту ОІД (рівноміцність) і порівняно однакової їх захищеності згідно зі ступенем можливих загроз (рівнопотужність).

Дотримання зазначених принципів дозволить не лише сформувати низку вимог до комплексної системи протидії соціотехнічним атакам і захисту від них, а й уникнути проблем, пов'язаних із надто високою вартістю реалізації цих вимог, неможливістю ефективного контролю за їх виконанням та труднощами їх засвоєння виконавцями. Окрім того, на базі цих принципів удається повністю нівелювати ризики всіх можливих загроз для об'єкта захисту, розробивши уніфіковану концепцію захисту інформації від соціотехніків щодо різних типів персоналу, обігової інформації та інформаційних систем і умов їх використання. Головне, аби роботи із захисту від соціотехнічних атак проводилися безперервно, на кожному етапі циркулювання інформації з урахуванням впливу персоналу та застосуванням низки певних ***перевентивних методів***.

Превентивні методи захисту від соціотехнічних атак можна поділити на ***правові*** — законодавчі та морально-етичні, ***організаційні*** — організаційно-адміністративні, організаційно-технічні й організаційно-економічні, а також ***інженерно-технічні*** — фізичні, технічні й програмні.

Законодавчі методи ґрунтуються на нормативно-правових актах, за допомогою яких регламентуються права і обов'язки співробітників, а також встановлюється відповідальність усіх співробітників і підрозділів, причетних до захисту інформації від соціотехнічних атак, за невиконання правил роботи з важливими даними, що може призвести до порушення їх захищеності.

Морально-етичні методи спираються на сформовані в колективі моральні норми та правила, неухильне дотримання яких сприяє захисту інформації від атак соціотехніків, а порушення прирівнюється до ігнорування правил поведінки в суспільстві чи колективі.

Організаційно-адміністративні методи передбачають:

• мінімізацію витоку інформації через персонал;

• організацію спеціального документообігу;

• відведення спеціальних захищених приміщень і засобів ЕОТ;

• використання сертифікованих програмних і технічних засобів;

• використання зареєстрованих носіїв інформації.

До найдієвіших серед них належать методи *антропогенного захисту*, в основу яких покладено:

1) привернення уваги людей до питань безпеки;

2) усвідомлення користувачами всієї серйозності проблеми та розробку політики безпеки системи;

3) вивчення та впровадження необхідних методів і дій для підвищення захисту інформаційного забезпечення.

Наприклад, ідеться про формування в персоналу навичок щодо розкриття намірів організації соціотехнічних атак і адекватного реагування на їх прояви. Одним із перших кроків, які має виконати працівник при спробі зловмисників анонімно (наприклад, по телефону, скайпу тощо) отримати інформацію

про установу, її керівництво або персональні дані окремих працівників,— спробувати з'ясувати:

1) чи справді прохач є тією особою, за яку він себе видає;

2) чи має цей прохач право на отримання запитуваної інформації.

Орієнтовний алгоритм подальших дій такого працівника унаочнює рис. 4.1 (додаток Г).

Єдиний, але дуже істотний недолік методів антропогенного захисту — їхня очевидна пасивність.

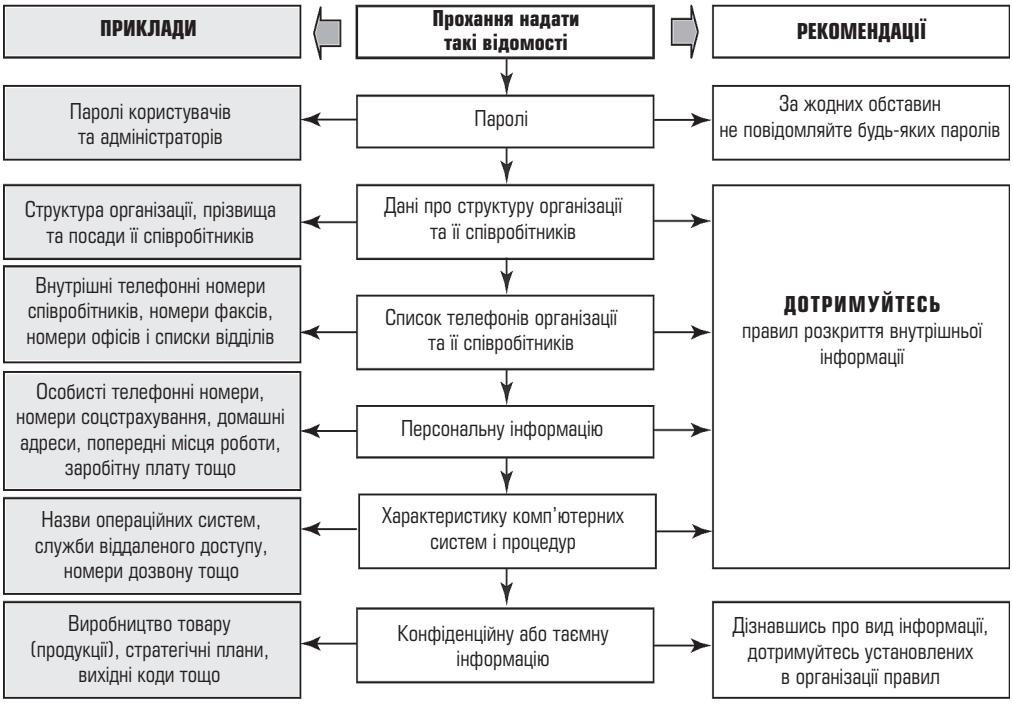


Рис. 4.1. Рекомендація щодо розкриття атаки, спрямованої на отримання інформації

Організаційно-технічні методи захисту реалізують через обмеження доступу до інформації сторонніх осіб; відімкнення від ЛОМ та мережі Інтернет осіб, які мають доступ до конфіденційної інформації; передавання конфіденційної інформації лише спеціальними інженерно-технічними засобами; нейтралізацію витоку інформації електромагнітними та акустичними каналами. Зазначені методи поділяють на *інформаційні*, *процедурні*, *класифікаційні*, *застережні*, *навчальні*, *спонукальні* [131].

Інформаційні методи включають у себе локальні заходи, що реалізуються в межах організації та спрямовані на інформування персоналу з питань реалізації соціотехнічних атак та нагадування про ризики їх настання. У цьому плані можливі такі заходи:

• розробка відповідних інформаційних статей, буклетів і брошур, календарів, пам'яток, які поширюються в роздрукованій або електронній формі;

• використання різноманітних повідомлень у системі корпоративних ресурсів, у локальній комп'ютерній мережі щодо правил поведінки з важливою інформацією (наприклад, при вході в систему користувачу з'являється пові-

домлення: «Перш ніж пересилати конфіденційну інформацію електронною поштою, неодмінно зашифруйте її!»);

• оголошення, що подаються через інформаційні дошки, електронні табло в громадський місцях (наприклад, у місцевому кафетерії, із часто оновлюваною інформацією про головні положення політики безпеки (ПБ)), спеціальні плакати, голосову пошту, місцеві гучномовці, спеціальні наклейки на телефонах (наприклад, «Чи справжнім своїм ім'ям назвався той, хто тепер телефонує?»).

Процедурні методи включають в себе розробку порядку дій, правил ПБ, рекомендацій, якими має керуватися персонал при використанні та наданні співробітникам чи стороннім особам корпоративної інформації. Це можуть бути:

• правила ПБ, зокрема положення щодо соціотехнічних атак, з якими має бути ознайомлений персонал;

• процедури, передбачені при прийомі та звільненні співробітників;

• порядок повідомлення працівників про зміни або нововведення в ПБ;

• дії персоналу в нештатних ситуаціях;

• рекомендації щодо надання будь-кому важливої інформації.

Класифікаційні методи полягають у виборі критеріїв поділу інформації на класи та обґрунтуванні класифікаційної структури за вибраними критеріями.

Застережні методи спираються на систему заходів, які мають на меті підвищення пильності та відповідальності персоналу завдяки втіленню в життя відповідних процедур безпеки. Може йтися, скажімо, про використання різноманітних ідентифікаторів (носіння бейджиків, включаючи тимчасові перепустки для співробітників, котрі з якихось причин не мають при собі перепускних ідентифікаторів); неодмінне супроводження відвідувачів; здійснення запиту щодо підтвердження особи, котра претендує на отримання важливої інформації; здійснення зворотного дзвінка в разі запиту важливої інформації; повідомлення адміністраторові з питань безпеки про підозрілі інциденти; документування розмови під час нестандартного запиту із намаганням якомога більше дізнатися про того, чий дзвінок викликав підозру.

Спонукальні методи мають на меті заохочувати працівників до посиленого захисту від соціотехнічних атак, що спираються на знання правил ПБ, успішне проходженнях несподіваних перевірок тощо. Як приклади застосування спонукальних методів слід розглядати подяки, відзначення найбільш надійного працівника місяця тощо.

Навчальні методи передбачають проведення заходів, спрямованих на здобуття персоналом відповідних знань, умінь і навичок протидії соціотехнічним атакам. Це може бути:

• організація занять із підвищення кваліфікації;

• проведення періодичних тренінгів на робочих місцях;

• використання автоматизованих систем перевірки стійкості співробітників щодо соціотехнічних атак, відповідний інструктаж.

Перевага організаційно-технічних методів полягає в тому, що вони, по-перше, дають змогу розв'язувати багато різнорідних проблем, по-друге, прості в реалізації, по-третє, допомагають швидко реагувати на небажані дії в мережі й, по-четверте, мають необмежені можливості модифікації та розвитку. Як недоліки слід розглядити високу залежність від суб'єктивних факторів, зокрема від рівня організації відповідної роботи в тому чи іншому підрозділі.

Організаційно-економічні методи охоплюють заходи зі стандартизації методів і всього арсеналу засобів інформації, сертифікації засобів ЕОТ згідно з вимогами інформаційної та кібернетичної безпеки, страхування інформаційних ризиків, ліцензування діяльності у сфері захисту інформації тощо.

Інженерно-технічні (фізичні, технічні та програмні) ***методи*** захисту від соціотехнічних атак реалізуються не лише через використання штатними службами безпеки активних і пасивних технічних засобів протидії сторонньому кібервпливу на кшталт відімкнення, упакування й опечатування з подальшим належним зберіганням відповідних носіїв інформації (що дозволяє звести до нуля ризик знищення даних у результаті роботи шкідливих програм і дій зловмисника та забезпечити достатній рівень оцінюваної вірогідності результатів), а й через виконання ними заходів із розроблення відповідних компонентів системи, навчання користувачів і обслуговувального персоналу з питань щодо форм і методів експлуатації ТЗ і ПЗ, а також контролю за дотриманням правил їх експлуатації. Недолік цього підходу полягає у високій чутливості до помилок, що можуть траплятися при встановленні й настроюванні засобів захисту, а також у складності управління відповідними процесами.

4.2.1. Засоби та заходи фізичного захисту інформації з обмеженим доступом

Фізичні методи захисту від соціотехнічних атак спираються на використання механічних, електричних, електронних та інших пристроїв і систем, які функціонують автономно, перешкоджаючи діяльності соціотехніків. Це можуть бути периметрові системи контролю, пропускні системи на базі технологій smart-card, touch-memory тощо [130–132]. Вони забезпечують фізичну безпеку споруд і приміщень (температура в приміщенні 10…26 °С, вологість повітря 35–50%), самої інформаційної системи, допоміжного обладнання (принтери, сканери тощо), носіїв інформації та каналів передавання (отримання) інформації. Головні заходи з фізичного захисту мають на меті захист від вогню, води, пилу, корозійних газів, електромагнітного випромінювання, вандалізму тощо, а також захист від несанкціонованого доступу до приміщень. При цьому вимоги до кожного захисного бар'єра та місця його розташування мають визначатися цінністю інформації, ризиком порушення безпеки та необхідністю дотримання чинних захисних заходів.

Діапазон засобів *фізичного захисту*, прийнятних для запобігання катастрофам чи їх мінімізації, дуже великий — від найнижчого рівня до найвищого. При цьому кожний рівень фізичного захисту має чітко визначені режимні території, зони чи приміщення, у межах яких необхідно забезпечити саме цей рівень захисту. Скажімо, для захисту периметра можуть створюватись системи охоронної та пожежної сигналізації, системи цифрового відеоспостереження, системи контролю та управління доступом (СКУД) тощо. Доцільно керуватись такими рекомендаціями [178]:

- режимні території, зони чи приміщення мають відповідати цінності інформації, що підлягає захисту;
- периметр безпеки має бути чітко визначений;
- допоміжне устаткування (ксерокс, факс тощо) має розміщуватися так, аби мінімізувати ризик НСД до інформації з обмеженим доступом;
- фізичні бар'єри мають у разі потреби сягати від підлоги до стелі, аби запобігти НСД до режимних приміщень;

• стороннім особам ні в якому разі не можна надавати інформацію про те, що відбувається на режимних територіях, у відповідних зонах чи приміщеннях;

• доцільно по змозі заборонити будь-кому працювати наодинці без належного контролю;

• інформаційну систему потрібно розташовувати у спеціально призначених для цього місцях, окремо від обладнання, контрольованого будь-якими сторонніми підрозділами;

• у неробочий час режимні території, зони чи приміщення мають бути фізично недоступні й періодично перевірятися охороною;

• у межах режимних територій, зон чи приміщень використання фотографічної, звукозаписувальної чи відеоапаратури має бути заборонено;

• стосовно режимних територій, режимних зон і приміщень варто установити належний контроль доступу.

Для реалізації заходів щодо контролю необхідно:

• вести облік дати й часу входу і виходу відвідувачів (відвідувачам може бути надано доступ лише конкретної, дозволеної інформації);

• вилучати права доступу до режимних територій, зон чи приміщень у тих співробітників, які звільняються з даного місця роботи;

• неухильно додержувати пропускного режиму та правил внутрішнього розпорядку, установленого в організації. Передусім ідеться про обмеження кола осіб, що мають доступ до ІзОД, доведення до відома виконавців усіх вимог щодо роботи з документами, які мають гриф обмеження доступу, забезпечення встановленого порядку користування ІзОД тощо.

4.2.2. Засоби та заходи технічного захисту інформації з обмеженим доступом

Найбільш потужні інструменти захисту від соціотехнічних атак включає в себе ***технічний захист***. Головні його методи мають на меті запобігти як несанкціонованому добуванню інформації, так і її зловмисному використанню. Технічні методи реалізуються завдяки впровадженню різних за типом (механічних, електромеханічних, електронних) пристроїв, які схемно вбудовуються в апаратуру систем обробки інформації або поєднуються з нею для захисту ресурсів від вторгнення соціотехніків. Такі пристрої або перешкоджають фізичному проникненню, або, якщо проникнення все-таки сталося, заважають несанкціонованому доступу до інформації (табл. 4.2), зокрема й через її маскування.

Передусім ідеться про такі запобіжники, як замки, ґрати на вікнах, захисна сигналізація тощо. Водночас вводяться в дію генератори шуму, мережні фільтри, сканувальні радіоприймачі та інші пристрої, що запобігають витоку інформації через потенційні технічні канали, або дають змогу їх виявити. При цьому для захисту інформації на рівні апаратного забезпечення використовуються апаратні ключі, системи сигналізації, засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах можуть бути використані такі *засоби мережного захисту* інформації:

• міжмережні екрани (*Firewall*) — для блокування атак із зовнішнього середовища (*Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall* від компанії *Nortel Networks*). Вони керують проходженням мережного трафіку згідно з правилами (*policies*)

Таблиця 4.2

Основні методи і засоби несанкціонованого отримання інформації та її захисту

Типова ситуація	Канал витоку інформації	Методи і засоби	
		отримання інформації	захисту інформації
Розмова в приміщенні та на вулиці	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
	Віброакустичний	Стетоскоп, вібродатчик	
	Акустоелектронний	Спеціальні радіоприймачі	
Розмова по телефону:	Акустичний	Підслуховування (диктофон, мікрофон тощо)	Шумові генератори, пошук закладних пристроїв, захисні фільтри, обмеження доступу
– проводовому	Сигнал у лінії	Паралельний телефон, пряме підмкнення, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наведення	Спеціальні радіотехнічні пристрої	Спецтехніка
– радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка
Дії з документом на паперовому носії:	Безпосередньо сам документ	Крадіжка, прочитування, копіювання, фотографування	Обмеження доступу, спецтехніка
– виготовлення	Продавлення стрічки або паперу	Крадіжка, прочитування	Оргтехзаходи
	Акустичний шум принтера	Апаратура акустичного контролю	Пристрої шумозаглушування
	Паразитні сигнали, наведення	Спеціальні радіотехнічні засоби	Екранування
– поштове відправлення	Безпосередньо сам документ	Крадіжка, прочитування	Спеціальні методи
Документ на машинному носії:	Носій	Крадіжка, копіювання, прочитування	Контроль доступу, фізичний захист, криптозахист
– виготовлення	Відображення на дисплеї	Візуальний, копіювання, фотографування	Контроль доступу, фізичний захист, криптозахист
	Паразитні сигнали, наведення	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, екранування
	Електричні та оптичні сигнали	Апаратні закладки	
	Програмний продукт	Програмні закладки	
– передавання документа по каналах зв'язку	Електричні та оптичні сигнали	Несанкціоноване підмкнення, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

безпеки. Як правило, міжмережні екрани встановлюються на вході мережі, аби розмежувати внутрішні і зовнішні (загального доступу) мережі;

• системи виявлення вторгнень (*IDS — Intrusion Detection System*), тобто спроб несанкціонованого доступу як іззовні, так і всередині мережі, а також захисту від атак типу «відмова в обслуговуванні» (*Cisco Secure IDS, Intruder Alert і NetProwler* від компанії *Symantec*). Ці системи завдяки використанню відповідних спеціальних механізмів, здатні запобігати шкідливим діям, знижуючи цим самим час простою в результаті атаки й витрати на підтримання роботоздатності мережі;

• засоби створення віртуальних приватних мереж (*VPN — Virtual Private Network*) — для організації захищених каналів передавання даних через незахищене середовище (*Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator*). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації завдяки її динамічному шифруванню;

• засоби аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації (*Symantec Enterprise Security Manager, Symantec NetRecon*). Їх застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Під *технічними каналами* розуміють канали сторонніх електромагнітних випромінювань і наведень, акустичні та оптичні канали тощо.

Захист інформації від її витоку технічними каналами зв'язку забезпечується в такий спосіб:

• використанням екранованого кабелю та прокладанням проводів і кабелю екранованих конструкціях;

• установленням на лініях зв'язку високочастотних фільтрів;

• побудовою екранованих приміщень («капсул»);

• використанням екранованого устаткування;

• установленням активних систем зашумлення.

Узагальнену схему можливих каналів витоку та несанкціонованого доступу до інформації, оброблюваної в типовому одноповерховому офісі, наведено на рис. 4.2, де використано такі позначення:

1) витік за рахунок структурного звуку в стінах і перекриттях;
2) знімання інформації зі стрічки принтера, погано стертих дискет і т. ін.;
3) знімання інформації з використанням відеозакладок;
4) програмно-апаратні закладки в ПЕОМ;
5) радіозакладки в стінах і меблях;
6) знімання інформації із системи вентиляції;
7) лазерне знімання акустичної інформації з вікон;
8) виробничі й технологічні відходи;
9) комп'ютерні віруси, логічні бомби тощо;
10) знімання інформації за рахунок наведень і «нав'язування»;
11) дистанційне знімання відеоінформації (оптика);
12) знімання акустичної інформації з використанням диктофонів;
13) розкрадання носіїв інформації;
14) високочастотний канал витоку в побутовій техніці;
15) знімання інформації спрямованим мікрофоном;
16) внутрішні канали витоку інформації (через обслуговувальний персонал);

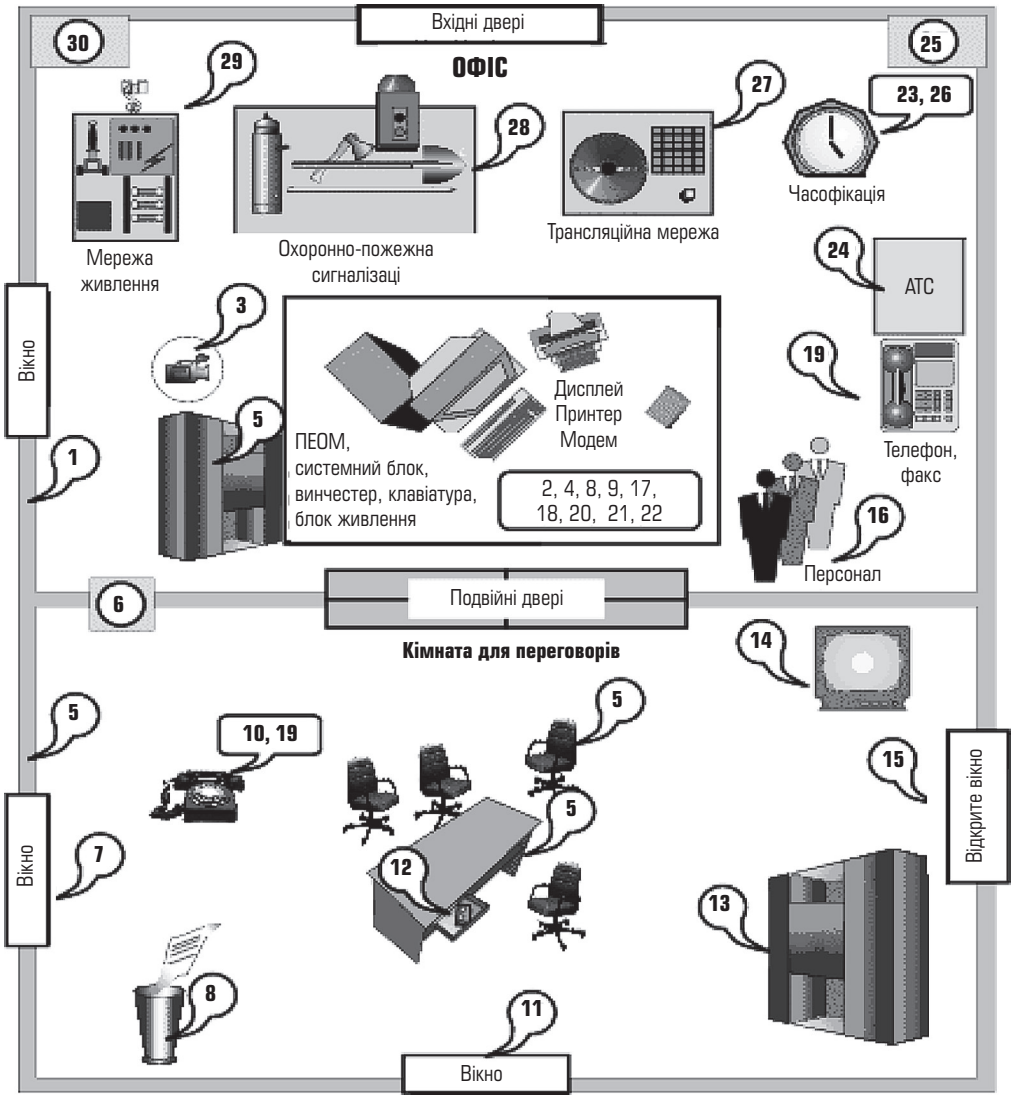


Рис. 4.2. Можливі канали витоку та несанкціонованого доступу

17) несанкціоноване копіювання;
18) витік за рахунок побічного випромінювання термінала;
19) знімання інформації за рахунок використання «телефонного вуха»;
20) знімання з клавіатури та принтера акустичним каналом;
21) знімання з дисплея по електромагнітному каналу;
22) візуальне знімання з дисплея та принтера;
23) наведення на лінії комунікацій і сторонні провідники;
24) витік через лінії зв'язку;
25) витік мережею заземлення;
26) витік мережею часофікації;
27) витік трансляційною мережею та гучномовним зв'язком;
28) витік охоронно-пожежною сигналізацією;
29) витік мережею електроживлення;
30) витік мережею опалення, газо- і водопостачання.

Склад засобів забезпечення технічного захисту інформації, зокрема й від соціотехнічних атак, перелік постачальників цих засобів, а також послуг з установлення, монтажу, налагодження та обслуговування визначають ті особи, які володіють, користуються та розпоряджаються інформацією з обмеженим доступом самостійно або за рекомендаціями фахівців у сфері технічного захисту інформації та відповідно до чинних нормативних документів у зазначеній сфері. Їх вибір зумовлюється особливостями фрагментарного чи комплексного захисту інформації. При цьому фрагментарний захист забезпечує протидію якійсь певній загрозі, а комплексний — одночасну протидію всій множині наявних загроз.

Засоби технічного захисту інформації можуть функціонувати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих в них складових елементів. Для оцінювання стану засобів технічного захисту інформації, що обробляється або циркулює в ІС, комп'ютерних мережах і системах зв'язку, а також для підготовки обґрунтованих висновків, використовуваних із метою ухвалення відповідних рішень, проводиться експертиза щодо стану справ у сфері технічного захисту інформації. Порядок розрахунку й інструментального визначення зон безпеки інформації, кроки з реалізації заходів, спрямованих на технічний захист інформації, визначення ефективності такого захисту та порядку атестації відповідних технічний засобів і робочих місць (приміщень) — усе це регламентується нормативними документами з ТЗІ.

Переваги методів технічного захисту інформації полягають у їхній надійності, максимальній незалежності від суб'єктивних факторів, а також у високій стійкостю до модифікації. До недоліків цих методів слід віднести недостатню гнучкість, порівняно великі обсяги й масу використовуваної апаратури та її високу вартість.

В основу ***програмних методів*** захисту інформації, зокрема й від соціотехнічних атак, покладено спеціальні прикладні пакети або окремі програми, що входять до складу програмного забезпечення систем обробки даних. Ці методи передбачають використання програм для ідентифікації та автентифікації користувачів, для контролю та розмежування доступу до інформації, шифрування інформації, вилучення залишкової (робочої) інформації типу тимчасових файлів, а також для тестового контролю системи захисту, її аудиту, моніторингу й антивірусного захисту.

Зазначені методи застосовують, аби забезпечити:

- ідентифікацію та автентифікацію користувачів, персоналу й ресурсів системи оброблення інформації;
- розмежування доступу користувачів до інформації, засобів обчислювальної техніки й технічних засобів інформаційних систем;
- цілісність інформації та конфігурування інформаційних систем;
- реєстрацію та облік дій користувачів;
- маскування оброблюваної інформації;
- реагування (сигналізація, відімкнення, зупинення робіт, відмова щодо виконання запиту) на спроби несанкціонованих дій.

4.2.3. Засоби та заходи криптографічного захисту інформації з обмеженим доступом

Найбільш ефективні методи захисту інформації від соціотехнічних атак базуються на ***криптографічних технологіях захисту***, завдяки яким забез-

печуються три основні типи послуг: *автентифікація* (яка включає в себе ідентифікацію), *неможливість відмови* від вчинених дій (*non-repudiation*) і *збереження таємниці*. Наприклад, ***ідентифікація*** означає перевірку щодо того, чи є відправник послання тією особою, за яку він себе видає. ***Автентифікація*** йде ще далі, установлюючи не лише особу відправника, а й відсутність змін у відповідному посланні. Реалізація вимоги стосовно ***неможливості відмови*** означає, що ніхто не має права заперечувати, що він відправив чи отримав певний файл або дані (це аналог відправлення звичайною поштою рекомендованого листа). І, нарешті, ***збереження таємниці*** — це захист послань від несанкціонованого перегляду [178].

Зауважимо, що ***криптографія*** (математичні методи перетворення даних для забезпечення інформаційної безпеки) дає змогу гарантувати як конфіденційність, так і цілісність даних, забезпечуючи водночас неспростовність здійсненої ідентифікації чи автентифікації. У разі , коли йдеться про особливо гостру потребу щодо гарантування конфіденційності, тобто коли інформація надзвичайно чутлива, доводиться зашифровувати її для зберігання чи передавання мережею. Якщо головна вимога — забезпечити цілісність (унеможливити випадкову чи навмисну заміну, вилучення або інше втручання) даних, які підлягають зберіганню чи обробці, використовують геш-функції, цифрові підписи тощо. Зокрема, засоби цифрових підписів виконують функції, аналогічні функціям засобів гарантування цілісності повідомлень. Водночас вони дають змогу підтверджувати неспростовність вчинених дій.

Розв'язуючи питання стосовно правомірності використання засобів шифрування, цифрових підписів чи інших механізмів забезпечення цілісності, необхідно спиратись на чинну нормативну й законодавчу базу, а також на вимоги щодо управління ключами (з урахуванням інфраструктури відкритих ключів). При цьому головне завдання полягає в неухильному підвищенні безпеки інформації без створення нових її вразливостей.

Методи криптографії (наприклад, ті, що ґрунтуються на використанні цифрових підписів) можуть застосовуватись для повідомлень, комунікацій та трансакцій з метою підтвердження чи спростування відправлення, передавання, подання, доставляння, оповіщення про отримання тощо. У ситуаціях, коли особливо важлива автентичність даних, для підтвердження їх вірогідності може використовуватись *цифровий підпис*. Така потреба постає передусім тоді, коли використовуються дані, на які посилається третя сторона, або коли для багатьох людей дуже важливо, щоб ті чи інші дані були якомога точніші. Цифрові підписи можна також використовувати для підтвердження того факту, що ті чи інші дані створено чи передано певною особою.

Застосування криптографії потребує додержання всіх правових і регуляторних вимог у цій сфері. Один із найважливіших аспектів криптографії — адекватна система управління ключами. Криптографія з відкритим ключем спирається на *концепцію ключової пари*. Кожна половина пари (один ключ) шифрує інформацію таким чином, що її може розшифрувати тільки інша половина (другий ключ). Одна половина ключової пари — особистий ключ, відома тільки його власникові. Друга половина — відкритий ключ, поширюється серед усіх кореспондентів власника цього ключа. Ключові пари характеризуються унікальною особливістю: дані, зашифровані будь-яким із ключів пари, можуть бути розшифровані тільки іншим ключем із цієї пари. Іншими словами, немає жодної різниці, особистий чи відкритий ключ використовується

для шифрування послання; одержувач зможе застосувати для розшифрування другу половину пари. Ключі можна використати і для забезпечення конфіденційності послання, і для автентифікації його автора. У першому випадку для шифрування послання відправник використовує відкритий ключ одержувача, а отже, воно залишатиметься зашифрованим доти, доки одержувач не розшифрує його особистим ключем. У другому випадку відправник шифрує послання своїм особистим ключем, до якого тільки він сам має доступ. При цьому слід ураховувати, що процедури управління ключами залежать від використовуваного алгоритму здійснення наміру щодо використання ключів та реалізовуваної політики безпеки.

У 1985 році для розв'язання завдань, з якими доводиться стикатися у практиці шифрування інформації, Коблиць і Міллер незалежно один від одного запропонували при побудові криптосистем використовувати алгебраїчні структури, визначені на множині точок, що належать еліптичним кривим.

Розглянемо випадок визначення еліптичних кривих над простими скінченними полями довільної характеристики і над полями Галуа характеристики 2.

Нехай $p > 3$ — просте число. При цьому $a, b \in GF(p)$ такі, що $4a^2 + 27b^2 \neq 0$. *Еліптичною кривою* E над полем $GF(p)$ називається множина розв'язків (x, y) рівняння $y^2 = x^3 + ax + b$ над полем $GF(p)$ разом із додатковою точкою ∞, яку називають *точкою нескінченності*. Позначимо кількість точок на еліптичній кривій E через $\#_E$. Верхня і нижня межі для $\#_E$ визначаються ***теоремою Хассе***:

$$p+1-2\sqrt{p} \le \#_E \le p+1+2\sqrt{p}. \tag{4.1}$$

Задамо бінарну операцію на E (в адитивному запису) такими правилами:

(I) $$\infty + \infty = \infty;$$

(II) $$\forall (x,y) \in E,\ (x,y) + \infty = (x,y);$$

(III) $$\forall (x,y) \in E,\ (x,y) + (x,-y) = \infty;$$

(IV) $$\forall (x_1,y_1) \in E,\ (x_2,y_2) \in E,\quad x_1 \neq x_2,\ (x_1,y_1) + (x_2,y_2) = (x_3,y_3),$$

де $x_3 = \lambda^2 - x_1 - x_2;\ y_3 = \lambda(x_1 - x_3) - y_1$ при $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$;

(V) $$\forall (x_1,y_1) \in E,\quad y_1 \neq 0,\quad (x_1,y_1) + (x_1,y_1) = (x_2,y_2),$$

де $x_2 = \lambda^2 - 2x_1;\ y_2 = \lambda(x_1 - x_3) - y_1,\ \lambda = \dfrac{3x_1^2 + a}{2y_1}$.

Множина точок еліптичної кривої E із заданої в такий спосіб сукупності утворює *абелеву групу*. Якщо $\#_E = p + 1$, то крива E називається *суперсингулярною*. При цьому суперсингулярна крива E над полем $GF(2^m)$ характеристики 2 задається в такий спосіб. Нехай $m > 3$ — ціле число. При цьому $a, b \in GF(2^m)$, $b \neq 0$. Еліптична крива E над полем $GF(2^m)$ називається *множиною розв'язків* (x, y) *рівняння*

$$y^2 + xy = x^3 + ax + b \tag{4.2}$$

над полем $GF(2^m)$ *разом із додатковою точкою* ∞, названою точкою нескінченності.

Кількість точок на кривій E також визначається *теоремою Хассе*:

$$q+1-2\sqrt{q} \le \#_E \le q+1+2\sqrt{q}\ , \tag{4.3}$$

де $q = 2^m$. Більш того, число $\#_E$ *парне*.

Операція додавання на E у цьому разі задається такими правилами:

(I) $$\infty + \infty = \infty;$$

(II) $$\forall (x,y) \in E,\ (x,y) + \infty = (x,y);$$

(III) $$\forall (x,y) \in E,\ (x,y) + (x, x+y) = \infty;$$

(IV) $$\forall (x_1,y_1) \in E,\ (x_2,y_2) \in E,\quad x_1 \neq x_2,\ (x_1,y_1) + (x_2,y_2) = (x_3,y_3),$$

де $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a;\quad y_3 + \lambda(x_1 + x_3) + x_3 + y_1$ при $\lambda = \dfrac{y_1 + y_2}{x_1 + x_2};$

(V) $$\forall (x_1, y_1) \in E,\quad x_1 \neq 0,\quad (x_1, y_1) + (x_1, y_1) = (x_2, y_2),$$

де $x_2 = \lambda^2 + \lambda + a;\quad y_2 = x_1^2 + (\lambda + 1)x_3$ при $\lambda = x_1 + \dfrac{y_1}{x_1}.$

У цьому разі множина точок еліптичної кривої E із заданої в такий спосіб сукупності також утворить *абелеву групу*. Користуючись операцією додавання точок на кривій, можна природним чином визначити *операцію множення* точки $P \in E$ на довільне ціле число n: $P_n = P + P + ... + P$, де операція додавання виконується n раз.

Тепер побудуємо однобічну функцію, на основі якої можна буде створити криптографічну систему. Нехай E — еліптична крива, $P \in E$ — точка на цій кривій. Візьмемо ціле число $n < \#_E$. Тоді як пряму функцію виберемо добуток P_n. Для його обчислення за оптимальним алгоритмом знадобиться не менш як $2\log_2 n$ операцій додавання.

Обернену задачу сформулюємо в такий спосіб: за заданою еліптичною кривою E, точкою $P \in E$ і добутком P_n знайти n.

Зауважимо, що всі відомі алгоритми розв'язування цієї задачі вимагають експоненціального часу.

Для встановлення захищеного зв'язку двоє користувачів A і B спільно вибирають еліптичну криву E і точку P на ній. Потім кожний із користувачів вибирає своє секретне ціле число — відповідно a і b. Користувач A обчислює добуток Pa, а користувач B — Pb. Далі вони обмінюються обчисленими значеннями. При цьому параметри самої кривої, координати точки P на ній і значення добутків є відкритими і можуть передаватися по незахищених каналах зв'язку. Зрештою користувач A множить знайдене значення на a, а користувач B множить здобуте ним значення на b. Згідно з властивостями операції множення чисел $ab = ba$. Таким чином, обидва користувачі дістануть одне й те саме секретне значення (координати точки ab), яке вони можуть використовувати для отримання ключа шифрування. Зловмисникові для відновлення ключа доведеться розв'язувати складну з обчислювального погляду задачу визначення a і b за відомими E, Pa і Pb.

Мішані програмно-апаратні методи реалізують ті самі функції, що й апаратні та програмні методи, узяті окремо, і мають проміжні властивості. Одним із прикладів їх застосування є формування в персоналу навичок адекватного реагування на будь-які прояви соціотехнічних атак. Одне з головних правил, яким має керуватись кожний працівник,— не довіряти нікому без ідентифікації особи. Орієнтовний алгоритм його реагування на можливу атаку ілюструє рис. 4.3 [133].

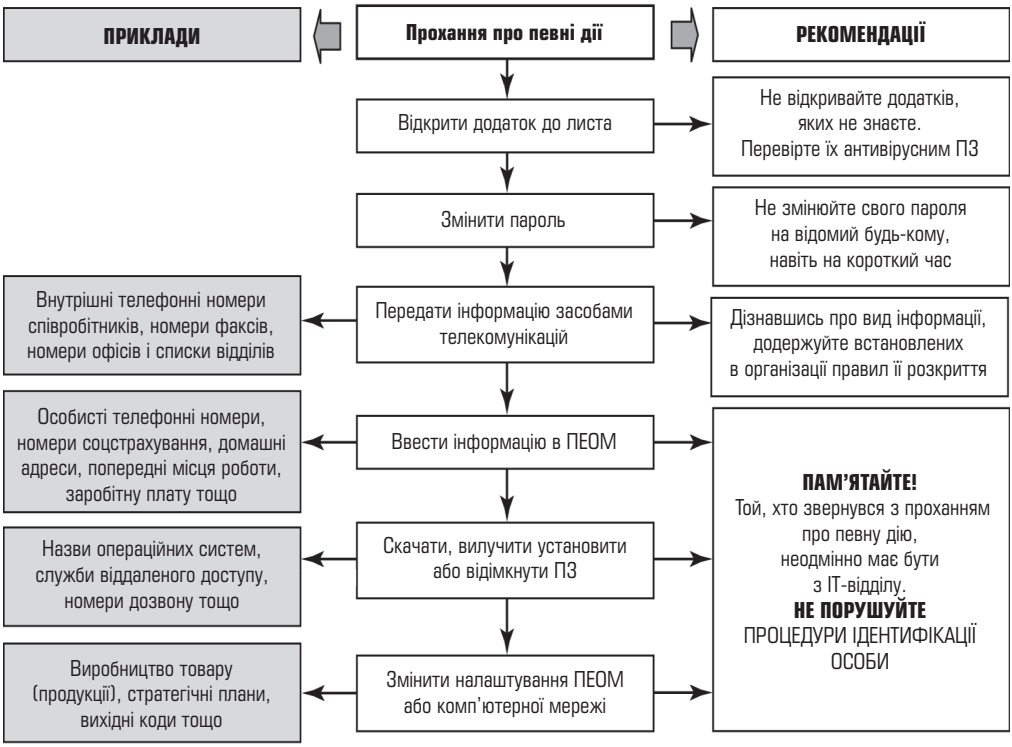


Рис. 4.3. Рекомендації з розкриття атаки, спрямованої на виконання будь-якої дії

Переваги методів програмного захисту — універсальність, гнучкість, надійність, простота встановлення, придатність для модифікації та розвитку. Недоліки — обмежена функціональність мережі, використання частини ресурсів файл-сервера й робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типів комп'ютерів (їхніх апаратних засобів).

4.3. Формалізована модель оцінювання загроз безпеці ІзОД

Щодо впливу на інформацію та систему її обробки найбільший інтерес становлять загрози, класифіковані за метою їх реалізації. На відповідному підґрунті будується, як правило, формалізована модель оцінювання ступеня порушення системи захисту інформації у досліджуваній системі. Згідно з нормативними документами ТЗІ України (НД ТЗІ 1.1-002-99 і НД ТЗІ 2.5-004-99) такі загрози полягають у порушенні *конфіденційності інформації*, її *цілісності* і *доступності* (рис. 4.4).

При цьому до загроз порушення ***конфіденційності інформації*** у ІС відносять спроби:

- несанкціонованого перехоплення електронних і акустичних випромінювань;
- примусового електромагнітного опромінювання (підсвічування) ліній зв'язку;
- несанкціонованого застосування закладених пристроїв і програмних закладок;
- відновлення тексту принтера та дистанційного фотографування;

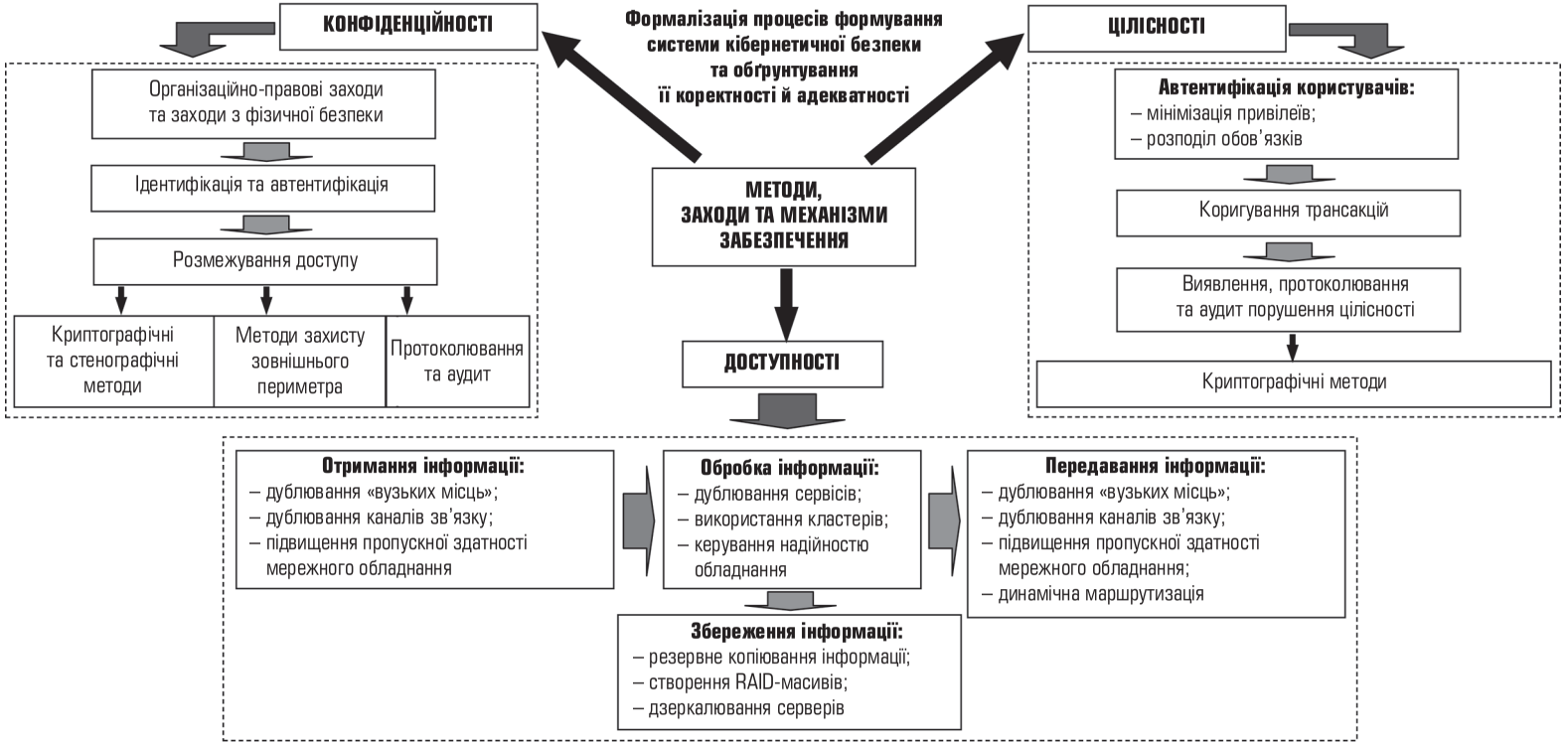


Рис. 4.4. Основні методи й заходи із забезпечення безпеки інформації

• розкрадання носіїв інформації та документальних відходів;

• читання або копіювання як відкритої, так і конфіденційної інформації, імпорту або експорту такої інформації, а також обміну нею між елементами обчислювальної мережі, що належать до різних класів захищеності;

• копіювання носіїв інформації з подоланням засобів захисту;

• маскування під зареєстрованого користувача або під запити системи;

• використання недоліків мов програмування та операційних систем;

• незаконне підімкнення до апаратури та ліній зв'язку;

• виведення з ладу механізмів захисту;

• упровадження та використання комп'ютерних вірусів.

Ці спроби можуть бути реалізовані порушником за умови подолання ним засобів:

• організаційного обмеження доступу ($p_{\text{о.о.д}}$);

• охоронної сигналізації ($p_{\text{о.с}}$);

• захисту від вірусних атак ($p_{\text{атак}}$);

• канального захисту від несанкціонованого доступу із телекомунікаційної мережі до ресурсів ЛОМ ($p_{\text{к.з.т.к.м}}$);

• управління доступом, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо ($p_{\text{у.ф.д}}$);

• адміністрування доступу до відповідних суб'єктів і об'єктів із використанням механізмів загального і спеціального ПЗ ($p_{\text{а.д}}$).

Згідно зі сказаним імовірність подолання неавторизованим користувачем зазначених засобів захисту можна визначити з виразу:

$$p_{\text{п.з.з}} = p_{\text{у.ф.д}}\, p_{\text{а.д}} \left[1 - (1 - p_{\text{о.о.д}})(1 - p_{\text{о.с}})(1 - p_{\text{атак}})(1 - p_{\text{к.з.т.к.м}})\right]. \qquad (4.4)$$

Подальше розкриття змісту інформації з обмеженим доступом може статися лише за тієї умови, що порушник після її отримання:

• знає мову, якою подається інформація (імовірність події — $p_{\text{мова}}$);

• знає і вміє застосовувати програмні засоби або апаратуру криптографічного перетворення (імовірність події — $p_{\text{п.з/кт.п}}$);

• має необхідні ключі або ключові набори для такого перетворення (імовірність події — $p_{\text{ключі}}$).

З огляду на сказане імовірність подолання неавторизованим користувачем засобів криптографічного захисту з урахуванням положень [1; 178–182] можна визначити з виразу:

$$p_{\text{КЗІ}} = p_{\text{мова}}\, p_{\text{п.з/кт.п}}\, p_{\text{ключі}}. \qquad (4.5)$$

Тоді ймовірність порушення конфіденційності інформації з подоланням розглянутих раніше засобів можна визначити так:

$$P_{\text{ПКІ}} = p_{\text{КЗІ}} \left[1 - (1 - p_{\text{п.з.з}})\right]. \qquad (4.6)$$

До загроз порушення ***цілісності інформації*** відносять:

• несанкціоновану модифікацію і/або вилучення програм і даних;

• вставляння, зміну або вилучення даних в елементах протоколу в процесі обміну інформацією між абонентами обчислювальної мережі;

• втрату даних у результаті збоїв, порушення роботоздатності елементів обчислювальної мережі або через некомпетентні дії суб'єктів доступу тощо.

Перелік класів і груп причин порушення цілісності інформації (ППЦІ) наведено в табл. 4.3.

