В. Л. БУРЯЧОК, В.Б. ТОЛУБКО,
В. О. ХОРОШКО, С.В. ТОЛЮПА

ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА: соціотехнічний аспект

Підручник

Cybersecurity

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

В. Л. БУРЯЧОК, В.Б. ТОЛУБКО,
В. О. ХОРОШКО, С.В. ТОЛЮПА

ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА:
соціотехнічний аспект

Підручник

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

Львів- 2018

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

Гриф надано Міністерством освіти і науки України

Рекомендовано вченою радою Державного університету телекомунікацій до друку та використання в навчальному процесі

Рецензенти:

Щербак Л. М. – доктор технічних наук, професор,
Дудикевич В. Б. – доктор технічних наук, професор,
Самохвалов Ю. Я. – доктор технічних наук, професор,

Бурячок В. Л.
Інформаційна та кібербезпека: соціотехнічний аспект. [Підручник].
Б 91 / В. Л. Бурячок, В.Б. Толубко, В. О. Хорошко, С.В. Толюпа /. – Львів: «Магнолія 2006», 2018 – 320с.

ISBN 978-617-574-126-9

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».

ISBN 978-617-574-126-9

ЗМІСТ

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
ІзОД	–	інформація з обмеженим доступом
ІКТ	–	інформаційно-комунікаційна технологія
ІБ	–	інформаційна безпека
ІТ	–	інформаційна технологія
ІР	–	інформаційний ресурс
ІТС	–	інформаційно-телекомунікаційна система
ІС	–	інформаційна система
КБ	–	кібернетична безпека
КР	–	кібернетична розвідка
КСЗІ	–	комплексна система захисту інформації
ЛОМ	–	локальна обчислювальна мережа
МР	–	мережева розвідка
НСД	–	несанкціонований доступ
ОС	–	операційна система
ПАК	–	програмно-апаратний комплекс
ПЕОМ	–	персональна ЕОМ
ПІБ	–	політика інформаційної безпеки
ПЗ	–	програмне забезпечення
РІ	–	розвідувальна інформація
РІТС	–	рзвідка інформаційно-телекомунікаційних систем
Рст	–	робоча станція
СІ	–	соціальний інжиніринг
СЗІ	–	система захисту інформації
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
КІБЕПРОСТІР, 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

Формування та розвиток сучасного інформаційного суспільства, факт створення якого офіційно було визнано представниками держав "Великої вісімки" в ході Окінавської зустрічі у липні 2000 року, базується, як відомо [1], на синтезі двох технологій – комп'ютерної і телекомунікаційної та визначається двома простими, але дуже змістовними законами. Перший закон, сформульований одним із засновників корпорації Intel Гордоном Муром, говорячи про те, що "… кількість транзисторів у процесорах збільшуватиметься вдвічі кожних півтора роки …", фактично пояснює виникнення нових, специфічних за формою і способами суб'єктів та об'єктів інформаційної інфраструктури, гарантоване зростання швидкості обчислень і об'ємів інформації, що при цьому обробляється, а також формування на рубежі тисячоліть так званого **інформаційного простору** – *глобального інформаційного середовища, яке в реальному масштабі часу забезпечує комплексну обробку відомостей про протиборчі сторони та їх навколишнє оточення в інтересах підтримки прийняття рішень по створенню оптимального, для досягнення поставлених цілей, складу сил і засобів та їх ефективного застосування в різних умовах обстановки*. Другий закон належить Роберту Меткалфу, винахіднику найпоширенішої на сьогодні технології комп'ютерної мережі Internet. Говорячи про те, що "… цінність мережі знаходиться у квадратичній залежності від кількості вузлів, які є її складовими …" він фактично констатує, що основу сучасного інформаційного суспільства становлять мережі різного функціонального призначення, сукупність і взаємозв'язок яких інформаційний простір власне і утворює [1], а також новітні інформаційно-телекомунікаційні (ІТ) технології, які останнім часом:

1) стали важливою складовою суспільного розвитку і розвитку світової економіки у цілому й разом з тим значною мірою змінили механізми функціонування багатьох суспільних інститутів та інститутів державної влади;

2) увійшли до числа найбільш суттєвих факторів, які впливають на формування сучасного високоорганізованого інформаційного середовища та дають можливість на якісно новому рівні інформаційного обслуговування у

віртуальному і реальному просторах вести повсякденну оперативну роботу, здійснювати аналіз стану і перспектив діяльності інформаційно-аналітичних підрозділів, а також добувати вихідні дані, що необхідні для прийняття раціональних і науково-обґрунтованих управлінських рішень.