Таблиця 4.3

Класи ППЦІ і перелік потенційно можливих причин порушення цілісності інформації

Найменування групи ППЦІ	Найменування ППЦІ
ВІДМОВИ	
1.1. Відмова основної апаратури	1.1.1. Повний вихід апаратури з ладу
	1.1.2. Неправильне виконання функцій
1.2. Відмови програм	1.2.1. Викривлення коду операції
	1.2.2. Викривлення адреси вибірки
	1.2.3. Викривлення адреси відсилання
	1.2.4. Викривлення адреси передачі керування
	1.2.5. Знищення фрагментів програми
	1.2.6. Неправильне розміщення програм у ЗП
1.3. Відмови людей	1.3.1. Повний вихід із ладу
	1.3.2. Систематично неправильне виконання функцій
1.4. Відмови носіїв інформації	1.4.1. Фізичне порушення носія інформації
	1.4.2. Погіршення характеристик носія
1.5. Відмови систем живлення	1.5.1. Аварійне відімкнення живлення
	1.5.2. Ушкодження ліній електроживлення
	1.5.3. Підвищення напруги, що не відновлюється
	1.5.4. Зниження напруги, що не відновлюється
	1.5.5. Зміна, що не відновлюється
1.6. Відмови систем забезпечення нормальних умов роботи апаратури та персоналу	1.6.1. Відімкнення систем кондиціонування забезпечення
	1.6.2. Зниження продуктивності систем контролю умов роботи кондиціонування апаратури
	1.6.3. Незабезпечення системою кондиціонування персоналу
	1.6.4. Відімкнення інших систем забезпечення нормальних умов роботи апаратури та персоналу
1.7. Відмови систем передавання даних	1.7.1. Повний вихід із ладу каналу зв'язку передавання даних
	1.7.2. Повний вихід із ладу засобів зв'язку
	1.7.3. Неправильне виконання функцій каналом зв'язку
	1.7.4. Неправильне виконання функцій засобами зв'язку
1.8. Відмови допоміжних матеріалів	1.8.1. Дефекти паперу для пристрою друку
ЗБОЇ	
2.1. Збої основної апаратури	2.1.1. Неправильне виконання функцій
2.2. Збої програм	2.2.1. Неправильне виконання коду операції
	2.2.2. Неправильне виконання адреси вибірки
	2.2.3. Неправильне виконання адреси відсилання
	2.2.4. Неправильне виконання адреси передавання керування

Продовження табл. 4.3

Найменування групи ППЦІ	Найменування ППЦІ
2.3. Збої людей	2.3.1. Тимчасовий вихід із ладу
	2.3.2. Епізодичне неправильне виконання функцій
2.4. Збої носіїв	2.4.1. Погіршення характеристик носіїв відновлювальної інформації
2.5. Збої систем живлення	2.5.1. Короткочасне вимикання живлення
	2.5.2. Короткочасне підвищення напруги
	2.5.3. Короткочасне зниження напруги
	2.5.4. Короткочасна зміна частоти струму
2.6. Збої системи забезпечення нормальних умов роботи	2.6.1. Короткочасне відімкнення систем забезпечення кондиціонування
	2.6.2. Короткочасне зниження продуктивності систем кондиціонування
	2.6.3. Короткочасне відімкнення інших систем забезпечення нормальних умов роботи апаратури і персоналу
2.7. Збої систем передавання даних	2.7.1. Неправильне виконання функцій передавання даних каналом зв'язку
	2.7.2. Неправильне виконання функцій засобами зв'язку
2.8. Збої допоміжних матеріалів	2.8.1. Дефекти в пристроях друку, що виправляються
	2.8.2. Дефекти паперу, що виправляються
ПОМИЛКИ	
3.1. Помилки основної апаратури	3.1.1. Неправильний монтаж схеми процедури апаратури
	3.1.2. Неправильний монтаж схеми переходу до процедури
	3.1.3. Неправильний монтаж схеми адреси вибірки
	3.1.4. Неправильний монтаж схеми адреси відсилання
3.2. Помилки програми	3.2.1. Неправильний код операції
	3.2.2. Неправильна адреса вибірки
	3.2.3. Неправильна адреса відсилання
	3.2.4. Неправильна передача керування
	3.2.5. Неправильне розташування елементів програм
3.3. Помилки людей	3.3.1. Неправильне сприйняття інформації
	3.3.2. Неправильний набір інформації
	3.3.3. Неправильний вибір процесу
	3.3.4. Випадкове втручання в процес
3.4. Помилки системи передавання даних	3.4.1. Неправильна схема комутації каналу передавання даних
	3.4.2. Неправильна схема комутації в каналі
	3.4.3. Неправильний монтаж схеми в пристроях зв'язку
СТИХІЙНІ ЛИХА	
4.1. Пожежа	4.1.1. Невелика (локальна)
	4.1.2. Середня
	4.1.3. Загальна (велика)

Продовження табл. 4.3

Найменування групи ППЦІ	Найменування ППЦІ
4.2. Повінь	4.2.1. Місцева (локальна)
	4.2.2. Середня (у межах будинку)
	4.2.3. Загальна (міська)
4.3. Землетрус	4.3.1. Легкий
	4.3.2. Середній
	4.3.3. Сильний
4.4. Ураган	4.4.1. Малий
	4.4.2. Середній
	4.4.3. Сильний
4.5. Вибух	4.5.1. Легкий
	4.5.2. Середній
	4.5.3. Сильний
4.6. Аварія	4.6.1. Невелика
	4.6.2. Середня
	4.6.3. Значна
ЗЛОЧИННІ ДІЇ	
5.1. Запам'ятовування інформації	5.1.1. Запам'ятовування інформації на пристроях наочного відображення інформації
	5.1.2. Запам'ятовування бланків із вихідними даними
	5.1.3. Запам'ятовування вихідної документації
5.2. Копіювання	5.2.1. Фотографування
	5.2.2. Виготовлення неврахованих копій документів
	5.2.3. Роздруковування масивів
5.3. Розкрадання	5.3.1. Розкрадання бланків із вихідними даними
	5.3.2. Розкрадання магнітних носіїв
	5.3.3. Розкрадання вихідних документів
5.4. Підміна	5.4.1. Підміна бланків
	5.4.2. Підміна магнітних носіїв
	5.4.3. Підміна вихідних документів
	5.4.4. Підміна апаратури
	5.4.5. Підміна елементів програм
5.5. Підімкнення	5.5.1. Підімкнення генератора завад
	5.5.2. Підімкнення реєструвальної апаратури
5.6. Злам	5.6.1. Злам апаратури
	5.6.2. Ушкодження програм
	5.6.3. Ушкодження елементів баз даних
	5.6.4. Ушкодження носіїв
	5.6.5. Ушкодження документів

Закінчення табл. 4.3

Найменування групи ППЦІ	Найменування ППЦІ
5.7. Диверсія	5.7.1. Створення пожежі
	5.7.2. Організація повені
	5.7.3. Організація вибуху
	5.7.4. Ушкодження системи електроживлення
	5.7.5. Ушкодження систем забезпечення нормальних умов роботи апаратури і персоналу
ПОБІЧНІ ЯВИЩА	
6.1. Електромагнітні	6.1.1. Випромінювання пристроїв наочного відображення інформації
	6.1.2. Випромінювання процесорів ЕОМ
	6.1.3. Випромінювання зовнішніх запам'ятовувальних пристроїв
	6.1.4. Випромінювання друкувальних пристроїв
	6.1.5. Випромінювання апаратури зв'язку
	6.1.6. Випромінювання ліній зв'язку
	6.1.7. Випромінювання допоміжної апаратури
6.2. Паразитні наведення	6.2.1. Наведення в комутаторах загального призначення
	6.2.2. Наведення в слабкострумових колах
	6.2.3. Наведення в мережах живлення
6.3. Зовнішні електромагнітні випромінювання	6.3.1. Випромінювання біля пристроїв наочного відображення інформації
	6.3.2. Випромінювання біля зовнішніх запам'ятовувальних пристроїв
	6.3.3. Випромінювання біля друкувальних пристроїв
	6.3.4. Випромінювання біля апаратури зв'язку
	6.3.5. Випромінювання біля процесорів
	6.3.6. Випромінювання біля ліній зв'язку
	6.3.7. Випромінювання біля допоміжних пристроїв
	6.3.8. Випромінювання в сховищах носіїв інформації
6.4. Вібрація	6.4.1. Мала
	6.4.2. Середня
	6.4.3. Велика
6.5. Зовнішні атмосферні умови	6.5.1. Зміна температури
	6.5.2. Підвищення вологості повітря
	6.5.3. Підвищення запиленості повітря
	6.5.4. Підвищення рівня радіації
	6.5.5. Зараження повітря отруйними речовинами
	6.5.6. Бактеріологічне зараження повітря

Загрози порушення цілісності інформації можуть бути реалізовані порушником за умови подолання засобів:

• організаційного обмеження доступу, охоронної сигналізації та управління доступом, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо, та адміністрування доступу, як і в разі загроз конфіденційності інформації (імовірність $p_{\text{н.з.з}}$ такої події визначено раніше);

• захисту цілісності від загроз у телекомунікаційних мережах ($p_{\text{ц.т.к.м}}$);

• захисту від спеціальних впливів на інформацію по ТКМ ($p_{\text{сп. впл}}$);

• контролю та поновлення цілісності інформації ($p_{\text{конт.ц}}$).

Отже, знаходимо *ймовірність порушення цілісності*:

$$P_{\text{ПЦІ}} = p_{\text{конт.ц}}\left[1-(1-p_{\text{п.з.з}})(1-p_{\text{сп.впл}})(1-p_{\text{ц.т.к.м}})\right]. \qquad (4.7)$$

До загроз порушення ***доступності інформації*** відносять:

• повторення або сповільнення елементів протоколу;

• придушення обміну в телекомунікаційних мережах;

• використання помилок або недокументованих можливостей служб і протоколів передавання даних для ініціювання відмови в обслуговуванні;

• перевитрату обчислювальних або телекомунікаційних ресурсів.

Ці загрози, як і всі розглянуті раніше, можуть бути реалізовані за умови подолання неавторизованим користувачем систем управління доступом до інформаційних ресурсяв ЛОМ (в обхід механізмів ідентифікації, автентифікації, надання певних повноважень чи привілеїв, із подальшою їх перевіркою в разі кожної зі спроб доступу до ресурсів). Саме тому *стійкість системи управління доступом* як імовірність її неподолання визначається стійкістю процесів ідентифікації та автентифікації самого адміністратора безпеки як користувача з найширшими повноваженнями:

$$p_{\text{с.с.у.д}} = 1 - p_{\text{п.з.з}}. \qquad (4.8)$$

Це завдання може розв'язуватись застосуванням у ІС засобів фільтрації типу міжмережних екранів (*firewall*, брандмауерів), сервісів-посередників (*proxyservices*) тощо. За середньої тривалості обслуговування в СІТС одного запиту та пуассонівського закону розподілу ймовірностей впливу знаходимо ймовірність того, що в момент звернення до інформаційного ресурсу він уже використовується:

$$p_{\text{вик.рес}} = 1 - p_0 = 1 - \exp\left\{-t_{\text{вик.рес}} \cdot \lambda_{\text{зап}}\right\}, \qquad (4.9)$$

де p_0 — імовірність відсутності впливів (імовірність того, що на певному часовому інтервалі виникне рівно нуль впливів); $t_{\text{вик. рес}}$ — середнє значення часу використання ресурсу.

Тоді ймовірність порушення доступності ресурсу набирає вигляду

$$P_{\text{ПДІ}} = 1-\left(1-p_{\text{вик.рес}}\right)\left(1-p_{\text{с.с.у.д}}\right). \qquad (4.10)$$

Отже, підсумкове значення ймовірності порушення системи захисту інформації в такій інформаційній системі, як ЛОМ (втілення загрози за метою реалізації) з урахуванням [1; 178–182] можна знайти з виразу

$$P_{\text{ПСЗІ}} = 1-(1-P_{\text{ПКІ}})(1-P_{\text{ПЦІ}})(1-P_{\text{ПДІ}}). \qquad (4.11)$$

Зауважимо, що поряд із загрозами за метою реалізації є сенс виокремити клас загроз, утворюваний подіями, які залежно від умов можуть вплину-

ти на кожну з відомих складових безпеки інформації, скориставшись механізмом:

• несанкціонованого доступу до ресурсів обчислювальної мережі без застосування штатних засобів обчислювальної техніки;

• несанкціонованого включення до складу комплексів засобів обробки та захисту інформації нових елементів або зміни режимів їхньої роботи;

• виконання програм або дій в обхід системи захисту;

• добору, перехоплення, розголошення або використання нестійких параметрів автентифікації і ключів шифрування (дешифрування);

• нав'язування раніше переданого або помилкового повідомлення, заперечення факту його передачі або прийому;

• некомпетентного використання, настроювання або адміністрування комплексів засобів обробки та захисту інформації;

• внесення деструктивних дій у технологію обробки даних тощо.

За принципами, характером та способами активного впливу на певний об'єкт, який може перебувати у стані зберігання, обробки або передавання інформації між вузлами ІС або всередині вузла, такі події можна класифікувати за трьома характерними ознаками:

1) вони використовують принцип доступу суб'єкта ІС (користувача, процесу) до певного об'єкта (файла даних, каналу зв'язку) або до прихованих каналів, тобто до шляхів передавання інформації;

2) забезпечують активний або пасивний вплив на складові безпеки інформації в ІС;

3) реалізують опосередкований і безпосередній вплив на всю систему, а також на систему дозволів в ІС.

До перелічених загроз безпеці інформації варто додати ще дві:

1) загрозу несанкціонованого обміну інформацією між користувачами;

2) загрозу відмови від інформації, тобто невизнання одержувачем (відправником) факту її одержання (відправлення).

Коли йдеться про відвернення загроз безпеці інформації в ІС за метою реалізації, то передусім слід подбати про забезпечення конфіденційності й цілісності інформації в системі, унеможлививши доступу до неї та модифікацію неавторизованим користувачем її змісту. У цьому плані є сенс вжити насамперед заходів організаційного обмеження доступом, а саме: адміністрування доступу, управління фізичним доступом, криптографічного перетворення, контролю цілісності та охоронної сигналізації.

Щоб запобігти переведенню ресурсу в режим штучної відмови — порушення доступності об'єкта за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, необхідно передбачити ще й такі механізми, як запобігання постійному чи занадто тривалому використанню зазначеного ресурсу; забезпечення стійкості та відновлення процесів у разі збоїв; резервування інформаційних об'єктів; ретельний аналіз потоків запитів від суб'єктів ЛОМ та телекомунікаційних мереж; постійний контроль та поновлення цілісності інформаційних об'єктів (наприклад, у каналах ІС).

Метод визначення значень показників уразливості ІзОД

Зауважимо, що в усій сукупності показників уразливості інформації особливе місце належить ***базовим показникам***. Вони характеризують уразливість інформації в якомусь одному структурному компоненті ІС за деяким

одним КНОІ стосовно того чи іншого потенційного порушника. Схему визначення таких показників в узагальненому вигляді наведено на рис. 4.5 [178].

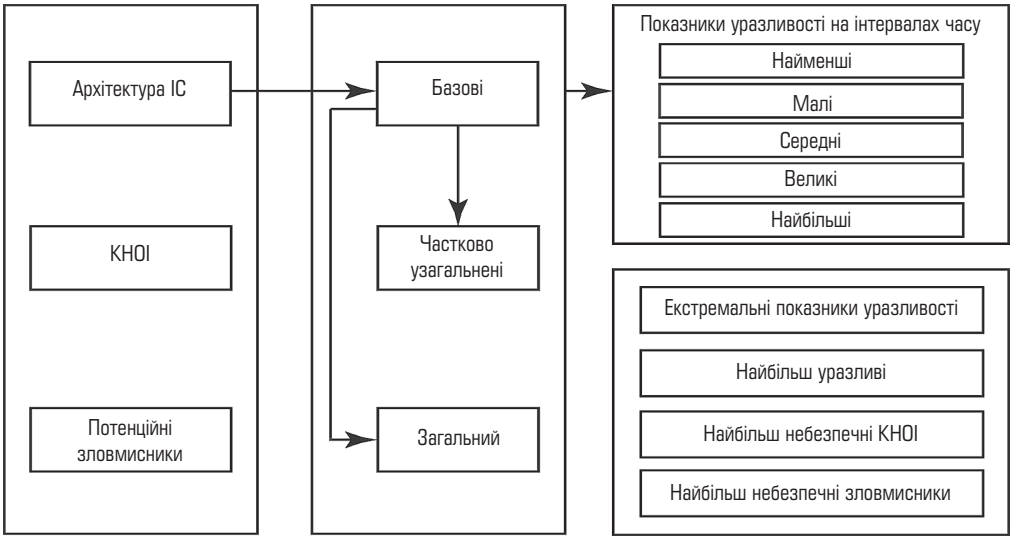


Рис. 4.5. Загальна схема визначення показників уразливості інформації

Значення базових показників визначаються архітектурою ІС (саме від архітектури залежить рівень захищеності кожного структурного компонента системи), множиною потенційно можливих КНОІ (тут засереджено потенціал злочинних дій у структурному компоненті), а також чисельністю потенційних порушників і їхньою здатністю чинити злочинні дії. При цьому варто пам'ятати, що несанкціоноване отримання інформації в сучасних ІС можливе не лише через безпосередній доступ до даних, а й за допомогою багатьох інших інструментів, які не потребують такого доступу.

Розглянемо узагальнену структурну схему потенційно можливих злочинних дій в ІС (рис. 4.6.).

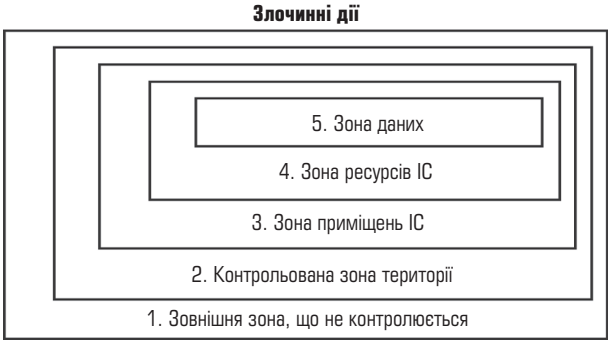


Рис. 4.6. Структурна схема потенційно можливих злочинних дій

Виділені зони характеризуються такими особливостями.

1. ***Зовнішня неконтрольована зона*** — територія навколо ІС, на якій ні персонал, ні засоби ІС не здійснюють жодних заходів для ЗІ.

2. ***Зона контрольованої території*** — територія навколо приміщення ІС, постійно контрольована персоналом або технічними засобами.

3. *Зона приміщень ІС* — внутрішній простір тих приміщень, в яких розташовано засоби системи.

4. *Зона ресурсів ІС* — та частина приміщень, звідки можливий безпосередній доступ до ресурсів системи.

5. *Зона даних* — та частина ресурсів системи, із яких можливий безпосередній доступ до інформації, що підлягає захисту.

Злочинні дії з метою несанкціонованого отримання інформації можливі в кожній із перелічених зон. При цьому несанкціоноване отримання інформації можливе в разі одночасного настання таких подій:

- порушник отримав доступ у відповідну зону;
- під час перебування порушника в зоні в ній з'явився відповідний КНОІ;
- відповідний КНОІ доступний порушникові;
- у КНОІ в момент доступу до нього порушника міститься інформація, що підлягає захисту.

Згідно з теоремою можливостей здатність несанкціонованого отримання інформації порушником k-ї категорії за j-м КНОІ в l-й зоні i-го структурного компонента ІС визначається такою залежністю:

$$P_{ijkl}^{(\text{п},l)} = P_{ikl}^{(\text{п},d)} \cdot P_{ijl}^{(\text{п},k)} \cdot P_{ijkl}^{(j,\text{н})} \cdot P_{ijl}^{(\text{п},u)}. \qquad (4.12)$$

Тут i, j, l — поточний ідентифікатор структурного компонента відповідно ІС, КНОІ, категорії потенційних порушників та зони злочинних дій; P_{ikl} — можливість доступу порушника k-ї категорії в l-ту зону i-го компонента ІС; P_{ijl} — можливість появи j-го КНОІ в l-й зоні i-го компонента ІС; P_{ijkl} — можливість доступу порушника k-ї категорії до j-го КНОІ в l-й зони i-го компонента за умови доступу порушника в зону; P_{ijl} — можливість наявності інформації, що підлягає захисту в j-му КНОІ l-ї зони i-го компонента в момент доступу туди порушника.

Наведена залежність справджується в тому разі, коли всі події, подані в правій частині формули, незалежні одна від одної, тобто настання будь-якої з них не впливає на можливість настання інших подій. У протилежному випадку необхідно враховувати коефіцієнти, що характеризують зв'язок між можливостями настання залежних подій. У даному випадку вважатимемо, що всі події незалежні.

Зауважимо, що базова можливість несанкціонованого отримання інформації розглядається незалежно від зони, про яку йдеться. Раніше зазначену базову можливість реалізації таких зловмисних дій було визначено як можливість несанкціонованого отримання інформації в одному компоненті ІС одним порушником певної категорії та щодо одного КНОІ. Позначимо розглядувану базову можливість як P_{ijk} та запишемо її в такому вигляді:

$$P_{ijk}^{(\text{п},\text{б})} = 1 - \prod_{l=1}^{5} \left[1 - P_{ijkl}^{(\text{п},\text{б})}\right] = 1 - \prod_{l=1}^{5} \left[1 - P_{ikl}^{(\text{п},d)} P_{ijl}^{(\text{п},k)} P_{ijkl}^{(\text{п},\text{н})} P_{ijl}^{(\text{п},u)}\right]. \qquad (4.13)$$

Значення частково узагальнених показників можуть визначатися в такий спосіб. Нехай $\{k^*\}$ — підмножина повної множини потенційно можливих порушників, які нас цікавлять. Тоді можливість несанкціонованого отримання інформації зазначеною підмножиною порушників щодо j-го КНОІ в i-му компоненті ІС визначається виразом:

$$P_{ij}^{(r)}\left\{k^*\right\} = 1 - \prod_{\forall k^*} \left[1 - P_{ijk}^{(\text{б})}\right]. \qquad (4.14)$$

Знак $\forall k^*$ ($\forall$ — квантор загальності) показує, що множення в дужках виконується для всіх k^*, які входять у розглядувану підмножину.

Аналогічно, якщо існує підмножина КНОІ, які становлять інтерес, то уразливість інформаційного компонента цієї підмножини КНОІ щодо k-го порушника можна визначити так:

$$P_i^{(r)}\left\{j^*\right\}k = 1 - \prod_{\forall j^*}\left[1 - P_{ijk}^{(б)}\right]. \tag{4.15}$$

Якщо $\{i^*\}$ — підмножина структурних компонентів ІС, які становлять інтерес, то уразливість інформації в них щодо j-го КНОІ та k-го порушника

$$P^{(r)}\left\{i^*\right\}jk = 1 - \prod_{\forall i^*}\left[1 - P_{ijk}^{(б)}\right]. \tag{4.16}$$

Кожний із наведених виразів дозволяє робити узагальнення за деяким одним параметром. Щоб дістати комплексний вираз, необхідно врахувати одночасно підмножини $\{i^*\},\{j^*\},\{k^*\}$. Тоді загальний показник уразливості

$$P^{(r)} = 1 - \prod_{\forall i^*}\left(1 - P_{ijk}^{(б)}\right)\prod_{\forall j^*}\left(1 - P_{ijk}^{(б)}\right)\prod_{\forall k^*}\left(1 - P_{ijk}^{(б)}\right). \tag{4.17}$$

Тепер знайдемо вирази, що описують ***екстремальні показники уразливості***. Як уже зазначалося, екстремальними можна вважати показники, які характеризують найбільш несприятливі умови захищеності інформації, тобто найуразливіший структурний компонент ІС і КНОІ та найнебезпечнішу категорію порушників.

З огляду на сказане використаємо такі позначення: i — найбільш уразливий структурний компонент ІС; j — найбільш небезпечний КНОІ та k — найнебезпечніша категорія порушників. Тоді маємо:

$$\bar{i} = iEp^{\text{у}} \to \max \forall i, \tag{4.18}$$

де $\bar{i}$ — це таке значення i, для якого заданий показник уразливості $p^{\text{у}}$ набуває максимального значення

Аналогічно:

$$\bar{j} = jEp^{\text{у}} \to \max \forall j, \tag{4.19}$$

$$\bar{k} = kEp^{\text{у}} \to \max \forall k. \tag{4.20}$$

Неважко помітити, що наведені вирази відповідають малим інтервалам часу, але їх не можна зводити до точки. При цьому процеси стосовно уразливості інформації, що відбуваються на таких інтервалах, можна вважати однорідними. Зі зростанням можливостей порушника щодо зловмисних дій і з розширенням можливостей щодо зміни стану ІС і умов обробки інформації час, необхідний для виконання відповідних змін, зростатиме.

Припустимо, що зазначений малий інтервал можна поділити на як завгодно малі проміжки, визначивши на кожному з них уразливість інформації. А оскільки процеси, що відбуваються на розглядуваному малому інтервалі часу, однорідні, то на кожному з таких малих інтервалів уразливість визначатиметься однозначно згідно з такою рівністю:

$$P^{\text{м}} = 1 - \prod_{t=1}^{N_t}\left(1 - P^{\text{т}}\right), \tag{4.21}$$

де $P^{\text{т}}$ — уразливість у точці (на дуже дрібному проміжку, утвореному внаслідок розбиття малого інтервалу); t — змінний індекс дрібних проміжків, на

які розбито малий інтервал; N_t — загальна кількість дуже дрібних проміжків.

Неважко помітити, що розглянутий підхід можна поширити на будь-які види інтервалів, подавши довільний великий інтервал деякою послідовністю менших інтервалів і т. д.

Проте наведені вирази справджуються лише в тому разі, якщо на всьому розглядуваному інтервалі часу умови для злочинних дій лишаються незмінними. У реальному житті вони можуть змінюватися, причому найважливіший фактор, що впливає на можливості вчинення порушень — це здатність системи ЗІ до відповідних активних дій. Технологія функціонування системи ЗІ має бути тим сильніша й активніша, чим вища уразливість інформації.

З урахуванням сказаного можемо записати:

$$P^{\text{т}}(t) = \oint\left[P^{\text{т}}(t-1)\right], \tag{4.22}$$

тобто значення точкового показника в кожній точці розглядуваного інтервалу являє собою деяку функцію від значення цього показника в попередній точці. Тоді вираз (4.21) можна записати в такому вигляді:

$$P^{\text{м}} = 1 - \prod_{t=1}^{N_t}\left\{1 - \oint\left[P^{\text{т}}(t-1)\right]\right\}. \tag{4.23}$$

Розглянуті моделі належать до класу аналітичних, оскільки дозволяють визначати необхідні значення показників уразливості за допомогою аналітичних обчислень.

Утім на практиці через складність відповідних моделей значення вихідних даних для визначення базового показника уразливості інформації можуть залежно від конкретних ситуацій у ІС та зовнішньому середовищі зазнавати всіляких змін, що не підлягають вираженню у вигляді конкретних формул.

Проте нерідко вдається структурувати досліджувані системи та процеси до такого ступеня, що задачу можна буде розв'язати методом моделювання.

Для складних ІС і слабоструктурованих схем функціонування систем обробки інформації найбільш адекватним засобом прогнозування показників уразливості буде статистика.

Для того щоб у статистичний спосіб безпосередньо спрогнозувати значення показників уразливості, потрібно буде залучити багатопараметричні статистичні дані стосовно передісторії досліджуваної ситуації, яких насправді бракує. Адже отримання таких даних становить дуже складну проблему.

Для спрощення задачі прогнозуватимемо не безпосередні показники уразливості, а ті величини, що входять у вираз для показників якості.

Як випливає з моделей оцінювання показників якості, до таких величин слід віднести:

- можливість прояву дестабілізуючих факторів (наявності КНОІ);
- можливість наявності інформації, що підлягає захисту, у конкретному місці під час прояву дестабілізуючих факторів;
- можливість несанкціонованого отримання інформації під впливом дестабілізуючих факторів, незважаючи на застосування заходів щодо ЗІ.

Розглянемо можливі підходи до прогнозування перелічених величин.

Можливість прояву дестабілізуючих факторів — P_{ijz}

Коли йдеться про сталий процес функціонування системи обробки інформації, то прояв дестабілізуючих факторів можна розглядати як випадковий пуассонівський процес.

Нехай *ijz* — інтенсивність потоку *i*-го фактора в *j*-му технічному засобі (ТЗ), що перебуває в *z*-му стані. Тоді згідно з властивостями пуассонівського процесу дістанемо:

$$P_{ijk} = f_{tijk} \cdot \sigma_t, \tag{4.24}$$

де σ_t — інтервал часу, істотно менший від того інтервалу, для якого визначено величину.

Оскільки в загальному випадку інтервал прогнозування цю умову незадовольнятиме, то є сенс подати величину P_{ijk} в такому вигляді:

$$P_{ijk} = 1 - \left(1 - \rho_{ijz}\right) \cdot \left(\frac{\Delta t}{\sigma_t}\right),$$

де Δ_t — інтервал прогнозування.

Отже, згідно з таким підходом увесь період прогнозування Δt можна поділити на менші інтервали тривалістю σ_t, записавши при цьому таке:

$$\bar{j} = jEp^{\text{у}} \to \max \forall j. \tag{4.25}$$

Тоді за умови, що $\Delta t >> \sigma_t$, можна записати:

$$P_j^{\text{м}} = \frac{\sum \gamma_{t\theta} \Delta t}{\frac{\Delta t}{\sigma t}} = \frac{\sigma t}{\Delta t} \sum \gamma_{j\theta}. \tag{4.26}$$

Значення функції визначаються за технологічним графіком обробки інформації у прогнозований період часу.

Можливість несанкціонованого отримання інформації під дією дестабілізуючих факторів, незважаючи на застосування засобів ЗІ

Тут, як і для попереднього параметра, прогнозування здійснюватимемо на малих інтервалах часу. Введемо функцію, що визначається такою умовою:

$$P_{ijk} = \begin{cases} 1, \text{ якщо } j\text{-й засіб захисту на } k\text{-му інервалі часу активно} \\ \quad \text{використовується в } i\text{-му ТЗ;} \\ 0 \text{ — у протилежному випадку.} \end{cases}$$

З урахуванням того, що $\Delta t >> \sigma_t$, можна стверджувати: можливість $P_{ik}^{\text{НО}}$ того, що при використанні η-го засобу захисту в *j*-му ТЗ несанкціонованого отримання інформації не відбудеться навіть у разі появи *i*-го дестабілізуючого фактора, визначається такою формулою:

$$P_{ik}^{\text{НО}} = \prod_{\forall \eta} \left(1 - P_{ij}^{\eta}\right) \cdot \frac{\sigma}{\Delta e} \sum N_{ji}^{\theta}. \tag{4.27}$$

Згідно з концепцією захисту інформації, що передбачає вжиття сукупності взаємозалежних організаційних заходів і застосування технічних систем, синтезованих на основі обраних критеріїв оптимізації з урахуванням обмежень і спрямованих на захист інформації при її формуванні, передаванні, прийманні, обробці та зберіганні з метою забезпечення її цілісності, формується поняття ***захищеності інформації в ІС,*** яке з кількох розглянутих далі вагомих причин слід вважати центральним у сфері кібербезпеки.

По-перше, саме завдання створити систему (модель) ЗІ постало завдяки досягненню високого науково-технічного рівня захищеності інформації в ІС. Зрештою сама методологія оцінювання захищеності інформації є, по суті, методологією наукового обґрунтування кількісних показників досягнення головної мети функціонування системи захисту.

По-друге, методологія оцінювання захищеності інформації в ІС — це передусім методологія наукового обґрунтування норм ефективності ЗІ. Оптимальний (або принаймні раціональний) вибір одиниць виміру і кількісних значень норм ефективності визначає категорію якості системи захисту, структуру та математичний апарат синтезу, аналізу й оптимізації моделі захисту, а отже, і остаточну якість захисту. Адже завищені норми ефективності призводять до підвищення витрат на створення системи захисту, а занижені норми просто не дозволяють досягати цілей захисту.

По-третє, методологія оцінювання захищеності інформації в ІС становить основу для досягнення реального рівня захисту інформації в конкретних системах і його порівняння з нормами ефективності захисту, а отже, і основу для розв'язання питань про методи й засоби організації системи захисту.

Визначаючи критерії якості захисту, а також структуру й математичний апарат синтезу, аналізу й оптимізації моделі системи захисту, методологія оцінювання захищеності інформації визначає цілі, засоби та методологію інженерного аналізу, спрямованого на виявлення потенційних стратегій нападу на інформацію в ІС, а також основні характеристики таких стратегій нападу, що дозволяють визначати можливі заходи захисту та вимоги до їхніх параметрів.

4.4. Доопрацювання засобів захисту інформації

Усі засоби захисту потрібно використовувати так, щоб вони не лише функціонували, а й діяли в цілком передбачуваний і належний спосіб. Це один із найважливіших аспектів безпеки, якому часто не приділяють належної уваги. Як правило, система чи служба вже існує, коли впроваджують її захист, а надалі він, по суті, лишається без нагляду. Існує навіть тенденція ігнорувати наявні засоби захисту, не приділяючи їм необхідної постійної уваги. Більш того, можливих втрат ефективності засобів захисту потрібно всіляко запобігати, а не констатувати як доконаний факт. Необхідно також досягати узгодженості дій із захисту, контролювати робоче оточення, переглядати записи у відповідному журналі та обробляти інциденти, аби гарантувати тривалість стану захищеності інформації. ***Доопрацювання***, хоча ним, на жаль, часто нехтують,— ***один із найважливіших механізмів безпеки інформаційних технологій***. Реалізовані засоби захисту безвідмовно працюють, якщо вони підлягають систематичній перевірці в реальному циклі ділової активності. Потрібно мати впевненість, що ці засоби використовують правильно і що будь-які інциденти й зміни в системі захисту негайно буде виявлено з невідкладним вжиттям відповідних заходів.

Вочевидь, із плином часу з'являється тенденція до погіршення роботи будь-яких служб чи механізмів. Доопрацювання здійснюється для виявлення відповідних негараздів та ініціювання коригувальних дій. Це єдиний спосіб підтримувати належний рівень засобів захисту системи інформаційних технологій.

Управління безпекою інформаційних технологій — процес безперервний, причому підпорядкований завданням реалізації плану безпеки інформаційних технологій [178].

Доопрацювання включає в себе:

• обслуговування засобів захисту для забезпечення їхньої безперервної ефективної роботи;

• перевірку, яка гарантує, що засоби захисту задовольняють вимоги, передбачені чинною методикою і реалізованими проектами;

• контроль активів, загроз, уразливості та засобів захисту, який має на меті запобігати винекненню ризикованих ситуацій;

• дослідження інциденту з метою гарантування відповідної реакції на небажані події.

Отже, доопрацювання — багатогранний тривалий процес, який має спонукати до критичного перегляду рішень, ухвалених раніше.

Супровід. Більшість засобів захисту потребує супроводу та підтримки — дій з боку керівництва, спрямованих на забезпечення правильного й відповідного функціонування цих засобів у процесі їхньої діяльності. Ці дії мають бути заплановані й виконувані згідно з графіком. Завдяки цьому накладні витрати можуть бути мінімізовані із запобіганням втратам цінності засобів захисту.

Для виявлення несправностей необхідна систематична перевірка. Захисний засіб, що ніколи не зазнавав перевірки, не може становити великої цінності, оскільки немає підстав вважати, що він заслуговує на довіру.

Діяльність із супроводу передбачає:

• перевірку журналів;

• зміну параметрів конntрольованих засобів, що має на меті врахувати поточний стан цих засобів;

• повторне ініціювання початкових даних або значень лічильників;

• адаптацію до нових версій.

Вартість супроводу та підтримки з боку керівництва завжди слід брати до уваги, коли йдеться про визначення і вибір засобів захисту. Адже витрати на супровід можуть бути дуже різні для різних засобів захисту. І саме цей чинник нерідко стає вирішальним, коли роблять вибір того чи іншого засобу. Загалом витрати із супроводу та підтримки слід мінімізувати, передусім і тому, що після здійснення вибору конкретних засобів захисту можуть знадобитися не лише одноразові, а й чималі витрати.

Обслуговування. Засоби захисту потребують висококваліфікованого обслуговування, зокрема й управління, коли йдеться про реалізацію повноцінної програми безпеки організації. Усі рівні керівництва несуть відповідальність за обслуговування, оскільки їхнє головне завдання — гарантувати:

• виділення необхідних ресурсів організації для обслуговування засобів захисту;

• періодичну переатестацію засобів захисту, аби ті могли надійно виконувати свої функції;

• модернізацію засобів захисту в разі появи нових безпекових вимог;

• чітко визначену відповідальність за обслуговування засобів захисту;

• незмінність визначеного рівня ефективності наявних засобів захисту в разі модифікації їхнього технічного й програмного забезпечення на базі розширення системи інформаційних технологій;

• запобігання новим загрозам або ураженням при модернізації технологій.

Якщо здійснено розглянуті заходи з обслуговування, то засоби захисту тривалий час виконуватимуть покладені на них функції, а це, у свою чергу, дасть змогу уникати несприятливих і збиткових уражень.

Відповідність засобів захисту. Перевірка засобів захисту на відповідність, тобто аудит чи ревізія захисту, — дуже важливий захід для гарантування відповідності й узгодженості цих засобів із планом безпеки системи інформаційних технологій. Аби гарантувати, що рівень безпеки інформаційних технологій справді ефективний, важливо, щоби впроваджувані засоби захисту завжди й повною мірою відповідали проекту чи плану захисту системи інформаційних технологій. Такий проект чи план необхідно затверджувати на всіх етапах проходження проектів і систем: під час проектування і впровадження, у процесі експлуатації, а також у разі внесення замін або здійснення переміщень.

Перевірку на відповідність доцільно планувати в поєднанні з іншими запланованими заходами. Вибіркові перевірки особливо корисні, коли потрібно з'ясувати, чи відповідає виконавчий персонал усім покладеним на нього вимогам. Процедури перевірки необхідні для забезпечення надійного функціонування засобів захисту, зокрема правильного їх упровадження та випробування (якщо таке знадобиться).

Там, де виявлено, що засоби захисту не відповідають безпеці, має бути складено й реалізовано план коригувальних дій з подальшим аналізом здобутих результатів. Перевірку відповідності захисту доцільно здійснювати стосовно:

- нових систем і після впровадження служб інформаційних технологій (після того, як ті було реалізовано);
- наявних систем після впровадження служб інформаційних технологій (такі перевірки мають здійснюватися систематично, наприклад щороку);
- наявних систем і служб інформаційних технологій у разі змін у методиках безпеки системи інформаційних технологій (мета — визначання коригувань, що знадобляться для забезпечення необхідного рівня захисту).

Перевіряти відповідність захисту може зовнішній чи внутрішній персонал, використовуючи контрольні списки щодо методики безпеки системи інформаційних технологій. При цьому ті засоби захисту, що забезпечують захист системи інформаційних технологій, можуть бути перевірені здійсненням:

- періодичного контролю і випробувань;
- вибіркових перевірок щодо рівня захисту, забезпечуваного у специфічних сферах критичності або важливості.

Під час будь-якої перевірки відповідності захисту можна здобути цінну інформацію про функціонування системи інформаційних технологій за допомогою:

- пакетів програм, що дають змогу фіксувати події;
- контрольних точок, які уможливлюють відстежування повної хронології подій.

Перевірки відповідності захисту, як і всі подальші регулярні перевірки, мають спиратись на найновіші погоджені переліки засобів захисту, складені за результатами аналізу ризиків, на методику безпеки системи інформаційних технологій, а також на затверджені керівництвом процедури функціонування захисту інформаційних технологій, побудовані з урахуванням звітів про

інциденти. Зазначені перевірки дають змогу визначити, чи реалізовано наявні засоби захисту, чи правильно їх упроваджено та введено в експлуатацію.

За нормального режиму функціонування системи необхідно щодня перевіряти, як використовуються засоби захисту. Співбесіди зазвичай також корисні за умови критичного ставлення до отриманих під час такого спілкування відомостей. Такий підхід допомагає скласти всеосяжний контрольний список і розробити доцільні форми звіту. Контрольні списки мають включати в себе загальну ідентифікаційну інформацію, наприклад, деталі конфігурації системи захисту, методичні документи, що враховують особливості навколишнього середовища. Фізичний захист має стосуватися як зовнішніх аспектів (особливість конструкції споруд, зокрема можливість проникнення всередину їх через отвори і прорізи люків), так і внутрішніх (міцність приміщень, облаштування системи виявлення і запобігання пожежам, включаючи сигналізацію). До завдань фізичного захисту належить і своєчасне виявлення потраплянь води або рідини, несправності систем живлення тощо.

Серед багатьох проблем, які не можна залишати поза увагою, слід згадати такі:

• зони, загрозливі щодо фізичного проникнення чи уникнення контролю (блокатори дверей, такі як кодові замки — клавішні чи карткові);

• неадекватні механізми чи неправильно встановленні технічні засоби (наприклад, датчики контролю взято неприйнятного для даної ситуації типу; бракує детекторів диму/нагрівання для приміщень, а ті, що є, встановлено з порушеннями; відсутня адекватна реакція на сигналізацію; пожежну сигналізацію не під'єднано до пункту контролю; у приміщенні зберігаються легкозаймисті матеріали; не повною мірою використовуються засоби резервного живлення та системи відновлення; не завжди прокладено кабелі відповідних типів і не завжди дотримано належної відстані від гострих країв. Щоб знайти недоліки в організації захисту щодо різних аспектів безпеки, зокрема захисту персоналу й управління процесом його захисту, захисту програмного забезпечення тощо, доцільно з'ясувати такі питання:

1) ***для захисту персоналу***: чи отримано інструкції; чи усунено виявлені прогалини; чи персонал дійсно усвідомлює ситуацію і добре обізнаний в захисті; чи залежить ключова функція від однієї особи;

2) ***для управління захистом***: як відбувається документообіг; чи можна документацію загального користування розглядати як справді актуальну; чи налагоджено постійний аналіз ризиків, перевірки стану та ведення звітності інцидентів; чи правильно складаються плани подальшої роботи і чи враховують вони реальну ситуацію в цій сфері;

3) ***для захисту програмного забезпечення***: чи здійснюється дублювання на необхідному рівні; чи можна оцінювати як ефективний вибір ідентифікатора/пароля користувача і процедури; чи охоплюють контрольні точки реєстрацію помилок; чи відповідають оцінювані продукти поставленим вимогам; чи необхідне дублювання для захисту комунікацій; за наявності віддаленого доступу — чи існує необхідне устаткування та програмне забезпечення і чи в належний спосіб усе це використовується; за наявності вимог щодо кодування або авторизації повідомлення — чи впроваджено достатньо ефективну систему управління ключами і відповідними операціями?

Загалом перевірка відповідності захисту — це достатньо складне завдання, розв'язання якого потребує чимало практичного досвіду та якомога повнішої

поінформованості. Ці дії виконуються незалежно від заходів щодо внутрішнього огляду чи контролю.

Керування змінами. Системи інформаційних технологій, як і оточення, в якому вони функціонують, постійно змінюються. Відповідні зміни розглядаються як результат появи нових особливостей і служб чи виявлення нових загроз і вразливостей. Ці зміни, усвою чергу, можуть призвести до винекнення нових загроз і вразливості. Як зміни системи інформаційних технологій можуть розглядатись:

- нові процедури;
- нові особливості;
- модифікації програм;
- апаратні перевірки;
- поява деяких груп нових користувачів (це можуть бути зовнішні чи якісь анонімні групи);
- додаткові роботи з мережами і з'єднаннями.

Якщо йдеться про заплановані зміни в системі, то передусім слід запобігти порушенням, що можуть викликати зміни в механізмах її захисту. Якщо система має пункт керування її конфігурацією чи іншу організаційну структуру з керування технічними змінами системи, то необхідно призначити системного фахівця та його представників на зазначеному пункті, зобов'язавши їх робити висновки про те, чи викликає хоч якусь зміну захисту виявлене порушення, а якщо так, то в який спосіб це відбувається. У разі змін, спричинених придбанням нових апаратних засобів, програмного забезпечення чи служб, необхідно здійснити аналіз, щоб установити нові вимоги захисту. Як правило, більшість змін, внесених у систему, слід розглядати як незначні, що не вимагають поглибленого аналізу ситуації, необхідного, коли зміни великі. Проте певного аналізу потребують навіть найменші зміни. Зрештою для обох типів змін потрібно оцінити як переваги, так і можливі втрати. Коли зміни незначні, це можна зробити неофіційно, під час зустрічей із фахівцями, але остаточні рішення керівництва мають бути задокументовані.

Контроль. Вирішальна стадія циклу захисту інформаційних технологій припадає на контроль усіх здійснюваних кроків. Якщо його проводять коректно, то це дає змогу адміністрації чітко з'ясувати:

- яких поставлених цілей вдалося досягти;
- чи достатньо переконливі здобуті досягнення, а також які специфічні ініціативи впроваджено.

Усі зміни в активах, загрозах, уразливості засобів захисту потенційно можуть мати істотний вплив на ризики, і раннє виявлення змін дозволяє вжити запобіжних заходів. Неодмінно слід вести журнали з безпеки для фіксування подій. Ці журнали слід періодично переглядати, аналізуючи вміщену там інформацію (бажано із залученням статистичних методів). Це допомагає вчасно визначити тенденції до тих чи інших змін і прогнозувати повтори несприятливих подій. Використовувати журнали тільки для аналізу подій, що вже сталися,— означає істотно обмежувати запобіжні можливості засобів захисту.

Контроль має охоплювати також процедури, пов'язані зі складанням звітності контролеру безпеки інформаційних технологій, а також із керуванням на постійній основі процесом забезпечення інформаційної безпеки.

Має бути складено план щоденного контролю. Це дасть змогу впровадити додаткові інструкції та процедури для гарантування поточного функ-

ціонування системи захисту. Користувачі, операційний персонал і розробники системи мають періодично отримувати відповідні консультації, аби мати переконання, що всі проблеми безпеки враховано і реалізовуваний план захисту інформаційних технологій морально не застарів.

Вагомий аргумент на користь контролю як важливого компонента супроводу безпеки інформаційних технологій — це те, що він сприяє виявленню змін, які впливають на захищеність системи.

Перевірці мають підлягати матеріальні носії інформації та її зміст, загрози й уразливості інформації, а також засобів, що підстраховують інформацію. Активи підлягають для виявлення змін їхньої вартості та відповідних змін щодо цілей безпеки системи інформаційних технологій. До таких варіацій можуть призвести зміни:

- бізнесових цілей організації;
- вимог до системи інформаційних технологій;
- інформації, оброблюваної в системі інформаційних технологій;
- устаткування інформаційних технологій.

Загрози та уразливості контролюють, маючи на меті виявляти зміни їхньої важливості (спричинені, наприклад, змінами оточення, інфраструктури чи технічних можливостей) та своєчасно фіксувати появу інших загроз чи уразливостей. До змін загроз і уразливостей можуть призводити, зокрема, зміни активів.

Засоби захисту постійно контролюють, перевіряючи передусім їхню продуктивність і ефективність. Робиться це для того, аби гарантувати їхню дієздатність щодо належного рівня захищеності системи інформаційних технологій. Вочевидь, що зміни активів, загроз і уразливостей впливають на ефективність і відповідність засобів захисту. Окрім того, коли впроваджують нові системи інформаційних технологій чи вносяться зміни до наявних систем, постає потреба гарантувати, що такі зміни не вплинуть на стан наявних засобів захисту і що нові системи оснащено відповідними засобами захисту.

Коли вдалося знайти аномалії в системі захисту, необхідно провести розслідування та повідомити всі обставини керівництву, яке має ухвалити відповідні рішення, зокрема й щодо перегляду політики безпеки системи інформаційних технологій та ініціювання аналізу можливих ризиків.

Щоб досягти погодженості з методикою безпеки системи інформаційних технологій, є сенс виділити певні ресурси для підтримання відповідного рівня щоденного контролю стосовно:

- наявних засобів захисту;
- упроваджених нових систем чи служб;
- запланованих змін у наявних системах чи службах.

Коли йдеться про розкриття справжньої природи того чи іншого складного випадку, необхідно передусім зібрати відповідну інформацію з різних журналів, подавши її у вигляді єдиного звіту щодо цього випадку. Такі зведені звіти випадків далі поглиблено аналізують. Складання звіту випадків — нелегке завдання, головний аспект якого — визначання умов, які дозволять з потрібним ступенем вірогідності поєднати різні записи в журналі.

Зусилля менеджменту стосовно щоденного моніторингу мають зосереджуватись на підготовці документації, що супроводжує оперативні процедури захисту, для подальшого використання. Така документація описує всі дії, спрямовані на гарантування необхідного рівня захисту всієї системи і окре-

мих служб, і нею надалі мають беззастережно керуватися в усіх системах і службах.

Конче потрібно задокументувати всі процедури з модифікації наявної конфігурації захисту, охопивши скориговані параметри захисту та щонайменші зміни будь-якої інформації з керування захистом. Зазначені зміни мають бути узгоджені з процесом керування конфігурацією системи. Необхідно визначити також процедури виконання ручного супроводу, аби гарантувати, що захист не зазнає загроз. Відповідний розподіл процедур має бути описаний для кожного задіяного компонента захисту.

Неодмінно слід визначити умови та періодичність аналізу журналів безпеки, із описом необхідних методів статистичного аналізу та їх застосування. Керівництво має подбати про чіткі інструкції щодо організації аудиту різних оперативних станів за порогом базового.

Обробка інцидентів. Уникнути небажаних інцидентів у сфері захисту неможливо. Кожний інцидент потребує дослідження, настільки глибокого, наскільки вагомого збитку він завдав. Регулювання інциденту допомагає адекватно реагувати на випадкові або навмисні збої нормального режиму роботи системи інформаційних технологій. Саме тому проекти звітності та розслідування інцидентів мають бути придатні для всієї організації та сервісних служб системи інформаційних технологій. Більш того, доцільно об'єднати міжорганізаційні плани звітності, аби дати чітке уявлення про місця, де виникали небажані інциденти, пов'язані з ними загрози, а також їхній вплив на активи інформаційних технологій та ділову активність.

Чіткий план реагування на інциденти має включати в себе вимоги щодо повної хронології всіх подій і заходів. Така інформація допоможе ідентифікувати джерела інцидентів, а також сприятиме зменшенню аналогічних ризиків у майбутньому. Слід визначити й безсумнівний позитивний наслідок зафіксованих інцидентів — готовність компаній інвестувати в засоби захисту.

Аналіз інциденту та його документування мають включати в себе відповіді на кілька головних запитань:

1) що сталося і коли саме;

2) чи діяв персонал згідно з планом;

3) чи вчасно необхідну інформацію було надано в розпорядження персоналу;

4) які дії персонал запропонував виконувати надалі в інший спосіб?

Відповіді на ці запитання допоможуть розкрити сутність інциденту, а також знизити відповідний ризик завдяки підвищенню релевантності проектів і методик захисту інформаційних технологій (сприятимуть, наприклад, удосконаленню засобів захисту, зменшенню уразливості та відповідному адаптуванню програми компетентності у сфері захисті).

Щоб правильно оцінити ризики й визначити ступінь їхньої серйозності, потрібно ретельно проаналізувати кожний із них. Для поглибленого аналізу ризиків і успішного їх усунення необхідна якомога повніша інформація про заходи із захисту. Потрібно зібрати цю інформацію, усебічно проаналізувати й з'ясувати, яку практичну користь з неї можна здобути.

Для якомога повнішого задоволення вимог дійсних і потенційних користувачів усі кроки з аналізу інцидентів слід підпорядковувати саме цим вимогам.

Перш ніж виконувати будь-яку операцію, потрібно скласти ґрунтовний опис інциденту згідно з програмою компетентності щодо захисту. При цьому

має бути гарантовано, що весь потенційно задіяний персонал чітко усвідомлює, у чому полягає дієвий аналіз інцидентів і як можна ефективно використати його результати.

Передусім ці результати дадуть змогу:

• запобігати інцидентам;

• узгоджувати відповідні інструкції з необхідним рівнем компетентності у сфері безпеки інформаційних технологій;

• постачати «аварійну» інформацію комп'ютерним групам реагування на надзвичайні обставини.

Як показує практика, дієвий аналіз небажаних інцидентів забезпечує:

• випереджувальне складання планів обробки зазначених інцидентів, спричинених зовнішньою чи внутрішньою атакою — як логічною так і фізичною, випадковою несправністю устаткування чи помилкою персоналу;

• навчання персоналу, призначеного для розслідування небезпечних випадків, яке дасть змогу сформувати спеціальні групи реагування на надзвичайні обставини.

Фахівці, що входитимуть до груп, мають не лише досліджувати наявні ризики, а й розробляти відновлювальні заходи. Група реагування на надзвичайні обставини може бути внутрішня чи зовнішня щодо організації (наприклад, контрактна).

Якщо за наявності плану відповідних заходів і підготовленого персоналу все ж відбувається небажаний інцидент, то передусім слід уникати поспішних рішень, дбаючи про збереження свідчень, які можуть допомогти в установленні джерела інциденту та забезпеченні захисту цінних активів. Усе це дасть змогу мінімізувати витрати, пов'язані як із самим інцидентом, так і з усуненням його наслідків.

Щоб ефективно запобігати інцидентам, кожна організація має систематично здійснювати:

• заздалегіть задокументовані запобіжні заходи, що включають у себе розробку інструкцій і процедур аналізу інцидентів (із постійним чітким веденням журналу їх реєстації), а також контроль зв'язків із громадськістю;

• інформування про інциденти та їхній вплив;

• оцінювання інцидентів щодо їх серйозності;

• відновлення нормальної діяльності, порушеної внаслідок інциденту;

• керування, спрямоване на обмеження збитків від інциденту, із неодмінним інформуванням керівництва вищого рівня;

• визначення процедур і обов'язків щодо постінцидентних заходів, зокрема досліджень легального характеру та аналізу ризиків.

Зауважимо, що аналіз небезпечних інцидентів дає найвищий ефект, коли йдеться про поєднання бази даних та організаційних зусиль кількох компаній у боротьбі з інцидентами.

Питання для самоконтролю

1. Назвіть канали несанкціонованого доступу до інформації.

2. За якими ознаками здійснюється класифікація каналів несанкціонованого отримання інформації?

3. На скільки класів поділяються канали несанкціонованого отримання інформації? Назвіть їх.

4. Фізичний захист ІзОД. Основні принципи фізичного захисту.

5. Технічний захист ІзОД. Основні принципи технічного захисту.

6. Криптографічний захист ІзОД. Основні принципи криптозахисту.

7. Назвіть основні методи і заходи забезпечення безпеки інформації.

8. Що може призвести до порушення конфіденційності інформації?

9. Що може призвести до порушення цілісності інформації?

10. Назвіть головні порушення цілісності інформації. Наведіть кілька прикладів із власного життєвого досвіду.

11. Що може призвести до порушення доступності інформації?

12. Опишіть загальну схему визначення показників уразливості інформації.

13. Яким особливостями характеризуються виділені зони безпеки інформації?

14. Що таке зовнішня неконтрольована зона?

15. Що таке зовнішня контрольована зона?

16. Що таке зовнішня зона приміщень ІС?

17. Що таке зовнішня зона ресурсів?

18. Що таке зовнішня зона даних?

19. Опишіть особливості проявів дестабілізуючих факторів.

20. Назвіть головні способи вдосконалення засобів захисту інформації.

РОЗДІЛ 5

СОЦІОІНЖЕНЕРНІ МЕТОДИ РОЗВ'ЯЗАННЯ ПРОБЛЕМ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ: ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРОНИКНЕННЯ

Соціоінженерний підхід, що сформувався на базі індустріальної соціології в1930-х роках, передбачає:

- орієнтацію на вивчення та зміну штучних соціальних систем, передусім соціальних організацій;
- застосування наукових методів і засобів у соціальному управлінні;
- безпосереднє поєднання прикладної соціології з практикою соціального управління;
- установку на використання соціальних ресурсів, людського потенціалу в організаціях;
- створення постійних або тимчасових служб, що професійно виконують соціальну роботу.

Насамперед здійснюється орієнтовне зондування досліджуваного соціального об'єкта й оцінюється реальна ситуація через її порівняння з нормативною моделлю. Розбіжність між наявним і бажаним станом справ означає, що існує певна соціальна проблема. Варіант її розв'язання являє собою певну ідею або гіпотезу, що характеризує способи досягнення цілей соціального управління. При цьому складається вичерпний перелік заходів, які дають змогу максимально наблизити (привести у відповідність) реальну ситуацію до нормативної моделі.

Збір і аналіз потрібної інформації дають змогу уточнювати шукані гіпотетичні рішення, виробляючи й реалізуючи на їх основі практичні рекомендації. Водночас здійснюється прогнозування можливих проблемних ситуацій, зумовлених нововведеннями. Такий неодноразово повторюваний цикл розв'язування соціальних проблем становить основу розв'язування проблем соціотехнічної безпеки установи.

Методи соціоінженерної діяльності постійно вдосконалюються, видозмінюються та коригуються відповідно до поточних умов і завдань. В основу цих методів покладено різні види прикладних соціологічних досліджень, виконання яких потребує знань у сфері соціальної діагностики й консультування, а також соціального нормування, прогнозування, програмування й проектування.

Соціальна діагностика — метод оцінювання стану соціального об'єкта. Вплив на організацію тут ґрунтується на саморефлексії: споглядання справжнього стану речей спонукає до намагань удосконалити роботу («ефект дзеркала»). Процес соціальної діагностики може включати в себе:

- виявлення пріоритетності окремих соціальних проблем;
- аналіз і оцінювання окремих показників соціального розвитку;
- аналіз і оцінювання стану соціальної організації в цілому;

• оцінювання результатів соціального розвитку за певний період;

• оцінювання ефективності проведених заходів.

Соціальне планування — метод наукового визначення цілей організації та засобів їх реалізації, згідно з яким загальні цілі конкретизуються у вигляді системи частинних цілей і знаходять вираження як сукупність соціальних показників, якщо не задаються вищими інстанціями. Найчастіше таке планування полягає в екстраполяції існуючих тенденцій.

Соціальне прогнозування, на відміну від соціального планування, що має директивний характер і передбачає однозначне вирішення, має ймовірнісний характер і включає в себе альтернативні вирішення.

Соціальне нормування — метод досліджень і розробок, за допомогою якого розв'язуються проблеми побудови й використання нормативів, що виражають типові вимоги до функціонування соціальних організацій.

Соціальне програмування — різновид соціального планування, під час якого чітко визначаються етапи розв'язування достатньо великих проблем, із виокремленням засобів, заходів, термінів та очікуваних результатів.

Соціальне проектування полягає в науково обґрунтованому визначенні головних параметрів майбутньої соціальної організації з прив'язуванням їх до конкретних умов функціонування останньої.

Соціальне консультування — метод удосконалення практики соціального керування та експертної допомоги керівникам у розв'язуванні складних завдань. Консультування здійснюють професійні консультанти, консультаційні організації, науковці, фахівці.

Розв'язування проблем соціотехнічної безпеки передбачає чітке фіксування застосовуваних способів і засобів організації соціальних процесів, а також відповідної послідовності дій органів управління та виконавців. Це дозволяє об'єднати зусилля керівників і виконавців у єдину систему, чітко визначивши межі дій кожного, а отже, і знизити витрати на підготовку й проведення окремих заходів. Завдяки такому підходу збагачується досвід розв'язування соціальних проблем.

Один із головних способів визначення рівня соціотехнічної безпеки підприємства полягає в оцінюванні ступеня готовності його ІКС до функціонування в умовах соціотехнічних атак проведенням так званих тестів на проникнення, тобто тестуванням системи захисту ІКС.

5.1. Тестування системи захисту інформації на проникнення

Тестування на проникнення, здійснюване за допомогою тестів на подолання захисту (*penetration testing — pentest,* пентест),— доволі популярна в усьому світі послуга, що дозволяє [134]:

• виявляти недоліки у сфері інформаційної безпеки (ІБ) із погляду стороннього спостерігача, не враховані при розробці політики безпеки;

• розкривати внутрішні і зовнішні спроби проникнення в інформаційну систему (ІС) й запобігати їм.

Тестування на проникнення зводиться до реалізації санкціонованої спроби обійти наявний комплекс засобів захисту ІС. У процесі його проведення аудитор відіграє роль зловмисника, мотивованого на порушення ІБ мережі замовника. Як правило, інтенсивній перевірці підлягають технічні засоби захисту корпоративної мережі. Проте залежно від поставлених умов об'єктом оцінювання можуть бути й інші, наприклад соціотехнічні, аспекти безпеки (рівень поінформованості користувачів тощо).

Тестування на проникнення має допомогти користувачеві з'ясувати, по-перше, чи всі положення політики безпеки досягають своїх цілей і використовуються згідно з попереднім задумом, а по-друге, чи існують прогалини в політиці безпеки, якими може скористатись зловмисник для досягнення своїх цілей. Таке тестування може проводитись як у складі аудиту на відповідність стандартам, так і у вигляді самостійної роботи. Наприклад, під час проведення аудиту на відповідність стандарту ISO 17799 елементи *pentest* можуть використовуватися для оцінювання ефективності реалізації таких захисних механізмів, як *захист від шкідливого коду* (10.4), *мережна безпека* (10.6) і т. ін. У вигляді самостійної роботи тести можуть мати на меті:

• по-перше, обґрунтування необхідності проведення робіт із підвищення захищеності;

• по-друге, визначення незалежної оцінки рівня безпеки інформаційної системи.

У першому випадку замовником тестування виступають, як правило, далекоглядні керівники IT підрозділів або підрозділів ІБ. Здобуті результати демонструють вищому керівництву недоліки існуючої системи управління інформаційною безпекою (СУІБ). Оскільки тестування на проникнення — порівняно недорогий вид послуг, то його найчастіше можна провести за рахунок бюджету відповідного підрозділу. У другому випадку роботи проводяться або після впровадження комплексу засобів захисту (КЗЗ), або перед уведенням тестованої системи в промислову експлуатацію. У цьому разі результати тестування дозволяють реально оцінити залишкові ризики, а можливо і виявити приховані недоліки в системі.

Типові тести такого роду спираються на використання (додаток Д):

1) методів соціоінженерії, які дають змогу виявляти рівень поінформованості користувачів;

2) технічних засобів (наприклад, нового web-нтерфейсу), що зазнають випробування на злам.

Плануючи тестування на проникнення, необхідно визначити межі та режим його проведення. Відповідні роботи можуть виконуватися з попереднім повідомленням персоналу (системних і мережних адміністраторів) або без такого попередження. Якщо користувачі й адміністратори не знають про «злам», що готується, керівництво має добру нагоду оцінити ефективність чинних механізмів виявлення та розслідування комп'ютерних інцидентів. Проте «прихований» тест підвищує ймовірність виникнення відмови через помилку експерта або не зовсім коректне настроювання серверів і мережного обладнання.

Залежно від вибору мережі, з якої здійснюється проникнення в систему, тести поділяють на дві групи:

1) *зовнішні* — моделюються дії зловмисника, що здійснює проникнення в інформаційну систему клієнта з мережі Інтернет;

2) *внутрішні* — моделюється поводження інсайдера (зловмисника, що якимось чином отримав доступ до внутрішньої мережі компанії й намагається через неї проникнути в інформаційну систему).

При цьому аудитори використовують методи, відомі як метод чорного і метод білого ящика.

Метод чорного ящика (*black box test*) полягає в оцінюванні захищеності інформаційних ресурсів (ІР) організації, доступ до яких можна отримати з мережі Інтернет, тобто йдеться про зовнішнє тестування на проникнення.

Моделюються дії зловмисника, що володіє тільки загальнодоступними відомостями про компанію (доменні імена, зовнішні IP-адреси тощо).

Метод білого ящика (*white box test*) передбачає оцінювання захищеності IP організації, доступ до яких можна отримати із внутрішньої мережі. Моделюються дії інсайдера, що заволодів певними відкритими або закритими інформаційними ресурсами, такими як структура мережі компанії, результати щоквартального сканування уразливостей, раніше проведених тестів на проникнення.

Таблиця 5.1

Алгоритм дій при використанні технічних і соціоінженерних методів під час комплексного тестування на проникнення

Технічні методи	Соціоінженерні методи
1. Отримання попередньої інформації про мережу Замовника. Використовуються ті самі джерела інформації, які доступні зловмисникам (Інтернет, новини, конференції). **2.** Складання карти мережі, визначення типів пристроїв, ОС, додатків за особливостями реакції на зовнішній вплив. **3.** Ідентифікація уразливостей мережних служб і додатків. **4.** Аналіз web-додатків Замовника. За допомогою автоматизованих утиліт і ручних методів виконується детектування на предмет: упровадження операторів SQL (SQL Injection); міжсайтового виконання сценаріїв (Cross-Site Scripting); підміни вмісту (Content Spoofing); виконання команд ОС (OS Commanding); виконання уразливостей, пов'язаних із некоректним настроюванням механізмів автентифікації та авторизації тощо. **5.** Експлуатація уразливостей. Методи та інструментарі вибираються індивідуально для кожного типу уразливості. Може бути використано не лише загальнодоступні утиліти, а й інструментарій власної розробки. **6.** За узгодженням із Замовником можуть проводитися базові роботи з контролю захищеності безпроводових мереж. **7.** За узгодженням із Замовником може бути проведено перевірку стійкості зовнішнього периметра й відкритих ресурсів на атаки типу відмови в обслуговуванні. При цьому оцінюють ступінь стійкості мережних елементів і можливий збиток при проведенні найбільш імовірних сценаріїв таких атак. **8.** Перевірка стійкості мережі до атак на канальному рівні. Проводиться моделювання атак на протоколи канального рівня STP, VTP, CDP, ARP. **9.** Аналіз мережного трафіку. У разі проведення робіт у мережі Замовника або якщо отримано таку можливість у ході експлуатації уразливостей, аналізується мережний трафік із метою отримання, наприклад, паролів користувачів, конфіденційних документів тощо. **10.** Перевірка стійкості маршрутизації. Проводиться моделювання маршрутів і проведення атаки типу відмови в обслуговуванні проти використовуваних протоколів маршрутизації. **11.** Перевірка можливості отримання зловмисником несанкціонованого доступу до конфіденційної інформації або інформації обмеженого доступу Замовника. Проводиться як перевірка прав доступу до різних IP Замовника із привілеями, отриманими на різних етапах тестування. **12.** Отримана в ході аналізу уразливостей і спроб їх експлуатації інформація документується та аналізується для вироблення рекомендацій щодо поліпшення захищеності мережі	**1.** Із Замовником узгоджуються методи соціальної інженерії, які буде використано при проведенні тесту, наприклад: • розсилання поштових/IM повідомлень від імені анонімних користувачів і співробітників Замовника, що містять: а) посилання на web-ресурси з виконуваним кодом; б) виконуваний код у тілі листа; в) прохання змінити паролі чи переслати їх або свою персональну інформацію тощо; • вибіркову перевірку виконання політики «чистого стола» (стікери з паролями; незаблоковані на період відсутності користувача консолі; наявність конфіденційних документів в офісі, доступних відвідувачам; залишені без догляду стільникові телефони й КПК тощо); • дзвінки користувачам від імені IT персоналу і персоналу служби ІБ із проханнями отримання/зміни пароля, пересилання конфіденційних документів тощо. **2.** Вибір цільових груп користувачів і визначення методів тестування для кожної із груп. **3.** Проведення тестування: розсилання поштових повідомлень, дзвінки користувачам, виїзд в офіс Замовника для проведення дослідження. **4.** Використання отриманих у результаті попередніх етапів привілеїв для отримання несанкціонованого доступу до ресурсів Замовника (див. *технічні методи*)
Аналіз і консолідація результатів різних тестів	

Найбільш близький до реальних дій зловмисників так званий ***комплексний тест на проникнення*** [136–139]. Використовуючи різні технічні й соціоінженерні прийоми (табл. 5.1), аудитори в ході його проведення намагатимуться обійти наявні захисні механізми, аби виконати поставлені Замовником завдання (підвищення привілеїв, отримання доступу до конфіденційної інформації, модифікація даних із СУБД тощо).

Усі спроби проникнення мають контролювати обидві сторони — як «зловмисник», так і «клієнт». Це допоможе протестувати систему набагато ефективніше. При цьому особа, яка проводить тестування, має відповідати таким вимогам:

- мати ґрунтовні технічні знання;
- уміти швидко налагоджувати контакти з людьми;
- справляти позитивне враження на керівництво та співробітників.

Більш того, ця особа, як і потенційний зловмисник, повинна мати достатньо часу, терпіння та технічного оснащення.

Залежно від поточних потреб і завдань клієнта можливі три різні за глибиною і складністю виконуваних перевірок рівні тестування на проникнення (табл. 5.2).

Таблиця 5.2

Рівні тестування на проникнення

Рівень 1	Рівень 2	Рівень 3
Автоматизована перевірка рівня захищеності інформаційних ресурсів щодо атак із боку шкідливого коду (хробаків) і зловмисників, які мають невисоку кваліфікацію (скажімо, хакерів-початківців). Виявлення уразливостей означає, що існує висока ймовірність реалізації загроз стосовно IP незалежно від ступеня його важливості й типу оброблюваної інформації	Автоматизована перевірка захищеності IP щодо цілеспрямованих атак зловмисників, які мають високу кваліфікацію та мотивацію. Виявлення уразливостей показує, що існують потенційні ризики стосовно IP та IC, що обробляють конфіденційну інформацію чи надають важливі сервіси, якими можуть скористатися зловмисники	Автоматизована перевірка захищеності IP проти цілеспрямованих атак із боку як внутрішніх, так і добре підготовлених зовнішніх зловмисників, що володіють інсайдерськими даними про тестовану систему або додаток. Це може бути інформація про конфігурацію системи, облікові записи користувачів і адміністраторів, вихідний код додатків, внутрішні регламенти, процедури тощо

Алгоритм цього процесу унаочнює рис. 5.1.

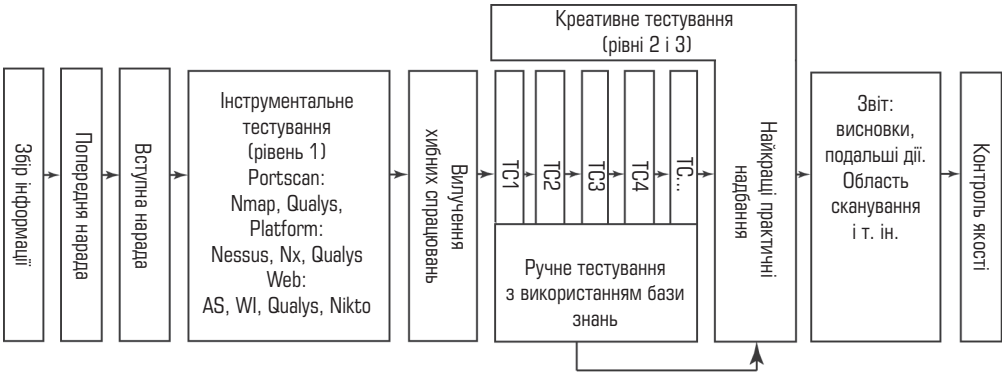


Рис. 5.1. Схема алгоритму реалізації тесту на проникнення

Тестування 1-го рівня виконується за допомогою спеціальних програмних засобів (сканерів уразливостей, типових наборів експлойтів і т. ін.). Тестування 2-го і 3-го рівнів здійснюється вручну, дозволяючи виявити уразливості, які не можуть бути знайдені в ході тестування 1-го рівня. На цьому етапі можуть бути виявлені, зокрема, уразливості, пов'язані з конфігурацією конкретних систем клієнта, а також нові уразливості в додатках, наприклад так звані уразливості нульової доби — *zero-day*. Після проведення тестування вручну виконавець аналізує результати, порівнюючи їх з результатами тестування 1-го рівня. Можна також провести аналіз пропущених уразливостей (*FalseNegatives — FN*), тобто уразливостей, які не вдалося знайти. Після виявлення таких уразливостей вибірково (за домовленістю із Замовником) здійснюються заходи з їх експлуатації (аби продемонструвати Замовникові можливі наслідки). Окремо слід обговорити процедуру виконання атак, які можуть істотно вплинути на функціонування систем і процесів Замовника, наприклад DoS атак.

За результатами роботи складається звіт, що містить:

- методику проведення тестування;
- висновки для керівництва, що включають у себе загальну оцінку рівня захищеності;
- опис виявлених недоліків СУІБ;
- опис ходу тестування з інформацією про всі виявлені уразливості та результати їх експлуатації;
- рекомендації з усунення виявлених уразливостей.

Логічним продовженням тестування на проникнення можуть бути роботи з побудови комплексної системи управління рівнем захищеності, проведення моніторингу захищеності периметра корпоративної мережі, розробка програми підвищення поінформованості з питань ІБ та впровадження системи управління ІБ.

Комплексна система управління рівнем захищеності має забезпечувати:

- пошук уразливих місць у системному й прикладному програмному забезпеченні, програмно-апаратних пристроях (операційних системах, СУБД, web-серверах, прикладних системах, міжмережних екранах, маршрутизаторах тощо), які може використати зловмисник для здійснення несанкціонованої діяльності;
- оцінювання рівня критичності ідентифікованих уразливостей, а також можливості їх експлуатації;
- надання рекомендацій з усунення знайдених уразливостей;
- формування трендів щодо змін стану захищеності протягом певного часу, на базі яких персонал, відповідальний за забезпечення ІБ Замовника, вчинятиме превентивні дії.

Побудова такої системи дозволить:

- підвищити рівень захищеності інформаційних систем компанії;
- знизити кількість інцидентів, пов'язаних із порушенням інформаційної безпеки;
- підвищити ефективність діяльності служби ІБ та її взаємодії зі службою ІТ;
- сформувати об'єктивну картину рівня захищеності як у межах окремих підрозділів, так і в усій організації загалом.

У процесі ***моніторингу захищеності периметра корпоративної мережі*** має бути реалізовано заходи щодо:

• ретельного дослідження периметра корпоративної мережі та організації його захисту (формують звіт стосовно виявлених уразливих і проблемних ділянок і рекомендації, спрямовані на їх усунення. Коли йдеться про усунення уразливостей, забезпечується консультування фахівців Замовника);

• формування графіка проведення моніторингу та здійснення політики з управління рівнем захищеності, основою якої може бути, наприклад, застосування одного із сканерів уразливостей, наведених у табл. 5.3 [135];

Таблиця 5.3

Мережні сканери безпеки

Назва	Версія	Посилання
Nessus	3.2.1	http://www.nessus.org/download
MaxPatrol	8.0 (Складання 1178)	http://www.ptsecurity.ru/maxpatrol.asp
Internet Scanner	7.2.58	http:// www-935.ibm.com/services/us/index.wss/ offering/ iss/a1027208
Retina Network Security Scanner	5.10.2.1389	http://www.eeye.com/html/products/retina/ index.html
Shadow Security Scanner (SSS)	7.141 (Build 262)	http://www.safety-lab.com/en/products/ securityscanner.htm
NetClarity Auditor	6.1	http://netclarity.com/ branch-nacwall.html

• визначення контактних осіб з боку Замовника, яким будуть надсилатися звіти (визначаються особи, з якими необхідно підтримувати оперативний зв'язок при виявленні висококритичних уразливостей);

• фіксування стану периметра мережі (за узгодженням із Замовником);

• проведення щоденного моніторингу інформації про уразливості мережних служб Замовника, доступних із мережі Інтернет;

• періодичного сканування мережного периметра відповідно до встановленого графіка (при виявленні змін мережного периметра, таких як поява нових вузлів, нових мережних служб, здійснюється аналіз цих змін із погляду безпеки);

• консультування фахівців Замовника на предмет серйозності виявлених уразливостей і способів їх усунення;

• внесення змін у політику та графік моніторингу в разі змін або в архітектурі мережного периметра, або у функціональному призначенні ресурсів чи в конфігурації засобів захисту.

Результати порівняльного аналізу мережних сканерів наведено в табл. 5.4.

На провідні позиції за всіма критеріями пропонованого порівняння вийшов сканер MaxPatrol, що, по-перше, забезпечує високоякісну ідентифікацію сервісів і додатків. Друга причина його домінування — повнота бази та її адекватність як поставленому завданню, так і сучасним вимогам загалом. Третя причина переможних оцінок — здатність поглиблено аналізувати версії додатків з урахуванням операційних систем, дистрибутивів і різних «відгалужень». І, зрештою, MaxPatrol має дуже зручний і логічний інтерфейс, що відбиває основні етапи роботи мережних сканерів безпеки. На другому місці опинився сканер Nessus. Він показав, у цілому, непогані результати, а в ряді момен-

тів був навіть точніший за сканер MaxPatrol. Головна причина відставання Nessus — це пропуски уразливостей, але не через відсутність перевірки в базі, як у більшості інших сканерів, а внаслідок особливостей реалізації. По-перше (і цим зумовлено значну частину пропусків), у сканері Nessus намітилася тенденція розвитку убік «локальних» або системних перевірок, що припускають підімкнення з обліковим записом. По-друге, у сканері Nessus враховано менше (порівняно з MaxPatrol) джерел інформації про уразливості. Це саме стосується сканера SSS, що спирається переважно на базу SecurityFocus. Результати інших сканерів, як випливає з табл. 5.4, істотно нижчі [135].

Таблиця 5.4

Результати порівняння мережних сканерів безпеки

Показник	MaxPatrol	Internet Scanner	Retina	Nessus	Shadow Security Scanner	NetClarity Auditor
Ідентифікація сервісів і додатків, бали	108	66	80	98	79	54
Знайдено уразливостей, усього	163	51	38	81	69	57
З них помилкових спрацьовувань (false positives)	8	3	4	7	36	14
Знайдено правильно (з 225 можливих)	155	48	34	74	33	43
Пропуски (false negatives)	70	177	191	151	192	182
З них через відсутність у базі	63	170	165	59	150	179
– через необхідність автентифікації	0	6	16	36	0	0
– з інших причин	7	1	10	56	42	3

Основна мета ***розробки програми поінформованості*** — сформувати механізм доведення вимог ІБ до всіх категорій співробітників компанії та контролю за поінформованістю співробітників. Усі співробітники повинні розуміти свої обов'язки й відповідальність за забезпечення ІБ. У загальному випадку порядок проведення робіт такий:

- визначення областей ІБ, в яких необхідно підвищити поінформованість співробітників;
- збір і аналіз чинних у компанії організаційних документів щодо ІБ, інформація з яких має бути доведена до співробітників;
- розробка вимог ІБ у тих сферах, в яких Замовник не має нормативних документів;
- формування програми поінформованості.

Результатом такої роботи має бути складена **Програма поінформованості співробітників з питань ІБ**, яка включає в себе перелік вимог стосовно ІБ і категорій співробітників, для яких призначено Програму, порядок її реалізації та способи доведення до співробітників положень Програми й контролю виконання її вимог; курси з питань інформаційної безпеки у форматі Microsoft PowerPoint, що охоплює різні сфери ІБ, контрольний список питань для кожного курсу. Можуть створюватися також маркетингові матеріали: листівки, постери, флешроли, відеоролики тощо.

У ході ***впровадження системи управління ІБ*** **(*СУІБ*)** необхідно визначити осіб, відповідальних за забезпечення ІБ, і регламентувати взаємодію між ними; формалізувати процеси управління системою захисту; визначити корпоративні норми й правила, яких мають дотримуватись усі співробітники компанії.

Існує чимало загроз ІБ, від яких неможливо або вкрай складно захиститися тільки технічними засобами. Передусім ідеться про внутрішні загрози, створювані співробітниками компанії. Адже близько 80% збитку завдають інциденти, викликані саме ними. У подоланні таких загроз на перший план виходять організаційні заходи. Організаційне забезпечення ІБ має спиратися на взаємозалежну структуру об'єднаних спільними принципами документів — від суто концептуальних до цілком конкретних, зорієнтованих на ту чи іншу технологію чи сферу діяльності (концепції ІБ, політики ІБ, інструкції та регламенти щодо ІБ). Наприклад, ***Концепція інформаційної безпеки*** має визначати мету, завдання та принципи забезпечення ІБ. У цій Концепції має бути описано об'єкти захисту із зазначенням критичних ресурсів і бізнес-процесів, побудовано моделі загроз і потенційного зловмисника, сформовано цільову функціональну архітектуру системи забезпечення ІБ, а також визначено зони відповідальності підрозділів компанії за забезпечення ІБ.

Документ, що визначає загальну політику безпеки, має містити:

- вимоги щодо автентифікації;
- вимоги щодо контролю й розмежуванню доступу;
- правила надання доступу до ресурсів;
- вимоги щодо обробки інформації, яка становить комерційну таємницю, і персональних даних;
- вимоги щодо роботи із засобами виключеного доступу, мобільними засобами доступу, електронною поштою, мережею Інтернет, засобами криптографічного захисту;
- вимоги щодо антивірусного захисту, резервного копіювання.

Інструкції з ІБ, на відміну від концепцій і політик, пов'язані безпосередньо з конкретними ролями, а ***регламенти з ІБ*** — із відповідними процесами. Інструкції розробляються для певних категорій персоналу (ролей) Замовника. Вони мають містити опис обов'язків, повноважень і відповідальності, що покладаються на ту чи іншу роль, опис того, як ця роль взаємодіє з іншими ролями. Інструкції може бути розроблено, наприклад, для адміністраторів ІБ, аудиторів ІБ, аналітиків ІБ. Окремо можуть розроблятися розділи щодо ІБ в інструкції для корпоративних користувачів і співробітників IT служби.

Регламенти призначено для того, щоб формалізувати процеси, пов'язані із забезпеченням ІБ, і визначити ролі, відповідальні за коректну організацію того чи іншого процесу. Регламенти можуть бути розроблені з метою:

- організації процесів резервного копіювання та відновлення;
- антивірусного захисту;
- випуску, експлуатації та відкликання криптографічних ключів;
- управління обліковими записами користувачів;
- обробки інцидентів ІБ;
- обробки позаштатних/надзвичайних ситуацій.

Отже тестування на проникнення, що імітує дії зловмисника згідно з поставленими цілями й неодмінно досвідченим фахівцем, практично завжди результативне. Саме воно дає змогу виявляти реальні проблеми інформаційної

безпеки в компанії й привертати до них увагу керівництва. Адже про наявну якість захисту найпереконливіше може засвідчити демонстрація успішного доступу до інформації, що вважається добре захищеною, або демонстрація повного контролю над особистими комп'ютерами відповідальних співробітників.

5.2. Постановка задачі експертного оцінювання

На кожному з рівнів тестування на проникнення нерідко доводиться оцінювати параметри інформаційно-комунікаційної системи. Такі оцінки знаходять безпосереднім вимірюванням, обчисленням за відомими аналітичними формулами, а також завдяки застосуванню неформальних методів оцінювання, що базуються на оцінках фахівців у відповідній сфері, насамперед методів експертного оцінювання.

Під ***експертним оцінюванням*** розуміють комплекс взаємозалежних заходів, що визначають мету роботи, умови й способи її організації і проведення, а також права та обов'язки залучених до такої діяльності осіб [140]. Експертне оцінювання поділяється на ***інтегральне*** (оцінюються кінцеві результати), ***диференційоване*** (оцінюються окремі складові проблеми) та ***структурне*** (оцінюється ступінь взаємодії між елементами об'єкта з метою їх подальшого аналізу і синтезу).

Здійснюється експертне оцінювання за певним набором критеріїв — так званих ***оцінних факторів***. Останні, у свою чергу, поділяються на ***основні*** і ***допоміжні***. Усі оцінні фактори можуть бути як ***детерміновані*** (визначаються на підставі суворих детермінованих залежностей), так і ***стохастичні*** (описуються випадковими величинами з відомим законом розподілу), а можуть мати й цілком ***невизначений характер*** (для кожного з них може бути відома лише область можливих значень). З огляду на сказане *будь-яке завдання експертного оцінювання можна сформулювати в такий спосіб*:

При заданих значеннях детермінованих $A_1, \ldots, A_i, \ldots, A_p$, невизначених $B_1, \ldots, B_i, \ldots, B_n$ і стохастичних $X_1, \ldots, X_i, \ldots, X_n$ факторів знайти оптимальне значення $Y_1, \ldots, Y_i, \ldots, Y_m$ з області $Q_{Y_1}, \ldots, Q_{Y_i}, \ldots, Q_{Y_m}$, тобто *розв'язати певну конфліктну ситуацію через вихід на нове цілісне бачення об'єкта (процесу) з ширшим колом інтересів* (рис. 5.2).

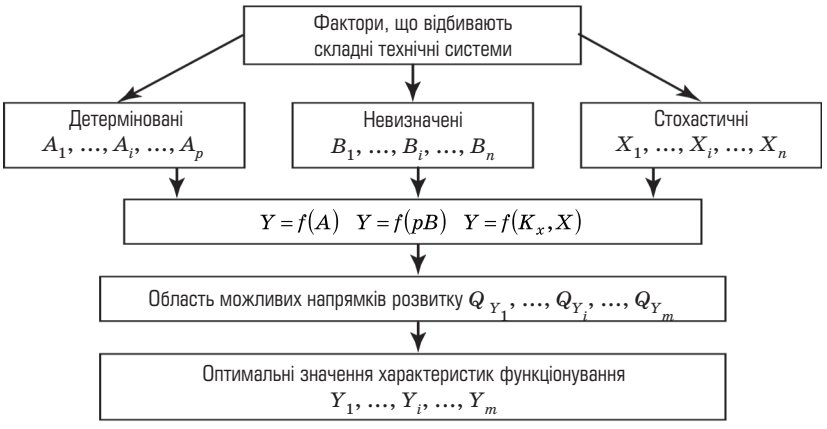


Рис. 5.2. Структурно-логічна схема проведення експертного оцінювання

Головні етапи розв'язання цього завдання такі:

• формулювання мети і завдань оцінювання;

• формування рішення щодо організації та проведення оцінювання, а також добір складу групи управління;

• добір експертної групи та формування опитувальних анкет;

• вибір методу отримання експертної інформації та способу її опрацювання;

• аналіз матеріалів експертного оцінювання;

• інтерпретація здобутих результатів і підготовка висновку для особи, яка ухвалює рішення (ОУР);

• упорядкування звіту.

Етап формулювання мети і завдань експертного оцінювання *є основний.* Багато в чому він визначається суттю досліджуваної проблеми. Від нього залежить також надійність і прагматична цінність очікуваного результату. Ступінь реалізації етапу здебільшого зумовлюється:

• повнотою наявної вхідної інформації та її надійністю;

• термінами і формою подання Замовникові здобутих результатів;

• можливістю залучення фахівців з інших галузей знань.

Завдання щодо організації та проведення експертного оцінювання ставить і оформлює у вигляді рішення Замовник. Цим самим рішенням визначається керівник експертизи, який, у свою чергу, формує експертну групу управління. На групу управління в процесі експертного оцінювання покладається не лише вся організаційно-планова робота із забезпечення сприятливих умов для ефективної творчої діяльності експертів, а й аналітична робота з добору експертної групи, визначення методів отримання та опрацювання інформації, упорядкування опитувальних анкет, змістовної інтерпретації здобутих результатів. Для розв'язання цих задач у групу управління доцільно включити висококваліфікованих комунікабельних фахівців як у галузі розглядуваної проблеми, так і в інших галузях знань — математиці, психології, соціології тощо.

Добір експертної групи і визначення її оптимального кількісного складу — надзвичайно важливе практичне завдання групи управління [141]. При цьому характеристики її членів визначаються на основі індивідуальних рис експертів, передусім їхньої компетентності, креативності, конформізму, ставлення до експертизи, конструктивності мислення, колективізму, самокритичності тощо.

Вибір методу отримання експертної інформації та способу її опрацювання здійснюється так: група управління розробляє докладний сценарій проведення збору та аналізу експертних думок (оцінок), що передбачає не лише конкретний вид експертної інформації (слова, умовні градації, числа, ранжування, розбиття або інші види об'єктів нечислової природи), а й конкретні методи аналізу цієї інформації (обчислення медіани Кемені, статистичний аналіз парних порівнянь, інші методи статистики об'єктів нечислової природи чи прикладної статистики).

Опрацювання та якісний аналіз експертної інформації — завершальний етап експертного оцінювання, що включає в себе:

• оцінювання ступеня погодженості думок експертів з урахуванням догм погодженості і одновимірності;

• виділення груп експертів із близькою думкою (за наявності істотної розбіжності в їхніх відповідях);

• виявлення розкиду думок, впливу характеристик експертів на зміст їхніх відповідей;

• ранжування відповідей в однорідних групах та формування об'єднаних відповідей.

При цьому *догма погодженості* передбачає, що рішення може бути ухвалено лише на основі погоджених думок експертів. Тому з експертної групи виключають тих, чия думка відрізняється від думки більшості. Це можуть бути особи, що потрапили до складу експертної комісії через непорозуміння або з міркувань, що не стосується їхнього професійного рівня. До такої категорії можуть належати й найбільш оригінальні мислителі, які проникли в досліджувану проблему набагато глибше за всіх інших. Перевірка погодженості здійснюється на основі коефіцієнтів рангової кореляції Кендалла або Спірмена, відомих як коефіцієнти конкордації. При цьому позитивний результат перевірки погодженості означає не більше і не менше, як відхилення статистичної гіпотези про незалежність і рівномірну розподіленість думок експертів на множині всіх ранжувань. *Догма одновимірності* відіграє роль у разі, коли конкретна (вузька) постановка задачі перед експертами має особливу вагу. Найчастіше ж такої постановки немає, причому намагання розробити узагальнений показник якості, наприклад у вигляді лінійної функції від певних змінних, не дають змоги зробити об'єктивні висновки. Альтернативою єдиному узагальненому показнику є математичний апарат типу багатокритеріальної оптимізації — множини Парето тощо. [142].

Інтерпретація здобутих результатів — етап, необхідний для організації зворотного зв'язку у процесі експертного оцінювання. Зворотний зв'язок з експертами група управління може здійснювати або за методом Дельфі, або за іншими методами (методом нарад тощо) з обговоренням результатів анонімних опитувань.

5.2.1. Процедура формування експертної групи

Добір кандидатів до складу експертної групи (колективу), істотно залежний від характеру та змісту досліджуваної проблеми, може проводитись через самооцінювання кандидатів в експерти, або за результатами їхньої минулої діяльності, або з урахуванням їхньої компетентності, або ж за результатами оцінювання кожного кандидата групою. Останній підхід найбільш ефективний. Зазначене оцінювання проводиться як соціометричне опитування (рис. 5.3) — покрокове формування як попереднього, так і остаточного складу експертної групи. Закінчується процес тоді, коли список експертів перестає поповнюватися новими прізвищами. Процедура добору може бути перервана й раніше, якщо буде зафіксовано близько 95% повторень. Як показує практика проведення експертиз, помилка в такому разі не має істотного впливу на подальші оцінки.

Завдання сформувати експертну групу за допомогою соціометричного опитування можна сформулювати так [143–146].

Нехай $EXP = (exp_1, \ldots, exp_n)$ — множина можливих кандидатів до експертної групи; H — кількість учасників експертної групи; k_i — ваговий коефіцієнт, тобто ступінь компетентності i-го кандидата; p_i — ознака щодо включення (p_i=1) або не включення (p_i=0) i-го кандидата в експертну групу; c_i — вартість послуг i-го кандидата; C — загальна вартість проведення експертизи.

Рис. 5.3. Алгоритм формування експертного колективу

Необхідно з урахуванням обмежень

$$\sum_{i=1}^{H} c_i p_i \leq C \text{ і } 20 \geq H \geq 10$$

(кількість експертів у групі має бути така, аби на кожне запитання анкети було отримано не менш як 15–20 оцінок, а кількість експертів з мінімальною компетентністю не повинна перевищувати 25% від загальної чисельності колективу) сформувати експертну групу, яка матиме максимальну компетентність:

$$\sum_{i=1}^{H} k_i p_i \to \max. \tag{5.1}$$

Така постановка задачі правомірна лише за умови, що кандидати до експертної групи за компетентністю якісно однорідні, тобто:

$$W_{гр} = \left(1 - \sigma_{гр}\right) \Big/ K_{гр}^{ср} \geq 0{,}8 \left(\text{висока однорідність}\right), \tag{5.2}$$

де $\sigma_{гр}$ — точність оцінювання, забезпечувана експертною групою; $K_{гр}^{ср}$ — середнє значення коефіцієнта K компетентності членів експертної групи.

Якщо склад експертної групи за компетентністю неоднорідний, то виникає, як правило, принципова помилка. Саме її поява змушує для визначення ступеня впливу компетентності кожного окремого експерта на результат експертизи застосовувати дисперсію або середньоквадратичне відхилення $\sqrt{\sigma^2}$. При цьому чим менша дисперсія (відхилення), тим менша помилка і тим вища точність оцінювання, яку забезпечує експерт.

Нехай σ_1, σ_2,..., σ_N — показники точності оцінювання (середні оцінки), що їх забезпечують N експертів. При цьому для кожного наступного експерта показники точності зменшуються рівномірно, тобто рівномірно в l разів збіль-

шується відхилення. Тоді показник точності групового оцінювання може бути обчислений з виразу:

$$\sigma_{\text{гр}} = \frac{1}{N}\sqrt{\sum_{i=1}^{N}\sigma_i^2}. \qquad (5.3)$$

Беручи до уваги, що всі експерти мають різну компетентність, упорядкуємо їх за цією ознакою: $\sigma_1 < \sigma_2 < \ldots < \sigma_N$. Звідси дістаємо такі співвідношення:

$$\sigma_1;\ \sigma_2 = l\,\sigma_1;\ \sigma_3 = l\,\sigma_2;\ \ldots;\ \sigma_N = l\,\sigma_{N-1},$$

або

$$\sigma_1;\ \sigma_2 = l\,\sigma_1;\ \sigma_3 = l^2\,\sigma_1;\ \ldots;\ \sigma_N = l^{N-1}\,\sigma_1.$$

Згідно з формулою (5.3)

$$\sigma_{\text{гр}} = \frac{1}{N}\sqrt{\sum_{i=1}^{N}\sigma_i^2} = \frac{1}{N}\sqrt{\sum_{i=1}^{N}\left(l^{i-1}\sigma_1\right)^2} = \frac{1}{N}\sqrt{\sum_{i=1}^{N}\left(l^{i-1}\right)^2\sigma_i^2} = \frac{\sigma_1}{N}\sqrt{\sum_{i=1}^{N}\left(l^2\right)^{i-1}}. \qquad (5.4)$$

З'ясуємо, як поводиться графік залежності $\sigma_{\text{гр}}$ від N при різних значеннях (рис. 5.4). Зі збільшенням кількості експертів помилка експертизи зростає. Найвища точність оцінювання досягається, як бачимо, за умови присутності в експертній групі лише одного фахівця. Якщо експертів у групі більш як один і точність оцінок кожного наступного з них відрізняється від попереднього на 5% ($l = 1{,}05$), то мінімальна помилка експертизи може бути досягнута при 16 експертах (верхня межа кількісного складу експертної групи — $m_{\text{в}}$=16). Якщо точність оцінок кожного наступного члена експертної групи відрізняється від попереднього на 10% ($l = 1{,}1$), то мінімум досягається за семи експертів (нижня межа — $m_{\text{н}}$= 7).

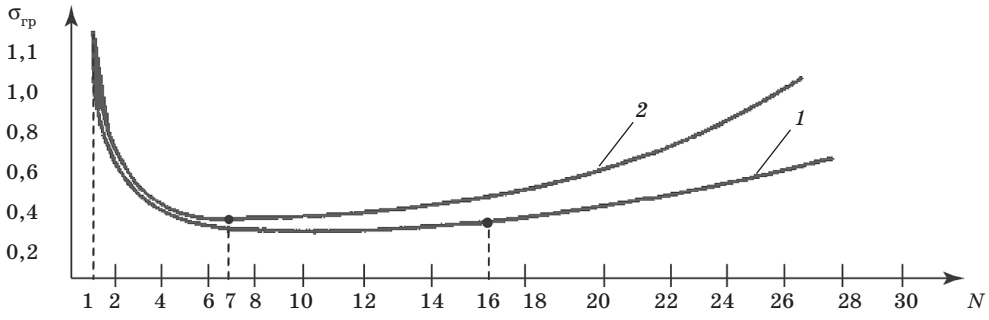


Рис. 5.4. Залежність середньої похибки $\sigma_{\text{гр}}$ від кількості N членів експертної групи при $l = 1{,}05$ (крива *1*) і $l = 1{,}1$ (крива *2*)

Таким чином, можна констатувати, що з урахуванням компетентності експертів в експертну групу доцільно включати не більш як 10–15 найкомпетентніших серед них. Водночас слід брати до уваги, що відповідно до масштабу експертного оцінювання експертних груп, які залучаються до роботи, може бути одна-дві, коли прогнозування стосується конкретних науково-технічних проблем, і досягати навіть кількох десятків, коли прогнозування охоплює комплексні галузеві проблеми.

5.2.2. Методи оцінювання компетентності представників експертної групи

Компетентність експерта — це ступінь його кваліфікації в певній галузі знань. Вона визначається за допомогою аналізу його професійної підготовки (посада, вчене звання, ступінь), професійної діяльності та світоглядних установок щодо перспектив розвитку досліджуваної проблеми. Компетентність експерта має поширюватися як на об'єкт оцінювання якості (*професійна компетентність*), так і на методологію оцінювання (*кваліметрична компетентність*). Професійна компетентність включає в себе знання історії досліджуваної проблеми. Кваліметрична компетентність забезпечує чітке розуміння експертом методів оцінювання, уміння користуватися різними типами оцінювальних шкал, розрізняючи при цьому достатньо велику кількість їх градацій.

Нині при оцінюванні професійної компетентності експерта користуються, як правило, методами *самооцінювання* [146], *взаємного оцінювання* [147] та *контрольних експертиз* [148].

Згідно з ***методом самооцінювання*** індивідуальну компетентність експерта оцінюють коефіцієнтом $k(0 \le k \le 1)$, який сам експерт визначає на основі власних суджень про ступінь $k_{\text{і}}$ своєї інформованості з проблеми, що розглядається, а також про ступінь $k_{\text{а}}$ аргументованості власних думок [141]:

$$k = 0{,}5(k_{\text{і}} + k_{\text{а}}). \tag{5.5}$$

Коефіцієнт інформованості визначають на основі самооцінювання експерта за десятибальною шкалою згідно з виразом

$$k_{\text{і}} = 0{,}1X_{\text{інф}}, \tag{5.6}$$

де $X_{\text{інф}}$ — бал, виставлений експертом.

Аналіз літератури [144–149] показує, що для оцінювання ступеня інформованості експерта можна рекомендувати таку 10-бальну шкалу:

$X_{\text{інф}} = 0$ — не знає даної проблеми (питання);

$0 < X_{\text{інф}} \le 2$ — слабко знає проблему, цікавиться нею не систематично;

$2 < X_{\text{інф}} \le 4$ — задовільно знає проблему, займається нею несистематично;

$4 < X_{\text{інф}} \le 6$ — добре знає проблему з попереднього досвіду роботи; тепер, можливо, не працює в даній галузі, але систематично нею цікавиться;

$6 < X_{\text{інф}} \le 8$ — добре знає проблему, постійно працює над нею і має опубліковані праці в даній галузі;

$8 < X_{\text{інф}} < 10$ — відмінно знає проблему, має в її розв'язанні загальновизнані результати і є одним із вітчизняних лідерів (авторитетом) у її розробці;

$X_{\text{інф}} = 10$ — міжнародний авторитет у даній галузі.

Коефіцієнт аргументованості визначають як функцію, що залежить від коефіцієнта $k_{\text{д}}$ довіри та коефіцієнта $k_{\text{в}}$ відповідності:

$$k_{\text{а}} = F(k_{\text{д}}, k_{\text{в}}). \tag{5.7}$$

Тут $k_{\text{д}} = k'k''$, а k' і k'', у свою чергу, набувають значень 1 або 0,5 згідно з табл. 5.5, а значення $k_{\text{в}}$ беруться з табл. 5.6.

У певному випадку функція F може являти собою середньоарифметичне значень $k_{\text{д}}$ і $k_{\text{в}}$.

Оцінюючи певне джерело за градаціями B, C і H та користуючись еталонними значеннями, поданими в табл. 5.6, експерт у порожніх клітинках такої

Таблиця 5.5

Числові значення множників k', k'' коефіцієнта $k_д$ довіри

Рівень обговорення проблеми	Рівень спеціалізації експерта	
	Галузь безпосередньої роботи $k'' = 1$	Суміжна галузь $k'' = 0,5$
Галузь безпосередньої роботи $k'' = 1$	$k' = 1$	$k' = 0,5$
Суміжна галузь $k'' = 0,5$	$k' = 0,5$	$k' = 1$

Таблиця 5.6

Еталонні значення оцінки коефіцієнта $k_в$ відповідності

Джерело аргументації	Ступінь впливу джерела на Вашу думку		
	В (високий)	С (середній)	Н (низький)
Проведений Вами теоретичний аналіз	0,3	0,2	0,1
Ваш виробничий досвід	0,5	0,4	0,2
Узагальнення праць вітчизняних авторів	0,05	0,05	0,05
Узагальнення праць зарубіжних авторів	0,05	0,05	0,05
Ваша особиста ознайомленість зі станом дослідженості даного питання в інших країнах	0,05	0,05	0,05
Ваша інтуїція	0,05	0,05	0,05
	max 1	max 0,8	max 0,5

таблиці проставляє власні значення. Їх підсумовування за кожним стовпцем дасть у результаті значення коефіцієнта $k_в$. При цьому саме інтервальний характер пропонованих шкал дозволить помітно підвищити їхню розрізнювальну здатність та забезпечить достатню значеннєву визначеність не тільки при доборі експертів, а і при аналізі компетентності експертної групи (колективу) в цілому.