Поступове й доволі умовне поєднання віртуального і реального просторів за допомогою ІТ систем (ІТС) і мережевих технологій різного функціонального призначення, які в процесах обробки, передачі та зберігання інформації використовують електромагнітний спектр і діють як єдине ціле, а також відповідного програмного забезпечення (ПЗ) призвело, як наслідок, до формування так званого ***кіберпростору*** (КбП) (рис. 1.1) – високорозвиненої моделі об'єктивної реальності, у якій відомості про особи, предмети, факти, події, явища і процеси:

подані у деякому математичному, символьному (у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень) або будь-якому іншому виді;

розміщуються в пам'яті будь-якого фізичного пристрою, спеціально призначеного для її зберігання, обробки й передачі;

перебувають у постійному русі по сукупності ІТ систем і мереж.

Рис. 1.1. Взаємозв'язок інформаційного і кіберпросторів

Вперше термін кіберпростір був використаним у згаданій вище Окінавській хартії глобального інформаційного суспільства та в Конвенції про злочинність у сфері комп'ютерної інформації від 23 листопада 2001 року. Сфера його дії в той час обмежувалась загальними межами правового регулювання суспільних відносин, специфічними об'єктами та інтересами суб'єктів правовідносин, а також комп'ютерними мережами, за допомогою яких можна брати участь у відповідних правовідносинах. Нині кіберпростір має досить багато визначень.

Так, наприклад, відповідно до:

1) міжнародного стандарту [2], кіберпростір – це середовище існування,

отримане у результаті взаємодії людей, програмного забезпечення і послуг в Інтернет за допомогою технологічних пристроїв і мереж, підключених до них, яке не існує у будь-якій фізичній формі;

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

3) офіційних документів Євросоюзу [2], кіберпрострір – це віртуальний простір, в якому циркулюють електронні дані світових ПК;

4) офіційних документів Великобритані [2], кіберпростір – це всі форми мережевої, цифрової активності, що включають у себе контент та дії, які здійснюються через цифрові мережі;

5) офіційних документів Німеччини [2], кіберпростір – це вся інформаційна інфраструктура, що доступна через Інтернет поза будь-якими територіальними кордонами.

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

поліморфний віртуальний простір, що генерує 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, що використовується для забезпечення певних інформаційних потреб;

штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене у результаті функціонування кібернетичних комп'ютерних систем управління і обробки інформації та забезпечує користувачам доступ до обчислювальних й інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою 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, у якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої 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 видно з викладеного, найбільш відмінними ознаками кіберпростору, як субстанції, створенню якої перш за все сприяли зміна характеру діяльності людини з прийняття рішень, впровадження електронно-цифрових форм створення, обробки, зберігання і переміщення інформації, перехід від паперового діловодства до електронного тощо переважна *більшість фахівців вважає* його неперевершені можливості зі створення багаточислених зв'язків між окремими індивідуумами і соціальними групами та з надання різнопланових інформаційних послуг. З урахуванням характерних рис кіберпростору, як сфери вчинення заздалегідь спланованих деструктивних дій на кшталт проникнення до ІТС один одного, блокування або виведення з ладу їх найбільш уразливих елементів, дезорганізації оборонних автоматизованих систем управління (АСУ) протилежної сторони, систем управління її транспортом і енергетикою, економікою й фінансовою системою тощо (наряду з наземною, морською й повітряно-космічною сферами) та так званого своєрідного містку між такими поняттями, як Internet і кібернетика це, в свою чергу, дає можливість:

виділити в ньому систему певних відносин між суб'єктами та об'єктами інформаційної й кібернетичної інфраструктури;

виокремити злочини, втручання і загрози, пов'язані з особливостями існування та передачі інформації;