Метод взаємного оцінювання полягає в обчисленні індивідуальних коефіцієнтів компетентності на основі матриць, складених експертами за результатами взаємного оцінювання. Цей метод, використовуваний за умови, що кандидати знають рівень фаховості один одного, полягає в оцінюванні кожним із них обсягу та якості знань решти кандидатів у формі відповідей на питання анкети. При складанні анкет за цим методом необхідно заздалегідь виявляти можливі цілі експертів, що суперечать меті експертизи, тобто виключати ті причини, які можуть спонукати експерта свідомо спотворювати оцінки щодо знань своїх колег. Однією з ефективних модифікацій методу взаємного оцінювання є така трикрокова процедура.

Крок 1. Члени групи управління висловлюють власну думку щодо осіб, яких доцільно включити у групу експертів. Названі особи діють, у свою чергу, так само. За кілька турів такого опитування складається доволі повний список кандидатів.

Крок 2. За результатами опитування формується матриця суміжності $Z = \|z_{ij}\|$, $i = \overline{1, n}$, $j = \overline{1, n}$, елементи якої дорівнюють одиниці, якщо кандидат

із номером i висловився на користь залучення в групу кандидата з номером j, і нулю — у протилежному випадку (i — номер рядка, j — номер стовпця матриці суміжності).

Крок 3. За матрицею суміжності $Z = \|z_{ij}\|$, $i = \overline{1, n}$; $j = \overline{1, n}$ обчислюються коефіцієнти γ_i компетентності кандидатів. Алгоритм відшукання значень γ_i полягає в тому, що на 1-й ітерації ($t = 1$) група управління обчислює відношення суми голосів, поданих за кандидата з номером γ_i, до загальної кількості всіх голосів (сума одиниць у матриці суміжності). На наступних ітераціях ($t > 1$) голоси зважуються коефіцієнтами $\gamma_i^{(t-1)}$ компетентності кандидатів, обчисленими на попередній ітерації.

Для цього діють за таким алгоритмом.

1. Задаємо критерій зупинки і необхідну точність ε обчислення $\gamma_i = \overline{1,n}$. Значення аргументу ε вибираємо на один-два порядки менше за $\frac{1}{n}$. Іноді як критерій зупинки використовують умову $t = t_{\text{потр}}$. При цьому потрібне значення $t_{\text{потр}}$ вибирають в діапазоні 3–5, що зумовлюється швидкою збіжністю процесу.

2. Припускаємо, що $t = 0$ і всі $\gamma_i^{(t)} = \frac{1}{n}$, $i = \overline{1,n}$.

3. Беремо $t = t+1$ і обчислюємо

$$\gamma_j^{(t)} = \frac{\sum_{i=1}^{n} x_{ij} \gamma_i^{(t-1)}}{\sum_{i=1}^{n} \sum_{j=1}^{n} x_{ij} \gamma_i^{(t-1)}}, \quad j = \overline{1,n}. \tag{5.8}$$

4. Перевіряємо умову $\left|\gamma_i^{(t)} - \gamma_i^{(t-1)}\right| \le \varepsilon$, $i = \overline{1,n}$. Якщо вона виконується, то переходимо до п. 5, інакше — до п. 3.

5. Обчислення припиняємо. Знайдені значення $\gamma_i^{(t)}$ вважаємо коефіцієнтами компетентності γ_i.

Розглянута процедура дозволяє не лише оцінити компетентність уже відібраних кандидатів, а й, можливо, виявити повну множину фахівців із даної проблеми та сформувати відповідний список.

І нарешті, метод оцінювання індивідуальної компетентності кандидатів полягає в перевірці вірогідності (надійності) суджень кожного з них під час проведення ***контрольних експертиз***. Контрольна експертиза передбачає опитування експертів із питань, яким у межах заданої шкали можна присвоїти додатний числовий еквівалент — коефіцієнт відносної важливості w_i, $i = \overline{1,N}$, такий що:

$$0 \le w_i \le 1, \quad \sum_{i=1}^{N} w_i = 1,$$

де N — загальна кількість поставлених запитань.

Можливо, керівникам опитування (але не опитуваним) будуть і заздалегідь доведені до відома вірогідні відповіді на такі запитання. Тоді коефіцієнт вірогідності суджень кожного експерта визначається як відношення кількості запитань, на які він дав правильні відповіді, до загальної кількості поставлених запитань:

$$\gamma_i^{[\text{вір}]} = \frac{N_{\Pi_i}}{N}, \quad i = \overline{1,n}, \tag{5.9}$$

де N_{Π_i} — кількість правильних відповідей i-го експерта.

Якщо вірогідні відповіді на поставлені запитання невідомі, то для оцінювання компетентності експертів можна скористатися підходом, в основу якого покладено опрацювання нормованих бальних оцінок. Згідно з цим підходом припускається, що спочатку всі експерти мають однакову компетентність. Як вагові коефіцієнти тоді беруть значення середньозважених оцінок усіх запитань, які нормуються їхньою сумою і використовуються як уточнені значення коефіцієнтів компетентності. Зрештою коефіцієнт компетентності експерта, оцінки якого ближчі до середньозважених, підвищується. Така процедура в ході контрольних експертиз може повторюватися неодноразово.

Наступний крок — математична обробка оцінок індивідуальної компетентності експертів, у результаті якої остаточно уточнюється склад експертної групи для забезпечення мінімального розкиду компетентності. Експерт, який отримав максимальний коефіцієнт компетентності, визначається як *Головний експерт*. Він виступає далі як *Особа, уповноважена ухвалювати рішення* (*ОУР*), на яку й покладається вибір найбільш раціонального рішення із сукупності можливих альтернатив.

5.2.3. Оцінювання відносної важливості порівнюваних параметрів

Дані, отримані в результаті опитування m експертів, являють собою оцінки відносної важливості кожного параметра. Ці оцінки можна подати табличноабо в балах, аби схарактеризувати відносну важливість C_{ij} j-го параметра з погляду i-го експерта за будь-якою шкалою або у вигляді рангових оцінок r_{ij}.

У першому випадку найчастіше використовуються 100- або 10-бальні шкали, де максимально можливому ступеню важливості відповідає оцінка у 100 або у 10 балів. У другому випадку найбільш важливому параметру приписують ранг 1, а найменш важливому — ранг n.

Експерти	Параметри (об'єкти, фактори, показники, заходи, напрямки дослідження тощо)					
	1	2	… …	j	… …	n
1	C_{11}, r_{11}	C_{11}, r_{11}		C_{1j}, r_{1j}		C_{1n}, r_{1n}
2	C_{21}, r_{21}	C_{22}, r_{22}		C_{2j}, r_{2j}		C_{2n}, r_{2n}
⋮						
i	C_{i1}, r_{i1}	C_{i2}, r_{i2}		C_{ij}, r_{ij}		C_{in}, r_{in}
⋮						
m	C_{m1}, r_{m1}	C_{m2}, r_{m2}		C_{mj}, r_{mj}		C_{mn}, r_{mn}

При цьому як показники узагальнених міркувань усіх m експертів, що взяли участь в оцінюванні, за кожним із j параметрів із сукупності n можливих найчастіше використовуються:

• по-перше, середнє арифметичне значення оцінок за j-м параметром:

$$\overline{C_j} = \frac{1}{m_j}\sum_{i=1}^{m_j} C_{ij}, \quad j=\overline{1,n}, \tag{5.10}$$

яке може змінюватись в інтервалі:

$0 \le \overline{C_j} \le 100$, якщо взято 100-бальну шкалу оцінок;

$0 \le \overline{C_j} \le 10$, якщо взято 10-бальну шкалу оцінок;

• по-друге, сума рангів оцінок, отриманих *j*-м параметром:

$$R_j = \sum_{i=1}^{m_j} r_{ij}, \quad j = \overline{1,n}. \tag{5.11}$$

Значення R_j визначається для кожного з параметрів і змінюється в інтервалі від одиниці до n. При цьому, як правило, найбільш важливому параметру (він має максимальний бал) приписується порядковий номер, що дорівнює одиниці, а найменш важливому — номер n. Чим менше значення R_j, тим значущішим (більш важливим) є досліджуваний параметр;

• по-третє, частота максимальних оцінок у балах або присудження експертами першого рангового місця *j*-му параметру:

$$K_j = m_j' \big/ m_j, \tag{5.12}$$

де m_j' — кількість експертів, які присудили *j*-му параметру перше місце або поставили йому максимальну оцінку в балах; m_j — кількість експертів, які оцінювали важливість *j*-го параметра.

Таким чином, методи соціальної інженерії, застосовувані зловмисником, становлять серйозну загрозу як для інформаційної, так і для соціотехнічної безпеки будь-якої організації. З огляду на це необхідно створити й розробити різні варіанти політики безпеки, визначити правила коректного використання телефонів, комп'ютерів і т. ін., а також провести тестування системи безпеки на проникнення, результати якого, у свою чергу, і мають забезпечити компанії захист від стороннього кібернетичного впливу. При цьому доцільно:

• не покладатися на систему внутрішньої ідентифікації;

• вводити в дію систему перевірки за допомогою зустрічного дзвінка, коли йдеться про повідомлення захищеної інформації;

• реалізовувати програму навчання користувачів у сфері безпеки;

• призначати відповідальних за технічну підтримку;

• створювати систему оповіщення про загрози.

Основні кроки посилення соціотехнічної безпеки можуть полягати в привернення уваги співробітників компанії до питань безпеки, усвідомленні ними всієї серйозності проблеми формування політики безпеки організації, а також у вивченні й упровадженні необхідних методів і дій для підвищення захисту інформаційного забезпечення.

5.3. Отримання вихідної інформації евристичного походження. Основні переваги та недоліки індивідуальних і колективних методів

Методи отримання експертної інформації поділяються на *методи індивідуального і методи колективного експертного оцінювання*. Загальний алгоритм опрацювання інформації евристичного походження наведено на рис. 5.5. У групі методів ***індивідуального експертного оцінювання*** найбільшого практичного застосування набули *морфологічний метод* (метод морфологічного аналізу), *метод сценаріїв,* підґрунтям для якого є *методи згортання* і *розгортання проблем*, а також *методи інтерв'ю* та *аналітичних доповідних записок* [149; 150].

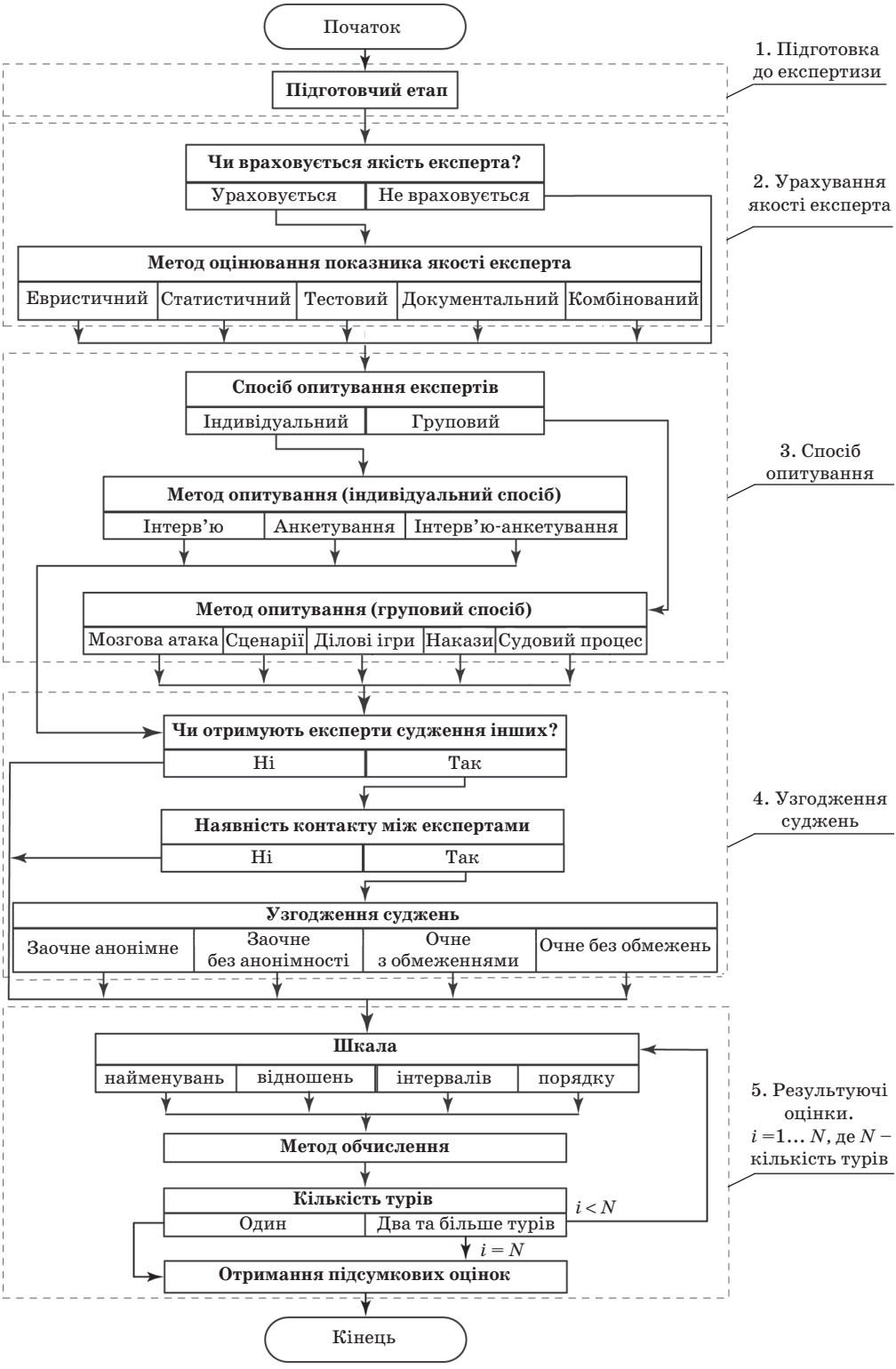


Рис. 5.5. Алгоритм опрацювання інформації евристичного походження

Морфологічний метод, уперше запропонований Ф. Цвіккі, дозволяє розв'язувати великомасштабні проблеми, зокрема конструкторські завдання загального плану. Забезпечує достатньо високий ефект при проектуванні об'єктів і пошуку системних вирішень. В основу цього методу покладено комбінаторику — систематичне дослідження всіх теоретично можливих варіантів вирішення, що випливають із закономірностей побудови аналізованого об'єкта.

Робочі процедури методи включають у себе:

• точне формулювання розв'язуваної проблеми та визначення її меж;

• визначення найважливіших (як уже досягнутих, так і теоретично можливих) характеристик і параметрів аналізованих об'єктів, що впливають на розв'язання поставленої проблеми;

• побудову морфологічної «множини», тобто морфологічної дво- чи тривимірної матриці виду

$$\begin{pmatrix} p_1^1 & p_1^2 & \cdots & p_1^{k_1} \\ p_2^1 & p_2^2 & \cdots & p_2^{k_2} \\ & & \vdots & \\ p_n^1 & p_n^2 & \cdots & p_n^{k_n} \end{pmatrix}; \qquad (5.13)$$

• аналіз здобутих варіантів вирішень і вибір відносно найкращого серед них на підставі індивідуальних оцінних критеріїв.

До недоліків морфологічного методу слід віднести порівняну його трудомісткість (необхідність перегляду варіантів) та відсутність надійного способу оцінювання ефективності застосування того чи іншого варіанта.

Метод сценаріїв належить до напіваналітичних методів. Застосовується для створення штучних ситуацій (сценаріїв) за відсутності реальних фактів, наприклад, при визначенні цілей і наслідків деякої операції, у виборі показників і критеріїв ефективності тощо. При цьому ***сценарій*** розуміють як логічний і правдоподібний опис подій із установленням орієнтовного часу та передумов їх настання. Складається сценарій для уточнення умов, за яких доведеться розв'язувати ту чи іншу проблему. Він стимулює та дисциплінує мислення експертів, змушує їх ураховувати деталі перебігу подій, висвітлювати взаємозв'язок багатьох факторів, будуючи спрощену модель надскладних реалій. Особлива увага при розробці сценаріїв приділяється «критичним» точкам, після яких події можуть розвиватися в різних напрямках.

Метод сценаріїв, як правило, базується на аналізі результатів, здобутих за допомогою *методів розгортання* (*згортання*) *проблем*. Ідея першого з них — методу *розгортання проблем*, полягає в послідовному поділі проблем певного рівня на підпроблеми, що являють собою елементи наступного рівня. Зрештою формується розгортка підпроблем. При цьому досить важливо, щоб не порушувався причинно-наслідковий зв'язок, тобто проблеми нижчих рівнів були зумовлені проблемами верхніх рівнів. Це досягається багатоетапним цілеспрямованим експертним опитуванням, що має тривати до повного узгодження суджень усіх експертів. Ідея методу *згортання проблем* полягає в послідовному зведенні проблем нижчих рівнів до проблем вищих рівнів. У результаті застосування методу формується проблема, розв'язувати яку доведеться в майбутньому. Отже, методи розгортання (згортання) проблем, застосування яких передбачає залучення груп експертів і здійснюється

покроково, забезпечують вибір одного опорного сценарію або мінімально можливу кількість таких сценаріїв.

Методи інтерв'ю та ***аналітичних доповідних записок*** використовують, коли йдеться про формування вихідної множини стратегій чи аналіз невизначеностей. Метод інтерв'ю полягає в опитуванні експерта за сформульованим заздалегідь переліком питань, на які він дає відповіді експромтом. Натомість складання аналітичних доповідних записок потребує тривалої та ретельної самостійної роботи експерта щодо аналізу тенденцій розвитку, оцінювання поточного стану і шляхів розвитку об'єкта дослідження.

Основні переваги методів індивідуального експертного оцінювання полягають в їх оперативності. Вони дають змогу з найменшими витратами повною мірою використовувати індивідуальні здібності експерта, який не зазнає тиску авторитетів. Головний недолік цих методів — високий ступінь суб'єктивності отримуваних оцінок, передусім через обмеженість знань одного фахівця.

У групі методів ***колективного експертного оцінювання*** найбільшого практичного застосування набули такі: *метод мозкової атаки*, *метод Дельфі*, *метод аналізу ієрархій*, *метод анкетування* та *метод колективного генерування ідей* [151]. Головні кроки реалізації цих методів унаочнює рис. 5.6.

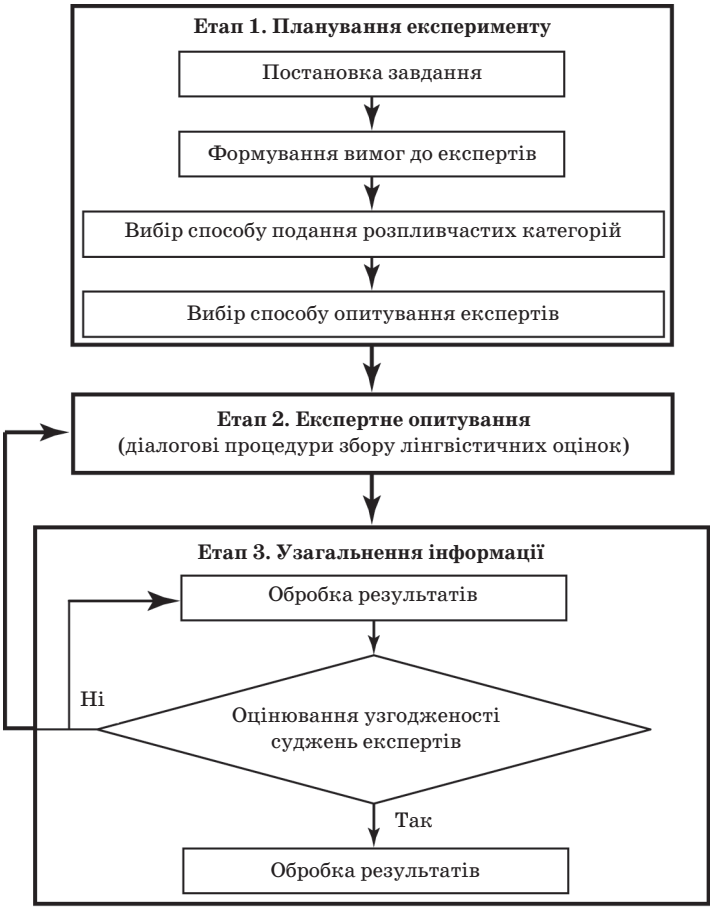


Рис. 5.6. Загальна схема збору та колективної обробки експертної інформації

Узагальнений алгоритм методів колективного експертного оцінювання

1. Надання організаторами експертизи кожному експертові інформації з проблеми у вигляді сформульованої мети опитування та анкети, що включає в себе сукупність оцінюваних факторів або подій.

2. Виконання кожним експертом сформульованого завдання незалежно від інших членів експертної групи.

3. Проведення організаторами експертизи статистичної обробки анкет, із виявленням та узагальненням аргументів, що відповідають різним судженням.

4. Формування організаторами експертизи колективного рішення та ознайомлення з ним членів експертної групи.

5. Пояснення з боку окремих членів експертної групи причин незгоди з ухваленим колективним рішенням та перегляд з ініціативи того чи іншого експерта власної позиції.

6. Проведення другого туру експертизи (починаючи з 2-го кроку), що дасть змогу звузити діапазон оцінок експертів.

При цьому процедура експертного оцінювання (цикл експертизи) може повторюватися 3–4 рази, до усталення суджень кожного експерта.

Метод мозкової атаки (Breinstorming), або ***мозкового штурму***, який 1939 року запропонував Осборн (м. Буффало, США),— один із методів колективного генерування ідей (пропозицій, гіпотез тощо). Спирається він на припущення, що серед розмаїття поданих ідей є принаймні кілька вартих уваги. Метод широко застосовується не лише в теорії та практиці управління, а й у процесах здобуття та використання соціологічної інформації, тобто в ситуаціях, коли необхідно скласти уявлення про напрямки формування (розвитку) певної проблеми; отримати набір варіантів можливих вирішень щодо реалізації цих напрямків; виявити коло чинників, що мають сприяти вибору раціонального варіанта шуканого розв'язку.

Головні етапи методу такі [152]:

1) формування групи управління (із 2–4 осіб) та експертної групи (із 10–15 осіб);

2) складання групою управління проблемної записки, де визначено мету дослідження та перелік обмежень, пропонованих до варіантів можливих розв'язань проблеми; масштаб і точність вимірювань та оцінок; організаційне, фінансове й матеріально-технічне забезпечення тощо. Вручення проблемної записки особисто кожному членові експертної групи або оголошення її змісту Головним експертом (особа, що ухвалює рішення) перед усіма членами експертної групи;

3) генерування кожним експертом власних ідей (гіпотез тощо) за певною проблемою. Критика попередніх висловлювань при цьому не припускається, але вітається комбінування та подальший розвиток ідей. Результатом етапу може стати формування списку варіантів можливих розв'язань проблеми;

4) систематизація (класифікація і групування) групою управління всіх висловлених ідей (пропозицій, гіпотез тощо);

5) аналіз і оцінювання експертною групою всіх висловлених ідей (пропозицій, гіпотез) щодо практичної реалізованості;

6) систематизація всіх висловлених зауважень та формування списку раціональних ідей (пропозицій, гіпотез) групою управління.

Основні правила, яких мають дотримуватись члени експертної групи в ході «мозкової атаки», формуються так:

• неприпустимість озвучення учасниками наради явно помилкових ідей;

• неприпустимість призупинення на нараді обговорення жодної з ідей, висловлених експертами;

• підтримання в ході наради ідей будь-якого роду, навіть якщо їх доречність або реалізованість здаються сумнівними;

• надання однакової підтримки всім учасникам наради, незважаючи на їхнє службове становище, вчене звання та досвід роботи.

Поряд із очевидними перевагами порівняно з іншими методами колективного експертного оцінювання, метод «мозкової атаки» має й певні недоліки. Наприклад, на судження більшості експертів можуть вплинути висловлювання найбільш авторитетних чи активних фахівців, що істотно знецінює здійснювані заходи. Або й навпаки: психологічні риси того чи іншого експерта стримують його, коли йдеться про дискусію та обстоювання власної позиції.

Метод Дельфі **(***the Delphi method***)** — метод групового експертного опитування зі збереженням анонімності суджень його учасників. Сутність методу полягає в тому, що результуючі прогнозні оцінки визначаються на підставі висловлювань учасників опитування, які обґрунтовують свої погляди на стан і розвиток певної проблеми чи проблемної ситуації [153]. Метод спирається на припущення, що прогнозування буде найбільш точним, якщо в опитуванні братиме участь не один, а від 20 до 60 експертів ($20 \le X \le 60$). При цьому узагальнена оцінка експертів має характеризуватися найменшою дисперсією, а медіанне значення індивідуальних оцінок — наближатися до фактичного значення прогнозованого показника. Процедура експертного опитування за методом Дельфі зводиться до формування групової думки стосовно пропонованих предметів обговорення. Група експертів згідно з переліком показників за темою дослідження [141; 153] складає анонімний прогноз на близьку і більш віддалену перспективу. Думки членів експертної групи зазнають обробки з використанням прийомів математичної статистики та евристичних методів (табл. 5.7) [154]. Узгодження отриманих індивідуальних оцінок забезпечується за рахунок послідовного анонімного ознайомлення кожного експерта з оцінками інших. Зворотний зв'язок, що регламентується аналітиками, дозволяє виявити переважні судження фахівців та досягти зближення їхніх точок зору на проблему. Такий зв'язок установлюється у вигляді повідомлення про середньостатистичний результат обробленої інформації по всій групі експертів на попередніх етапах опитування. Ураховуючи цю інформацію, кожний експерт коригує власний прогноз, кінцевим результатом якого знову вважається середній показник, що повідомляється експертам, і весь процес повторюється.

У своєму первісному вигляді метод Дельфі мав низку недоліків, зумовлених здебільшого особливостями організації опитування (змістом анкети) і суб'єктивними основами самого методу, що відбивають великий вплив поглядів авторів запитань і якості добору експертів. Головні з них такі:

• зниження ваги значення, що надається подіям більш віддаленого майбутнього;

• схильність до передбачень інтуїтивного характеру і намагання спрощувати зміст прогнозу.

Таблиця 5.7

Статистичні та евристичні показники математичної статистики

Вид показників	Формула	Позначення
Статистичні	$\overline{\varphi(i)}=\dfrac{\sum_{j=1}^{m}\varphi(i)_j}{m}$	$\overline{\varphi(i)}$ — середньоарифметичне значення вагомості i-го показника; $\varphi(i)_j$ — вагомість, зазначена j-м експертом щодо i-го показника; m — кількість експертів
	$\overline{\sigma}=\sqrt{\dfrac{\sum_{j=1}^{m}\left[\varphi(i)_j-\overline{\varphi(i)}\right]^2}{m}}$	$\overline{\sigma}$ — середньоквадратичне відхилення для i-го показника
	$V=\dfrac{\overline{\sigma}}{\varphi(i)}\cdot 100$	V — коефіцієнт варіації (коефіцієнт мінливості думок експертів) щодоо i-го показника
Евристичні	$s=\sum_{i=1}^{m}\rho_i$	ρ_i — ранг оцінки вагомості i-го показника (ціле або дробове число)
	$\overline{s}=\dfrac{s}{n}$	$\overline{s}$ — середньоарифметичне значення суми рангів за всіма n показниками
	$d_i=s-\overline{s}$	d_i — відхилення суми рангів від середньоарифметичного значення
	$T_i=\sum_{l=1}^{L}\left(t_l^3-t_l\right)$	T_i — показник зв'язаності рангів; L — кількість груп зв'язаних рангів; t_l — кількість зв'язаних рангів в l- й групі
	$W=\dfrac{12\sum_{i=1}^{n}d_i^2}{m^2\left(n^3-n\right)-m\sum_{i=1}^{n}T_i}$	W — коефіцієнт конкордації. Основний показник, що характеризує погодженість думок експертів за всіма n показниками
	$\chi_R^2=\dfrac{12\sum_{i=1}^{n}d_i^2}{mn(n+1)-\dfrac{1}{n-1}\sum_{i=1}^{n}T_i}$	Фактичне значення критеріальної статистики χ_R^2, розподіленої за χ^2 при $\theta=n-1$

Для усунення зазначених недоліків методу Дельфі та відшукання нових сфер його застосування останнім часом було впроваджено нові підходи до формування експертних груп, а також новітні методи оцінювання міркувань експертів із застосуванням багатовимірних шкал і моделювання. Це дозволило підвищити надійність методу, особливо в разі прогнозування на період від одного до трьох років, а іноді й на триваліший період часу, застосовувати його з метою:

1) визначення переліку найбільш важливих подій;

2) висловлювання переліку припущень щодо часу, коли ці події можуть відбутися;

3) формулювання переліку припущень про можливості виникнення подій у певний час;

4) прогнозування наслідків певних подій у разі їх настання;

5) оцінювання бажаності наслідків певних подій у разі їх виникнення;

6) обґрунтування причин існування вкрай протилежних думок на будь-якому етапі процесу ухвалення рішення;

7) опису та оцінювання альтернативних подій, які могли би збільшити (зменшити) можливість виникнення бажаних (небажаних) серед них.

Метод аналізу ієрархій (MAI) [141; 143] — системна процедура для ієрархічного подання елементів (об'єктів, зразків і систем техніки), які визначають суть будь-якої (довільної) проблеми. Метод поєднує в собі процедури багатокритеріального опису проблеми, синтезу різних міркувань, отримання пріоритетності функцій і критеріїв, а також відшукання альтернативних рішень (рис. 5.7). Головне основне призначення методу — підтримання ухвалення рішень за допомогою ієрархічної декомпозиції досліджуваної проблеми на простіші складові із подальшим рейтингуванням обраних альтернатив на основі їх попарного порівняння.

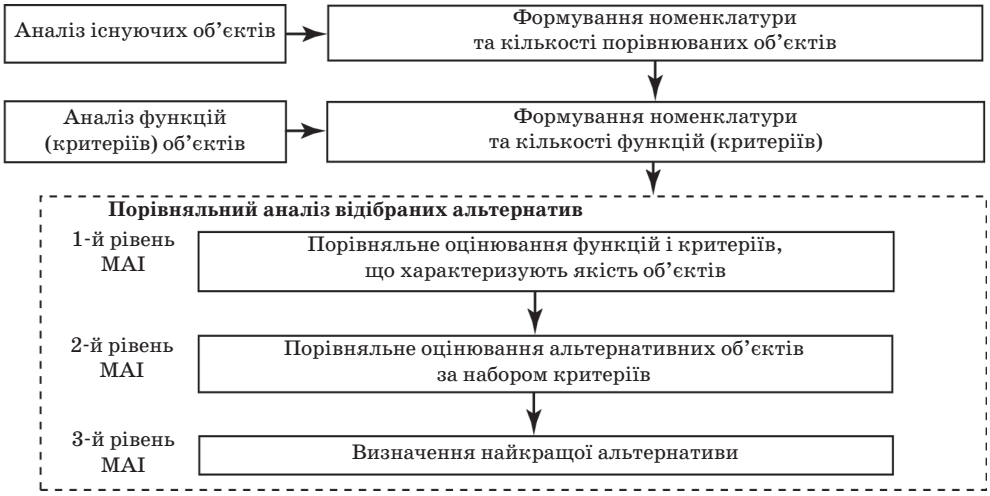


Рис. 5.7. Схема проведення досліджень

У результаті декомпозиції проблеми виокремлюють мету, наприклад придбання найкращого програмного засобу (ПЗ) серед сукупності аналогічних засобів. Ця мета відповідає 1-му рівню ієрархії. Наступний, 2-й рівень включає в себе основні функції, що мають бути реалізовані цим ПЗ. Після поділу функцій 2-го рівня може бути сформовано 3-й рівень як сукупність критеріїв (підфункцій) 2-го рівня і т. д. Останній рівень утворюють альтернативи, тобто варіанти ПЗ, що реалізують зазначені дослідником функції та підфункції.

Для оцінювання альтернатив і визначення серед них найважливішої (найбільш раціональної для розв'язання конкретного завдання) застосовують метод попарного порівняння оцінок функцій і критеріїв з погляду їхнього впливу на ціль та порівняння обраних альтернатив між собою за кожним критерієм окремо. При цьому на різних рівнях ієрархії застосовуються різні принципи:

- на 1-му — принцип ідентичності та декомпозиції;
- на 2-му — принцип дискримінації та порівняльного аналізу;
- на 3-му — принцип синтезування (табл. 5.8).

Насамперед експерти здійснюють парні порівняння оцінюваних критеріїв. Для цього кожний експерт використовує спеціальну вербально-числову шкалу (табл. 5.9). Головна мета її застосування — забезпечити об'єктивність оцінок, полегшити завдання залучених до експертизи фахівців і забезпечити єдине тлумачення оцінок різними експертами.

Таблиця 5.8

Зміст рівнів ієрархії МАІ

Рівень ієрархії	Застосовуваний на етапі принцип МАІ	Операції, які мають місце на кожному з рівнів
1-й	Принцип ідентичності та декомпозиції	**1.** Складання та попереднє обґрунтування переліку та кількості оцінних показників. **2.** Підготовка таблиці вихідних даних (у кількісному або якісному вираженні) для всіх варіантів зразка СТС. **3.** Структурування проблеми та її декомпозиція в ієрархію (мережу)
2-й	Принцип дискримінації та порівняльного аналізу	**1.** Оцінювання кожного варіанта (альтернативи) за обраними критеріями (показниками) і формування матриць попарних порівнянь для рівнів ієрархії 2-го і 3-го. **2.** Проведення експертизи й заповнення попарних порі нянь. Порівняння відбувається згідно з вербальною шкалою, із урахуванням впливу порівнюваних зразків СТС на спільну для них характеристику. Для визначення альтернативи можуть бути використані судження як одного експерта, так і колективні погляди групи експертів. Емпіричним шляхом установлено, що найбільш оптимальною в кількісному плані є група експертів з 10–15 осіб. 3. Виявлення найважливішого варіанта (альтернативи)
3-й	Принцип синтезування	1. Визначення локальних пріоритетів. 2. Оцінювання погодженості матриць попарних порівнянь. 3. Визначення глобальних (складових) пріоритетів. 4. Порівняння глобальних пріоритетів СТС й вибір однієї з альтернатив для подальшої розробки

Отже, за допомогою зазначеної шкали l-й експерт заповнює матрицю виду:

$$A_l = \left\| \begin{matrix} a_{11}^{(l)}, a_{12}^{(l)}, \ldots, a_{1m}^{(l)} \\ a_{21}^{(l)}, a_{22}^{(l)}, \ldots, a_{2m}^{(l)} \\ \vdots \\ a_{m1}^{(l)}, a_{m2}^{(l)}, \ldots, a_{mm}^{(l)} \end{matrix} \right\|, \; l = \overline{1,n}, \tag{5.14}$$

де n — кількість експертів; $a_{jk}^{(l)}$ — результат порівняння l-м експертом j-го показника з k-м, $j = \overline{1,m}$, $k = \overline{1,m}$.

Попарне порівняння об'єктів має бути виконано за умови, що важливість одного об'єкта порівняно з іншим дорівнює k $(k = \overline{1,9})$. Тоді важливість другого об'єкта порівняно з першим дорівнює $1/k$ (має виконуватись властивість оберненої симетричності). При цьому елементи матриць попарних порівнянь a_{jk} розглядаються як оцінки відношення w_j до w_k, тобто $a_{jk} = \omega_j / \omega_k$, де $\omega = \{\omega_1, \omega_2, \ldots, \omega_m\}$ — вектор дійсних шуканих коефіцієнтів відносної важливості (ВВ) показників, оцінка коефіцієнтів яких зводиться до обчислень за формулою $\omega_i = 1/a_{ki}$, де $i = \overline{1,m}$.

Наступним кроком є нормалізація здобутих таким чином значень числового стовпця діленням кожного з них на їхню загальну суму:

$$c_i = a_i \Big/ \sum_{i=1}^{m} a_i, \tag{5.15}$$

де c_i — нормалізований компонент власного вектора сформованої матриці за зарядом i.

Таблиця 5.9

Оцінна шкала відносної важливості (ваг)

Інтенсивність відносної важливості v_{jk}	**Визначення**	**Пояснення**
1	Рівна важливість	Однаковій внесок двох видів діяльності в досягнення обраної мети
3	Помірна перевага одного над іншим	Досвід і судження (експертний аналіз) дають незначну перевагу одного виду діяльності над іншим
5	Істотна або велика перевага	Досвід і судження (експертний аналіз) дають велику перевагу одного виду діяльності над іншим
7	Значна перевага	Одному виду діяльності надається настільки велика перевага, що він стає практично значним
9	Дуже велика перевага	Очевидність переваги одного виду діяльності над іншим підтверджується найбільше
2, 4, 6, 8	Проміжні рішення між двома сусідніми судженнями	Застосовуються в компромісних випадках
Обернені розміри цих чисел	Якщо при порівнянні одного виду діяльності з іншим отримано, наприклад, 3, то результат оберненого порівняння дорівнює 1/3	—

Оскільки на 1-му рівні ієрархії завжди перебуває один елемент (фокус проблеми), що передбачено методичними положеннями MAI, то матриця попарних порівнянь для елементів 2-го рівня також буде одна. Як наслідок, її нормований власний вектор $C(c_i, c_2, ..., c_m)$ і буде вектором пріоритетів 2-го рівня ієрархії.

Для визначення пріоритетів окремих компонентів (починаючи з третього і до останнього) інших рівнів ієрархічної структури досліджуваного процесу кількість матриць попарних порівнянь завжди відмінна від одиниці. У разі повної ієрархії кількість зазначених матриць зумовлюється кількістю структурних елементів вищого рівня, а в разі неповної ієрархії — кількістю причинно-наслідкових зв'язків між сусідніми рівнями. Тому постає потреба зважувати нормалізовані вектори, здобуті з матриць попарних порівнянь для елементів нижчого рівня, на пріоритети елементів вищого рівня. Це досягається множенням матриці нормалізованих векторів, розрахованих для кожного причинно-наслідкового зв'язку між елементами сусідніх рівнів, праворуч на вектор пріоритетів елементів вищого рівня. У матричному вигляді розрахунки здійснюються за формулою

$$B^{r+1} = C^{r+1} \cdot B^r, \tag{5.16}$$

де B^{r+1}, B^r — вектор пріоритетів елементів ієрархії на рівні відповідно r+1 і r; C^{r+1} — матриця нормалізованих векторів елементів рівня r+1 ієрархії [141; 143].

Оскільки за низької погодженості матриці зменшується об'єктивність ухваленого рішення щодо вибору раціонального варіанта із заданої множи-

ни альтернатив, необхідно проаналізувати її погодженість, тобто виконання рівності

$$b_{ji}b_{ik}=b_{jk} \tag{5.17}$$

Для того щоб обчислити індекс погодженості, необхідно спочатку знайти суму елементів кожного стовпця порівнянь, потім суму елементів першого стовпця збільшити на значення першого компонента нормалізованого вектора пріоритетів, суму елементів другого стовпця збільшити на значення другого компонента і т. д. Нарешті знайдені числа слід додати з урахуванням власного числа λ_{max} матриці B.

Якщо судження експертів цілком погоджені, то має виконуватися рівність $Bw = mw$. Якщо погодженість елементів матриці відсутня і має місце непослідовність у відповідях експертів, то виконується рівність $Bw = \lambda_{max}w$. Тоді завдання оцінювання коефіцієнтів відносної важливості зводиться до визначення максимального власного значення матриці B та відповідного йому власного вектора w з використанням ступеневого алгоритму.

Для характеристики ступеня погодженості суджень кожного експерта в методі Сааті розглядається величина C.I. (*Consistency Index*) — так званий *індекс узгодженості*:

$$C.I. = k_{\text{узгодж}} = (\lambda_{\max} - m)/(m-1). \tag{5.18}$$

Матрицю попарних порівнянь, отриманих від експерта, можна використовувати для подальших розрахунків без уточнення, якщо

$$k_{\text{відп}} = k_{\text{узгодж}} / k_{\text{вип}} < 0{,}1\ ,$$

де $k_{\text{відп}}$ — відношення відповідності (*consistency ratio*); $k_{\text{вип}}$ — випадковий індекс (*random index*).

Якщо $k_{\text{узгодж}}$ поділити на число, що відповідає випадковій узгодженості матриці B того самого порядку, дістанемо відношення узгодженості (ВУ), яка має не перевищувати значення 0,1. У деяких випадках воно може досягати 0,2, але не більше.

Незважаючи на те, що МАІ не має строгого наукового обґрунтування, він знайшов широке практичне застосування завдяки своїй простоті й наочності. Наприклад, застосування МАІ як методологічної основи в методиках порівняльної воєнно-економічної оцінки озброєння дає змогу:

- по-перше, виключити застосування апарату регресійного аналізу;
- по-друге, більш об'єктивно враховувати якісні характеристики в корисності системи;
- по-третє, завдяки ієрархічному поданню структури розв'язуваної задачі (проблеми) чітко виражати судження експертів;
- по-четверте, усувати необхідність пошуку функціональних залежностей корисності (важливості) альтернативи від її частинних критеріїв;
- по-п'яте, завдяки використанню попарних порівнянь частинних критеріїв у шкалі відношень уникати необхідності нормування метричних критеріїв і зменшувати похибку при переведенні якісних характеристик у числові (експертові значно простіше порівняти два неметричні критерії, аніж присвоїти їм числові значення).

Проте докладне дослідження МАІ дало змогу виявити такі його істотні недоліки:

- неузгодженість, зумовлену труднощами оцінювання відношень складних елементів (1-й вид неузгодженості);

• неузгодженість, зумовлену запропонованою дискретною шкалою для оцінювання елементів (2-й вид неузгодженості);

• різке зростання кількості оцінок зі збільшенням (понад 9) кількості порівнюваних елементів у наборі;

• перерахунок відношень значущості елементів у їхню важливість здійснюється наближеним методом;

• відсутність формального механізму синтезу колективного судження, завдяки якому воно виробляється безпосередньо в експертній групі під час проведення «круглого столу» (дебати з досягненням консенсусу).

Метод анкетування — один із найбільш перспективних методів розв'язування проблем соціального, політичного та воєнного змісту [141; 143; 152; 153]. Ідеться про безпосереднє використання суджень та інтуїції експертів у деякій формалізованій структурі. При цьому експерти, що входять до складу різних організацій, об'єднуються в кілька груп, що дозволяє спростити адміністративне управління їхньою роботою. У кожній групі призначається виконавець. Він несе відповідальність за організацію роботи своєї групи, основним способом збору інформації якої є опитувальний листок — ***анкета***, що містить логічно поєднану систему питань з досліджуваної проблеми.

В анкетах варто передбачити стандартний перелік питань або подій, щодо яких експерти мають висловитися. Питання в анкетах необхідно формулювати так, аби поряд з якісною можна було б дати кількісну характеристику відповідей експертів. Окрім цільових запитань анкета має містити інформацію про правила її заповнення та передбачати можливість уточнення питань і відповідей. А для того щоб експертні висновки забезпечували об'єктивність інформації, при складанні анкет необхідно також передбачити й включення низки показників компетентності експертів стосовно кожної з поданих ними оцінок.

Опитування експертів здійснюється анонімно в кілька етапів. Під етапом розуміється сукупність операцій зі збору та обробки експертних висновків (думок і оцінок), виконання яких закінчується отриманням остаточного результату щодо певної частини проведеного експерименту. Кожний етап проводиться в кілька турів — циклів робіт з експертами. Тур включає в себе постановку завдання експертам, збір і обробку думок (оцінок) експертів. Кількість турів на кожному етапі визначається складністю і кількістю взаємозалежних запитань, а також необхідним ступенем подібності експертних висновків при відшуканні остаточного результату з оцінюваного питання.

На першому етапі проводять опитування за анкетами з питань відкритого типу. Надалі опитування, як правило, проводять за анкетами, що містять питання закритого типу. При цьому в анкеті не повинно бути запитань, що припускають подвійне тлумачення. Сама побудова запитань має бути така, щоб експерт послідовно розкривав суть проблеми, щоразу спираючись на інформацію, яка міститься в попередніх запитаннях. Це означає, що відповіді на перші в загальній ієрархії запитання мають базуватися на найбільш надійній і доступній для експерта інформації, а також мати, по змозі, якісний характер. Експерт має зазначити, наприклад, розбіжність альтернатив за перевагою. Наступні запитання анкети мають складатися так, аби для відповіді на них була потрібна більш досконала інформація, наприклад у формі діапазонів значень чинників, що цікавлять дослідника. Заключні питання анкети мають бути такі, аби для відповіді на них знадобилася інформація у вигляді точкової

оцінки (числа). Якщо, наприклад, мета експертизи полягає у виявленні відносного внеску кожного з чинників у досягнення цілі операції, то останнім в анкеті повинне бути запитання: «Який, на Вашу думку, внесок кожного чинника в підвищення ефективності? Оцініть внесок кожного чинника за десятибальною шкалою». Якщо експертові відразу поставити останнє питання, то він не зможе відразу дати на нього відповідь або й взагалі її не буде. Організація анкети за принципом логічного ув'язування й ускладнення запитань дозволяє експертові самому глибше розібратися в проблемі і видати обґрунтовану й несуперечливу інформацію.

Залежно від мети туру та змісту поставлених в анкеті запитань відповіді експертів можуть спиратися на один із таких підходів: *логічний* (експерт на основі логічних міркувань, синтезуючи наявні в його розпорядженні матеріали, формує відповідь на поставлене запитання); *якісний* (експерт, виокрелюючи найбільш важливі ознаки й досліджуючи вже наявну їх градацію, будує узагальнену відповідь на основі кількох ознак); *комплексний* (ідеться про синтез двох попередніх підходів, коли поряд із якісною здійснюється й логічна градація); *каталізаційний* (експерт, спираючись на певну вихідну інформацію, має оцінити й доповнити її).

При застосуванні методу анкетування обробка експертних даних (залежно від складності або ступеня невизначеності проблеми, її конкретних аспектів і динаміки) здійснюється різними математичними методами або їх поєднанням. Це дозволяє отримати узагальнену думку (оцінку) експертів та визначити ступінь узгодженості окремих експертних висновків. Отже, метод анкетування як упорядкований і систематизований процес виявлення в певній послідовності суджень фахівців раціонального зерна, відкриває реальні можливості для поглибленого вивчення тих проблем, які не піддаються розв'язанню іншими методами.

Окрім перелічених методів для отримання колективної експертної оцінки доволі часто застосовують *методи компенсації, комісій* та *зваженої суми оцінок критеріїв, методи індивідуального* та *безпосереднього оцінювання, метод розміщення* тощо [151].

Метод компенсації використовується при попарному порівнянні альтернатив. ***Метод комісій*** припускає вільне обговорення проблеми між експертами. Його успіх багато в чому залежить від добору складу відповідної комісії та рівня організації її роботи. Основний недолік — намагання кожного експерта досягти компромісу. ***Метод зваженої суми оцінок критеріїв*** передбачає, що кожній альтернативі приписується кількісна (бальна) оцінка за кожним із критеріїв. Критеріям приписуються кількісні ваги, що характеризують їхню порівняльну важливість. Ваги множаться на критеріальні оцінки, а далі здобуті показники підсумовуються. Саме так визначається цінність альтернативи. Далі вибирається альтернатива з найбільшим показником цінності.

Індивідуальний метод, або ***метод узгодження оцінок***, полягає в тому, що кожний експерт дає оцінку події незалежно від інших, а далі за допомогою деякого прийому ці оцінки поєднуються в одну узагальнену (погоджену) оцінку.

Оскільки висновки, яких доходять фахівці, часто залежать від сфери їхніх наукових і особистих інтересів, сформованих поглядів і переконань, диктуються необхідністю підтримання репутації, то, бажано, аби всі вихідні дані, на базі яких формуються оцінки, були обґрунтовані й доступні для перевірки та критики.

Метод безпосереднього оцінювання використовується в тих випадках, коли існує чітка різниця між розглядуваними альтернативами або вони підлягають безпосередньому вимірюванню, маючи однакову природу. Сутність методу полягає в тому, що експерт має кожну з розглядуваних складних систем поставити на відповідне їй місце згідно зі ступенем наявності тієї чи іншої властивості або із запропонованим цим самим експертом коефіцієнтом значущості. У такому разі більше значення комплексної оцінки відповідає кращій системі.

Метод розміщення (*judgmental bootstrapping*) часто використовується при створенні комп'ютерних експертних програм. Експерти залучаються з різним рівнем компетентності або зі знаннями лише про окремі аспекти проблеми, через що їхні прогнози не підлягають безпосередньому порівнянню. Якщо при експертному оцінюванні зазвичай вважають, що думки всіх фахівців однаково вагомі, то метод розміщення передбачає, що до одних експертів варто прислухатися більш уважно, ніж до інших. Фахівці ранжуються залежно від оціненого рівня їхньої компетентності (принаймні із суб'єктивного погляду аналітика) та обсягу інформації про досліджувану проблему, яким вони володіють. Після цього за доволі складною схемою відбувається «зважування» і визначення кінцевого прогнозу, під переважним впливом думки найбільш авторитетних експертів.

Описані методи експертного оцінювання базуються на відповідних процедурах опитування, які різняться за формою спілкування з експертом та способом поставлення йому запитань. До таких процедур належать *очні* та *заочні*, *відкриті* і *закриті опитування*. При виборі конкретної процедури опитування слід ураховувати реальні обмеження щодо проведення експертизи, а також переваги і недоліки кожної процедури.

Очні опитування мають переваги перед заочними за інформативністю. Вони дозволяють унеможливити неправильне тлумачення з боку експерта запитань анкети, а також оперативно конкретизувати поставлені запитання завдяки новим формулюванням і уточненням. Проте для скорочення витрат на отримання інформації та уникнення психологічного тиску на експерта з боку ОУР (що може призвести до спотворення отримуваної інформації) доцільно застосовувати ***метод заочного опитування***. Але й він має певні недоліки. Головний із них той, що в ході заочного опитування експерт взагалі може не дати відповіді на деякі питання анкети через їх нерозуміння.

Важливу роль у процедурах експертного опитування відіграє спосіб постановки запитань. Якщо ОУР очікує на конкретну відповідь на те чи інше запитання, але не має впевненості щодо готовності повідомити повну інформацію, є сенс провести ***процедуру закритого опитування***. Вона передбачає постановку перед експертом таких запитань, у формулювання яких свідомо включено перелік альтернативних відповідей. Якщо запитання передбачає відповідь у формі лише «так» або «ні», то таке запитання називається *суто закритим*. Якщо потрібно зазначити один із більш ніж двох запропонованих варіантів відповіді, то таке запитання називається *відкритим*.

Процедуру відкритого опитування застосовують, як правило, у ситуаціях, що вимагають нетривіального рішення (за своїм цільовим призначенням така процедура подібна до колективного генерування ідей). Ідеться про завдання з формування вихідної множини стратегій, вибору показників і критеріїв ефективності, прогнозування поведінки інших суб'єктів операції, а також

про з'ясування за допомогою експертів нечітких моментів проблемної ситуації. Процедура забезпечує повну свободу відповідей експерта із зазначеної проблеми. Недоліки процедури зумовлюються тим, що неодмінно доводиться застосовувати неформальні методи опрацювання отриманої інформації, припускаючи довільну інтерпретацію запитань і відповідей, а також тим, що для її реалізації необхідна справді висока кваліфікація експертів.

Отже, всі індивідуальні та групові методи експертного оцінювання характеризуються відносною простотою та зручністю застосування. Вони придатні для прогнозування практично будь-яких ситуацій (наприклад, на ранніх етапах розробки або модернізації СТС), зокрема за умов неповної, невизначеної або неточної початкової інформації.

Важлива особливість таких методів полягає в тому, що вони дозволяють:

- установлювати ступінь складності і актуальності ситуацій (проблем);
- визначати основні чинники виникнення тих чи інших ситуацій (проблем), а також критерії їх оцінювання;
- виявляти найважливіші механізми впливу на досягнення поставлених цілей та взаємозв'язки між ними;
- оцінювати ступінь актуальності поставлених проблем у контексті завдань розвитку світової науки;
- ранжування ситуацій (проблем) шляхом багатокритеріального кількісного оцінювання для вибору найкращої альтернативи.

До основних недоліків таких методів слід віднести суб'єктивізм думок експертів і обмеженість їхніх суджень.

5.4. Опрацювання інформації евристичного походження

Одне з принципових питань, що неодмінно постає при використанні суджень експертів,— це питання про те, якою мірою досягається об'єктивність дослідження. На практиці об'єктивність може бути забезпечено за рахунок високої компетентності членів експертної групи, а також аргументованості їхніх суджень з оцінюваних питань, які здебільшого не одностайні. Тому постає завдання щодо їх систематизації та формалізації. Для цього останнім часом застосовують методи *парних порівнянь*, *ранжування* і *шкальних оцінок*, *методи теорії корисності* та *теорії проспектів*, *методи ELECTRE* та ін.

Метод попарних порівнянь має на меті визначити порядок розміщення n певних чинників (об'єктів) з погляду їхньої важливості (переваги) за допомогою їх попарного порівняння [155]. При цьому експерт, розглядаючи всі можливі пари досліджуваних чинників (об'єктів), вказує в кожній із них той, що, на його думку, найсильніше впливає на наслідок. Постає цілком логічне запитання: як дістати оцінку всієї сукупності об'єктів за результатами порівняння окремих пар цих об'єктів, виконаного групою експертів.

Припустимо, що кожний з m експертів, оцінюючи вплив на результат усіх пар чинників (об'єктів), дає таку числову оцінку:

$$r_{ij}^{h} = \begin{cases} 1, \text{ якщо чинник } O_i \text{ має більше значення, ніж } O_j, \\ 0{,}5, \text{ якщо чинники } O_i \text{ та } O_j \text{ рівноправні,} \\ 0, \text{ якщо чинник } O_i \text{ має менше значення, ніж } O_j. \end{cases}$$

Тут $h = \overline{1,m}$ — номер експерта; $i = \overline{1,n}$, $j = \overline{1,n}$ — номери об'єктів, досліджуваних під час експертизи.

Нехай при цьому m_i експертів надали перевагу чиннику O_i, m_j експертів — перевагу чиннику O_j, тоді як m_p експертів висловились за те, що порівнювані чинники рівноправні.

Тоді математичне сподівання дискретної випадкової величини r_{ij} набирає такого вигляду:

$$x_{ij} = M\left[r_{ij}^h\right] = 1 \cdot \frac{m_i}{m} + 0{,}5 \cdot \frac{m_p}{m} + 0 \cdot \frac{m_j}{m}, \quad h = \overline{1,m}. \tag{5.19}$$

Звідси, беручи до уваги, що загальна кількість експертів $m = m_i + m_p + m_j$, а отже, $m_p = m - (m_i + m_j)$, дістаємо:

$$x_{ij} = \frac{m_i}{m} + 0{,}5 \cdot \frac{\left(m - m_i - m_j\right)}{m} = \frac{1}{2} + \frac{m_i - m_j}{2 \cdot m}, \tag{5.20}$$

причому $x_{ij} + x_{ji} = 1$.

Таким чином, сукупність значень x_{ij} утворює матрицю розміру $n \times n$, елементи якої — це математичне сподівання оцінок всіх парних порівнянь даних чинників (табл. 5.10). Це дозволить визначити коефіцієнти відносної важливості чинників, тобто сформувати вектор $k = \left[k_1, k_2, \ldots, k_n\right]^T$.

Один зі способів відшукання значень елементів вектора k полягає в застосуванні наведеного далі ітераційного алгоритму.

1. Початкова умова: $t = 0,\ k^0 = \underbrace{[1\,1 \ldots 1]^T}_{n}$.

2. Рекурентні співвідношення: $k^t = \frac{1}{\lambda^t} \cdot X \cdot k^{t-1};\ \lambda^t = [1\ 1 \ldots 1] \cdot X \cdot k^{t-1},\ t = \overline{1,n}$, де X — матриця, елементи якої являють собою математичне сподівання оцінок пар об'єктів; k^t — вектор порядку t, побудований із коефіцієнтів відносної важливості даних чинників; $\sum_{i=1}^{n} k_i^t = 1$ — умова нормування.

3. Ознака закінчення алгоритму $\left\| k^t - k^{t-1} \right\| < E$.

Таблиця 5.10

Результати попарних порівнянь різних чинників

	O_1	...	O_j	...	O_n
O_1					
⋮					
O_i		$x_{ij} = M\left[r_{ij}\right]$			
⋮					
O_n					

$\Rightarrow$

k
k_1
⋮
k_i
⋮
k_n

Якщо матриця X невід'ємна і нерозкладна (переставленням рядків і стовпців її не можна звести до трикутного вигляду), то зі зростанням порядку $t \to \infty$ величина λ^t збігається до її максимального власного значення, тобто $k = \lim_{t \to \infty} k^t;\ \sum_{i=1}^{n} k_i = 1$. Це твердження, що випливає з теореми Перрона–Фробеніуса, доводить збіжність наведеного алгоритму.

Приклад 5.1 [143].

Припустимо, що на підставі опитування трьох ($m = 3$) експертів про ступінь впливу на остаточний результат трьох ($n = 3$) різних чинників побудовано такі таблиці парних порівнянь:

Експерт 1(R_1)

	O_1	O_2	O_3
O_1	0,5	1	1
O_2	0	0,5	0
O_3	0	1	0,5

Експерт 2(R_2)

	O_1	O_2	O_3
O_1	0,5	0,5	0,5
O_2	0,5	0,5	0,5
O_3	0,5	0,5	0,5

Експерт 3(R_3)

	O_1	O_2	O_3
O_1	0,5	1	0,5
O_2	0	0,5	0
O_3	0,5	1	0,5

Щоб дістати групову оцінку ступеня впливу кожного з об'єктів на результат, побудуємо матрицю математичних сподівань оцінок кожної з пар чинників:

	O_1	O_2	O_3
O_1	3/6	5/6	4/6
O_2	1/6	3/6	1/6
O_3	2/6	5/6	3/6

Значення елементів цієї матриці обчислено з таких виразів:

$$x_{11}=\frac{1}{2}+\frac{0-0}{2\cdot 3}=\frac{1}{2};\ x_{12}=\frac{1}{2}+\frac{2-0}{2\cdot 3}=\frac{5}{6};\ x_{13}=\frac{1}{2}+\frac{1-0}{2\cdot 3}=\frac{4}{6};$$

$$x_{21}=1-x_{12}=\frac{1}{6};\ x_{23}=\frac{1}{2}+\frac{0-2}{2\cdot 3}=\frac{1}{6};$$

$$x_{31}=1-x_{13}=\frac{2}{6};\ x_{32}=1-x_{23}=\frac{5}{6}.$$

Для наочності подамо кожний із кроків формування вектора відносної важливості:

Крок 0. $k^0=[1\ \ 1\ \ 1]^T.$

Крок 1.

$$Y^1=X\cdot k^0=\frac{1}{6}\begin{bmatrix}3&5&4\\1&3&1\\2&5&3\end{bmatrix}\cdot\begin{bmatrix}1\\1\\1\end{bmatrix}=\frac{1}{6}\begin{bmatrix}3+5+4\\1+3+1\\2+5+3\end{bmatrix}=\frac{1}{6}\begin{bmatrix}12\\5\\10\end{bmatrix},$$

$$\lambda^1=[1\ \ 1\ \ 1]\cdot Y^1=[1\ \ 1\ \ 1]\cdot\frac{1}{6}\begin{bmatrix}12\\5\\10\end{bmatrix}=\frac{1}{6}\cdot 27=\frac{27}{6},$$

$$k^1=\frac{1}{\lambda^1}\cdot Y^1=\frac{6}{27}\cdot\frac{1}{6}\begin{bmatrix}12\\5\\10\end{bmatrix}=\frac{1}{27}\begin{bmatrix}12\\5\\10\end{bmatrix}=\begin{bmatrix}0{,}444\\0{,}185\\0{,}370\end{bmatrix}.$$

Крок 2.

$$Y^2=X\cdot k^1=\frac{1}{6}\begin{bmatrix}3&5&4\\1&3&1\\2&5&3\end{bmatrix}\cdot\frac{1}{27}\begin{bmatrix}12\\5\\10\end{bmatrix}=\frac{1}{6\cdot 27}\begin{bmatrix}36+25+40\\12+15+10\\24+25+30\end{bmatrix}=\frac{1}{6\cdot 27}\begin{bmatrix}101\\37\\79\end{bmatrix},$$

$$\lambda^2=[1\ \ 1\ \ 1]\cdot Y^2=[1\ \ 1\ \ 1]\cdot\frac{1}{6\cdot 27}\begin{bmatrix}101\\37\\79\end{bmatrix}=\frac{217}{6\cdot 27},$$

$$k^2=\frac{1}{\lambda^2}\cdot Y^2=\frac{6\cdot 27}{217}\cdot\frac{1}{6\cdot 27}\begin{bmatrix}101\\37\\79\end{bmatrix}=\frac{1}{27}\begin{bmatrix}101\\37\\79\end{bmatrix}=\begin{bmatrix}0{,}465\\0{,}171\\0{,}364\end{bmatrix}.$$

$$\max\left(|0{,}465-0{,}444|,\ \ |0{,}171-0{,}185|,\ \ |0{,}364-0{,}370|\right)=0{,}021>0{,}001.$$

Крок 3. Здійснюючи ітераційний процес доти, доки норма оцінки не буде менша від заданої $\left(\max_i \left|k_i^t - k_i^{t-1}\right| < 0{,}00\right)$, дістаємо, що за групову оцінку ступеня впливу на результат можна взяти вектор коефіцієнтів відносної важливості об'єктів виду $k = k^4 = \begin{bmatrix}0{,}468 & 0{,}169 & 0{,}363\end{bmatrix}^T$.

Метод ранжування застосовують, як правило, тоді, коли необхідно впорядкувати в часі або просторі певні чинники (об'єкти), які визначають кінцеві результати, але не піддаються безпосередньому вимірюванню [152; 156]. Для цього експерт має розташувати їх у тому порядку, який він вважає найбільш раціональним (порядку зростання або спадання) і приписати кожному з чинників (об'єктів) певне число натурального ряду — порядковий номер, або *ранг*. Порядковий номер, що дорівнює 1, отримує найкращий чинник (об'єкт), а найменш важливому присвоюється порядковий номер n. Параметри $x_1, x_2, \ldots, x_n$ можуть включати в себе групи чинників (об'єктів), рівнозначних щодо їхньої важливості. Для кожної групи рівнозначних чинників (об'єктів) їхні ранги однакові, найчастіше дробові. Їх обчислюють як середнє арифметичне відповідної вибірки порядкових номерів чинників, що входять до певної групи. Нехай, наприклад, чинники x_2, x_7, x_1, x_5 рівнозначні й мають порядкові номери від 1 до 4. Ранг кожного з даних чинників визначається так: $\frac{1+2+3+4}{4} = 2\frac{1}{2}$.

Якщо ранжування виконують кілька, скажімо m, експертів, то для кожного чинника спочатку обчислюють суму рангів, отриману від усіх експертів, а потім згідно зі здобутим результатом установлюють його остаточний ранг. Найвищий (перший) ранг присвоюють чиннику, який набрав найменшу суму рангів, і, навпаки, чиннику, який набрав найбільшу суму рангів, присвоюють найнижчий ранг. Решту чинників упорядковують згідно зі значенням суми рангів того чинника, який має перший ранг.

На підставі здобутих даних формують матрицю рангів $\|x_{ij}\|$ $\left(i = \overline{1,n};\ j = \overline{1,m}\right)$ розміром $n \times m$, де n — кількість розглядуваних чинників;, m — кількість експертів:

Чинник	Експерти			
	1	2	...	m
k_1	x_{11}	x_{12}	...	x_{1m}
k_2	x_{21}	x_{22}	...	x_{2m}
⋮	⋮	⋮	...	⋮
k_n	x_{n1}	x_{n2}	...	x_{nm}

Значення x_{ij} характеризують порядок надання переваги i-му чиннику j-м експертом перед іншими чинниками. При цьому суму рангів для i-го чинника з урахуванням компетентності експертів можна обчислити за формулою

$$x_i = \sum_{j=1}^{m} p_j \cdot x_{ij}, \qquad (5.21)$$

де p_j — показник компетентності експертів, $0 \le p_j \le 1$; $j = \overline{1,m}$

Знайдені значення дозволяють упорядкувати чинники за ланцюжком нерівностей: $x_r < x_l < \ldots < x_q$ де $x_r = \min_i x_i$, $x_l = \min_{i, i \ne r} x_i$, $x_q = \max_{i, i \ne r, i \ne l} x_i$.

Наступним кроком визначається середній ранг, тобто середнє статистичне значення i-го чинника за формулою

$$S_i = \sum_{j=1}^{m} x_{ij} / m, \qquad (5.22)$$

де j — номер експерта, $j = \overline{1,m}$; i — номер ознаки, $i = \overline{1,n}$.

Зауважимо, що процедура побудови таких ранжувань коректна лише в тому разі, коли ранги призначаються як порядкові номери місць чинників у вигляді натуральних чисел $1,2,\ldots,n$. При цьому ранги чинників не дають змоги встановити, на скільки або у скільки разів один чинник переважніший за інший.

Проте для використання знань, отриманих від експертів, необхідно не лише впорядкувати або ранжувати розглядувані чинники за ступенем їхнього впливу на кінцевий результат, а й обчислити кількісну оцінку ступеня такого впливу. Найпростіший метод розв'язання цієї задачі зводиться до застосування комплексного підходу, що передбачає перехід від матриці ранжувань до матриці попарних порівнянь згідно з таким алгоритмом.

Усі експерти на основі матриці $\|x_{ij}\|$ будують m матриць X_j, $j = \overline{1,m}$, попарних порівнянь деяких чинників i та r.

Елементи цих матриць визначаються з умови:

$$X_j = \|x_{ir}^j\| = \begin{cases} 1, \text{ якщо } O_i^j > O_r^j, \text{ тобто } x_{ij} < x_{rj}, \\ 0{,}5, \text{ якщо } O_i^j \approx O_r^j, \text{ тобто } x_{ij} = x_{rj}, \\ 0, \text{ якщо } O_i^j < O_r^j, \text{ тобто } x_{ij} > x_{rj}. \end{cases} \qquad (5.23)$$

Тут, як і раніше, m — кількість експертів; j — номер експерта.

До отриманих m матриць застосовується метод обробки попарних порівнянь, ітераційна процедура якого дозволяє обчислювати коефіцієнти відносної важливості об'єктів за ступенем їхнього впливу на результат.

Приклад 5.2 [143].

Нехай троє експертів ($m = 3$) провели ранжування трьох чинників ($n = 3$) за ступенем їхнього впливу на певний результат. Матриця рангів має такий вигляд:

Чинник (об'єкт)	Експерт 1	Експерт 2	Експерт 3
O_1	1	1	2
O_2	2	3	1
O_3	3	2	3

Матриці попарних порівнянь для першого, другого і третього експертів набирають такого вигляду:

$$X_1 = \|x_{rj}^1\| = \begin{Vmatrix} 0{,}5 & 1 & 1 \\ 0 & 0{,}5 & 1 \\ 0 & 0 & 0{,}5 \end{Vmatrix}, \; X_2 = \|x_{rj}^2\| = \begin{Vmatrix} 0{,}5 & 1 & 1 \\ 0 & 0{,}5 & 0 \\ 0 & 1 & 0{,}5 \end{Vmatrix}, \; X_3 = \|x_{rj}^3\| = \begin{Vmatrix} 0{,}5 & 0 & 1 \\ 1 & 0{,}5 & 1 \\ 0 & 0 & 0{,}5 \end{Vmatrix}.$$

Використовуючи метод обробки попарних порівнянь, дістаємо послідовність векторів коефіцієнтів відносної важливості чинників:

Крок	Чинники (об'єкти)		
	O_1	O_2	O_3
0	1,0	1,0	1,0
1	0,481	0,330	0,185
2	0,489	0,346	0,156
3	0,5	0,348	0,152
4	0,5	0,349	0,151

Ітераційна процедура із заданою точністю ($E = 0{,}001$) збігається на четвертому кроці до значень, що являють собою компоненти такого вектора: $K = [0{,}500 \quad 0{,}349 \quad 0{,}151]^T$. Цим самим знайдено кількісну оцінку ступеня впливу кожного чинника (об'єкта) на результат, здобутий на основі вихідного ранжування.

Одним із різновидів методу ранжування є ***метод ідеальної точки***, який запропонували К. Юнг і С. Ванг [150]. Метод базується на тому, що найкращі розв'язки характеризуються найменшою відстанню від розв'язку від'ємно-ідеального. При цьому передбачається, що кожний критерій має монотонно спадну або монотонно зростаючу корисність. Тоді додатно-ідеальний розв'язок формується з найкращих значень критеріїв за всіма альтернативними варіантами, а від'ємно-ідеальний — із найгірших.

Алгоритм методу включає в себе такі кроки.

Крок 1. Формування зваженої нормалізованої матриці альтернатив-критеріїв. Для цього попередньо визначається вагомість $W = (w_1, w_2, ..., w_k, ..., w_q)$ кожного критерію для кожної альтернативи C_{ik}, де $k = \overline{1,q}$ — кількість критеріїв, $i = \overline{1,n}$ — кількість альтернатив.

Крок 2. Визначення додатно-ідеального A^+ та від'ємно-ідеального A^- розв'язку:

$$A^+ = \left\{ \max_i V_{ik} \middle| i \in [1,n], k \in [1,q] \right\} = \left\{ V_l^+ \ldots V_k^+ \ldots V_q^+ \right\}, \tag{5.24}$$

$$A^- = \left\{ \max_i V_{ik} \middle| i \in [1,n], k \in [1,q] \right\} = \left\{ V_l^- \ldots V_k^- \ldots V_q^- \right\}. \tag{5.25}$$

Крок 3. Обчислення відстані від поточної альтернативи до додатно-ідеальної та від'ємно-ідеальної точки за такими відповідно формулами:

$$G_j^+ = \sqrt{\sum_{k=1}^{q} \left(V_{ik} - V_k^+ \right)^2}, \tag{5.26}$$

$$G_j^- = \sqrt{\sum_{k=1}^{q} \left(V_{ik} - V_k^- \right)^2}. \tag{5.27}$$

Крок 4. Обчислення відносної близькості альтернативи a_i до додатно-ідеальної точки A^+ за формулою $L_i^+ = \dfrac{G_i^-}{G_i^+ + G_i^-}$, $0 < L_i^+ < 1$. Чим ближче L_i^+ до одиниці, тим a_i ближче до A^+.

Крок 5. Ранжування альтернативних варіантів за спаданням. Якщо $L_i^+ > L_j^+$, то $a_i > a_j$.

Як бачимо, точність і надійність процедури ранжування значною мірою залежать від кількості n розглядуваних чинників. І чим таких чинників менше

($n < 10$), тим вища їх розрізнюваність із погляду експерта, а отже, тим надійніше можна встановити ранг чинника.

Французька школа теорії ухвалення рішень, очолювана Б. Руа [157; 158], запропонувала свого часу конструктивний підхід до формування рішень, у рамках якого методи, моделі та концепції почали розглядатися як допоміжні засоби практичного аналізу ситуації. Вони дозволяли дослідникові не лише усвідомити мету ухвалення рішення, а й краще зрозуміти переваги особи, яка ухвалює рішення (ОУР). Невдовзі такий підхід дістав узагальнену назву — ***метод ELECTRE***.

Метод ELECTRE полягає в тому, що навіть у разі математичного домінування однієї альтернативи над іншою ОУР може вважати альтернативу a_i майже стовідсотково кращою за альтернативу a_j. При цьому головні кроки ОУР такі.

1. Формування матриці альтернатив-критеріїв. Для цього попередньо визначається вагомість $W = (w_1, w_2, ..., w_k, ..., w_q)$ кожного критерію для кожної альтернативи C_{ik}, де $k = \overline{1,q}$ — кількість критеріїв, $i = \overline{1,n}$ — кількість альтернатив.

2. Нормалізація побудованої матриці за правилами:

$$C_{ik}^r = \frac{C_{ik} - C_k^{\min}}{C_k^{\max} - C_k^{\min}}$$ — для критерію ефективності (чим значення більше, тим краще);

$$C_{ik}^r = \frac{C_k^{\max} - C_{ik}}{C_k^{\max} - C_k^{\min}}$$ — для критерію вартості (чим значення менше, тим краще),

де $C_k^{\max}$ і $C_k^{\min}$ — максимальне і мінімальне значення k-го критерію на всьому наборі альтернатив.

3. Визначення масивів узгодженості і неузгодженості.

Для пари альтернатив a_i та a_j множина критеріїв поділяється на дві підмножини. При цьому масив узгодженості містить усі критерії, за якими a_i переважніша за a_j: $F_{ij} = \{k \mid V_{ik} > V_{jk}\}$, і, навпаки, масив неузгодженості містить решту критеріїв: $G_{ij} = \{k \mid V_{ik} < V_{jk}\}$.

4. Розрахунок індексів узгодженості і неузгодженості.

Індекс узгодженості визначається як сума ваг критеріїв, що входять у масив узгодженості: $f_{ij} = \sum_{k \in F_{ij}} W_k$. *Індекс неузгодженості* відбиває ступінь того, наскільки альтернатива a_i гірша за a_j, і визначається так:

$$g_{ij} = \max_{k \in G_{ij}} \left| V_{ik} - V_{jk} \right| \Big/ \max_{k \in [1,g]} \left| V_{ik} - V_{jk} \right|. \qquad (5.28)$$

Очевидно, що $f_{ij} \in [0,1]$ і $g_{ij} \in [0,1]$. Більше значення f_{ij} означає, що a_i переважніша за a_j. Більше значення g_{ij} означає, що за критерієм неузгодженості альтернатива a_j, навпаки, є переважніша за a_i.

5. Визначення індексів домінування (порогів) узгодженості і неузгодженості. На цьому етапі ОУР задає значення P і Q — відповідно порогу узгодженості і неузгодженості:

$$\text{якщо } f_{ij} > P \text{ і } g_{ij} < Q, \text{ то } a_i > a_j. \qquad (5.29)$$

Недолік методу ELECTRE полягає в тому, що він виступає як допоміжний засіб, а не інструмент вироблення найкращого рішення. Зрештою цей метод, на відміну від аксіоматичного підходу, не дозволяє інтелектуалізувати весь

процес ухвалення рішення, оскільки вироблення остаточного рішення завжди залишається за ОУР, тобто за керівником.

Метод шкальних оцінок дає змогу знайти кількісну оцінку ступеня важливості кожного з чинників (параметрів), що належать певній сукупності [159; 160], відносно шкали їх певних базових (еталонних) значень. У цьому разі оцінки відносної важливості кожного чинника подаються в балах за деякою β-бальною шкалою. Найчастіше використовується 100-бальна шкала, де максимально можливій важливості відповідає оцінка в 100 балів, мінімально можливій — оцінка в 0 (нуль) балів.

При обробці експертних даних результати опитування зводяться в таблицю (табл. 5.11), де C_{ij} — відносна важливість параметра x_i з погляду j-го експерта, що виражається або відповідним балом, або значенням рангу.

Таблиця 5.11

Результати опитування експертів за методом шкальних оцінок різних чинників

Експерт	Чинники (параметри)					
	x_1	x_2	…	x_i	…	x_n
1	C_{11}	C_{12}	…	C_{1i}	…	C_{1n}
2	C_{21}	C_{22}	…	C_{2i}	…	C_{2n}
⋮	⋮	⋮	…	⋮	…	⋮
j	C_{j1}	C_{j2}	…	C_{ji}	…	C_{jn}
⋮	⋮	⋮	…	⋮	…	⋮
m	C_{m1}	C_{m2}	…	C_{mi}	…	C_{mn}

Середньоарифметичне значення оцінок C_i кожного з чинників визначається за формулою $C_i = \frac{1}{m_i}\sum_{j=1}^{m_i} C_{ji}$, де m_i — кількість експертів, що оцінювали важливість чинника x_i.

Значення C_{ij}, а отже, і C_i можуть подаватися як у балах, так і в рангах. У першому випадку значення C_i називають середнім балом чинника x_i, у другому — середнім рангом цього чинника. Якщо ранжування чинників здійснювати за методом попарних порівнянь, то дані таблиць від m експертів зводяться в одну загальну таблицю — *сумарну матрицю порівнянь*. У кожній клітинці ij цієї таблиці міститься певне число γ_{ij}, що аргументує перевагу i-го чинника над j-м згідно з висновками всіх m експертів. За повної згоди експертів C_n^2 клітинок загальної таблиці міститимуть число $\gamma = m$, а решта — нулі (0). За мінімальної кількості згод кожна клітинка міститиме число $\gamma = \frac{1}{2}m$, якщо m парне і $\gamma = \frac{1}{2}(m+1)$, якщо m непарне.

Підсумовування чисел γ_{ij} по рядках із подальшим діленням здобутого результату на m дає середнє ранжування чинників x_1, x_2, …, x_n, що, у свою чергу, являє собою показник узагальненої думки про важливість чинників (чим менша сума по рядку j, тим важливішу роль відіграє i-й чинник. Що ж до сум по стовпцях, то там картина протилежна.

Оскільки показник узагальненої думки C_i та еталонне значення — це, по суті, одне й те саме (вони різняться лише своїм призначенням), то надалі для спрощення міркувань вживатимемо термін ***центр групування шкальних***

оцінок, вважаючи, що це поняття включає в себе два попередніх. Методика пошуку центра групування експертних даних на шкалі оцінок для будь-якого закону розподілу використовує або середньостатистичне, або середньозважене значення оцінок. Такий підхід (особливо використання середньозваженого значення) дозволяє з достатнім ступенем наближення об'єктивно визначати центр групування. Проте в разі великого діапазону значень шкали врахування всіх без винятку значень може, як показано далі, призвести до відчутного зсуву центра групування.

Нехай C — центр групування оцінок, коли задано розподіл експертів за значеннями, які вони надають. Відомо також, що

$$C = F(k, h, W_h), \tag{5.30}$$

де k — кількість експертів у групі; h — крок пошуку області групування; W_h — діапазон значень оцінок, якому відповідає кількість експертів, не менша за θ_k, при найменшому кроці ($0 < \theta_k < 1$).

Візьмемо шкалу зі значеннями i, де $i = 0, 1, 2, \ldots, n$. Тоді m_i — це кількість експертів, що дали i-те значення. Якщо в групі k експертів, то $\sum_{i=1}^{n} m_i = k$.

На першому кроці пошуку центра групування ($h = 1$) визначаються ті пари значень, що задовольняють таку нерівність:

$$\sum_{i \in W_h}^{n} m_i \geq \theta_k. \tag{5.31}$$

Припустимо, що оцінки експертів розподілилися так, як це зображено на рис. 5.8.

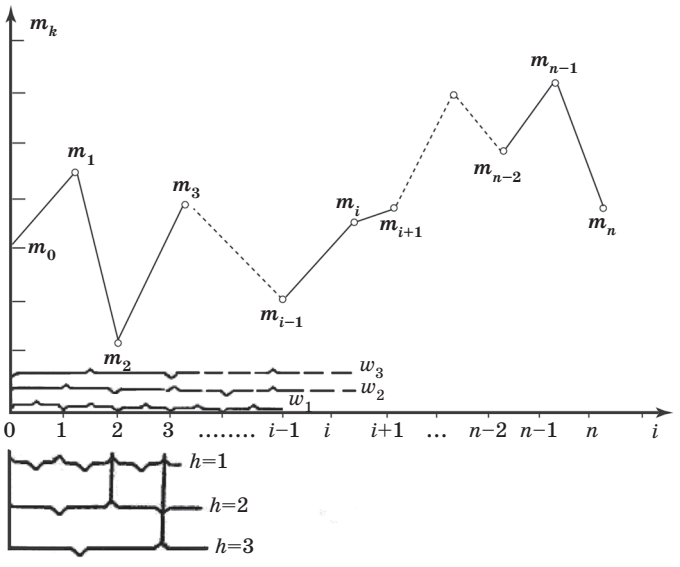


Рис. 5.8. Розподіл оцінок висловлювань експертів

Тоді можливі три випадки:

1) жодна пара значень на даному кроці пошуку не задовольняє нерівність (5.31). Тоді крок пошуку області групування зростає на одиницю, тобто область «зважування» розширюється, і процедура пошуку повторюється;

2) існує рівно одна область на шкалі за даного кроку пошуку, що задовольняє нерівність (5.31). У цьому разі область групування знайдено, причому центр групування визначається як середньозважене всіх значень, що належать зазначеній області:

$$C = \sum_{i \in W_h}^{n} i m_i \Big/ \sum_{i \in W_h}^{n} m_i; \qquad (5.32)$$

3) існує кілька областей, що задовольняють нерівність (5.31). Тоді область групування визначається в такий спосіб: ліва межа являє собою найменше значення для всіх значень знайдених областей, а права межа — відповідно їхнє найбільше значення. Область групування визначається як середньозважене всіх значень, що належать області групування:

$$C = \sum_{i \in G}^{n} i m_i \Big/ \sum_{i \in G}^{n} m_i, \qquad (5.33)$$

де G — множина всіх значень шкали, що належать області групування.

Приклад 5.3 [143].

Дано шкалу від нуля (0) до 10 і відповідну кожному значенню шкали кількість m_i експертів.

i	0	1	2	3	4	5	6	7	8	9	10
m_i	3	17	9	1	31	3	2	4	15	12	3

Нехай $\theta = 0{,}5$, оскільки 50%-кове порівняння на практиці найпоширеніше. Загальна кількість експертів $m = 100$. Узявши $h = 1$, обчислимо кількість експертів, що припадає на кожну область. Результати обчислень подамо у вигляді таблиці:

W_1	0–1	1–2	2—3	3–4	4—5	5–6	6–7	7–8	8–9	9–10
$\sum_{i \in W_1} m_i$	20	26	10	32	34	5	6	19	27	15

Отже, як випливає з таблиці, жодна область при заданому кроці не задовольняє нерівність (5.31). Тому, збільшивши крок пошуку, виконаємо підрахунок для розширених областей:

W_2	0–2	1–3	2–4	3–5	4–6	5–7	6–8	7–9	8–10
$\sum_{i \in W_2} m_i$	29	27	41	35	36	9	21	31	30

Як бачимо і на цьому кроці немає жодної області, що задовольняє співвідношення (5.32). Тому, знову збільшивши крок пошуку, повторимо процедуру:

W_3	0–3	1–4	2–5	3–6	4–7	5–8	6–9	7–10
$\sum_{i \in W_3} m_i$	30	58	44	37	40	24	33	34

У цьому разі існує рівно одна область, що задовольняє співвідношення (5.33), — область 1–4. Вона і є областю групування. Використовуючи співвідношення (5.33), знаходимо значення центра групування

$$C_1 = \sum_{i \in G}^{n} i m_i \Big/ \sum_{i \in G}^{n} m_i = \frac{1 \cdot 17 + 2 \cdot 9 + 3 \cdot 1 + 4 \cdot 31}{17 + 9 + 1 + 31} = \frac{162}{58} \approx 3.$$

Якщо за центр групування взяти середньозважене значення всієї шкали, то дістанемо

$$C_1 = \sum_{i \in G}^{n} i m_i \Big/ \sum_{i \in G}^{n} m_i = \frac{475}{100} \approx 5.$$

Як бачимо з наведеного прикладу, підрахунок через область групування дав корекцію порядку 40% порівняно із середньозваженим значенням.

Отже, застосування методів попарних порівнянь, ранжування і шкальних оцінок, методів теорії корисності та теорії проспектів, а також методів ELECTRE істотно допомагає здійснювати математичну обробку інформації евристичного походження та інтерпретувати її. Для цього можуть використовуватися:

- показники узагальненої думки (середнє арифметичне оцінок, медіана оцінок, центр групування оцінок і частота максимальних оцінок у балах);
- показники ступеня погодженості думок експертів (коефіцієнт варіації оцінок, коефіцієнт конкордації/коефіцієнт згоди і діапазон квартилів).

5.5. Оцінювання ступеня погодженості суджень групи експертів та їх статистичної вірогідності

Якісний аналіз експертної інформації як заключний етап експертного оцінювання включає в себе [143; 161; 162]:

- оцінювання ступеня погодженості думок експертів;
- виокремлення груп експертів із близькою думкою (за наявності істотної розбіжності в їхніх відповідях);
- виявлення розкиду думок, впливу характеристик експертів на зміст їхніх відповідей;
- ранжування відповідей в однорідних групах та формування об'єднаних відповідей.

Як показники ступеня погодженості суджень експертів найчастіше за все використовують *коефіцієнт варіації* [163], *коефіцієнт парної рангової кореляції* та *коефіцієнт конкордації*.

Коефіцієнт варіації v_j характеризує відносний ступінь варіювання параметрів і обчислюється за формулою, %:

$$v_j = \frac{S_j}{C_i} \cdot 100, \tag{5.34}$$

де $S_j = \sqrt{D_j}$ — стандартне (середньоквадратичне) відхилення оцінок, отриманих j-м параметром [141];

$$D_j = \frac{1}{m_j - 1} \sum_{i=1}^{m_j} \left(C_{ij} - \overline{C_j} \right)^2$$

— дисперсія оцінок.

Чим менше v_j, тим вищий ступінь погодженості групи експертів щодо відносної важливості j-го параметра (чинника). Наближене значення похибки коефіцієнта варіації можна обчислити за формулою

$$S_{v_j} = \frac{v_j}{\sqrt{2 m_j}} \sqrt{1 - 2 \left(\frac{v_j}{100} \right)^2}. \tag{5.35}$$

Із певним наближенням можна вважати, що в генеральній сукупності коефіцієнт варіації для j-го параметра становить $v_j \pm 3 S_{v_j}$.

Коефіцієнт парної рангової кореляції $\rho_{\alpha\beta}$ характеризує окремих експертів, міркування яких у цілому погоджені, або, навпаки, експертів, які мають різкі розбіжності в судженнях про важливість чинників. Цей коефіцієнт набуває значень від -1 до 1 ($-1 \le \rho_{\alpha\beta} \le 1$) і подається формулою

$$\rho_{\alpha\beta} = 1 - \frac{\sum_{j=1}^{p} \psi_j^2}{\frac{1}{6}\left(p^3 - p\right) - \frac{1}{12}\left(T_\alpha - T_\beta\right)}, \tag{5.36}$$

де Ψ_j — модуль різниці рангів R_{α_j} і R_{β_j} оцінок j-го параметра (чинника), призначених відповідно експертом α і β,

$$\psi_j = \left| R_{\alpha_j} - R_{\beta_j} \right|; \tag{5.37}$$

T_α, T_β — показники зв'язаних рангів у ранжуваннях експертів α і β; p — загальна кількість груп ранжувань.

При цьому можливі такі випадки:

$$\rho_{\alpha\beta} = \begin{cases} 0 \text{ — показники незалежності (відсутність зв'язку між судженнями експертів),} \\ 1 \text{ — ранжування за показниками однакове (погодженість думок),} \\ -1 \text{ — ранжування за показниками цілком протилежне.} \end{cases}$$

Коефіцієнт рангової кореляції для сумарного ранжування, який запропонували 1940 року М. Кендалл та Б. Сміт [164], дістав назву ***коефіцієнта конкордації W***. Він характеризує ступінь погодженості суджень групи експертів у цілому, по всій сукупності параметрів (об'єктів, чинників, показників, заходів, напрямків дослідження тощо) і обчислюється за таким алгоритмом.

Крок 1 [165–167]. Визначається середньоарифметичне значення сум рангів оцінок, отриманих усіма параметрами:

$$\overline{R} = \frac{1}{n}\sum_{j=1}^{n} R_j, \tag{5.38}$$

де R_j — сума рангів оцінок, отриманих j-м параметром.

Крок 2. Обчислюється відхилення d_j сум рангів оцінок, отриманих j-м параметром, від середнього арифметичного сум рангів оцінок, отриманих усіма параметрами:

$$d_j = R_j - \overline{R}. \tag{5.39}$$

Крок 3. Обчислюється сума квадратів цих відхилень:

$$S = \sum_{j=1}^{n} d_j^2. \tag{5.40}$$

Крок 4. Визначається показник T_i зв'язаних (однакових) рангів оцінок, призначених i-м експертом. Якщо всі n рангів, призначених i-м експертом, різні, то $T = 0$. Якщо серед рангів є однакові, то $T_i = \sum_{l=1}^{L}\left(t_l^3 - t_l\right)$.

Розглянемо приклад розрахунку T_i для одного експерта, результати опитування якого з приводу відносної важливості дев'яти параметрів ($j = 1, \ldots, 9$) подано в наведеній далі таблиці.

Кількісна оцінка	Параметри								
	1	2	3	4	5	6	7	8	9
Бали	70	100	90	70	100	70	80	50	40
Ранги	6	1,5	3	6	1,5	6	4	8	9

У цьому прикладі $L = 2$ (одна група відповідає оцінці у 100 балів, ранг 1,5; друга — 70 балів, ранг 6). Кількість зв'язаних рангів у першій групі $t_1 = 2$, тобто є дві оцінки по 100 балів; у другій групі $t_2 = 3$ (три оцінки по 70 балів). Звідси

$$T = \sum_{l=1}^{6}\left(t_l^3 - t_l\right) = \left(2^3 - 2\right) + \left(3^3 - 3\right) = 30. \tag{5.41}$$

Крок 5. Визначається *коефіцієнт конкордації* [141]:

$$W = \frac{S}{Sm} = \frac{12\Delta S^2}{m^2\left(p^3 - p\right)}, \tag{5.42}$$

де $\Delta S^2 = m^2 \sum_{i=1}^{n}\left(C_i - \frac{1}{2}(p+1)\right)^2$ — міра ступеня узгодженості думок експертів (сума квадратів відхилень фактичних значень рангів від їхніх ідеальних значень).

Значення коефіцієнта конкордації може змінюватися в інтервалі $0 \le W \le 1$. При цьому

$$W = \begin{cases} 0, \text{ якщо міркування експертів не збігаються,} \\ 1, \text{ якщо міркування експертів повністю збігаються.} \end{cases}$$

Якщо в ранжуванні є однакові ранги [164–167], то коефіцієнт конкордації обчислюється за формулою:

$$W = \frac{12S}{z^2\left(p^3 - p\right) - z\sum_{i-1}^{z} T_i}, \tag{5.43}$$

де $S = \sum_{i=1}^{n}\left(\sum_{j=1}^{m} r_{ij} - \bar{r}^{\,2}\right)$, $\bar{r} = \frac{1}{n}\sum_{i=1}^{n} r_i$, $r_i = \sum_{j=1}^{m} r_{ij}$,

z — кількість груп ранжувань зв'язаних (однакових) рангів; T_i — кількість зв'язаних рангів у i-му ранжуванні; r_{ji} — матриця результатів ранжування i-ї альтернативи j-м експертом.

Приклад груп зв'язаних рангів подано в наведеній далі таблиці. Маємо три групи ($L = 3$) рангів, для яких $t_1 = 2$, $t_2 = 3$, $t_3 = 2$:

$$T_i = (2^3 - 2 + 3^2 - 3 + 2^3 - 2) = 36\ .$$

Оцінка, подана j-м експертом	Параметри								
	a	b	c	d	e	f	g	h	k
Ранги	5	1,5	3	7,5	1,5	7,5	5	9	5

Крок 6. Оцінюється статистична вірогідність коефіцієнта конкордації W за допомогою перевірки нульової гіпотези H_0: $W = 0$. При цьому методика перевірки залежить від значень m та n. У разі невеликих m ($m \le 10$) і $n \le 7$ для перевірки нульової гіпотези, коли рівень значущості $q = 0{,}05$, можна скористатися такими табличними значеннями S:

Кількість експертів $(i=\overline{1,m})$	Кількість параметрів $(j=\overline{1,n})$				
	3	4	5	6	7
3	—	—	64,6	103,9	157,3
4	—	49,5	88,4	143,3	217,0
5	—	62,6	112,3	182,4	276,2
6	—	75,7	136,1	221,4	335,2
8	48,1	101,7	183,7	299,0	453,1
10	60,0	127,8	231,2	376,7	571,0

При $n > 7$ і значенні m, що змінюється від 3 до 20, використовують зазвичай критеріальну статистику χ^2_R, розподілену за χ^2 при $\theta = n - 1$:

$$\chi^2_R = \frac{12S}{mn(n+1)}. \tag{5.44}$$

Якщо кількість зв'язків велика або вони мають значну довжину, відповідний вираз набирає такого вигляду:

$$\chi^2_R = \frac{12S}{mn(n+1) - \frac{1}{n-1}\sum_{j=1}^{m} T_i}. \tag{5.45}$$

Правила ухвалення статистичного рішення:

- гіпотеза H_0 приймається при $\chi^2_R < \chi^2_{q,\theta}$;
- гіпотеза H_0 відхиляється, якщо $\chi^2_R \geq \chi^2_{q,\theta}$, де $\chi^2_{q,\theta}$ критичне значення при $\theta = n - 1$ та заданому таблично рівні значущості q:

Кількість ступенів свободи	Рівні значущості		Кількість ступенів свободи	Рівні значущості	
	$q = 0{,}2$	$q = 0{,}1$		$q = 0{,}2$	$q = 0{,}1$
1	1,5	2,7	16	20,5	23,5
2	3,2	4,6	17	2,61	24,8
3	4,6	6,3	18	22,8	26,0
4	6,0	7,8	19	23,9	27,2
5	7,3	9,2	20	25,0	28,4
6	8,6	10,6	21	26,2	29,5
7	9,8	12,0	22	27,3	30,8
8	11,0	13,4	23	28,4	32,0
9	12,2	14,7	24	29,6	33,2
10	13,4	15,0	25	30,7	34,4
11	14,6	16,3	26	31,8	35,6
12	15,8	18,5	27	32,9	36,7
13	17,0	19,8	28	34,0	37,9
14	18,2	21,1	29	35,1	39,1
15	19,3	22,3	30	36,3	40,3

Нульову гіпотезу можна знайти й інакше, скориставшись тією самою, таблицею і взявши в ній значення $q_{\text{табл}}$ для емпіричного χ^2_R при $\theta = n - 1$. Далі порівнюють $q_{\text{табл}}$ із заданим $q = 10\%$. Якщо $q_{\text{табл}} < 10\%$, то маємо невипадкову узгодженість суджень групи експертів.

Незалежно від використовуваних коефіцієнтів у результаті розрахунків дістають квадратну матрицю, що характеризує ступінь близькості експертів за характером відповідей. Цю матрицю можна розбити на однорідні групи, скориставшись одним з алгоритмів таксономії (багатовимірної класифікації). Результати таксономії з визначеною щільністю зводяться до однієї з трьох ситуацій:

1) відповіді більшості експертів утворюють компактну групу, склад якої стабільний при різних розбиттях;

2) у процесі розбиття виокремлюється кілька стабільних, чітко розмежованих груп;

3) відповіді експертів рівномірно розташовані в просторі ознак (альтернатив), але на різних етапах розбиття утворюють нестабільні групи.

У першому випадку існує достатня погодженість думок більшості експертів. У другому можна висунути гіпотезу про неоднорідність колективу експертів, виявивши набір об'єктивних характеристик експертів, що зумовлюють цю неоднорідність, та сформувавши впорядковану послідовність ознак для кожної виокремленої групи експертів. Третій випадок означає або невдалу з погляду набору альтернатив і кількості градацій шкали побудови анкети опитування, або сильно виражену неоднорідність та некомпетентність експертної групи. Можливий вплив і обох причин одночасно. Тоді переходять до поглибленого дослідження відповідей за окремими альтернативами, і в тому разі, коли щодо ступеня варіації за деякими з них спостерігаються різкі розбіжності, то можливі два рішення: або переробити анкету опитування, або ранжувати лише ті альтернативи, щодо яких існує досить висока погодженість експертів.

Приклад 5.4 [143]. Оцінювання відносної важливості п'яти параметрів.

Спираючись на результати колективної експертизи, розв'яжемо статистичну задачу щодо оцінювання відносної важливості п'яти параметрів. Початкову інформацію наведено в поданій далі таблиці.

Експерт $(i=\overline{1,10})$	Параметри ($n=5$)									
	1-й		2-й		3-й		4-й		5-й	
	Бали	Ранг	Бали	Ранг	Бали	Ранг	Бали	Ранг	Бали	Ранг
1	100	1	10	5	80	3	70	4	90	2
2	80	2,5	60	4	100	1	10	5	80	2,5
3	80	3	80	3	100	1	10	5	80	3
4	20	4,5	2	4,5	100	1	40	3	90	2
5	100	1	10	5	80	2,5	30	4	80	2,5
6	90	2	30	4	100	1	50	3	10	5
7	30	3	10	5	100	1	20	4	80	2
8	80	2	60	3	90	1	40	4	20	5
9	100	1	10	4,5	80	3	10	4,5	90	2
10	80	2	20	4	100	1	10	5	60	3
R_j	22		42		15,5		41,5		29	
Загальний ранг	2		5		1		4		3	

Середнє значення рангів обчислюємо так:

$$\overline{R_j} = \frac{1}{5}\sum_{j=1}^{5} R_j = \frac{150}{5} = 30.$$

Для визначення коефіцієнта конкордації W необхідно d_j, S і T_i, скориставшись відповідно формулою (5.39), (5.40) і (5.41).

Значення d_j і d_j^2 подано в таблиці:

d_j	8	12	−14,5	11,5	−1
d_j^2	64	144	210,25	132,25	1

Сума квадратів відхилень $S = 551{,}5$. Показники зв'язаних рангів для кожного i-го експерта мають такі значення:

$$T_1 = 0;\ T_2 = (2^3 - 2) = 6;\ T_3 = (3^3 - 3) = 24;\ T_4 = (2^3 - 2) = 6;\ T_5 = (2^3 - 2) = 6;$$

$$T_6 = 0;\ T_7 = 0;\ T_8 = 0;\ T_9 = (2^3 - 2) = 6;\ T_{10} = 0;\ \sum_{i=1}^{10} T_i = 48.$$

Коефіцієнт конкордації W знаходимо згідно з (5.42):

$$W = \frac{12 \cdot 551{,}5}{10^2 \cdot \left(5^2 - 5\right) - 10 \cdot 48} = \frac{6606}{11520} = 0{,}55.$$

Оскільки $n < 7$, то оцінювання значущості емпіричного коефіцієнта виконаємо для критичних значень S (для коефіцієнта W). Якщо рівень значущості $q = 0{,}05$, $n = 5$ і $m = 10$, то $S_{\text{кр}} = 231{,}2$. Емпіричне значення $S = 551{,}5$. Оскільки $S > S_{\text{кр}}$, то нульова гіпотеза H_0: $W = 0$ відхиляється, причому із заданим рівнем значущості q приймається суттєвість значення $W = 0{,}55$. Тобто маємо суттєву узгодженість суджень експертів при оцінюванні відносної важливості параметрів.

Приклад 5.5 [143]. Оцінювання відносної важливості восьми параметрів.

Скориставшись результатами колективної експертизи, розв'язати статистичну задачу щодо оцінювання відносної важливості восьми параметрів.

Результати опитування п'яти експертів наведено в таблиці.