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

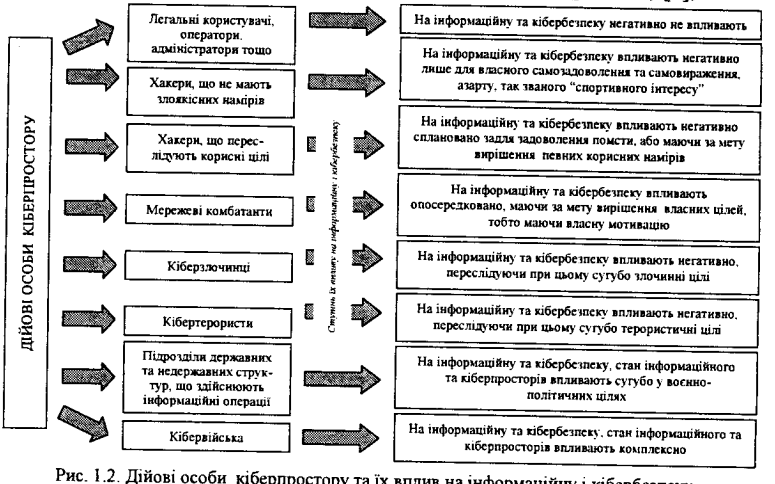


Рис. 1.2. Дійові особи кіберпростору та їх вплив на інформаційну і кібербезпеку

розглядати його з 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 передачі даних) рівні тощо.

Зважаючи на таке, а також враховуючи результати проведеного багатокритеріального аналізу (табл. 1.1) та відсутність в Україні гостованого визначення цього терміну, під **кіберпростором** будемо розуміти *віртуальне комунікаційне середовище, утворене системою зв'язків між користувачами та об'єктами інформаційної інфраструктури, а саме електронним інформаційним ресурсом (IP), системами і мережами усіх форм власності, що керуються автоматизованими системами управління й використовуються як для перетворення та передавання інформації, яка в них циркулює з метою забезпечення інформаційних потреб суспільства, так й для впливу на аналогічні об'єкти протиборчої сторони.*

Таблиця 1.1

Аналіз дефініцій поняття кібербезпека за базовими критеріями

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

У таблиці використані такі ідентифікатори [2]: ***Virt*** - критерій віртуальності, ***HF*** – критерій врахування людського чинника, ***Soft*** – критерій врахування ПЗ, ***PhI*** – критерій наявності фізичної інфраструктури, ***Net*** – критерій наявності мережевої складової, ***INet*** – критерій врахування поняття Інтернету, ***IServ*** – критерій можливості надання інформаційних послуг, ***IRes*** – критерій врахування інформаційних ресурсів, ***MSys*** – критерій наявності системи управління, ***IPr*** – критерій врахування інформаційних процесів.

Нині про важливість кіберпростору свідчить поява концепцій ведення боротьби у ньому та створення у ЗС ряду країн світу спеціальних структур на кшталт (рис.1.3):

об'єднаного Кіберкомандування (U.S. Cyber Command - USCYBERCOM) та спеціалізованого кібернетичного розвідувального центру у складі ЗС США;

Управління мережевих 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, призначених для ведення так званої **кіберборотьби** – *комплексу заходів, спрямованих на здійснення управлінського та/або деструктивного впливу на автоматизовані IT системи протиборчої сторони й захисту від такого впливу власних інформаційно-обчислювальних ресурсів шляхом використання спеціально розроблених програмно-апаратних засобів, а також проведення ряду спеціалізованих навчань.*

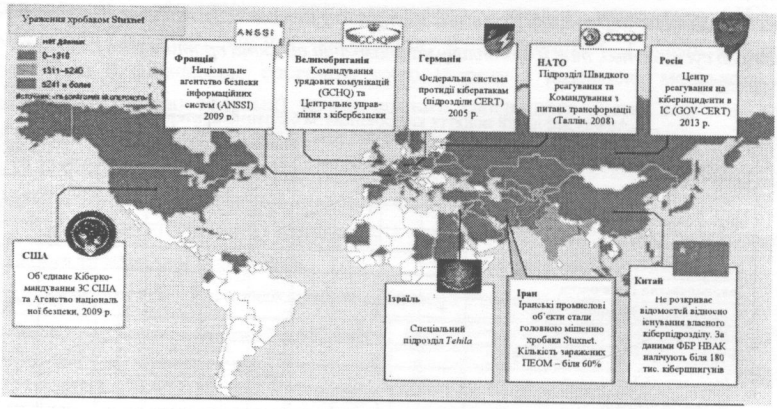


Рис. 1.3. Маштаби ураження та протидії сторонньому кібервпливу

Такий стан справ, а також глибинні зміни у відношенні більшості держав земної кулі до безпеки власних інформаційного і кіберпросторів призвели й до значних змін у захисті ІР, тобто інформації та засобів її обробки, а також у захисті кіберсередовища у якому така інформація циркулює (рис. 1.4), а саме до інформаційної і кібербезпеки.