Експерт $(i = \overline{1,5})$	**Параметри (n = 8)**															
	1-й		2-й		3-й		4-й		5-й		6-й		7-й		8-й	
1	90	2	40	4	100	1	50	3	10	6,5	0	8	10	6,5	30	5
2	30	3	20	4,5	100	1	20	4,5	80	2	10	6	0	7,5	0	7,5
3	80	2	60	3,5	100	1	40	5	20	6	0	8	10	7	60	3,5
4	100	1	10	6	90	2,5	10	6	90	2,5	20	4	0	8	10	6
5	80	1,5	40	4	80	1,5	10	6	60	3	0	7,5	0	7,5	20	5
R_j	9,6		22,0		7		24,5		20		33,5		36,5		27	
Загальний ранг	2		4		1		5		3		7		8		6	
d_j	−13		−0,5		−15,5		2		−2,5		11		14		4,5	

Показники зв'язаних рангів для кожного i-го експерта мають такі значення:

$$T_1 = (2^3 - 2) = 6;\ T_2 = (2^3 - 2) + (2^3 - 2) = 12;\ T_3 = (2^3 - 2) = 6;$$
$$T_4 = (2^3 - 2) + (3^3 - 3) = 30;\ T_5 = (2^3 - 2) + (2^3 - 2) = 12.$$

Середнє значення рангів: $\overline{R_j} = \frac{1}{8}\sum_{j=1}^{8} R_j = \frac{180}{5} = 22{,}5.$

Сума квадратів d_j така: $S = \sum_{j=1}^{8} d_j^2 = 757.$

Коефіцієнт конкордації обчислюємо згідно з (5.43):

$$W = \frac{12 \cdot 757}{5^2 \cdot \left(8^2 - 8\right) - 5 \cdot 66} = \frac{9084}{12300} = 0{,}7.$$

Для оцінювання емпіричного коефіцієнта $W = 0{,}7$ висловимо нульову гіпотезу про відсутність погодженості суджень експертів H_0: $W = 0$. Оскільки $n > 7$, то для перевірки H_0 скористаємося формулою (5.45):

$$\chi_R^2 = \frac{12 \cdot 757}{5 \cdot 8 \cdot (8+1) - \frac{1}{8-1} \cdot 66} = \frac{9084}{350{,}6} = 25{,}35.$$

Знаходимо $\chi^2_{q,\theta}$. При $q = 0{,}1$ і $\theta = n - 1 = 8 - 1 = 7$, дістаємо $\chi^2_{10\%,7} = 12$. Оскільки $\chi_R^2 \geq \chi^2_{q,\theta}$, то H_0 відхиляється й приймається гіпотеза H_1 щодо наявності погодженості в думках експертів. Схему, що унаочнює алгоритм розв'язування статистичної задачі з оцінювання відносної важливості параметрів за результатами колективної експертизи, наведено на рис. 5.9.

Отже, коефіцієнти варіації, парної рангової кореляції та конкордації допомагають визначити ступінь погодженості суджень експертів.

Приклад застосування соціоінженерних методів розв'язання проблем інформаційної кібербезпеки подано в додатку Е.

Питання для самоконтролю

1. Назвіть характерні риси соціоінженерного підходу. Дайте визначення таких методів соціоінженерної діяльності, як соціальна діагностика, соціальне планування та прогнозування.

2. Що являє собою процедура тестування системи захисту на проникнення? У чому полягає її сутність? Як класифікують тести на проникнення?

3. Схарактеризуйте комплексний тест на проникнення. Дотримання яких технічних і соціоінженерних правил він вимагає?

4. На яких рівнях має проводитись тестування на проникнення? Розкрийте їх сутність.

5. Що є логічним продовженням тесту на проникнення? Які завдання покладаються на комплексну систему управління рівнем захищеності?

6. Яких заходів необхідно вживати в процесі моніторингу захищеності периметра корпоративної мережі?

7. З якою метою розробляється програма поінформованості? Які роботи мають бути виконані в процесі її реалізації?

8. Розкрийте особливості впровадження системи управління інформаційною безпекою.

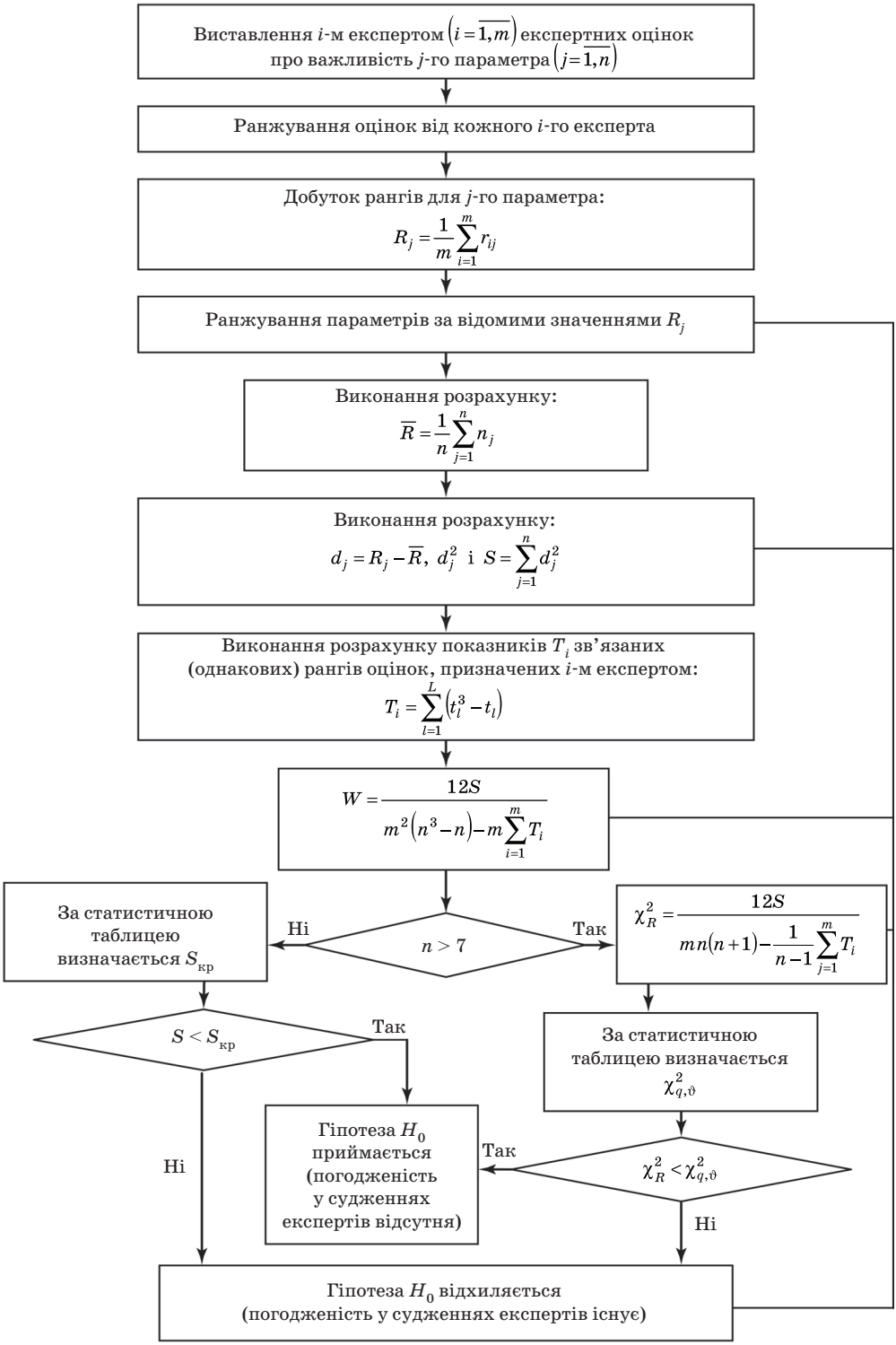


Рис. 5.9. Схема алгоритму розв'язання статистичної задачі з оцінювання відносної важливості параметрів (об'єктів, чинників тощо) за результатами колективної експертизи

9. Який процес називають експертним оцінюванням? Назвіть головні етапи його реалізації.

10. Розкрийте сутність головних етапів експертного оцінювання.

11. В який спосіб відбувається формування експертної групи?

12. Назвіть методи оцінювання індивідуальної компетентності представників експертної групи. Стисло розкрийте їхню сутність.

13. Які методи застосовують, аби отримати експертну інформацію евристичного походження? Стисло опишіть алгоритм опрацювання такої інформації.

14. Розкрийте сутність та етапність реалізації методів колективного експертного оцінювання.

15. Метод мозкової атаки: призначення, етапи реалізації, переваги та недоліки.

16. Метод Дельфі: сутність та призначення.

17. Метод аналізу ієрархій: призначення, використовувані принципи, переваги та недоліки.

18. Метод анкетування: алгоритм реалізації.

19. Назвіть основні переваги та недоліки індивідуальних і групових методів експертного оцінювання.

20. Схарактеризуйте головні методи опрацювання інформації евристичного походження.

21. Метод попарних порівнянь: призначення, приклади застосування.

22. Метод ранжування: призначення, приклади застосування.

23. Метод ідеальної точки: алгоритм реалізації та приклади застосування.

24. Метод ELECTRE: алгоритм реалізації та приклади застосування.

25. Метод шкальних оцінок: алгоритм реалізації та приклади застосування.

26. У чому полягає аналіз експертної інформації? Назвіть показники ступеня погодженості суджень експертів.

27. Розкрийте сутність коефіцієнтів варіації та парної рангової кореляції.

28. Розкрийте сутність коефіцієнта конкордації. Наведіть приклади його застосування.

ПІСЛЯМОВА

Усе викладене в підручнику, як і щоденна життєва практика, переконливо доводить: забезпечення інформаційної і кібернетичної безпеки — процес безперервний, надзвичайно складний і багатогранний, причому успіх у його реалізації зумовлюється соціумом і залежить від кожного його представника, але передусім від неухильно здійснюваної державної політики в цій сфері, цілеспрямованих зусиль усіх гілок влади, наукової громадськості, керівників усіх рівнів. Водночас систематизовані заходи із запобігання численним загрозам не повинні перешкоджати дедалі стрімкішому формуванню національного інформаційного і кібернетичного простору, а також інтеграції України у світове інформаційне суспільство. Саме тому стратегічним завданням державної політики має стати формування комплексної системи інформаційної і кібернетичної безпеки, в основу якої покладено науково обґрунтовані політичні, соціальні й економічні критерії та світовий досвід щодо правових і організаційних аспектів функціонування.

Сьогодні, як показує практика, одним із найефективніших засобів профілактики, протидії та боротьби з усілякими кібернетичними втручаннями і загрозами стає розвідка ІТ систем, яка все виразніше перетворюється з діяльності, спрямованої на своєчасне викриття ознак підготовки ймовірного зловмисника до нападу, на діяльність, що має на меті досягти стійкої інформаційної переваги над ним. Насамперед ідеться, вочевидь, про кібербезпеку. Адже її інструментарій завдяки раціональному поєднанню чотирьох основних процедур — пошуку, збору, обробки та подання інформації в інтересах певних сил — дозволяє вживати найбільш ефективних заходів щодо розвідувальної діяльності у відкритих і відносно відкритих електронних джерелах.

У доволі широкому спектрі відомих методів кіберрозвідки (SQL-ін'єкції, експлойти, віруси, переповнення буфера, DoS і DDoS атаки, бекдори, руткіти та інші способи проникнення й виведення систем з ладу) незмінно лідирує соціальна інженерія. Саме цей підхід у поєднанні з деперсонофікованими центрами інтернет-доступу, портативною ЕОТ, сертифікованими БД (БЗ) пошукових матеріалів і джерел інформації дає змогу неавторизованим користувачам та підрозділам спеціального призначення досягати вагомих результатів:

- викривати ознаки підготовки протиборчих сторін до збройного нападу, визначати порядок їхніх дій та очікувані ризики;
- відстежувати всі етапи проходження інформації, що циркулює в ІТС;
- уникати ускладнень у процесі пошуку, оброблення, нагромадження та зберігання інформації.

Оскільки всі методи й прийоми, до яких вдаються неавторизовані користувачі, спираються здебільшого на маніпулювання слабкостями людської психіки, то можна впевнено стверджувати: універсальних засобів протидії атакам соціальних інженерів, на жаль, не існує. Утім наявність чітко здійснюваної політики безпеки, застосування технологій, що взаємодоповнюють системи розпізнавання атак (IDS), даючи змогу відстежувати всі пакети, які проходять через мережний інтерфейс, вивчення слабких ланок прикладного ПЗ згідно з даними корпорацій CERT (http://www.cert.com) і Bugtrad (http://www.securityfocus.com), а також дослідження спеціальних аналітичних додатків із використанням log-файлів операційних систем та мережних log-файлів — усе це сприятиме адекватному реагуванню на спроби зловмисників отримати доступ до корпоративних ресурсів або розголосити інформацію, пов'язану із системою безпеки, та максимально зменшити можливі наслідки в разі реалізації таких атак.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бурячок, В. Л. Основи формування державної системи кібернетичної безпеки: монографія/ В. Л. Бурячок.— К.: НАУ, 2013.— 432 с.

2. Гнатюк, С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. О. Гнатюк// Безпека інформації.— 2013.— Т. 19, № 2.— С. 118–129.

3. GAO-10-606. CYBERSPASE United States Faces Challenges in Addressing Global Cybersecurity and Governance, Washington, July 2010 [Електронний ресурс].— Режим доступу:

http://web.ebscohost.com.

4. GAO-10-628. Key Private and Public Cyber Expectations Need to Be Consistently Addressed United States Government Accountability Office, Washington, July 2010 [Електронний ресурс].— Режим доступу:

http://web.ebscohost.com.

5. Рада національної безпеки і оборони України: експертні консультації Україна – НАТО з питань кібернетичного захисту [Електронний ресурс].— Режим доступу:

http://www.rainbow.gov.ua/news/ 1076.html

6. Корченко, О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О. Г. Корченко, В. Л. Бурячок, С. О. Гнатюк // Безпека інформації.— 2013.— Т. 19, № 1.— С. 40–45.

7. Мельник, С. В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С. В. Мельник, О. О. Тихомиров, О. С. Лєнков // Зб. наук. праць Військового ін-ту КНУ ім. Тараса Шевченка.— К.: ВІКНУ, 2011.— Вип. 30.— С. 159–165.

8. Словник термінів із кібербезпеки / За заг. ред. О. В. Копана, Є. Д. Скулиша — К.: ВБ «Аванпост-Прим», 2012.— 214 с.

9. Бурячок, В. Л. Кібернетична безпека — головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спец. техніка.— 2011.— № 3.— С. 104–114.

10. Про ратифікацію Конвенції про кіберзлочинність: за станом на 14.10.2010 р. / Закон, затверджений ВР України 07.09.2005, № 284-IV [Електронний ресурс].— Режим доступу:

http://zakon4.rada.gov.ua/laws/show/2824-15.— Офіц. вид.— К.: Відомості Верховної Ради України від 10.02.2006.

11. Про інформацію: за станом на 09.05.2011 р. / Закон, затверджений ВР України 02.10.1992, № 2657-XII [Електронний ресурс].— Режим доступу:

http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Відомості Верховної Ради України від 01.12.1992.

12. Про основи національної безпеки України: за станом на 20.07.2010 р. / Закон, затверджений ВР України 19 червня 2003 р., № 964-IV [Електронний ресурс].— Режим доступу:

http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 30.07.2003, № 139.

13. Про державну службу спеціального зв'язку та захисту інформації: за станом на 07.08.2011 р. / Закон, затверджений ВР України 23 лютого 2006 року, № 3475-IV [Електронний ресурс].— Режим доступу:

http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 11.04.2006, № 68.

14. Про телекомунікації: за станом на 15.10.2011 р. / Закон, затверджений ВР України, 18.11.2003, № 1280-IV [Електронний ресурс].— Режим доступу:

http://zakon1.rada. gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Урядовий кур'єр від 24.12.2003, № 243.

15. Про захист інформації в інформаційно-телекомунікаційних системах: за станом на 30.04.2009 р. / Закон, затверджений ВР України 05.07.1994, № 80/94-ВР [Електронний ресурс].— Режим доступу:

http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Відомості Верховної Ради України від 02.08.1994.

16. Про доступ до публічної інформації: за станом на 09.06.2013 р. / Закон, затверджений ВР України 13.01.2011, № 2939-VI [Електронний ресурс].— Режим доступу:
http://zakon4.rada.gov.ua/laws/show/2939-17.— Офіц. вид.— К.: Відомості Верховної Ради України від 12.08.2011.

17. Про оборону України: за станом на 01.07.2013 р. / Закон, затверджений ВР України 06.12.1991, № 1932-XII [Електронний ресурс].— Режим доступу:
http://zakon4.rada.gov.ua/laws/show/1932-12.— Офіц. вид.— К.: Відомості Верховної Ради України від 03.03.1992.

18. Про засади внутрішньої і зовнішньої політики: за станом на 01.07.2010 р. / Закон, затверджений ВР України 01.07.2010, № 2411-VI [Електронний ресурс].— Режим доступу:
http://zakon4.rada.gov.ua/laws/show /2411-17.— Офіц. вид.— К.: Відомості Верховної Ради України від 08.10.2010.

19. Про об'єкти підвищеної небезпеки: за станом на 18.11.2012 р. / Закон, затверджений ВР України 18.01.2001, № 2245-III [Електронний ресурс].— Режим доступу:
http://zakon4.rada.gov.ua/laws/show/2245-14.— Офіц. вид.— К.: Відомості Верховної Ради України від 13.04.2001.

20. Про Стратегію національної безпеки України: за станом на 12.02.2007 р. / Указ Президента України від 12.02.2007 р., № 105/2007 [Електронний ресурс].— Режим доступу:
http://zakon1.rada.gov.ua/cgi-bin/laws/maincgi.— Офіц. вид.— К.: Урядовий кур'єр від 07.03.2007, № 43.

21. Про Доктрину інформаційної безпеки України: за станом на 08.07.2009 р. / Указ Президента України від 8.02.2009 р., № 514/2009 [Електронний ресурс].— Режим доступу:
http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi.— Офіц. вид.— К.: Офіційний вісник України від 20.07.2009.

22. Про Воєнну доктрину України: за станом на 22.06.2012 р. / Указ Президента України від 15.06.2004, № 648/2004 [Електронний ресурс].— Режим доступу:
http://zakon4.rada.gov.ua/laws/show/648/2004.— Офіц. вид.— К.: Офіційний вісник України від 13.08.2004.

23. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: за станом на 09.01.2007р. / Закон, затверджений ВР України 09.01.2007, № 537-V [Електронний ресурс].— Режим доступу:
http://zakon4.rada.gov.ua/laws/show/537-16.— Офіц. вид.— К.: Відомості Верховної Ради України від 23.03.2007.

24. Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України: проект за станом на 06.03.2013 р. № 2483 [Електронний ресурс].— Режим доступу:
http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=45998

25. 11–12 лютого в Україні пройшли Консультації експертів «Україна – НАТО» з питань кібернетичного захисту [Електронний ресурс].— Режим доступу:
http://zik.com.ua/ua/news/2010/02/12/216707.

26. Шеломенцев, В. П. Сутність організаційного забезпечення системи кібернетичної безпеки України та напрями його удосконалення [Електронний ресурс] / В. П. Шеломенцев.— Режим доступу:
http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe? C21COM=2&I21DBN=UJRN&P21DBN=UJRN&Z21ID=&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/boz_2012_2_36.pdf.

27. Практика ИБ \ SANS: топ 20 наиболее критичных защитных мер и средств [Електронний ресурс].— Режим доступу:
https://www.sugarsync.com/pf/D6870693_7400982_60553

28. Семенов, Ю. А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности [Електронний ресурс] / Ю. А. Семенов.— Режим доступу:
http://book.itep.ru/10/2012.htm

29. Competitive intelligence [Електронний ресурс].— Режим доступу:
http://en.wikipedia.org/wiki/Competitive_intelligence.

30. Карпов, Г. Атака на DNS или ночной кошмар сетевого администратора [Електронний ресурс] / Геннадий Карпов.— Режим доступу:
http://www.hackzone.ru/articles/dns-poison.html, 02.06.2007.

31. Examining port scan methods — Analyzing Audible Techniques [Електронний ресурс].— Режим доступу:
http://www.windowsecurity.com/whitepapers/ xamining_port_scan_ methods_Analyzing_ Audible_Techniques.html.

32. Инциденты информационной безопасности: рекомендации по реагированию.— М.: Group-IB и LETA, 2011.— 20 с.

33. Харченко, В. П. Кибертерроризм на авиационном транспорте / [В. П. Харченко, Ю. Б. Чеботаренко, О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк] // Проблеми інформатизації та управління: Зб. наук. праць.— 2009.— Вип. 4 (28).— С. 131–140.

34. Дубов, Д. В. Кібербезпека: світові тенденції та виклики для України / Д. В. Дубов, М. А. Ожеван.— К.: НІСД, 2011.— 30 с.

35. Шеломенцев, В. П. До концепції законопроекту про кібернетичну безпеку / В. П. Шеломенцев // Боротьба з Інтернет-злочинністю: матеріали міжнар. наук.-техн. конф.— Донецьк: ДЮІ МВС України, 2013.— С. 12–14.

36. Peter Neumann. Computer-Related Risk. ACM Press/Addison Wesley, 1995.

37. Гавриш, С. Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії [Електронний ресурс] / С. Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика).— Режим доступу:

http://archive.nbuv.gov.ua/portal/soc_gum/bozk/2009_20/20text/g20_01.htm

38. Pollitt, M. M. «A Cyberterrorism Fact or Fancy?» / M. M. Pollitt // Proceedings of the 20th National Information Systems Security Conference, 1997.— P. 285–289.

39. Довгань, О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О. Д. Довгань, В. Г. Хлань // Інформаційна безпека людини, суспільства, держави.— 2011.— № 3 (7).— С. 49–53.

40. Denning, D. E. The Terrorism Research Center [Електронний ресурс] / D. E. Denning.— Режим доступу:

http://www.washprofile.org/en/node/686

41. Травников, Ю. Преступления в паутине: границы без замков [Електронний ресурс] / Ю. Травников // Ukrainian Scientific Journal of Information Security.— 2013.— Vol. 19, issue 2.— P. 128.— Режим доступу:

http://www.pl-computers.ru/article.cfm?Id=742&Page=3

42. Климчик, О. О. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів / О. О. Климчик, Р. М. Кравченко // Інформаційна безпека людини, суспільства, держави.— 2010.— № 1 (3).— С. 26–30.

43. Малышенко Д. Г. Противодействие компьютерному терроризму — важнейшая задача современного общества и государства / Д. Г. Малышенко // ВНИИ МВД России, «Вестник РАЕН».— 2004.— Т. 3, № 4.

44. Старостина, Е. Терроризм и кибертерроризм — новая угроза международной безопасности [Електронний ресурс] / Е. Старостина.— Режим доступу:

http://www.crime–research.ru/articles /starostina

45. Kerr, K. Putting cyberterrorism into context [Електронний ресурс] / K. Kerr.— Режим доступу:

http://www.auscert. org.au/ render.html?it=3552

46. Бутузов, В. М. Протидія комп'ютерній злочинності в Україні (системно структурний аналіз): монографія / В. М. Бутузов.— К.: КІТ, 2010.— 145 с.

47. Гаврилов, Ю.В. Современный терроризм: сущность, типология, проблемы противодействия / Ю. В. Гаврилов, Л. В. Смирнов.— М.: ЮИ МВД РФ, 2003.— 66 с.

48. Тропина, Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате / Т. Л. Тропина: сб. науч. трудов междунар. конф. «Информационные технологии и безопасность».— Вып. 3.— К.: НАН Украины, 2003.— С. 173–181.

49. Вехов, В. Б. Компьютерные преступления: способы совершения, методики расследования. / В. Б. Вехов.— М.: Право и закон, 1998.— С. 29–37.

50. Мазуров, В. А. Кибертерроризм: понятие, проблемы противодействия / В. А. Мазуров [Електронний ресурс].— Режим доступу:

http://www.tusur.ru/filearchive/reports-magazine/2010-1/41-45.pdf.

51. Международное сотрудничество в борьбе с компьютерной преступностью: проблемы и пути их решения: материалы междунар. науч.-практ. конф.— Донецк.: ДЮИ ЛГУВД, 2007.— 352 с.

52. Касперский, Е. Киберпреступность как бизнес [Електронний ресурс] / Евгений Касперский.— Режим доступу:

http://www.crime-research.ru/analytics/cybercrimes20101/2.

53. Бурячок, В. Л. Кіберзлочинність і кібертероризм — загрози національній безпеці та інтересам України / В. Л. Бурячок, О. В. Шарий // Вісник воєнної розвідки.— 2010.— № 21.— С. 24–29.

54. Гриняев, С. Н. США развертывают систему информационной безопасности [Електронний ресурс] / С. Н. Гриняев.— Режим доступу:
http://www.cnews.ru/security/part3/rus-edu.shtml, 24.05.2010.

55. Ільяшов, О. А. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу / О. А. Ільяшов, В. Л. Бурячок // Наука і оборона.— 2010.— № 4.— С. 35–40.

56. Бурячок В. Л. Завдання, форми та способи ведення воєн у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона.— 2011.— № 3.— С. 35–42.

57. Грищук, Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія / Р. В. Грищук.— Житомир: Рута, 2010.— 280 с.

58. Бурячок, В. Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем / В. Л. Бурячок // Захист інформації.— 2011.— № 3 (52).— С. 19–27.

59. Бурячок, В. Л. До питання організації та проведення розвідки у кібернетичному просторі / В. Л. Бурячок, Г. М. Гулак, В. О. Хорошко // Наука і оборона.— 2011.— № 2.— С. 19–23.

60. Бурячок, В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем / В. Л. Бурячок, О. Г. Корченко, Л. В. Бурячок // Захист інформації.— 2012.— № 4(57).— С. 5–12.

61. [Електронний ресурс].— Режим доступу:
ru.wikipedia.org.

62. Современные угрозы и каналы утечки информации в компьютерных сетях [Електронний ресурс].— Режим доступу:
http://bibliofond.ru/view.aspx?id=67579.

63. Бурячок, В. Л. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення / В. Л. Бурячок, Л. В. Бурячок, Т. Я. Костюк // Вісник воєнної розвідки.— 2011.— 24.— С. 67–74.

64. Гвильдис, Е. А. Человеческий фактор в проблеме обеспечения информационной безопасности компании: сб. науч. тр.— К.: НАУ, 2007.— С. 166–171.— («Защита информации»).

65. Материалы семинара «Современные технологии управления» [Електронний ресурс].— Режим доступу:
Www.kommersant.ru.

66. Маслоу, А. О менеджменте / А. Маслоу.— СПб: Питер, 2003.— 416 с.

67. Гаврюшин, Е. И. Человеческий фактор в обеспечении безопасности конфиденциальной информации [Електронний ресурс] / Е. И. Гаврюшин.— Режим доступу:
Www.bezpeka.desant.com.ua.

68. Мирошниченко, А. Зарплата и пустота / Андрей Мирошниченко // Банковское обозрение.— 2006.— № 10(88).

69. Бондаренко, Е. Социальные сети как инструмент развития: виды и возможности [Електронній ресурс] / Е. Бондаренко.— Режим доступу:
http://www.trainings.ru/library/articles/?id=10067

70. Все социальные сети развиваются по графику [Електронний ресурс].— Режим доступу:
http://www.soobshestva.ru/news/?p=233

71. Гуц, А. К. Социальные системы. Формализация и компьютерное моделирование: учеб. пособие / А. К. Гуц.— Омск: Изд-во Омск. гос. ун-та, 2000.— 160 с.— (PDF-текст).

72. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов.— СПб.: БХВ-Петербург, 2007.— 368 с.

73. Сообщества.РУ: социальные сети и формирование групп [Електронний ресурс].— Режим доступу:
http://www.soobshestva.ru/news/?p=243

74. Эйдман, И. В. Свободный человек в мире социальных сетей. Каким будет новое глобальное интернет-общество [Електронний ресурс].— Режим доступу:
http://www.vremya.ru/2008/22/4 /197454.html

75. International Network for Social Network Analysis [Електронний ресурс].— Режим доступу:
http://www.insna.org/

76. Каталог русских web 2.0 сайтов, социальных сетей и сервисов [Електронний ресурс].— Режим доступу:
Catalogr.ru

77. Кутик М. Две трети украинских компаний видят в социальных сетях угрозу IT-безопасности [Електронний ресурс] / Максим Кутик.— Режим доступу:
http://ain.ua/2011/12/01/66860

78. Остапенко, Г. А. Информационные риски в социальных сетях: монография / [Г. А. Остапенко, Л. В. Паринова, В. И. Белоножкин, И. Л. Батаронов, К. В. Симонов] / Под ред. чл.-кор. РАН Д. А. Новикова.— Воронеж: Изд-во «Научная книга», 2013.— 160 с.

79. Губанов, Д. А. Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А. Новиков, А. Г. Чхарташвили / Под ред. чл.-кор. РАН Д. А. Новикова.— М.: Физ.-мат. гиз., 2010.— 228 с.

80. Офіційний сайт Trenfrr http [Електронний ресурс].— Режим доступу: www.trendrr.com/ 16.12.2009

81. Офіційний сайт Trackur http [Електронний ресурс].— Режим доступу: www.trackur.com/ 16.12.2009

82. Офіційний сайт Sentiment Metrics http [Електронний ресурс].— Режим доступу: www.sentimentmetrics.com/ 16.12.2009

83. Цвиркун, А. Д. Основы синтеза структуры сложных систем.— М.: Наука, 1982.— 200 с.

84. Краснощеков, П. С. Информатика и проектирование / П. С. Краснощеков, А. А. Петров, В. В. Федоров.— М.: Знание, 1986.— 48 с. (сер. «Математика, кибернетика» № 10).

85. Советов, Б. Я. Моделирование систем / Б. Я. Советов, С. А. Яковлев.— М.: Высш. шк., 1985.— 217 с.

86. Бусленко, Н. П. Моделирование сложных систем / Н. П. Бусленко.— М.: Наука, 1978.— 399 с.

87. Дружинин, В. В. Проблемы системологии / В. В. Дружинин, Д. С. Контуров.— М.: Сов. радио, 1976.— 296 с.

88. Клиланд, Д. Системный анализ и целевое управление: пер. с англ./ Д. Клиланд, В. Кинг — М.: Сов. радио, 1974.— 280 с.

89. Радвик, Б. Военное планирование и анализ систем / Б. Радвик.— М.: Воениздат, 1972.— 478 с.

90. Моисеев, Н. Н. Математические задачи системного анализа: 2-е изд. / Н. Н. Моисеев.— М.: Наука, 2012.— 488 с.

91. Громов, Ю. Ю. Системный анализ в информационных технологиях: учеб. пособие / [Ю. Ю. Громов, Н. А. Земской, А. В. Лагутин, О. Г. Иванова, В. М. Тютюнник].— Тамбов: Изд-во Тамбов. гос. техн. ун-та, 2004.— 176 с.

92. Романов, А. И. Основы теории телекоммуникационных сетей: учеб. пособие для вузов / А. И. Романов.— К.: ВІТІ НТУУ «КПІ», 2002.— 157 с.

93. Пятибратов, А. П. Вычислительные машины, сети и телекоммуникационные системы: учеб.-метод. комплекс / А. П. Пятибратов, Л. П. Гудино, А. А. Кириленко.— М.: Изд. центр ЕАОИ, 2009.— 292 с.

94. Бройдо, В. Л. Вычислительные системы, сети и телекоммуникации: учебник для вузов: 2-е изд. / В. Л. Бройдо.— СПб.: Питер, 2004.— 703 с.

95. Рыбаков, Ф. И. Системы эффективного взаимодействия человека и ЭВМ / Ф. И. Рыбаков.— М.: Радио и связь, 1985.— 200 с.

96. Шибанов, В. С. Средства автоматизации управления в системах связи / В. С. Шибанов, Н. И. Лычагин.— М.: Радио и связь, 1990.— 232 с.

97. Вологій, Б. Ю. Технологія моделювання алгоритмів поведінки інформаційних систем / Б. Ю. Вологій.— Львів: Вид.-во НУ «Львівська політехніка», 2004.— 220 с.

98. Козиол, Дж. Искусство взлома и защиты систем / [Дж. Козиол, Д. Личфилд, Д. Эйтэл и др.].— СПб.: Питер, 2006.— 416 с.

99. Кузнецов, М. Социальная инженерия и социальные хакеры / М. Кузнецов, И. Симдянов.— СПб.: БХВ-Петербург, 2007.— 368 с.

100. Мошенничество с помощью фарминга: перенаправление на фальшивые сайты [Електронний ресурс].— Режим доступу: http://www.microsoft.com/rus/athome/security/privacy/pharming.mspx

101. Бычек, В. Социальная инженерия в интеллектуальной битве «добра» и «зла» [Електронний ресурс] / В. Бычек, Е. Ершова.— Режим доступу: http://www.aladdin-rd.ru/press/publications/11475, 20.12.2006.

102. Бурячок, В. Л. Поняття кібервійни та розвідки інформаційно-телекомунікаційних систем у контексті захисту держави від стороннього кібернетичного впливу / В. Л. Бурячок, О. А. Ільяшов, Г. М. Гулак // Збірник матеріалів круглого столу «Актуальні питання підготовки фахівців із розслідування кіберзлочинів», 25.11.2011.— К.: Наук.-вид. відділ НА СБ України, 2011.— С. 27–32.

103. Касперски, К. Секретное оружие социальной инженерии [Електронний ресурс] / Крис Касперски.— Режим доступу: http://kpnc.opennet.ru/SOC_ENG.pdf.

104. Современные угрозы и каналы утечки информации в компьютерных сетях [Електронний ресурс].— Режим доступу:
http://bibliofond.ru/view.aspx?id=67579.

105. The risk of social engineering on information security: a survey of it professionals [Електронний ресурс].— Режим доступу:
http://www.

106. Атаки на электронную почту: теперь это личное [Електронний ресурс].— Режим доступу:
http://www.slideshare.net/CiscoRu/targeted-attacks

107. Фишинговая атака на пользователей ВКонтакте [Електронний ресурс].— Режим доступу:
http://www.ferra.ru/ru/soft/news/2011/08/17/vkontakte-fish/

108. «Вишинг» [Електронний ресурс].— Режим доступу:
http://www.iz-news.ru/news/317/

109. Корченко, А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / А. Г. Корченко.— К.: МК-Пресс, 2006.— 320 с.

110. Конеев, И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев.— СПб.: БХВ- Петербург, 2003.— 752 с.

111. Чириль, Дж. Защита от хакеров (+CO) / Дж. Чириль.— СПб.: Питер, 2002.— 480 с.

112. Мак-Клар, С. Секреты хакеров. Безопасность сетей — готовые решения / Стюард Мак-Клар, Джоел Спенбреб, Джордж Курц.— 4-е изд.: пер. с англ.— М.: Изд. дом «Вильямс», 2004.— 656 с.

113. Коул Е. Руководство по защите от хакеров / Ерик Коул: пер. с англ.— М.: Изд. дом «Вильямс». 2002.— 640 с.

114. Бабок, В. П. Інформаційна безпека та сучасні мережені технології: англ.-укр.-рос. словник термінів / В. П. Бабок, В. Г. Корченко.— К.: НАУ, 2003.— 670 с.

115. Mitnik, Kevin U. The Art of Deception / Kevin U. Mitnik, William L. Simon, Steve Wozniak.— Wiley, 2002.— 304 с.

116. Корченко, А. Г. Несанкционированный доступ к компьютерным системам и методы защиты: учеб. пособие / А. Г. Корченко.— К.: КМУГА, 1998.— 116 с.

117. Cialdini, Robert B. The Science of Persuasion / Robert B. Cialdini // II Scientific American Magazine.— 2001.— № 2.— P.76–81.

118. Кузнецов, И. Н. Информация: сбор, защита, анализ: учебник по информационно-аналитической работе / И. Н. Кузнецов.— М.: ООО «Изд.-во «Яуза», 2001.— 100 с.

119. Корченко, О. Г. Класифікація методів соціального інжинірингу / О. Г. Корченко, Є. В. Паціра, Д. А. Пуха // Захист інформації.— К.: НАУ.— 2007.— № 4.— С. 37–45.

120. Шейнов, В. П. Искусство управлять людьми: учеб.-метод. пособие / В. П. Шейнов.— Мн.: Харвест, 2005.— 512 с.

121. Касперски, К. Секретное оружие социальной инженерии / К. Касперски // Журнал сетевых решений.— 2012.— № 9.— С. 12–15.

122. Митник, К. Д. Искусство обмана: учеб.-метод. пособие / К. Д. Митник.— NYC: Wiley Books. 2008.— 273 с.

123. Шудрова, К. Социальная инженерия в информационной безопасности / К. Шудрова // Директор по безопасности.— 2012.— № 10.— С. 13–17.

124. Конри-Мюррей, Э. Защита пользователей от атак [Електронний ресурс] / Э. Конри-Мюррей.— Режим доступу:
<http://www.docflow.ru/news/analytics/detail.php?ID=1526> (15.04.2011).

125. Лукацкий, А. В. Инженеры человеческих душ [Електронний ресурс] / А. В. Лукацкий.— Режим доступу:
< http://citforum.ru/internet/securities/soc_eng.shtml> (29.11.12).

126. How to Protect Insiders from Social Engineering Threats [Електронний ресурс].— Режим доступу:
http://www.microsoft.com/downloads/details.aspx?FamilyID=05033e55-aa96-4d49-8f57-c47664107938&DisplayLang=en

127. Краткое описание атак с использованием социальной инженерии [Електронний ресурс].— Режим доступу:
http://itband.ru/2009/07/social-engineering/

128. Портал http://socialware.ru/

129. Домарев, В. В. Безопасность информационных технологий: системный поход.— К.: ООО «ТИД Диа Софт», 2004.— 992 с.

130. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»).— М.: Оружие и технологии, 2009.

131. Гришина, Н. В. Организация комплексной защиты информации.— М.: Гелиос АРВ, 2007.— 256.

132. Официальный сайт «Лаборотории Касперского».— Режим доступу:
http://www.securelist.com/ru/

133. Защита пользователей от социальной инженерии [Електронний ресурс].— Режим доступу:
http://stud-baza.ru/sotsialnaya-injeneriya-vidyi-printsipyi-zaschita-doklad-kompyuternyieseti

134. Тесты на проникновение [Електронний ресурс].— Режим доступу:
http://www.ptsecurity.ru/services/pen/

135. Лепихин, В. Б. Сравнительный анализ сканеров безопасности. Ч. 1: тест на проникновение (краткое резюме) [Електронний ресурс].— Режим доступу:
http://www.itshop.ru/Sravnitelnyy-analiz-skanerov-bezopasnosti-Chast-1-test-na-proniknovenie-kratkoe-rezyume/l9i22670

136. Соколов, А. Тестирование на проникновение: инструментальный анализ уязвимостей или имитация действий злоумышленника? [Електронний ресурс] /Андрей Соколов.— Режим доступу:
http://www.nobunkum.ru/ru/pentest

137. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? [Електронний ресурс] /А. Дорофеев.— Режим доступу:
http://www.npo-echelon.ru/doc/inside-dorofeev.pdf

138. Соколов, А. Тесты на проникновение повысят интерес топ-менеджмента к ИБ [Електронний ресурс] /Андрей Соколов.— Режим доступу:
http://www.cnews.ru/reviews/free/security2009/articles/pentest.shtml

139. Сердюк В. Тест на проникновение как эффективный инструмент для оценки реальной защищенности банка от внешних угроз [Електронний ресурс] /В. Сердюк.— Режим доступу:
http://www.abajour.ru/files/Serduk_04-2010.pdf

140. Райхман, Э. П. Экспертные методы в оценке качества товаров / Э. П. Райхман, Г. Г. Азгальдов.— М.: Экономика, 1974.— 151 с.

141. Саати Т. Аналитическое планирование. Организация систем / Т. Саати, К. Кернс; пер с англ. под ред. И. А.Ушакова.— М.: Радио и связь, 1991.— 224 с.

142. Комаринський, Я. Фінансово-інвестиційний аналіз: навч. посібник / Я. Комаринський, І. Яремчук.— К.: Укр. енцикл., 1996.— 298 с.

143. Бурячок, В. Л. Технологія прийняття рішень у складних соціотехнічних системах: монографія / В. Л. Бурячок, В. О. Хорошко; за заг. ред. д-ра. техн. наук, проф. В. О. Хорошка.— К.: ДУІКТ, 2012.— 344 с.

144. Добров, Г. И. Экспертные оценки в научно-техническом прогнозировании / [Г. И. Добров, Ю. А. Ершов, Е. И. Левин, Л. П. Смирнов]; под общ. ред. В. С. Михалевича.— К.: Наук. думка, 1974.— 160 с.

145. Бешелев, С. Д. Математико-статистические методы экспертных оценок / С. Д. Бешелев, Ф. Г. Гурвич.— М.: Статистика, 1980.— 263 с.

146. Элти, Д. Экспертные системы: концепции и примеры / Д. Єлти, М. Кумбс.— М.: Финансы и статистика, 1987.— 191 с.

147. Ф. Хейрес-Рот. Построение экспертных систем: пер с англ. Ф. Херес-Рот, Д. Уотерман, Д. Ленан; под ред. Ф. Херес-Рота.— М.: Мир, 1987.— 441 с.

148. Евланов, Л. С. Экспертные оценки в управлении / Л. С. Евланов, В. А. Кутузова.— М.: Экономика, 1978.— 133 с.

149. Самохвалов, Ю. Я. Экспертное оценивание: методический аспект / Ю. Я. Самохвалов, Е. М. Науменко.— К.: ДУИКТ, 2007.— 263 с.

150. Литвак, Б. Г. Экспертная информация. Методы получения и анализа / Б. Г. Литвак.— М.: Радио и связь, 1982.— 184 с.

151. Китаев, Н. Н. Групповые экспертные оценки / Н. Н. Китаев.— М.: Знание, 1975.— 64 с.

152. Экспертные системы: принципы работы и примеры / [А. Брукинг, П. Джонс, Ф. Кокс и др.]; под ред. Р. Форсайта.— М.: Радио и связь, 1987.— 224 с.

153. Частиков, А. П. Разработка экспертных систем. Среда CLIPS / А. П. Частиков, Д. Л. Белов, Т. А. Гаврилова.— М.: BHV, 2003.— 608 с.

154. Уотермен Д. Руководство по экспертным системам / Л. Уотермен; пер. с англ. под ред. В. Л. Стефанюка.— М.: Мир, 1989.— 388 с.

155. Дэвид, Г. Метод парных сравнений / Г. Дэвид; пер. с англ. Н. Космарской и Д. Шмерлинга.— М.: Статистика, 1978.— 144 с.

156. Раушенбах, Г. В. Экспертные оценки в медицине: научный обзор / Г. В. Раушенбах, О.В. Филиппов.— М.: ВНИИММТИ Минздрава СССР, 1983.— 80 с.

157. Руа, Б. Классификация и выбор при наличии нескольких критериев: вопросы анализа и принятия решений / Б. Руа.— М.: Мир, 1976.— С. 80–107.

158. Гафт, М. Г. Принятие решений при многих критериях / М. Г. Гафт.— М.: Знание, 1979.— 64 с.

159. Герасимов, Б. М. Людино-машинні системи прийняття рішень з елементами штучного інтелекту / Б. М. Герасимов, В. О. Тарасов, І. В. Токарев.— К.: Наук. думка, 1993.— 184 с.

160. Гмошинский, В. Г. Теоретические основы инженерного прогнозирования / В. Г. Гмошинский, Г. И. Флиорент.— М.: Наука, 1973.— 304 с.

161. Статистические методы анализа экспертных оценок: ученые записки по статистике. Т. 29 / Под ред. Т. В. Рябушкина.— М.: Наука, 1977.— 384 с.

162. Методы анализа данных, оценивания и выбора в системных исследованиях: сб. тр.— М.: ВНИИСИ, 1986.— Вып. 14.— 124 с.

163. Бурячок, В. Л. Методичні аспекти експертного аналізу зразків техніки у прогнозуванні їх використання та розвитку / М. М. Мітрахович, В. Л. Бурячок, М. І. Луханін // Наука і оборона.— 2002.— Вип. № 4.— С. 36–41.

164. Кендал, М. Ранговые корреляции / М. Кендал: пер. с англ. под. ред. Е. М. Четыркина и Р. М. Энтона.— М.: Статистика, 1975.— 213 с.

165. Кенуй, М. Г. Быстрые статистические вычисления / М. Кенуй; пер с англ.— М.: Статистика, 1979.— 69 с.

166. Осипов, В. П. Справочник по методам решения статистических задач / [В. П. Осипов, Н. В. Осипов, В. С. Рубцов, Ю. И. Радковец].— К.: КВИРТУ ПВО, 1989.— 132 с.

167. Нечаев, А. Н. Оперативно-информационная подготовка: комплекс программ решения статистических задач по результатам качественных измерений: метод. рекомендации / [А. Н. Нечаев, В. П. Осипов, Н. В. Осипов и др.]; под ред. д-ра физ.-мат. наук, проф. В. Л. Макарова.— К.: КВИРТУ ПВО, 1991.— 116 с.

168. «Аль-Каида» захватила советское оружие со складов в Ливии [Електронний ресурс].— Режим доступу:
http://mignews.com.ua/ru/print-articles/68145.html.

169. В войне против Каддафи применили кибернетическое оружие [Електронний ресурс].— Режим доступу:
http://ru.tsn.ua/svit/v-voyne-protiv-kaddafi-primenili-kiberneticheskoe-oruzhie.html.

170. Щербаков, В. «Цифровая крепость» Пентагона готовится к эффективной обороне [Електронний ресурс] / Владимир Щербаков.— Режим доступу:
http://topwar.ru/1775-prostranstvo-virtualnoe-borba-realnaya.html.

171. США начали тестирование системы защиты от кибератак [Електронний ресурс].— Режим доступу:
http://www.rian.ru/technology/20100928/ 280150370.html.

172. DHS' Cyber Storm III to test Obama's national cyber response plan [Еектронний ресурс].— Режим доступу:
http://www.nextgov.com/nextgov/ng_20090826_9168.php.

173. В США начались учения в сфере государственной кибербезопасности [Електронний ресурс].— Режим доступу:
http://rus.ruvr.ru/2010/09/28/22791049.html.

174. Димлевич, Н. Информационные войны в киберпространстве — Великобритания и Израиль [Електронний ресурс] / Николай Димлевич.— Режим доступу:
http://www.fondsk.ru/news/2010/11/08/informacionnye-vojny-v-kiberprostra nstve-velikobritanija-i-izrail.html, 08.11.2010.

175. Евросоюз проведет масштабные киберучения [Електронний ресурс].— Режим доступу:
http://www.cybersecurity.ru/crypto/105202.html, 12.10.2010;
[Електронний ресурс].— Режим доступу:
http://it.tut.by/news/88048.html, 13.10.2010;
[Електронний ресурс].— Режим доступу:
http://weeknews.net/news/main-news/340-evrosoyuz-provedet-masshtabnye-kiber-ucheniya.html, 14.10.2010.

176. В Евросоюзе прошли первые киберучения [Електронний ресурс].— Режим доступу:
http://www.securitylab.ru/news/399329.php., 7.11.2010.

177. В Европе отрепетировали глобальную кибератаку [Електронний ресурс].— Режим доступу:
http://inforotor.ru/visit/8145146?url, http://vlasti.net/news /108922, 7.11.2010.

178. В ЕС проведен кибернетический стресс-тест [Електронний ресурс].— Режим доступу:
http://www.k2kapital.com/news/405763/, 10.11.2010.

179. Бурячок, В. Л. Політика інформаційної безпеки: підручник / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко; за заг. ред. д-ра техн. наук, проф. В. О. Хорошка.— К.: ПВП «Задруга», 2014.— 222 с.

180. Бурячок В. Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем / В. Л. Бурячок // Захист інформації.— 2011.— № 3(52).— С. 19–27.

181. Ільяшов, О. А. Стратегія оцінювання захищеності спеціальних інформаційно-телекомунікаційних систем за метою реалізації / О. А. Ільяшов, В. Л. Бурячок // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення: VI-й НПС ВІТІ НТУУ «КПІ» МО України, 20.10.2011 р.: тези доповідей.— К.:, 2011.— С. 109–110.

182. Василенко В. С. Оцінювання ризиків безпеці інформації в локальних обчислювальних мережах [Електронний ресурс] / В. С. Василенко, О. С. Бордюк, С. М. Полянський.— Режим доступу:

http://www.rusnauka.com/11_EISN_2010/ Informatica/64068.doc.htm.

183. Информационные войны в киберпространстве — США. Часть I: Политика и геополитика [Електронний ресурс].— Режим доступу:

http://mywebs.su/blog/politic/2619.html

184. CSIC Commission on Cybersecurity for the 44th Presidency, Securing Cyberspace, December 2008, at 11.

185. Иванов, В. Пентагон создает кибервойска. Американское военное ведомство всерьез берется за хакеров всех мастей [Електронний ресурс].— Режим доступу:

http://nvo.ng.ru/forces/2009-12-11/14_kibervoiska.html

186. Димлевич, Н. Информационные войны в киберпространстве — США [Електронний ресурс].— Режим доступу:

http://www.otechestvo.org.ua/main/201011/1520.htm, 15.11.10

187. Lynn III, W. J. Defending a New Domain: The Pentagon's Cyberstrategy / William J. Lynn III // Foreing Affairs. September/ October 2010.

188. Правительство Соединенных Штатов приступило к операции «Кибершторм-3», которая должна выявить способность крупнейших государственных систем выдерживать кибератаки [Електронний ресурс].— Режим доступу:

http://infox.ru/hi-tech/internet/2010/09/29/SSHA_ pristupayut_k_i.phtml

189. Защита от кибератак [Електронний ресурс].— Режим доступу:

http://www.nato.int/cps/ru/SID-CE91277B-6E527592/natolive/news_61562.htm

190. Мир вступил в эпоху сетевых войн и конфликтов [Електронний ресурс].— Режим доступу:

http://www.rodon.org/polit-100408112419

191. Димлевич, Н. Информационные войны в киберпространстве — Великобритания и Израиль [Електронний ресурс].— Режим доступу:

http://www.otechestvo.org.ua/main/201011/1612.htm

192. Голубев, В. А. Проблемы борьбы с кибертерроризмом в современных условиях [Електронний ресурс] / В. А. Голубев.— Режим доступу:

http://www.crime-research.ord/library/e-terrorizm.htm, 11.04.2003

193. Голубев, В. А. Компьютерная преступность: мотивация и субъект [Електронний ресурс] / В. А. Голубев.— Режим доступу:

http://www.crime-research.ru/news/2004.10.21/1547

194. Димлевич, Н. Об использовании информационного оружия в киберпространстве [Електронний ресурс] / Николай Димлевич.— Режим доступу:

http://romachev.ru/

195. Бурячок, В. Л. Стратегія оцінювання рівня захищеності держави від ризику стороннього кібернетичного впливу / [В. Л. Бурячок, О. Г. Корченко, В. О. Хорошко, В. А. Кудінов] // Захист інформації.— 2013.— Т. 15, № 1.— С. 5–14.

ДОДАТОК А
Заходи США та керівництва НАТО щодо захисту власного кібернетичного простору

Сьогодні найбільш досконала система кіберзахисту ***критично важливої інфраструктури*** (передусім інформаційної і/або кібернетичної інфраструктури, ураження або знищення якої може призвести до втрати роботоздатності відповідного простору й поставити під загрозу суспільну та державну безпеку в цілому) функціонує у США. Національну політику країни в цій сфері формує Агентство національної безпеки (АНБ), а найважливіші стратегічні питання розв'язуються, як правило, на рівні Ради національної та внутрішньої безпеки країни. Відповідні рішення подаються як директиви Президента. При цьому **АНБ розглядає кібернетичний захист як забезпечення *конфіденційності*, *цілісності* та *доступності* інформації, що циркулює в інформаційно-телекомунікаційних системах.**

Уперше питанням кіберзахисту приділив увагу Президент США Б. Клінтон. У липні 1996 року він оголосив, зокрема, про формування Президентської комісії із захисту критичних інфраструктур (PCCIP). У заключному звіті, виданому в жовтні 1997 року, комісія повідомила, що сьогодні «...загрози критичним інфраструктурам реальні. ...Через взаємозв'язок і взаємозалежність вони можуть бути уразливі щодо нових форм і способів нападу. ...Навмисна експлуатація цих слабких місць може мати серйозні наслідки для економіки, безпеки і життя...». PCCIP також відзначила, що кіберзагрози змінили обстановку: «...У минулому ми були захищені від нападів ворога на інфраструктури широкими океанами й дружніми сусідами. Сьогодні еволюція кіберзагроз разюче змінила ситуацію. У кіберпросторі національні кордони відсутні. Електрони не зупиниш для того, щоб перевірити паспорт. Потенційно небезпечні кібернапади можуть бути задумані та підготовлені заздалегідь, а для їх втілення у життя знадобиться не більше кількох хвилин або й навіть секунд без можливості ідентифікувати нападника або встановити його місце розташування...». Рекомендації PCCIP призвели до видання Директиви Президента № 63 (PDD-63, червень 1998 року), якою було створено Національний центр захисту інфраструктур (NIPC), Офіс безпеки критичних інфраструктур (CIAO), Національну раду із захисту інфраструктур (NIAC) та приватні Центри розподілу і оцінки інформації (ISACs). Згодом 24 вересня 1999 року для просування по шляху вдосконалення прийомів і методів роботи з доказами комп'ютерних злочинів у США було відкрито Комп'ютерну судову лабораторію Міністерства оборони (*Defense Computer Forensics Laboratory — DCFL*). Її робота була спрямована передусім на обробку комп'ютерних доказів злочинів і шахрайства, а також на проведення контррозвідувальних заходів для всіх організацій, що здійснюють протикримінальні та контррозвідувальні дослідження. При цьому як Виконавче агентство для DCFL було визначено управління спеціальних досліджень ВПС США. Сьогодні до беззаперечних надбань лабораторії можна віднести вдалий захист і подальше розслідування наслідків атак на національ-

ні мережі США, відомих як «Сонячний схід» («*Solar Sunrise*»), «Цифровий демон» («*Digital Demon*») та «Місячний лабіринт» («*Moonlight Maze*»).

У січні 2001 року Рада національної та внутрішньої безпеки США ухвалила Національний план захисту інформаційних систем. А через події, що сталися 11 вересня 2001 року, Сенат США вже 13 вересня того ж року не тільки ухвалив законопроект «*Combating Terrorism Act of 2001*», що дозволив Федеральному бюро розслідувань застосовувати військову систему тотального спостереження *Carnivore* (відому також як *DCS1000*), а й збільшив асигнування на її розвиток.

У 2002 році Пентагон надав одній із найбільших науково-дослідних установ США (університету *Carnegie Mellon*) 35,5 млн дол. на проведення досліджень у сфері боротьби з кібертероризмом. П'ятирічний грант передбачав розвиток ідентифікаційних технологій, покликаних захистити користувачів мережі Інтернет від несанкціонованого доступу до їхніх конфіденційних даних. Протягом 2003–2006 років у США було ухвалено чотири національні стратегії в галузі безпеки (рис. Д.А.1), що фактично визначили розвиток безпекової ситуації у світі на початку XXI сторіччя.

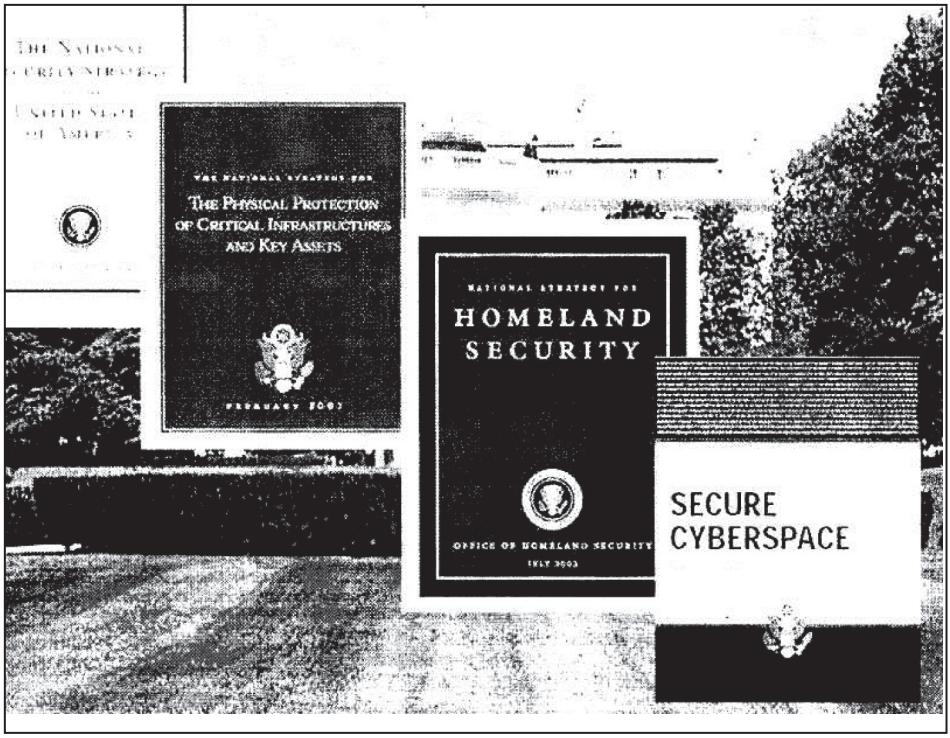


Рис. Д.А.1. Чотири національні стратегії США, ухвалені на початку XXI сторіччя: Стратегія національної безпеки, Національна стратегія з фізичного захисту критичної інфраструктури та об'єктів національного майна, Стратегія внутрішньої безпеки та Національна стратегія захисту кіберпростору

Згідно з цими стратегіями було сформульовано такі головні принципи:

• кіберпростір має бути визнаний таким самим простором війни, як море, суша і повітря;

• кібероборона має вийти за рамки воєнних кібервідділів і поширитись на комерційні мережі відповідно до завдань забезпечення національної безпеки;

• кібероборона має спиратись на співпрацю з міжнародними союзниками для ефективного запобігання загрозам.

Зокрема, у Національній стратегії з фізичного захисту критичної інфраструктури та об'єктів національного майна (2003) визначено цілі та принципи забезпечення національної інфраструктури США, а також передбачено умови об'єднання зусиль різних державних і комерційних структур, спрямованих на підвищення ступеня їх захищеності. Національна стратегія захисту кіберпростору (2003) має на меті гарантувати захист технічних і програмних засобів, об'єднаних у комп'ютерні мережі, а також систем, на які покладено розв'язання завдань управління та інформаційного забезпечення на різних рівнях державних, суспільних і приватних структур, у тому числі в різних сферах національної економіки. Реалізація цієї стратегії має запобігати кібератакам щодо об'єктів критичної інфраструктури, зменшувати їх ефективність, а також максимально скорочувати період ліквідації наслідків нападів на комп'ютерні мережі. Національна військова стратегія з проведення кібернетичних операцій (2006) визначає основні напрямки та сфери дій кіберспільноти США в кіберпросторі. Для посилення захисту комп'ютерних мереж від кібернетичних нападів у 2004 році при Департаменті внутрішньої безпеки (*Department of Homeland Security*), відповідальному за забезпечення безпеки і надійності національних IT технологій та комунікаційної інфраструктури, було сформовано Відділ національної кібернетичної безпеки (*National Cyber Security Division — NCSD*). Ця структура відразу з моменту [183] її відкриття в тісній співпраці з урядом, промисловістю, науковими установами та міжнародними організаціями розпочала перетворення кібернетичної безпеки на справді національний пріоритет, із розробкою основних принципів її створення, що включають у себе:

1) подальший розвиток кіберпростору, із неодмінним удосконаленням широкосмугових мереж;

2) чіткий розподіл відповідальності за кібербезпеку, налагодження якомога тіснішої взаємодії в цьому питанні між федеральними відомствами, місцевою владою та приватним бізнесом;

3) заохочення та належне фінансування інноваційних розробок, таких як створювані на базі Міністерства внутрішньої безпеки програмні продукти *Einstein-2* і *Einstein-3*, призначені для ідентифікації, реєстрації, блокування та знищення шкідливих кодів у точках мережного доступу;

4) координацію та ефективний розподіл потоків інформації.

Наприклад, у рамках проекту *Einstein-2* зазначене міністерство впроваджує сигнатурні сенсори, здатні в режимі реального часу контролювати вхідний інтернет-трафік американського уряду на предмет виявлення спроб несанкціонованого доступу до нього, здійснюючи пошук зловмисного контенту. Проект *Einstein-3* фактично являє собою систему динамічної оборони, що запобігає вторгненню й знижує уразливість відомчого кіберпростору. Його мета — посилити ключові функції захисту відомчих інформаційних систем. Ідеться передусім про ідентифікацію та аналіз зловмисного мережного трафіку, підвищення рівня поінформованості про складну ситуацію та автоматичне реагування на можливі кіберзагрози до настання значущих наслідків. Зазначений проект має підтримувати вдосконалений інформаційний обмін з усіма

федеральними відомствами, уможливлюючи автоматичне оповіщення про виявлені спроби вторгнення в мережі. Варто наголосити, що обмін інформацією про кібератаки відбуватиметься на суто законих підставах, а для запобігання можливим порушенням конфіденційності та прав громадян такий обмін охоплюватиме тільки діяльність, пов'язану із забезпеченням внутрішньої безпеки, розвідкою та обороною.

У січні 2008 року згідно з відповідними директивами директорів Департаментів національної і внутрішньої безпеки США постала надзвичайна ініціатива з питань національної кібернетичної безпеки (*Comprehensive National Cybersecurity Initiative — CNCI*), яка формалізувала серію постійних кроків у напрямку подальшого захисту федеральних урядових систем США від кібернетичних нападів і загроз. На національному рівні зазначена ініціатива зосереджувалась на питаннях:

• установлення лінії захисту для зменшення наявних уразливостей та запобігання можливим вторгненням і нападам;

• захисту від усього спектра загроз із використанням розвідки та посилення безпеки системи постачання;

• формування майбутнього інформаційного середовища через постійне удосконалення наукових досліджень і розробок, системи освіти та інвестицій у передові технології.

Не втратила активності політика США у сфері кібербезпеки й за Адміністрації Б. Обами. Наприкінці травня 2009 року президент США оголосив свій намір розглядати безпеку кіберпростору як одну з пріоритетних проблем його Адміністрації. До особливо ефективних її кроків у цьому напрямку слід віднести такі заходи.

1. Збільшення державного замовлення на розробку нових засобів ведення війни та нових, більш захищених військових мереж.

2. Оприлюднення у травні 2009 року Огляду політики кібербезпеки (*Cyberspace Policy Review*) — комплексного документа, що визначив основні пріоритети нової команди у сфері кібербезпеки, окресливши контури майбутньої Стратегії національної безпеки США в цьому напрямку [184]. У проекті стратегії кіберзагрозам вперше було відведено окреме місце в загальній структурі загроз Сполученим Штатам і визначено основні принципи побудови комплексної системи кібербезпеки держави на базі створення умов для подальшого розвитку кіберпростору; розподіл відповідальності за кібербезпеку; створення ефективної скоординованої системи розподілу інформації та реагування на інциденти; упровадження інноваційних розробок; удосконалення підготовки фахівців із кібербезпеки тощо. На підставі спеціального Огляду політики кібербезпеки, що його підготував апарат Білого дому спільно з комісією з питань кібербезпеки Центру стратегічних і міжнародних досліджень, Президент США ухвалив рішення про створення в Білому домі Відділу з кібербезпеки, а також про формування в Міністерстві оборони США спеціального військового підрозділу — кіберкомандування, головними завданнями якого мали стати захист від інтернет-атак, а також їх організація.

3. Створення у травні 2009 року штабу з питань національної безпеки (*National Security Staff*) та призначення координатора з питань кібербезпеки (*Cyberspace Coordinator*), який одночасно є членом Ради з національної безпеки та Ради з національної економіки.

4. Створення наказом міністра оборони США від 23.06.2009 року у складі збройних сил США Об'єднаного кіберкомандування США (*U.S. Cyber Command-USCYBERCOM*) [184–186].

Примітка. У структурі Стратегічного командування США (USSTRATCOM) Об'єднане кіберкомандування підпорядковується директору АНБ генералу К. Александеру й має власну штабквартиру у Форт-Міді, штат Меріленд. Приблизна чисельність структури — 30 000 військових. Її основне призначення — захист військової частини кіберпростору, тобто домена .mil, та одночасна підтримка доменів «.gov» та «.com». Повномасштабне функціонування нового підрозділу розпочалося в жовтні 2010 року.

У безпосередньому підпорядкуванні USCYBERCOM перебувають:

а) кіберкомандування військово-морських сил США (*Fleet Cyber Command — FLTCYBERCOM*), створене на базі Військово-морської розвідки та Управління з питань зв'язку і комп'ютерних мереж, якому було передано командування мережних операцій ВМС США (*Naval Network Warfare Command — NAVNETWARCOM*), інформаційних операцій ВМС США (*NAVY Information Operations Commands*) та операцій у сфері кібероборони (*NAVY Cyberdefense Operations Command*). На *FLTCYBERCOM* покладено здійснення мережних та інформаційних операцій, радіотехнічної розвідки (*SIGINT*), радіоелектронної боротьби (*Electronic Warfare*), а також забезпечення роботоздатності сегмента комп'ютерної мережі МО США *Global Information Grid* (*GIG*), що належить до сфери відповідальності воєнно-морського відомства. Крім того, до *FLTCYBERCOM* увійшов криптологічний орган ВМС США *NAVY's Service Crypto logic Commander*;

б) оперативно-тактична група сухопутних військ *Army Cyberspace Task Force* (*ACTF*), створена у складі Управління з питань операцій, боєздатності й мобілізації (*Directorate of Operations, Readiness and Mobilization — DORM*). На *ACTF* покладено завдання з об'єднання зусиль штабу СВ щодо управління інформаційними системами, розробки політики здійснення операцій у кіберпросторі, а також затвердження вимог і надання ресурсів для створення перспективних тактичних і стратегічних засобів ведення бойових дій у кіберпросторі;

в) космічний і кібернетичний підрозділи 24-ї повітряної армії збройних сил США. На них покладається відповідальність за проведення бойових кібероперацій в інтересах ВПС США, об'єднаних угруповань військ на полі бою, забезпечення глобальної мережної інфраструктури ВПС США, здійснення атак на автоматизовані інформаційні системи противника, експертиза захищеності електронних систем ВПС тощо.

5. Створення у складі президентської адміністрації Центру кібернетичної безпеки, посади радника президента США з питань кібербезпеки, якого включено до складу Ради національної та внутрішньої безпеки країни, а також розробка проектів нормативних документів, спрямованих на посилення взаємодії у сфері кібербезпеки союзників США та захист власного інтернет-простору в разі виникнення ситуацій, що загрожують національній безпеці. Наприклад, для законодавчого забезпечення зазначеної діяльності Конгрес США розробив новий законопроект «Кібернетична безпека 2009», який установлював стандарти кібернетичної безпеки та визначав завдання і обов'язки урядових і приватних організацій, що мають здійснювати контроль за функціонуванням об'єктів критично важливої інфраструктури.

6. Оголошення про додаткові заходи з посилення внутрішньої кібербезпеки. Так, із 1 жовтня 2009 року адміністрація Б. Обами дала старт програмі з укомплектування Департаменту національної безпеки новими співробітниками, які мають опікуватися забезпеченням безпеки високотехнологічних систем у США. За офіційним даними, протягом наступних трьох років до складу кібервійськ при спеціальному кібербезпековому Департаменті управління національної безпеки (*Department of Homeland Security*) було включено близько 1000 чоловік — професійних програмістів, IT аналітиків та інженерів, із досвідом розслідування зламів і відстеження хакерських атак. Утім потреба в таких фахівцях неухильно зростає, і це чітко усвідомлює адміністрація Б. Обами. Скажімо, у супровідному документі до програми спеціально орга-

нізованих урядом заходів «Кіберзмагання США» (*U.S. Cyber Challenge*) наводиться думка одного з експертів, що реальна потреба країни у фахівцях із кібербезпеки сягає від 10 000 до 30 000.

7. Завершення в жовтні 2009 року здійснюваного згідно із затвердженою концепцією *Air Force Mission Statement* формування у структурі 8-ї повітряної армії ВПС США нового командування — *Air Force Cyber Operations Command* (*AFCOC*). Головні цілі підрозділу — забезпечення безпеки військових мереж зв'язку та автоматизованих інформаційних систем підприємств національного військово-промислового комплексу і організацій, що працюють за контрактом з Міноборони США, а також керівництво інформаційними операціями в кіберпросторі.

Примітка. На AFCOC покладено такі головні функції:

• розпізнавання та запобігання кібератакам, спрямованим на військові та цивільні інформаційні мережі, що належать до критично важливих елементів інформаційної інфраструктури США;

• здійснення з метою здобуття переваги над супротивником інформаційних операцій під час бойових дій як у глобальному масштабі, так і в межах конкретного театру воєнних дій (ТВД);

• своєчасне вжиття відповідних заходів і відновлення нормального функціонування власних інформаційних мереж;

• безперервне відстежування ситуації в кіберпросторі та виконання відповідних операцій — як наступальних (постановка завад системам зв'язку комплексами радіоелектронної боротьби; вплив на радіоелектронну апаратуру спрямованими електромагнітними імпульсами; проведення мережних атак), так і оборонних (використання завадостійких систем зв'язку; програмно-апаратних засобів міжмережного захисту; шифрування інформації, що зберігається в базах даних; оснащення автоматизованих інформаційних систем електронікою, стійкою до електромагнітних імпульсів);

• забезпечення цілісності мережної інфраструктури (залучення мереж, що самоорганізуються, та безпроводового передавання даних; проведення перевірок електронних компонентів радіоапаратури; застосування захищених комп'ютерних мереж).

8. Початок реалізації у січні 2010 року управлінням перспективних досліджень Пентагону (ДАРПА) програми «Національний кіберполігон» [183]. Її мета — створити до 2015 року центр із запобігання кібератакам, устаткування та програмне забезпечення якого мають уможливити моделювання масштабних акцій проти американських інформаційних і телекомунікаційних мереж, навчання співробітників щодо дій із їх нейтралізації, а також проектування систем захисту інформаційних ресурсів. До роботи над цим проектом залучено компанію «Локхід-Мартін» та університет Дж. Хопкінса. Водночас в інтересах Міноборони США активізовано діяльність корпорації *SAIC*, яка розробляє методики та програмні засоби ведення наступальних (атакувальних) дій у кіберпросторі, а також корпорації *Boeing*, яка виконує наукові та науково-дослідні роботи зі створення в інтересах ВПС США систем моніторингу, розробляючи, зокрема, дослідний варіант системи, що матиме сервіс-орієнтовану архітектуру та здатність оптимізувати управління кібернетичними ресурсами через автоматизацію оповіщення про загрозу кібератак та вжиття заходів із їх нейтралізації.

9. Створення на авіабазі Лакленд (штат Техас) першого спеціалізованого кібернетичного розвідувального центру, до складу якого ввійшли 68-ма ескадрилья мережних операцій (68-th *Network Warfare Squadron*) та 710-та ланка інформаційних операцій (710-th *Information Operations Flight*). Поряд із цим центром розташовано також 67-ме мережне крило космічного командування ВПС, розвідуправління ВПС, техаський криптологічний центр АНБ,

об'єднане командування інформаційних операцій, групу криптологічної підтримки ВПС тощо.

10. Оприлюднення Стратегії національної безпеки (2010), в якій уперше у загальній структурі загроз США окреме місце відведено саме кіберзагрозам, а також Міжнародної стратегії для кіберпростору (*International Strategy for Cyberspace*) — документів, що відбивають цілісне бачення урядом США перспектив розвитку кіберпростору.

11. Ухвалення нової доктрини кібербезпеки. Про її спрямованість можна судити з опублікованої у вересні 2010 року програмної статті заступника глави Пентагону Вільяма Лінна III із символічною назвою «Захищаючи новий простір». Головна думка статті: відтепер США вважають кіберпростір таким самим потенційним полем бою, як суша, море й повітря [187]. Підтвердженням цього стало публічне оголошення Вільямом Лінном III на конференції *Virus Bulletin* 2010 (Ванкувер, Канада) п'яти принципів, на яких базуватиметься надалі стратегія кібербезпеки США:

1) визнання кіберпростору новою зоною воєнних дій;

2) захист цивільної інфраструктури;

3) застосування заходів колективної оборони;

4) трансформація пасивної оборонної концепції в активну (використання та своєчасне оновлення антивірусних програм; удосконалення засобів захисту; застосовування детекторів вторгнення та програм моніторингу безпеки — усе це дасть змогу відбити близько 80% кібернападів. Для відбиття інших 20% необхідні інструменти, здатні не тільки виявляти, а й блокувати злоякісні коди);

5) розробка нових програмних продуктів безпекового спрямування.

Нині адміністрація президента США працює над створенням, по-перше, незалежних і автономних систем мобільного зв'язку в інших країнах світу, а по-друге, тіньових інтернет-схем — так званого компактного інтернету у валізі, який можна було б легко розгорнути на території іншої країни, швидко налагодити та встановити безпроводовий зв'язок на достатньо великій за площею території.

У питаннях забезпечення загальної безпеки та оборони НАТО керується Стратегічною концепцією, ухваленою на Вашингтонському ювілейному саміті у квітні 1999 року [188; 189]. Головні принципи цієї концепції полягають у забезпеченні:

- стабільності середовища безпеки Євроатлантичного регіону;
- розвитку демократичних інститутів;
- мирного залагодження конфліктів;
- створення трансатлантичного форуму консультацій щодо життєвих спільних інтересів та мобільності в ухваленні рішень;
- спрямування політики безпеки на стримування та оборону;
- партнерства та розвитку відповідних широкомасштабних програм;
- посилення прозорості взаємної довіри і спроможності діяти спільно.

У системі забезпечення кіберзахисту, зокрема й захисту від тероризму, Альянс керується рішеннями відповідної технічної Програми (так званого «Празького пакета»), ухваленої 21–22 листопада 2002 року главами держав і урядів НАТО на зустрічі у верхах у Празі. Цей документ передбачав три етапи практичної діяльності країн-членів. Перший — створення діючого нині Координаційного центру НАТО з реагування на комп'ютерні інциденти (КЦНРКІ)

і забезпечення його тимчасової робочої конфігурації. Другий етап — забезпечення повної готовності КЦНРКІ. Третій етап — проведення низки заходів з інтеграції досвіду, здобутого на першому і другому етапах, та використання новітніх методів кіберзахисту для зміцнення потенціалу НАТО в цій царині. У 2006 році голови урядів і держав під час Ризького саміту (Латвія) на додачу до вже чинних документів дали завдання Раді НАТО впровадити захист інформаційних систем Альянсу від кібератак. Ухваленням Комплексних політичних настанов учасники саміту визнали, що «...тероризм, а також розповсюдження зброї масового знищення будуть, напевне, головними загрозами Альянсу протягом наступних 10–15 років...». У січні 2008 року Рада НАТО ухвалила стратегію кіберзахисту, спрямовану на забезпечення ефективного й результативного протистояння Альянсу щодо кіберагресії. Ця стратегія містить вказівки цивільним і військовим установам НАТО стосовно вироблення взаємоузгодженого підходу до розв'язання проблем, а також рекомендації країнам-членам щодо захисту їхніх національних систем. У квітні того ж року (на Бухарестському саміті НАТО) керівництво Альянсу ухвалило такі концептуальні документи: «Політика Північноатлантичного Союзу в сфері кібернетичного захисту», де передбачено об'єднання національних і колективних зусиль та ресурсів у згаданій сфері, та «Настанова Північноатлантичної Ради щодо співробітництва у сфері кібернетичного захисту з державами-партнерами та міжнародними організаціями». Цей самий саміт ухвалив рішення про створення Керівного відомства з кіберзахисту. Листопадовий саміт Альянсу започаткував розробку Плану дій у сфері кібероборони. Згідно з цим планом у травні 2008 року було підписано документ про формальне заснування Центру координації зусиль із питань кіберзахисту (далі — Центр або інакше К-5) зі штаб-квартирою у м. Таллінн (Естонія). Нині штат співробітників Центру складається з 30 фахівців (як військовослужбовців, так і цивільних осіб) — представників країн-донорів: Естонії, Німеччини, Італії, Латвії, Литви, Словаччини та Іспанії.

Керує цим Центром організаційний комітет учасників, на який покладено такі завдання:

- оцінювання та затвердження програми роботи Центру;
- залучення країн — членів НАТО до боротьби з кібертероризмом;
- організація взаємодії з іншими країнами;
- збір, аналіз та збереження даних про кібератаки;
- інформування про кібератаки та методи захисту від них.

Центр проводить дослідження й тренінги з питань захисту інформації та протидії кібертероризму. У кожній з країн-донорів для забезпечення цих потреб розгорнуто власні центри комп'ютерного реагування.

На один зі спеціалізованих відділів Центру покладено розв'язання правових питань і проблем організації та стандартизації діяльності Центру у сфері боротьби з кібертероризмом. Робота цього відділу має на меті розробку концепції та стратегії кіберзахисту (без права затвердження); проведення аналізу кібероперацій, зокрема наступальних, оборонних та повсякденних; формування аналітичних засад кіберзахисту; поширення інформації; правове регулювання взаємовідносин; розробку словників спеціалізованих термінів. Ще один спеціалізований відділ опікується розв'язанням суто технічних питань. Його діяльність включає в себе моніторинг можливих кібератак; виявлення

кібернападів та пом'якшення їхніх впливів; моделювання можливих ситуацій; проведення тренувань із питань захисту від кібернападів.

Фахівці Центру (із залученням представників інших зацікавлених сторін) виконують:

• розробку на замовлення НАТО концепції кібервійни (концепція розглядає інформаційний простір як «паралельне поле бойових дій» у майбутніх конфліктах — як політичних, так і військових);

• складання словника термінів, що стосуються кібероборони;

• формування доктрини та стратегії кіберзахисту;

• моделювання певних ситуацій із розробкою методик оцінювання відповідних рівнів безпеки і кіберзагроз, а також моделювання можливих відповідей на кібератаки;

• завдання щодо надання юридичної підтримки зазначеної діяльності.

Центр фактично виконує роль модератора (координатора) усіх зазначених дій.

Наступним важливим кроком стало створення у структурі НАТО Управління кібернетичного захисту, що координує правові, політичні та оперативно-технічні заходи окремих країн-членів та Альянсу в цілому у сфері захисту від кібернетичних загроз. Із цією самою метою 22 січня 2009 у м. Обераммергау (Німеччина) відбувся симпозіум на тему: «НАТО і його партнери: обличчями разом до загроз від Мережі». За результатами зазначеного зібрання було скориговано напрямки кіберзахисту. Тоді ж розпочалась розробка відповідної стратегічної концепції Альянсу щодо реагування на ключові виклики. Передусім ішлося про принципові підходи до розв'язання таких нагальних проблем:

1) захист інформаційної складової системи безпеки та оборони країн-членів;

2) урахування інтересів країн-членів у формуванні загальної системи життєдіяльності Альянсу, а також урегулювання двосторонніх відносин країн-членів з країнами не членами НАТО;

3) реагування на зростаючу небезпеку з боку загроз нової генерації, таких як тероризм, передусім із його численними проявами в кіберпросторі, піратство тощо;

4) подальше розширення НАТО з одночасним налагодженням глобального партнерства за межами Євроатлантичного регіону;

5) перспективи відносин між НАТО та Росією, між НАТО та Європейським Союзом;

6) упровадження систем протиракетної оборони;

7) забезпечення енергетичної безпеки;

8) перебіг довгострокових операцій під проводом НАТО, зокрема місії в Афганістані та Іраку.

З огляду на те, що ймовірність «асиметричних атак» із використанням кіберзброї стрімко зростає, до власних дієвих заходів із захисту національного кіберпростору вдаються практично всі країни. У цьому плані на особливу увагу заслуговує позиція **Великобританії**, зумовлювана не в останню чергу громадськістю країни. Із цього приводу чітко висловився директор лондонського Міжнародного інституту стратегічних досліджень Джон Чіпмен [190], наголосивши, що перед світовою спільнотою насамперед постає завдання усвідомити, що являє собою «кібернетичний конфлікт», що вважати «кібернападом»

і як оцінити момент, коли такий конфлікт чи напад відбувається. Адже «... з погляду кібервоєн перед нами взагалі постає інтелектуальний виклик на зразок ...» загрози ядерної війни.

Із метою моніторингу інформаційного простору та своєчасного реагування на кіберзагрози, що стосуються здебільшого виведення з ладу комп'ютерних систем та полювання за цінною інформацією (фішинг), у складі Кабінету міністрів Великобританії створено Центральне управління з кібербезпеки (ЦУКБ) [183; 190]. Управління є основним органом, відповідальним за формування національної стратегії у сфері інформаційної безпеки країни. Поряд із з цим на території країни вступив у дію закон про тероризм, що прирівнює комп'ютерних хакерів до бойовиків Ірландської республіканської армії. Зазначений нормативний акт має посилити боротьбу з різними угрупованнями, які використовують територію Об'єднаного Королівства для своєї діяльності. Відповідно до нього в разі зламу хакерами комп'ютерної системи, що забезпечує національну безпеку країни, а також спроб з їхнього боку вплинути в будь-який спосіб на державні структури або загрожувати суспільству такі особи можуть бути звинувачені в тероризмі з усіма наслідками, що з цього випливають.

У 2010 році до виконання завдань із забезпечення кібернетичної безпеки та захисту британських інформаційних систем і мереж у повноцінному режимі приступив Оперативний центр забезпечення кібербезпеки (*Cyber Security Operations Center*). Його мета — координація зусиль уже існуючих різноманітних центрів із кібербезпеки різних відомств щодо захисту критичної інфраструктури у сфері IT технологій та створення майданчика для співпраці між урядом та приватним сектором із проблем кібербезпеки [190; 191]. Окрім того, у Великобританії в складі Штабу урядового зв'язку ефективно працює Командування урядових комунікацій (*Government Communications Headquarters — GCHQ*), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів. Вони працюють у тісному контакті з ЦУКБ.

У країнах континентальної Європи — Франції, Італії, ФРН та інших — розгортаються аналогічні процеси. До розряду пріоритетних висуваються питання правових і організаційних механізмів регулювання у сфері використання комп'ютерних мереж. Першою міжнародною угодою щодо юридичних і процедурних аспектів розслідування та кримінального переслідування кіберзлочинів стала Конвенція про кіберзлочинність, ухвалена Радою Європи 23 листопада 2001 року [192; 193]. Конвенцією передбачаються скоординовані на національному і міждержавному рівнях дії, спрямовані на запобігання несанкціонованому втручанню в роботу комп'ютерних систем. Наприклад, у **Франції** для забезпечення безпеки урядових інформаційних систем від кібератак було створено Центр інформаційних систем Служби безпеки (*Central Information Systems Security Service*), підпорядкований Генеральному секретаріату з оборони та національної безпеки. Наприкінці 2009 — на початку 2010 року при цьому центрі створено Національну агенцію безпеки інформаційних систем, яка перебуває в безпосередньому підпорядкуванні прем'єр-міністра Франції. Головні завдання агенції такі: узгодження, розробка та реалізація міжвідомчих заходів із забезпечення інформаційної безпеки національних інформаційних систем; виявлення кіберзагроз, їх оцінювання, а також координація заходів протидії. Безпосередню реалізацію заходів щодо

використання ІТ технологій для впливу на інформаційні й телекомунікаційні об'єкти іноземних держав покладено на головне управління безпеки інформаційних систем (ГУ БІС) — міжвідомчу структуру при кабінеті міністрів країни.

Нормативно-правову основу діяльності зазначених структур становить концепція інформаційного протиборства в комп'ютерних мережах (*Lutte Informatique — LI*), розроблена загальновійськовим центром концепцій і доктрин (*Centre Interarmees de Concept, de Doctrines et d'Experimentations — CICDE*) Міністерства оборони Франції у тісній співпраці з Комітетом начальників штабів, Службою військової розвідки, штабами родів військ, Службою із забезпечення безпеки військових об'єктів, Генеральною делегацією з озброєнь, Національною жандармерією та зовнішньою розвідкою. Фахівці CICDE розглядають кіберпростір як реальне фізичне поле, що охоплює соціальну, технічну (інформаційні системи й мережі) та інтелектуальну (процеси обробки інформації) сфери. Виокремлюють дві групи наступальних заходів на базі концепції LI.

1. Заходи розвідувального характеру:

• акції, спрямовані на збір відомостей про ІТС противника;

• проникнення в автоматизовані ІТС противника для добування розвідданих, зокрема щодо його намірів.

2. Заходи деструктивного характеру:

• спотворення, підміна або знищення інформації для зниження ефективності управлінських рішень;

• акції, спрямовані на порушення цілісності, погіршення функціонування або руйнування ІТС противника.

Французькі експерти виокремлюють три етапи проведення операцій у кіберпросторі: підготовчий етап, у ході якого основні зусилля зосереджуються на зборі інформації щодо противника; другий етап — здійснення впливу на противника; третій етап — забезпечення безпеки власного інформаційного простору.

В **Італії** головним координуючим органом із питань інформаційної безпеки країни став Національний центр інформатики у сфері державного управління, створений при Президії ради міністрів Італії. Окрім того, у Генеральному штабі ЗС Італії створено Управління інформації та безпеки, що відповідає за інформаційну безпеку систем і ресурсів збройних сил держави.

У **ФРН** підходи до проблем інформаційних і кібервоєн та захисту власної ІТ інфраструктури від кіберзагроз ті самі, що й у США та Великобританії. Ідеться про ведення наступальних і оборонних операцій для досягнення національних цілей. Певна особливість полягає у створенні для боротьби зі злочинами у сфері високих технологій спеціалізованих поліцейських та військових підрозділів, які проводять моніторинг інформаційних систем, передусім мережі Інтернет для виявлення кіберзлочинів та здійснення оперативно-розшукових заходів. Так, у лютому 2009 року в структурі Бундесверу було створено управління мережних операцій [194]. Це була реакція на масовані атаки, яких зазнавали обчислювальні мережі ЗС Німеччини. Зокрема, з 14 по 16 лютого 2009 року внаслідок таких атак кілька сотень ПЕОМ та сервер головного інформаційного сайту Міноборони було виведено з ладу на певний час.

Діяльність управління має забезпечувати вплив на комп'ютерні мережі супротивника через використання, спотворення, підміну або знищення ін-

формації, що міститься в базах даних комп'ютерів та інформаційних мереж, а також зниження ефективності їхнього функціонування або виведення з ладу. Серед завдань цього підрозділу слід згадати вивчення можливості та наслідків застосування кіберзброї, формування основ ведення кібервоєн, що визначають умови проведення атак на комп'ютерні мережі, а також регламентують права й обов'язки виконавців і осіб, що віддають відповідні розпорядження. Це управління опікується й розробкою методик захисту власних мереж і протидії сторонньому кібернетичному впливу. Окрім цього, у ФРН створено центр забезпечення безпеки інформаційної техніки зі штатом близько 500 співробітників та річним бюджетом понад 50 мільйонів євро, а в рамках реалізації концепції з кіберзахисту в структурі командування Бундесверу сформовано підрозділ інформаційних і комп'ютерних мережних операцій (*Abteilung der Informations und Computernetzwerkoperationen*). Головні завдання цього підрозділу такі: створення нових методів кібератак, проникнення в комп'ютерні мережі інших держав, проведення операцій із деструктивного впливу на мережі та управляючі системи цих держав і блокування їхньої роботи. Штат підрозділу налічує понад 100 експертів у галузі інформаційних технологій, що практикують хакерські методи віддаленого проникнення в комп'ютерні системи стратегічного призначення супротивника з метою несанкціонованого копіювання або знищення інформації, а також виведення з ладу його інформаційних систем і мереж.

Нещодавно уряд ФРН відкрив Національний центр захисту від кібератак, що має боротися з електронним шпигунством і створювати системи забезпечення електронної безпеки. У ФРН функціонує дослідний центр інформаційних технологій міністерства оборони цієї країни. Для ведення інформаційно-психологічних операцій у збройних силах сформовано відповідні батальйони.

В **Ізраїлі** завдання з планування та реалізації заходів щодо порушення функціонування об'єктів інформаційної й телекомунікаційної інфраструктури інших держав покладено на розвідувальне управління та управління зв'язку і комп'ютерних систем Генштабу національних збройних сил. Для захисту національного кіберпростору при Міністерстві фінансів Ізраїля створено спеціальний підрозділ *Tehila*. На нього покладено такі завдання [183; 191]:

- забезпечення захищеного обміну даними через мережу Інтернет між державними відомствами;
- створення безпечних програмно-апаратних платформ для web-сайтів і ресурсів урядових організацій;
- припинення поширення через мережу Інтернет протиправної інформації;
- координація зусиль зацікавлених відомств щодо протидії кібератакам.

Оперативне відбиття нападу на національні комп'ютерні мережі (якщо алгоритм комп'ютерної атаки відомий) у *Tehila* забезпечує чергова група. У разі виявлення нестандартної схеми дій супротивника до роботи береться група експертів, що проводить всебічний аналіз ситуації та виробляє інструкції для чергового персоналу.

На початку 2010 року Тель-Авів ухвалив концепцію, що припускає кібератаки на сервери й електронні адреси, через які потенційні супротивники вдаються до спроб руйнування інформаційного простору, комп'ютерних систем і електронних баз даних Ізраїлю. У зв'язку з цим групу *Tehila* наділено додатковими повноваженнями, що передбачають можливість проведення нею наступальних акцій на закордонні комп'ютерні системи без узгодження їх

із міжнародними організаціями та іноземними державами. Такий підхід до розв'язання проблемних питань пояснюється відсутністю відповідних міжнародних правових механізмів, які обмежують використання програмно-апаратних засобів для ураження інформаційно-телекомунікаційних систем.

Через зростання кількості кібератак із боку ісламських екстремістів у мережі Інтернет у червні 2010 року Тель-Авів ухвалив рішення про створення підрозділу, який має спеціалізуватися на протиборстві кібертероризму та проведенні спеціальних операцій у мережі Інтернет, а також в інформаційних мережах урядових, силових, фінансових та інших структур потенційного супротивника. Цей підрозділ було сформовано у складі спеціального підрозділу радіоелектронної розвідки розвідувального управління Генштабу. Водночас Ізраїль здійснює добір найбільш обдарованих фахівців у галузі IT технологій для армії та цивільних структур. Організовано взаємодію з неурядовою хакерською групою «Гілад тім», створеною в 2009 р., яка має досвід «зламу» урядових сайтів Туреччини, Лівану й ряду ісламських організацій.

Загалом про рівень занепокоєності провідних держав світу у сфері кібербезпеки свідчить їхнє бажання врегулювати на міжнародному рівні можливість визнання кібератаки «актом війни». Так, 30 січня 2010 року під час Всесвітнього економічного форуму в Давосі сенатор США від Республіканської партії С. Коллінз зазначила, що США всерйоз розглядають питання про ставлення до кібератак як до оголошення війни. 12 травня цього ж року помічник заступника міністра оборони США з політичних питань Дж. Міллер взагалі заявив, що США готові завдати військового удару у відповідь на кібератаки на свої комп'ютерні мережі. Така позиція США щодо тлумачення кібератак та потенційних кібервоєн набуває свого продовження і в межах НАТО: група експертів під керівництвом М. Олбрайт у червні 2010 року запропонувала розглядати масштабні кібератаки як такі, що підпадають під п'яту статтю Північноатлантичного договору і вважаються атаками на всіх членів Альянсу. Така позиція НАТО знайшла відображення і в новій Стратегічній концепції НАТО [191], якою передбачено розширення організаційних і військових можливостей НАТО в протидії кібернападам та створення єдиного інформаційного (кібернетичного) простору блоку.

Головний зміст концепції полягає в об'єднанні коаліційних і національних органів управління, військових формувань, засобів розвідки та передавання інформації. При цьому передбачено впровадження у військах єдиних процедур планування та ухвалення рішень. З огляду на організаційну та технічну складність реалізації згаданого проекту очікується, що необхідну інфраструктуру буде створено до 2015 року, а повної оперативної готовності досягнуто в період 2020–2025 років.

Отже, провідні держави світу дедалі більше уваги приділяють розвитку та захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом становить проблему забезпечення кібербезпеки кожної країни.

ДОДАТОК Б
Навчання Cyber Storm та Cyber Europe: мета, хід і результати

Як показує практика, послуги з виявлення та запобігання несанкціонованим проникненням в інформаційні системи (мережі) державних установ, а також із підготовки останніх до захисту від внутрішніх і зовнішніх кібернетичних втручань і загроз стають дедалі більш пріоритетними у сфері кібербезпеки [168], а навчання з цих питань виступають як практично єдина форма перевірки здатності державних установ протистояти кібератакам як національного, так і світового масштабу. Саме тому провідні країни світу приділяють цим питанням найпильнішу увагу. Одним із беззаперечних лідерів у цій сфері визнано Сполучені Штати Америки, де відповідні заходи під кодовою назвою «Cyber Storm» проводяться з 2006 року.

За результатами першої операції Cyber Storm I, що завершилась у лютому 2006 року, керівництво США виявило надзвичайно низький рівень підготовки співробітників, причетних до об'єктів критично важливої інфраструктури, чинити опір сторонньому кібернетичному впливу. Як з'ясувалося, при кібератаках люди здебільшого просто не розуміли, що відбувається, та до кого вони могли б за певних умов звернутись по допомогу. Результати операції Cyber Storm II, проведеної в березні 2008 року, були не набагато кращі. Адже більшість співробітників, відповідальних за об'єкти критично важливої інфраструктури, також не змогли правильно зорієнтуватися в ситуації, аби скористатися наявними засобами для боротьби з кіберзлочинами. Одним із останніх кроків на цьому шляху стало проведення триденних навчань Cyber Storm III, що були організовані міністерством внутрішньої безпеки США. За даними агентства Рейтер та інших ЗМІ [169–171], навчання розпочалися 30 вересня 2010 року. Ішлося про випробування нової системи протистояння кібератакам, яка має захистити інфраструктуру енерго- і водопостачання, а також банки країни. Приводом для проведення навчань стали хакерські напади на інтернет-сайти державних установ і найбільших компаній США, здійснені в День незалежності 4 липня 2009 року. Зазначені напади призвели до збоїв у роботі сайтів Організації Об'єднаних Націй, штаб-квартира якої міститься в Нью-Йорку. Окрім того, зазнали кібервзламів Держдепартамент, Пентагон та інші ключові відомства. У зазначених навчаннях участь узяли тисячі фахівців з 11 американських штатів, 60 приватних компаній та 12 зарубіжних країн. Серед іноземних партнерів США були представники від Австрії, Великобританії, Канади, Франції, Японії, Німеччини, Угорщини, Італії, Голландії, Нової Зеландії, Швеції та Швейцарії. З урядових структур окрім Білого дому, розвідки та правоохоронних органів до навчань залучилися сім американських міністерств: торгівлі, оборони, енергетики, національної безпеки, юстиції, транспорту та фінансів.

Навчання мали на меті підвищити готовність фахівців до кібератак через імітування дій зловмисників, а також дослідити наявні процеси обміну інформацією між федеральними службами, державною владою та приватни-

ми особами. В офіційному повідомленні DHS ішлося про те, що ці навчання мали перевірити на міцність об'єкти критично важливої інфраструктури, з'ясувавши їхню здатність долати втрати в найбільш важливих аспектах сучасного життя. Серед імітованих наслідків нападу — завдання збитків важливим державним і приватним об'єктам, таким як комунікаційні мережі, енергосистеми тощо.

У процесі навчань його учасники, не завдавши реальних збитків телекомунікаційним системам і мережам, зімітували понад півтори тисячі кіберзагроз. Серед них були такі, як масове розсилання спаму з вірусами, атаки через USB-пристрої, цілеспрямовані атаки ботнетів, атаки типу «відмова в обслуговуванні» (DDoS атаки на окремі сервери державних установ), фішингові атаки, міжсайтовий скриптинг, атаки щодо мобільних пристроїв і безпроводових мереж. Робилися також спроби підмінити DNS-сервери й замінити сертифікати, використовувані для автентифікації в державних автоматизованих інформаційних системах.

Зрештою було підтверджено здатність потужних державних установ, а також об'єктів критично важливої інфраструктури чинити належний опір кібератакам національного масштабу.

Так само й країни Європейського Союзу приділяють питанням захисту інформаційного та кіберпростору все більшу увагу. Що ж до перших кібернавчань, то їх було проведено 4 листопада 2010 року під девізом «Cyber Europe-2010». У них взяли участь всі 27 країн — членів ЄС на той час, а також Ісландія, Норвегія та Швейцарія. Навчання відбулися за сприяння Європейського агентства з мережної та інформаційної безпеки — *European Network and Information Security Agency* (*ENISA*), а також Об'єднаного наукового центру Європейської комісії — *Joint Research Centre* (*JRC*), [172–178]. Штаб Cyber Europe-2010, що розташовувався в Афінах (Греція), координував роботу більш ніж 150 експертів — представників 70 громадських організацій з усієї Європи. За словами В. Узуніса, старшого консультанта агентства ENISA, у рамках навчань планувалося активізувати пошук найкращих способів захисту від масштабних вірусних інфекцій та атак ботнетів і при цьому «...виробити єдиний підхід до захисту, створити єдиний кіберпростір і налагодити контакти між країнами — учасницями проекту...». На його думку, «...такі заходи вкрай важливі для відпрацьовування реальних відповідних дій на загрози, які можуть відбутися...». В. Узуніс також наголосив, що зазначені заходи особливо актуальні в умовах, коли кожна з країн ЄС має свій власний механізм забезпечення IT безпеки, який здебільшого не передбачає, на жаль, взаємодії навіть із найближчими сусідами. У ході навчань моделювалась глобальна DDoS атака на критично важливі елементи системи управління, результатом якої в реальних умовах стало б поступове порушення зв'язку між різними країнами Євросоюзу (за час навчань було проведено близько 320 аналогічних симуляцій). До речі, атаки точно такого типу навесні 2007 року зазнала Естонія.

За повідомленням прес-служби Єврокомісії, головне завдання держав — учасниць ЄС полягало в тому, аби перевірити свої можливості щодо спільного функціонування в умовах «загального відімкнення мережі», а отже, і втрати зв'язку між критичними об'єктами інфраструктури цих країн, коли громадяни, компанії та державні структури позбавлялися доступу до web-сервісів. Представникам відповідальних міністерств і відомств у державах ЄС потрібно було продемонструвати свою здатність шукати й знаходити обхідні шляхи

до відновлення комунікацій. За висновком представників Єврокомісії, якби не дії висококваліфікованих фахівців щодо зміни маршрутів трафіку в обхід ушкоджених з'єднань, доступність основних web-послуг для населення та бізнесу навіть у ході симуляції можливих атак могла б опинитися під загрозою. Згідно з повідомленням BBC News, 10 листопада 2010 року фахівці від ENISA підготували попередній звіт про перебіг і наслідки проведених навчань. У ньому йшлося про те, що хід навчань як у технічній, так і в комунікаційній сфері продемонстрував злагодженість дій учасників у досягненні поставленої мети. Що ж до недоліків, то вони стосувались передусім забезпечення належного рівня підготовки до навчань у загальноєвропейському масштабі (більшість країн — членів ЄС у сфері інформаційної безпеки мають переглянути власну національну політику). Особливий наголос фахівці від ENISA зробили на тому, що Cyber Europe-2010 — це лише перший крок у справі формування стратегії забезпечення комплексної безпеки на території об'єднаної Європи. Зазначені навчання мають надати поштовх до розробки програми широкої кооперації у сфері захисту комп'ютерних мереж країн Європи. Насамперед слід сформувати єдиний підхід до захисту; створити єдиний інформаційний і кібернетичний простір; налагодити міцні контакти між країнами — учасницями проекту.

4 жовтня 2012 року під егідою Єврокомісії за участю фахівців із понад 25 країн ЄС та чотирьох країн спостерігачів відбулися чергові кібернавчання типу «стрес-тест» під назвою Cyber Europe-2012. За інформацією, яку надала прес-служба Європейського агентства з мережної та інформаційної безпеки, під час начань було змодельовано широкомасштабну DDoS атаку на сайти й сервери державних органів влади країн ЄС, інтернет-провайдерів, великих фінансових установ та телекомунікаційних компаній. Сценарій атаки передбачав, що кілька кримінальних угруповань створили близько 1200 окремих інцидентів та розіслали 30 000 спам-листів. Потрібно було з'ясувати, наскільки продуктивно структури, що беруть участь у навчаннях, зможуть взаємодіяти, реагуючи на постійні атаки з боку зловмисників як на власні web-сайти, так і на державні ІС банківської сфери.

Навчання 2012 року мали набагато більший масштаб і межі застосування порівняно з навчаннями 2010 року. Віце-президент Єврокомісії Н. Крус заявила: «Це було вперше, що банки та інтернет-провайдери взяли участь у навчаннях із протидії кібератакам по всій території ЄС... Навчання являє собою предмет співробітництва на європейському рівні для підтримання функціональної інтернет-інфраструктури» Під час навчань використовувалась автономна система, якій були притаманні головні характеристики та продуктивність критично важливих інформаційних (кібернетичних) інфраструктур. Жодну з реальних інфраструктур у дію введено не було.

Згідно з результатами навчань Cyber Europe-2010 та Cyber Europe-2012 напрошується такий висновок: Європі необхідно вжити додаткових заходів, щоб підготуватися до захисту від кібератак майбутнього. Адекватна реакція на такі виклики не забарилася. Європейські інститути вже створили систему комп'ютерного реагування на надзвичайні ситуації (CERT-EU) з метою захисту власних інформаційної та кібернетичної інфраструктури від зловмисних впливів та інцидентів у сфері високих технологій. Зокрема, Єврокомісія розробила Стратегію інформаційної безпеки, що включає в себе законодавчі ініціативи, спрямовані на підвищення мережної та інформаційної безпеки на всій території ЄС.

ДОДАТОК В
Організація маловитратної timing атаки

Термін «маловитратна атака» означає, що для успіху нападникові достатньо мати змогу спостерігати лише за частиною мережі, наприклад бути одним із Tor-вузлів.

Основна ідея — раціонально використовувати неминуче, здавалося б, обмеження всіх анонімізувальних систем із малими затримками. Оскільки системи з малими затримками не можуть дозволити собі вносити в потік будь-які затримки, то часові характеристики (*timing* патерн) пакетів зберігаються вдовж усього ланцюжка. Атака матиме місце через те, що розроблювачі Tor (від англ. *The Onion Router* — вільне програмне забезпечення для реалізації другого покоління так званої цибульної маршрутизації. Дозволяє встановлювати анонімне мережне з'єднання, захищене від прослуховування) вважали неймовірною появу в мережі глобального пасивного спостерігача. Така ситуація не розглядалася й не входила в модель загроз.

Мета атаки — визначити, які саме вузли використовуються тепер для організації Tor-ланцюжків. У разі успіху це сильно зашкодить анонімізувальній здатності Tor. Адже нападник не бачить усіх зв'язків у мережі. Утім ніщо не завадить йому виступити в ролі одного з вузлів Tor і виміряти затримки між собою та рештою вузлів. Знаючи ці затримки, можна опосередковано оцінити обсяг трафіку, який передає кожний вузол у кожний момент часу. Далі, знаючи розподіл обсягу трафіку в часі для всіх вузлів мережі, можна з використанням техніки Danezis 2004 будувати достатньо точні прогнози про те, які вузли передають трафік з однаковими характеристиками, тобто виявляти анонімізувальні ланцюжки.

Реалізація атаки. Архітектура Tor сприяє атаці. Tor-вузол виділяє кожному з'єднанню окремий буфер, обробка буферів відбувається в режимі *round robin fashion*. Якщо в буфері немає потоку — він ігнорується, починається обробка наступного буфера. Зауважимо, що з міркувань підтримання продуктивності змішування було вилучено. Таким чином, коли встановлюється нове з'єднання, скасовується існуюче або змінюється трафік у поточному з'єднанні, відбуваються зміни навантаження на Tor-вузол. Це позначається на швидкості відповідей іншим вузлам, які вже встановили або тільки збираються встановити з'єднання з даним вузлом. Саме з таких причин змінюється навантаження й на інших Tor-вузлах. Виходить, що зміна трафіку на Tor-вузлі відбивається на навантаженні з'єднаних із ним вузлів. Отже, вузли в одному ланцюжку будуть мати схожі картини розподілу навантаження в часі. Зауважимо, що зміна трафіку можлива не тільки з описаних причин, а й з тих чи інших внутрішніх причин Tor-вузла. Наприклад, коли йдеться про навантаження на CPU, такі затримки не враховуються й можуть знизити ефективність атаки. Для успішної атаки особі, яка нападає, достатньо бути одним із клієнтів мережі Tor. Такий вузол називається *шкідливим* (*corrupt node*), або *зондом* (*probe node*). Модель атаки зображено на рис. Д.В.1.

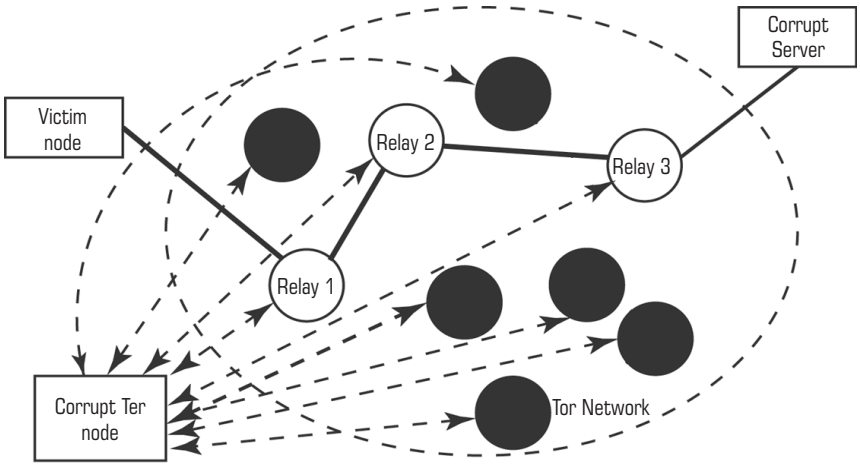


Рис. Д.В.1. Модель маловитратної timing-атаки на Tor:

● — Other Tor nodes; ——— — Victim Circuit; ◯ — Tor relay; ◂- - - - - -▸ — Latency monitoring connection

Головні етапи атаки (рис. Д.В.2). Шкідливий Tor-вузол установлює з'єднання з іншими Tor-вузлами для вимірювання затримок цих зв'язків. Протягом деякого часу він спостерігає за затримками в усіх цих з'єднаннях. Результати вимірювання затримок використовуються для оцінювання обсягів трафіку, переданих кожним Tor-вузлом (навантажень на Tor-вузли), з якими шкідливий вузол має з'єднання. На основі знання обсягів трафіків виводяться патерни останніх. Коли нападник знає патерни трафіків усіх вузлів, він може здійснити атаку (Danezis 2004, Levine et al. 2004). Атака буде ще ефективніша, якщо нападник контролює сервер, до якого під'єднується користувач Tor. Адже в цьому разі немає потреби виявляти патерн трафіку — нападник сам може видозмінювати трафік так, аби його легко було виявити.

At a corrupt node	**At a corrupt server**
Preparation	
Find a list of all other nodes ($\{1, 2, ..., N\}$)	Prepare target stream ($S(t)$)
Action	
1. for $i = 1$ to N make connection to each $node_i$;	
2. for $i = 1$ to N	
2.1 while t record latency of each $node_i$ ($L(i)$);	send $S(t)$
2.2 derive $\rightarrow T(i)$ traffic load of $node_i$	
2.3 compare $T(i)$ with the server traffic $S(t)$	
2.4 if $T(i) \approx S(t)$ then $node_i$ is a relay in the path.	
3. Obtain a path, for example, $node_1 \rightarrow node_3 \rightarrow node_6$	

Рис. Д.В.2. Алгоритм маловитратної атаки

Мета атаки: відстежити шлях між клієнтським вузлом жертви та захопленим сервером. Це знизить анонімізувальну здатність системи до рівня звичайної proxy. Зрештою автори доходять висновку про те, що атака буде ефективна для всіх анонімізувальних систем із малими затримками, включаючи Tarzan і MorphMix.

ДОДАТОК Г
Віруси в соціальних мережах

Якщо при вході на сайти, такі як, скажімо, «Одноклассники» (рис. Д.Г.1) або «ВКонтакте» (рис. Д.Г.2), ви отримали пропозицію відправити sms-повідомлення з кодом підтвердження про валідацію акаунту — це означає, що у вашому комп'ютері оселився вірус. Слід пам'ятати, що в разі справжньої валідації жодних sms-повідомлень користувачеві відправляти не доводиться.

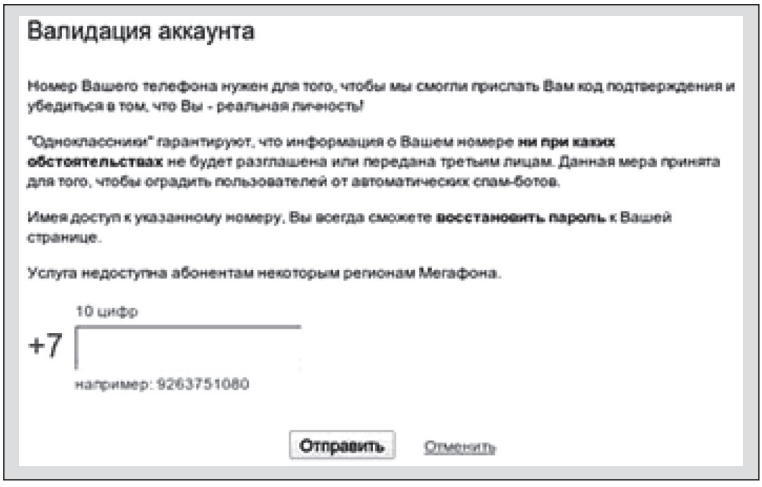


Рис. Д.Г.1. Валідація акаунту «Одноклассники»

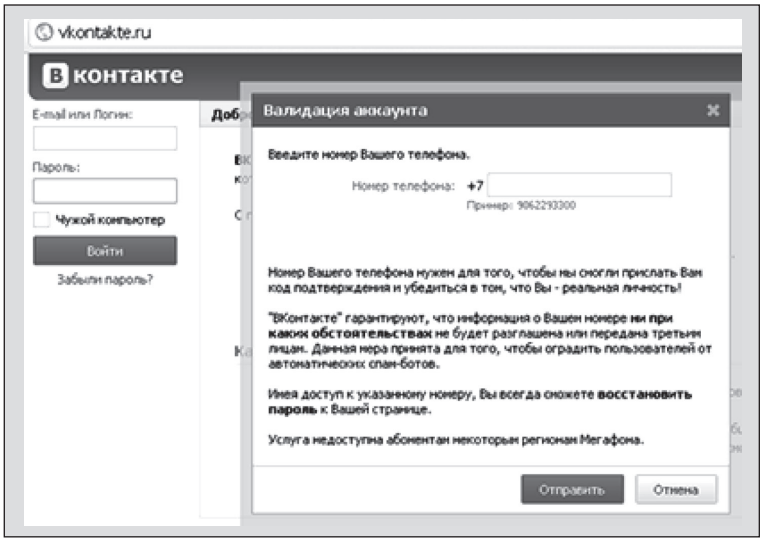


Рис. Д.Г.2. Валідація акаунту «ВКонтакте»

Яким же чином можна позбавитися такого шкідника?

Для цього необхідно вилучити шкідливий додаток і виправити підмінений файл hosts. За замовчуванням файл має лише один незакоментований рядок такого виду:

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
# 102.54.94.97 rhino.acme.com # source server
# 38.25.63.10 x.acme.com # x client host
127.0.0.1 localhost
```

Вірус прописує в ньому перенапрямлення на свій сайт-клон. Виходить, що в адресному рядку ви бачите адресу потрібного вам сайту. Проте насправді відкрито зовсім інший ресурс, тоді як зовні досягається повна схожість з оригіналом.

Розглянемо три способи розв'язання цієї проблеми.

Спосіб 1. Використання безплатної програми CureIt! Вона здатна виявляти зміни у файлі hosts і не тільки знешкоджувати сам вірус, а й усувати заподіяну вірусом шкоду.

Спосіб 2. Дії вручну. Спочатку необхідно скачати Process Explorer і запустити його. У списку процесів знайти файл lsass.exe і визначити до нього шлях доступу (рис. Д.Г.3). Якщо файл lsass.exe перебуває НЕ в папці WindowsSystem32, то необхідно запам'ятати зазначений шлях, виділити процес лівою кнопкою миші й натиснути червоний хрестик угорі (ще можна виділити процес правою кнопкою миші й вибрати з випадного меню пункт «Kill process»). Тим самим процес роботи вірусу буде вилучено з пам'яті. Далі необхідно зайти в папку, шлях до якої ви запам'ятали, і видалити файл із жорсткого диска.

Після цього необхідно замінити файл hosts, що міститься в папці C:WindowsSystem32Drivers, зазначеним файлом. Для цього в 64-розрядній системі Windows файл варто скопіювати за такою адресою: C:WindowsSysWOW64DriversEtc. Після виправлення файла необхідно запустити командний рядок: Пуск, Виконати, уводимо: cmd, тиснемо «Ok». Далі в чорному віконці варто по черзі ввести такі команди:

1) route -f

2) ipconfig /flushdns (кожну команду підтверджуємо клавішею «Enter»).

Для завершення роботи комп'ютер необхідно перезавантажити.

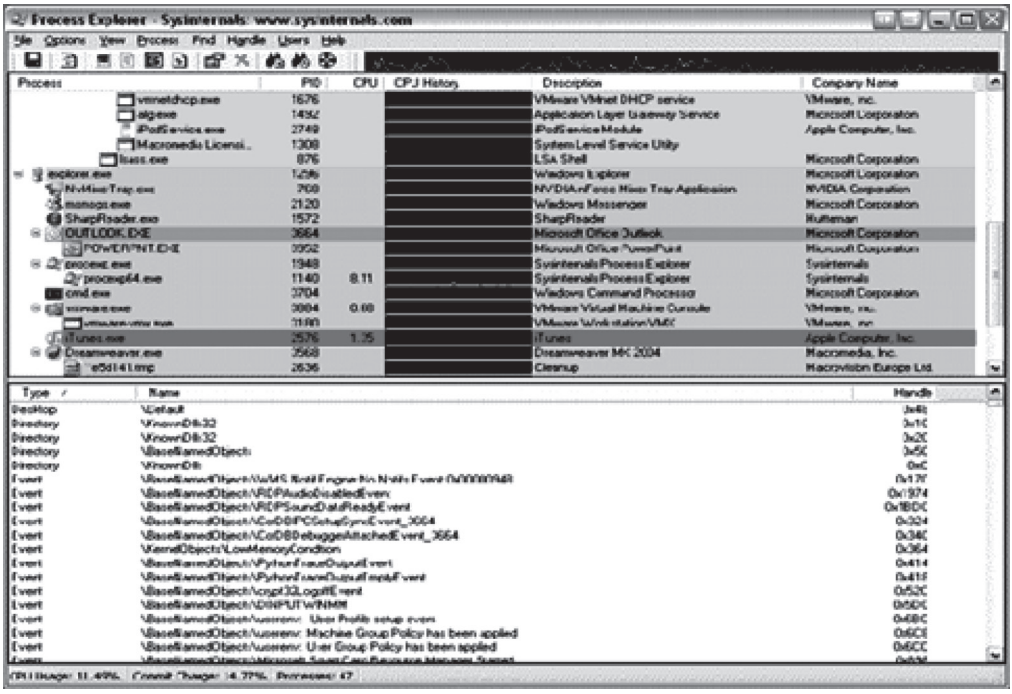


Рис. Д.Г.3. Визначення шляху доступу до файла lsass.exe

Спосіб 3. Деякі антивіруси можуть знешкодити тіло вірусу, але не здатні виправити файл hosts, як це робить утиліта CureIt!, або очистити маршрути й кеш, як це здійснюється командами в другому способі.

У цьому разі достатньо тільки виконати наведені раніше команди й виправити файл hosts, закачавши його за зробленим раніше посиланням, зредагувавши вручну в блокноті або скориставшись спеціальною програмою від Microsoft. Проте якщо в результаті файл і далі буде ушкоджений, це означає, що вірус усе ще не вилучено і вам доводиться скористатися одним із перших двох способів.

ДОДАТОК Д

Тест на проникнення та рекомендації стосовно розробки і впровадження політики безпеки організації (установи) (І. Вінклер, National computer security association)

Експеримент провели з дозволу компанії. Про його хід було проінформовано тільки керівництво вищого рівня.

Першим кроком експерименту стало використання атакувальниками методів соціального інжинірингу (СІ), за допомогою яких без особливих труднощів і пояснень вони виконали відповідний пошук в мережі Інтернет та сформували для себе уявлення про досліджувану організацію. Вивчення баз даних організації дозволило встановити імена багатьох її співробітників та її керівництва. Пошук у телефонному довіднику дав телефонний номер офісу компанії, розташованого поблизу від атакувальників. Дзвінок в офіс дав змогу отримати копію щорічного звіту компанії, а також безплатний телефонний номер компанії. Об'єднавши дані щорічного звіту з даними, узятими з мережі Інтернет, атакувальники мали вже відомості про імена й посади багатьох осіб із керівництва разом з інформацією про проекти, над якими вони працюють.

Наступним кроком було отримання телефонного довідника компанії. Це дозволило встановити імена ще низки співробітників і дістати повне уявлення про організаційну структуру компанії. За безплатним телефонним номером було здійснено дзвінок на основний номер компанії для контакту зі службою розсилання. Той, хто телефонував цього разу, представився як новий співробітник і намагався довідатися, яку інформацію потрібно вказати для пересилання поштою в межах США та за кордон. Отримана відповідь показала, що для цього достатньо лише знати, по-перше, особистий номер співробітника, а по-друге, номер торговельного центру. Дзвінок у відділ графіки підтвердив важливість цих двох чисел. Використовуючи телефонний довідник, атакувальники почали дзвонити десяткам службовців у різних відділах, аби отримати їхні особисті номери, які можна було б використати для подальших атак. Номери отримували в такий спосіб: той, хто телефонував, видавав себе за співробітника відділу кадрів, який помилково подзвонив не тому співробітникові, і при цьому запитував потрібний йому номер. Потім атакувальники вирішили спробувати дізнатися імена нових співробітників, розраховуючи на їхню недостатню обізнаність із можливими загрозами для компанії.

Таким чином, із використанням інформації, роздобутої на першому кроці атаки, зловмисники встановили імена кількох керівників компанії. Телефонний довідник допоміг з'ясувати ім'я тієї особи, яка швидше за все і є керівником. Що ж до встановлення імен нових службовців, то з цією метою було задіяно такий прийом: озвучування від імені керівника побажання особисто познайомитися з новими службовцями компанії. Для цього атакувальники планували спочатку заявити, що вони виконують доручення керівника, а потім, що керівник невдоволений через якість отриманої інформації. Утім суто технічне сприяння супроводжувало їхні дії: на дзвінок у відділ по робо-

ті з новими співробітниками відповів автосекретар. Повідомлення дозволило атакувальникам установити таке: 1) відділ переїхав; 2) ім'я особи, за якою закріплено телефонний номер; 3) новий телефонний номер. Особливу цінність становила інформація про ім'я зазначеної особи, оскільки це дає змогу додзвонювачеві ставити максимально правдоподібні запитання. Зрештою атакувальники мали імена всіх співробітників, що почали працювати протягом поточного тижня, а також назви майже всіх відділів, де вони працюють.

Проте, як з'ясувалося, атакувальникам варто уникати контакту зі співробітниками відділу ІС, які, безперечно, усвідомлюють важливість захисту паролів. Саме тому при дзвінках новим співробітникам зловмисники видавали себе за співробітників відділу ІС і проводили з ними короткий інструктаж з комп'ютерної безпеки. У ході цього інструктажу атакувальник отримав базову інформацію, зокрема про типи використовуваних комп'ютерних систем, наявні додатки, номер співробітника, ідентифікатор користувача й пароль.

Проаналізувавши результати цього експерименту, І. Вінклер запропонував комплекс заходів із розробки й упровадження політики безпеки, які дозволять захиститися від СІ. Наведемо основні з них.

1. *Не покладатися на систему внутрішньої ідентифікації.* Атакованих іноді просять автентифікуватися, указавши свій особистий номер. На радість зловмисників, такий прийом спрацьовує в їхніх інтересах.

З огляду на це компаніям варто мати власні ідентифікатори для робіт, пов'язаних із підтримкою ІС. Наявність такого ідентифікатора дозволить відокремити функції технічного супроводу від інших і гарантуватиме додаткову безпеку як для робіт із супроводу, так і для взаємодії співробітників в організації;

2. *Реалізовувати систему перевірки за допомогою зустрічного дзвінка, коли йдеться про повідомлення захищеної інформації.* Від багатьох атак можна було б захиститися, якби працівники компанії здійснювали перевірку особистості того, хто дзвонить, набираючи його телефонний номер, зазначений у телефонному довіднику компанії.

Ця процедура не дуже зручна в повсякденній роботі, але порівняння з можливими втратами показує повну виправданість таких запобіжних заходів. Якщо співробітників зобов'язати робити зустрічні дзвінки кожному, хто просить повідомити персональну або конфіденційну інформацію, то ризик витоку інформації вдасться мінімізувати. Використання автоматичного визначення номера також може стати у пригоді для досягнення цієї мети.

3. *Реалізовувати програму навчання користувачів у сфері безпеки.* Хоч як це не дивно, але багато комп'ютерних користувачів у наданні свого пароля сторонній особі не вбачають нічого поганого. Компанії витрачають величезні суми, закуповуючи найсучасніше обладнання та програмне забезпечення, тоді як до навчання користувачів належного ставлення немає.

Комп'ютерні професіонали мають усвідомлювати: те, що для них цілком зрозуміле, може бути абсолютно невідоме для багатьох інших. Добра програма навчання користувачів може бути реалізована з мінімальними витратами й зберегти компанії мільйони.

4. *Призначити відповідальних за технічну підтримку*. Кожний співробітник компанії зобов'язаний особисто познайомитися з відповідальним за технічну підтримку й звертатися з усіх питань лише до нього. Як показує практика, на 60 користувачів достатньо одного відповідального.

Користувачі повинні негайно зв'язуватися з аналітиком, якщо до них звертається особа, яка представилась як співробітник служби технічної підтримки.

5. *Створити систему оповіщення про загрози*. Атакувальники знають, що навіть коли їх вдалося виявити, працівники компанії не мають змоги попередити один одного про атаки. Через це атака може тривати (навіть із мінімальними змінами) і після компрометації. Насправді компрометація тільки посприяє атаці, бо атакувальники довідаються, що саме не спрацьовує.

ДОДАТОК Е

Стратегія оцінювання рівня кіберпотужності об'єкта інформаційної діяльності в умовах стороннього кібернетичного впливу та реагування на його прояви

Під забезпеченням інформаційної та кібернетичної безпеки об'єкта інформаційної діяльності (ОІД) розумітимемо виконання низки заходів щодо запобігання впливу на відповідну АС ОІД випадкових чи навмисних втручань у штатні режими її функціонування, а також щодо захисту інформації, яка циркулює в такій АС, від впливу внутрішніх і зовнішніх кібернетичних втручань і загроз.

Нині існує кілька принципових підходів, які сприяють виконанню зазначених заходів. По-перше, слід згадати *фрагментарний*, а по-друге, *комплексний* підхід. Останній поєднує різнорідні заходи протидії загрозам ОІД і традиційно реалізується у вигляді трьох взаємодоповняльних напрямків: *правового, організаційного* та *інженерно-технічного*. Задачі, які доводиться при цьому роз'язувати, належать до класу багатокритеріальних. Для колегіального ухвалення шуканих рішень за невизначеності та конфлікту застосовують різні методи, зокрема методи *математичного моделювання*, методи *формування* та *дослідження узагальнених показників якості* з використанням графоаналітичного та подібного до нього підходів. Утім коли йдеться про розв'язання складних завдань оцінювання та вибору будь-яких об'єктів, у тому числі спеціального призначення, а також аналізу та прогнозування ситуацій із великою кількістю значущих факторів, найвищу ефективність забезпечують ***експертні методи***.

Річ у тім, що експертні методи дають змогу поглиблено вивчати явища, які істотно впливають на рівень захищеності як держави в цілому, так і окремих об'єктів її інформаційної та кібернетичної інфраструктури від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз, виявляти в досліджуваних процесах головне, не відкидаючи тих деталей і взаємозв'язків, без яких не можна побудувати адекватну модель поставленої проблеми. Мета побудови такої моделі — оцінювання готовності об'єктів інформаційної та кібернетичної інфраструктури до безпечного функціонування в умовах стороннього впливу, а також установлення на підставі *індексу кіберпотужності* $G^{\text{рівень}}_{\text{захищ}}$ вимог до власних систем кібербезпеки. Значення цього індексу залежить від того, скільки було виявлено відхилень від штатного режиму функціонування IP, IT систем і мереж, а також програмно-апаратних засобів в результаті аналізу за позиціями таких чотирьох категорій.

1. Чинна нормативно-правова база.

2. Стан соціально-економічного розвитку держави.

3. Наявність розгалуженої технологічної інфраструктури.

4. Ступінь використання ІКТ та ІТС у розвитку інформаційного суспільства.

Кожна з цих категорій включає в себе кілька узагальнених індикаторів.

1.1. Ставлення керівництва держави до питань забезпечення кібербезпеки: чинна національна стратегія (доктрина тощо) із кібербезпеки; нормативно-законодавче забезпечення сфери кібербезпеки; міжнародні зобов'язання країни у сфері кібербезпеки; співробітництво державних і приватних структур у сфері кібербезпеки.

1.2. Стан розвитку політики кіберзахисту: рівень діяльності керівництва держави щодо питань кіберзахисту; рівень діяльності суб'єктів інформаційної і кіберінфраструктури з питань кіберзахисту.

2.1. Рівень освіти, науки і техніки: частка населення з вищою освітою; частка населення, що володіє іноземною, передусім англійською мовою; частка НДР та ДКР із питань кібербезпеки; рівень залучення до виконання НДДКР інженерно-технічного персоналу.

2.2. Рівень розвитку інноваційного середовища: стан витрат на проведення НДДКР; стан патентно-раціоналізаторської роботи (кількість патентів); стан залучення приватного та венчурного капіталу;

3.1. Якісний стан технологічної інфраструктури: рівень використання мережі Інтернет (зокрема поширення Wi-Fi точок доступу); рівень використання засобів мобільного зв'язку та соціальних мереж.

3.2. Рівень упровадження технологічної інфраструктури — рівень фінансування заходів із упровадження ІКТ (у співвідношенні до ВВП); рівень безпеки сервісів.

4.1.Використання ІКТ у корпоративних мережах; інтелектуальних транспортних системах.

4.2. Використання ресурсів мережі Інтернет для розміщення пропозицій щодо надання товарів і послуг; замовлення товарів і послуг.

На основі наведених раніше індикаторів, що характеризують здатність ОІД забезпечувати кібербезпеку та підтримувати безпечне функціонування власних об'єктів інформаційної і кібернетичної інфраструктури, розробимо ієрархічну схему відповідних показників (табл. Д.Е.1), де значення параметрів i-го рівня визначаються значеннями параметрів $(i+1)$-го рівня [195]. При цьому категоріям поставлено у відповідність сукупність специфічних індикаторів, які, у свою чергу, описано елементарними характеристиками, котрі дістали назву показників.

Таблиця Д.Е.1

Ієрархічна схема рівня критичності кібербезпеки

1-й рівень	Рівень критичності кібербезпеки							
2-й рівень (категорії)	Наявність нормативно-правової бази		Стан соціально-економічного розвитку держави		Наявність розгалуженої технологічної інфраструктури		Ступінь використання ІКТ та ІТС	
3-й рівень (індикатори)	Ставлення керівництва держави до питань забезпечення кібербезпеки	Стан розвитку політики кіберзахисту	Рівень освіти, науки та техніки	Рівень розвитку інноваційного середовища	Якісний стан технологічної інфраструктури	Рівень упровадження технологічної інфраструктури	Використання інформаційно-комунікаційних технологій у ЛОМ	Використання ресурсів мережі Інтернет у комерційній діяльності
4-й рівень (показники)	$A1_1$, $A1_2$, $A1_3$, $A1_4$	$A2_1$, $A2_2$	$B1_1$, 1_2, $B1_3$, $B1_4$	$B2_1$, $B2_2$, $B2_3$	$C1_1$, $C1_2$	$C2_1$, $C2_2$	$D1_1$, $D1_2$	$D2_1$, $D2_2$

Кожній категорії 2-го рівня, кожному індикатору 3-го рівня та кожному показнику 4-го рівня ієрархії за певним правилом, наприклад за допомогою експертного опитування [195], можна поставити у відповідність деяке число (табл. Д.Е.2, Д.Е.3). Обов'язкова умова при цьому така: сума ваг категорій, індикаторів і показників одного й того самого рівня завжди має дорівнювати одиниці.

Таблиця Д.Е.2

Значення вагових коефіцієнтів категорій та індикаторів рівня критичності кібербезпеки

Позначення категорій та індикаторів рівня критичності	Позначення вагових коефіцієнтів категорій та індикаторів	Значення вагових коефіцієнтів категорій та індикаторів	Сума вагових коефіцієнтів індикаторів
<НАЯВНІСТЬ НОРМАТИВНО-ПРАВОВОЇ БАЗИ>	$g1$	0,26	
<Ставлення керівництва держави до питань забезпечення кібербезпеки>	$a1$	0,75	1,0
<Стан розвитку політики кіберзахисту>	$a2$	0,25	
<СТАН СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ ДЕРЖАВИ>	$g2$	0,25	
<Рівень освіти, науки та техніки>	$b1$	0,68	1,0
<Рівень розвитку інноваційного середовища>	$b2$	0,32	
<НАЯВНІСТЬ РОЗГАЛУЖЕНОЇ ТЕХНОЛОГІЧНОЇ ІНФРАСТРУКТУРИ>	$g3$	0,26	
<Якісний стан технологічної інфраструктури>	$c1$	0,22	1,0
<Рівень упровадження технологічної інфраструктури>	$c2$	0,78	
<СТУПІНЬ ВИКОРИСТАННЯ ІКТ ТА ІТС>	$g4$	0,23	
<Використання інформаційно-комунікаційних технологій>	$d1$	0,71	1,0
<Використання ресурсів мережі Інтернет>	$d2$	0,29	

Значення категорій та індикаторів якості визначаються згідно з табл. Д.Е.3 [195].

За формулами (Д.Е.2), (Д.Е.3), (Д.Е.5), (Д.Е.6), (Д.Е.8), (Д.Е.9), (Д.Е.11) і (Д.Е.12), наведеними в табл. Д.Е.3, із використанням даних анкети експерта (табл. Д.Е.4), яка регламентує значення показників та їхніх вагових коефіцієнтів, обчислюються значення індикаторів 3-го рівня:

- <ставлення керівництва держави до питань забезпечення кібербезпеки>;
- <стан розвитку політики кіберзахисту>;
- <рівень освіти, науки та техніки>;
- <рівень розвитку інноваційного середовища>;
- <якісний стан технологічної інфраструктури>;
- <рівень фінансування технологічної інфраструктури>;
- <використання інформаційно-комунікаційних технологій>;
- <використання ресурсів мережі Інтернет>.

Таблиця Д.Е.3

Процедури визначення категорій
та індикаторів рівня критичності кібербезпеки

<НАЯВН. НОРМАТ.-ПРАВ. БАЗИ> = $a1$ <*ставлення керівництва до кібербезпеки*> + $a2$ <*стан розвитку політики кіберзахисту*> де $a1$, $a2$ — вагові коефіцієнти відповідних індикаторів 3-го рівня; $a1 + a2 = 1$	(Д.Е.1)
<*Ставлення керівництва до кібербезпеки*> $= a1_1 \cdot A1_1 + a1_2 \cdot A1_2 + a1_3 \cdot A1_3 + a1_4 \cdot A1_4 = \sum_i a1_i \cdot A1_i;\ i = \overline{1,4}$, де $a1_1$, $a1_2$, $a1_3$, $a1_4$ — вагові коефіцієнти показників 4-го рівня для $A1_1$, $A1_2$, $A1_3$ і $A1_4$; $a1_1 + a1_2 + a1_3 + a1_4 = \sum_i a1_i = 1$	(Д.Е.2)
<*Стан розвитку політики кіберзахисту*> $= a2_1 \cdot A2_1 + a2_2 \cdot A2_2 = \sum_i a2_i \cdot A2_i;\ i = \overline{1,2}$, де $a2_1$, $a2_2$ — вагові коефіцієнти відповідних показників 4-го рівня для $A2_1$ і $A2_2$; $a2_1 + a2_2 = \sum_i a2_i = 1$	(Д.Е.3)
<СТАН СОЦІАЛ.-ЕКОН. РОЗВИТКУ> = $b1$ <*рівень освіти, науки, техніки*> + $b2$ <*рівень розвитку інновац. середовища*> де $b1$, $b2$ — вагові коефіцієнти відповідних індикаторів 3-го рівня; $b1 + b2 = 1$	(Д.Е.4)
<*Рівень освіти, науки, техніки*> $= b1_1 \cdot B1_1 + b1_2 \cdot B1_2 + b1_3 \cdot B1_3 + b1_4 \cdot B1_4 = \sum_i b1_i \cdot B1_i;\ i = \overline{1,2}$, де $b1_1$, $b1_2$, $b1_3$, $b1_4$ — вагові коефіцієнти показників 4-го рівня для $B1_1$, $B1_2$, $B1_3$ і $B1_4$; $b1_1 + b1_2 + b1_3 + b1_4 = \sum_i b1_i = 1$	(Д.Е.5)
<*Рівень розвитку інновац. середовища*> $= b2_1 \cdot B2_1 + b2_2 \cdot B2_2 + b2_3 \cdot B2_3 = \sum_i b2_i \cdot B2_i;\ i = \overline{1,3}$, де $b2_1$, $b2_2$, $b2_3$ — вагові коефіцієнти показників 4-го рівня для $B2_1$, $B2_2$, і $B2_3$; $b2_1 + b2_2 + b2_3 = \sum_i b2_i = 1$	(Д.Е.6)
<НАЯВНІ РОЗГЛУЖ. ТЕХНОЛОГ. ІНФРАСТ-РИ> = $c1$ <*якісний стан технолог. інфраст-ри*> + $c2$ <*рівень упровадж. технолог. інфраст-ри*> де $c1$, $c2$ — вагові коефіцієнти відповідних індикаторів 3-го рівня; $c1 + c2 = 1$	(Д.Е.7)
<*Якісний стан технолог. інфраст-ри*> $= c1_1 \cdot C1_1 + c1_2 \cdot C1_2 = \sum_i c1_i \cdot C1_i;\ i = \overline{1,2}$, де $c1_1$, $c1_2$ — вагові коефіцієнти відповідних показників 4-го рівня для $C1_1$ і $C1_2$; $c1_1 + c1_2 = \sum_i c1_i = 1$	(Д.Е.8)
<*Рівень упровадж. технолог. інфраст-ри*> $= c2_1 \cdot C2_1 + c2_2 \cdot C2_2 = \sum_i c2_i \cdot C2_i;\ i = \overline{1,2}$, де $c2_1$, $c2_2$ — вагові коефіцієнти відповідних показників 4-го рівня для $C2_1$ і $C2_2$; $c2_1 + c2_2 = \sum_i c2_i = 1$	(Д.Е.9)
<СТУПІНЬ ВИКОРИСТ. ІКТ ТА ІТС> = $d1$ <*використання ІКТ*> + $d2$ <*використання мережі Інтернет*> де $d1$, $d2$ — вагові коефіцієнти відповідних індекаторів 3-го рівня; $d1 + d2 = 1$	(Д.Е.10)

$<$*Використання ІКТ*$> = d1_1 \cdot D1_1 + d1_2 \cdot D1_2 = \sum_i d1_i \cdot D1_i;\ i = \overline{1,2}$, де $d1_1$, $d1_2$ — вагові коефіцієнти відповідних показників 4-го рівня для $D1_1$ і $D1_2$; $d1_1 + d1_2 = \sum_i d1_i = 1$	(Д.Е.11)
$<$*Використання мережі Інтернет*$> = d2_1 \cdot D2_1 + d2_2 \cdot D2_2 = \sum_i d2_i \cdot D2_i;\ i = \overline{1,2}$, де $d2_1$, $d2_2$ — вагові коефіцієнти відповідних показників 4-го рівня для $D2_1$ і $D2_2$; $d2_1 + d2_2 = \sum_i d2_i = 1$	(Д.Е.12)

Примітка. Вираз $< x >$ позначає числове значення показника властивості x.

За формулами (Д.Е.1), (Д.Е.4), (Д.Е.7) і (Д.Е.10) табл. Д.Е.3 із використанням даних табл. Д.Е.4 та попередньо отриманих значень показників 3-го рівня обчислюються значення комплексних показників (категорій) 2-го рівня:

а) $G_1^{\text{факт}}$ — наявність нормативно-правової бази;

б) $G_2^{\text{факт}}$ — стан соціально-економічного розвитку держави;

в) $G_3^{\text{факт}}$ — наявність розгалуженої технологічної інфраструктури;

г) $G_4^{\text{факт}}$ — ступінь використання ІКТ та ІТС.

Індекс кіберпотужності $G^{\text{рівень захищ}}$ з погляду одного експерта можна обчислити за такою формулою [195], %:

$$G^{\text{рівень захищ}} = \left(\sum_{i=1}^{n} \left(g_i \cdot G_i^{\text{факт}} \right) \right) \cdot 100, \qquad \text{(Д.13)}$$

де g_i — вагові коефіцієнти категорій 2-го рівня ієрархії $G_i^{\text{факт}}$;

n — кількість категорій (у даному разі $n = 4$).

Ухвалення рішення щодо здатності держави протистояти кібератакам буде здійснюватися за 100-бальною шкалою на підставі такого правила:

• якщо $90 \le G^{\text{рівень захищ}} \le 100$, то рівень захищеності держави від ризику стороннього кібервпливу вважається достатньо високим для підтримки безпечного функціонування об'єктів її інформаційної та кібернетичної інфраструктури;

• якщо $45 \le G^{\text{рівень захищ}} < 90$, то рівень захищеності держави від ризику стороннього кібервпливу вважається припустимим для підтримки безпечного функціонування об'єктів її інформаційної і кібернетичної інфраструктури;

• якщо $G^{\text{рівень захищ}} < 45$, то рівень захищеності держави від ризику стороннього кібервпливу вважається недостатнім.

Отже, запропонована стратегія дасть змогу отримати кількісну оцінку рівня захищеності ОІД від ризику стороннього кібернетичного впливу, встановити вимоги до формування цими органами власних систем кібернетичної безпеки, а також розробити заходи, спрямовані на підвищення результативності такої роботи. Підставою для таких дій може слугувати виявлення відхилень від штатного режиму функціонування державних ІР, ІТ систем і мереж, а також відповідних програмних і апаратних засобів. Ідеться, наприклад, про виявлення таких ознак:

• виведення з ладу окремих компонентів радіоелектронних систем;

• зміна алгоритмів функціонування ПЗ систем управління в ІТ системах і мережах;

Таблиця Д.Е.4

Анкета експерта для оцінювання рівня критичності кібербезпеки

Позначення показника	Питання, на які має відповісти експерт для визначення значення показника	Відповіді на питання	Значення показника	Ваговий коефіцієнт	
				Позначення	Значення
$A1_1$	Чи існує в державі національна стратегія (доктрина, концепція тощо) з кібербезпеки?	1. Стратегія зрозуміла, чітко визначено цілі та терміни реалізації. 2. Стратегія нечітка, незрозуміла чи суто формальна. 3. Стратегія тільки розробляється. 4. Стратегія відсутня	1,0 0,4 0,2 0	$a1_1$	0,4
$A1_2$	Чи функціонує в державі система нормативно-законодавчого забезпечення сфери кібербезпеки?	1. Законодавство охоплює всі аспекти кібербезпеки. 2. Існують певні закони, але виконуються лише окремі з них. 3. Існують певні закони, проте жодний із них не виконується. 4. Законодавство не сформовано	1,0 0,6 0,2 0	$a1_2$	0,3
$A1_3$	Чи виконуються на державному рівні міжнародні зобов'язання у сфері кібербезпеки?	1. Держава практично виконує міжнародні угоди. 2. Держава ратифікувала підписані міжнародні угоди. 3. Держава приєдналася до міжнародних угод. 4. Держава не має підписаних міжнародних зобов'язань	1,0 0,6 0,2 0	$a1_3$	0,2
$A1_4$	Чи налагоджено співробітництво державних і приватних структур у сфері кібербезпеки?	1. Держава докладає значних зусиль для розвитку державно-приватного співробітництва. 2. Держава докладає певних активних, але не достатньо результативних зусиль для розвитку державно-приватного співробітництва. 3. Державно-приватне співробітництво не налагоджено	1,0 0,5 0	$a1_4$	0,1
$A2_1$	Яку роль відіграє діяльність керівництва держави в питаннях кіберзахисту?	1. У державі створено орган виконавчої влади, відповідальний за кіберзахист, діяльність якого визнано ефективною. 2. У діяльності органу виконавчої влади, відповідального за кіберзахист, є недоліки. 3. Орган виконавчої влади, що має відповідати за кіберзахист, у державі відсутній	1,0 0,5 0	$a2_1$	0,5

Продовження табл. Д.Е.4

Позначення показника	Питання, на які має відповісти експерт для визначення значення показника	Відповіді на питання	Значення показника	Ваговий коефіцієнт	
				Позначення	Значення
$A2_2$	Який рівень діяльності суб'єктів інформаційної інфраструктури щодо питань кіберзахисту?	1. Рівень реагування з боку суб'єктів інформаційної і кібернетичної інфраструктури на прояви стороннього кібервпливу вищий від середнього. 2. Рівень реагування з боку суб'єктів інформаційної і кібернитичної інфраструктури на прояви стороннього кібернетичного впливу періодичний і спонтанний. 3. Суб'єкти інформаційної і кібернитичної інфраструктури питаннями реагування на прояви стороннього кібервпливу не переймаються	1,0 0,5 0	$a2_2$	0,5
$B1_1$	Яка частка* населення в державі має вищу освіту? * Визначається як відсоткове відношення молоді віком від 18 до 22 років, яка здобуває освіту за денною формою навчання, до загальної кількості студентів зазначеного віку в країні	1. Висока. 2. Середня. 3. Низька	1,0 0,5 0	$b1_1$	0,2
$B1_2$	Яка частка* населення в державі володіє іноземною, передусім англійською, мовою? * Визначається на основі інформації державного центру з вивчення англійської мови	1. Висока. 2. Середня. 3. Низька	1,0 0,5 0	$b1_2$	0,2
$B1_3$	Яка частка* НДДКР у державі присвячено дослідженню питань кібербезпеки? *Визначається на основі інформації органу держреєстрації НДДКР	1. Висока. 2. Середня. 3. Низька	1,0 0,5 0	$b1_3$	0,3
$B1_4$	Який рівень* залучення до виконання НДДКР за напрямом кібербезпеки інженерно-технічного персоналу? *Визначається як кількість фахівців, залучених до виконання НДДКР на 1 млн чоловік населення країни	1. Достатній. 2. Середній. 3. Недостатній	1,0 0,5 0	$b1_4$	0,3

Позначення показника	Питання, на які має відповісти експерт для визначення значення показника	Відповіді на питання	Значення показника	Ваговий коефіцієнт	
				Позначення	Значення
$B2_1$	Який стан* витрат у державі на проведення НДДКР у сфері кібербезпеки? * Визначається як відношення поточних і капітальних витрат на проведення НДДКР до рівня ВВП	1. Достатній. 2. Середній. 3. Недостатній	1,0 0,5 0	$b2_1$	0,3
$B2_2$	Який стан* у державі патентно-раціоналізаторської роботи у сфері кібербезпеки? * Визначається як кількість заявок на отримання патентів на 1 млн чоловік населення країни	1. Достатній. 2. Середній. 3. Недостатній	1,0 0,5 0	$b2_2$	0,4
$B2_3$	Який стан* залучення приватного та венчурного капіталу у сферу кібербезпеки? * Визначається у відсотковому відношенні приватного та венчурного капіталу до рівня ВВП країни	1. Достатній. 2. Середній. 3. Недостатній	1,0 0,5 0	$b2_3$	0,3
$C1_1$	Який рівень* використання мережі Інтернет? * Свідчить про кількість Інтернет-користувачів на 100 чоловік та розраховується на основі інформації JiWire (бази даних щодо Wi-Fi – точок доступу у 142 країнах)	1. Високий. 2. Середній. 3. Низький	1,0 0,5 0	$c1_1$	0,5
$C1_2$	Який рівень* використання засобів мобільного зв'язку та соціальних мереж? * Свідчить про кількість користувачів мобільного зв'язку на 100 чоловік та відсоткове відношення кількості користувачів до загальної кількості Інтернет-користувачів	1. Високий. 2. Середній. 3. Низький	1,0 0,5 0	$c1_2$	0,5
$C2_1$	Який рівень* фінансування заходів з упровадження ІКТ? * Визначається у відсотковому відношенні загальних витрат на програмне забезпечення, апаратні засоби та ІТ-послуги до рівня ВВП	1. Достатній. 2. Середній. 3. Недостатній	1,0 0,5 0	$c2_1$	0,5

Позначення показника	Питання, на які має відповісти експерт для визначення значення показника	Відповіді на питання	Значення показника	Ваговий коефіцієнт	
				Позначення	Значення
$C2_2$	Який рівень* безпеки сервісів? * Свідчить про кількість серверів, що використовують технології шифрування даних для безпечного обміну даними	1. Достатній. 2. Середній. 3. Недостатній	1,0 0,5 0	$c2_2$	0,5
$D1_1$	Який рівень використання ІКТ у корпоративних мережах?	1. Широке використання корпоративних мереж на всій території країни. 2. Рівень розвитку корпоративних мереж достатньо високий. 3. Розробляються плани для впровадження корпоративних мереж. 4. Корпоративних мереж у країні не існує	1,0 0,6 0,2 0	$d1_1$	0,5
$D1_2$	Який рівень використання ІКТ в інтелектуальних транспортних системах?	1. Рівень використання ІТС для виконання важливих функцій високий. 2. Рівень використання ІТС для виконання важливих функцій нижчий від середнього. 3. Інтелектуальних транспортних систем не існує	1,0 0,5 0	$d1_2$	0,5
$D2_1$	Яка частка користувачів використовує Інтернет для розміщення пропозицій щодо надання товарів і послуг?	1. Понад 55%. 2. Від 25 до 54%. 3. До 24%	1,0 0,5 0	$d2_1$	0,5
$D2_2$	Яка частка користувачів використовує Інтернет для замовлення товарів і послуг?	1. Понад 80%. 2. Від 40 до 79%. 3. До 39%	1,0 0,5 0	$d2_2$	0,5

• несанкціоновані зміни у файлах (обсяг цих змін та дата останньої модифікації);

• порушення безпеки інформаційного обміну, протоколів передавання даних вхідного або вихідного трафіку, а також прав доступу користувачів до ІР;

• уповільнення завантаження та процесів роботи ПЕОМ;

• зменшення обсягів вільної оперативної пам'яті;

• виконання неконтрольованих процесів тощо.

Окрім того, як відхилення слід розглядати численні завантаженні ОС, неможливість збереження файлів у необхідних каталогах, а також появу незрозумілих системних повідомлень, деяких музичних і візуальних ефектів.

ЗМІСТ

РОЗДІЛ 5
СОЦІОІНЖЕНЕРНІ МЕТОДИ РОЗВ'ЯЗАННЯ ПРОБЛЕМ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ: ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРОНИКНЕННЯ

НАВЧАЛЬНЕ ВИДАННЯ

Володимир Леонідович БУРЯЧОК
Володимир Борисович ТОЛУБКО
Володимир Олексійович ХОРОШКО
Сергій Васильович ТОЛЮПА

ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА:
Соціотехнічний аспект
Підручник

За загальною редакцією
доктора технічних наук,
професора В. Б. ТОЛУБКА

Редакційна обробка
та коректура О. П. Бондаренко, Т. В. Ількевич
Комп'ютерна обробка та верстка О. Ю. Апухтіна,
В. В. Бельський

Підписано до друку _____ 2015 р.
Формат 70 × 100/16. Друк офсетний. Папір офсетний. Гарнітура SchoolBookC.
Умовн. друк. арк. 18. Наклад ____ прим.