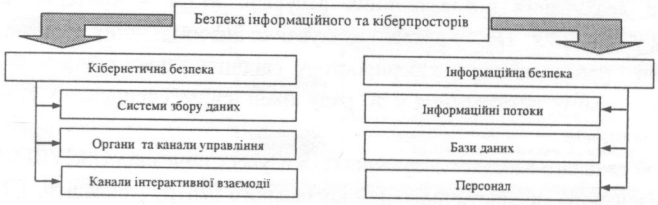


Рис. 1.4. Об'єкти впливу в інформаційному і кіберпросторах

При цьому **інформаційна безпека** (ІБ) у найбільш загальному виді може бути визначена як *стан захищеності інформаційного простору держави за якого неможливе нанесення збитку властивостям об'єкта безпеки, обумовленим інформацією та інформаційною інфраструктурою та який забезпечує формування, використання і розвиток національної інфосфери в інтересах оборони* (рис. 1.5).

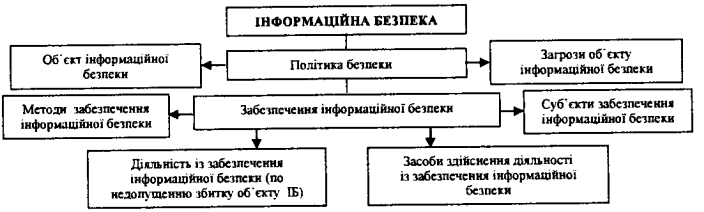


Рис. 1.5. Структура поняття «Інформаційна безпека»

Спектр інтересів ІБ з точки зору інформації, інформаційних систем (ІС) та інформаційних технологій (ІТ), як об'єктів безпеки може бути поділений на такі основні категорії: доступність – можливість за прийнятний час отримати певну інформаційну послугу, цілісність – актуальність і непротиречивість інформації, її захищеність від руйнування та несанкціонованого змінювання, конфіденційність – захист від несанкціонованого ознайомлення (рис. 1.6).

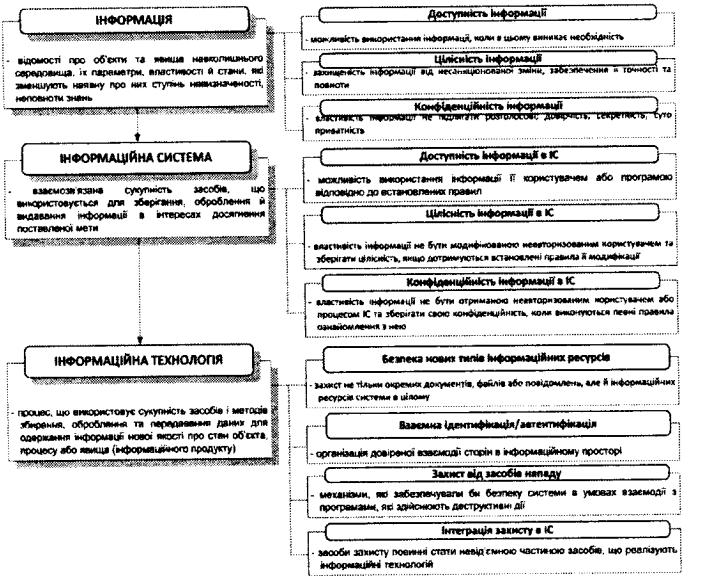


Рис. 1.6. Інформаційні системи та технології як об'єкти ІБ

Головними загрозами, які можуть призвести до порушення цих категорій, а також негативно вплинути на компоненти ІС, що призведе до їх втрати, знищення або збою функціонування є розголошення інформації, її витік або несанкціонований доступ до такої інформації (рис. 1.7).

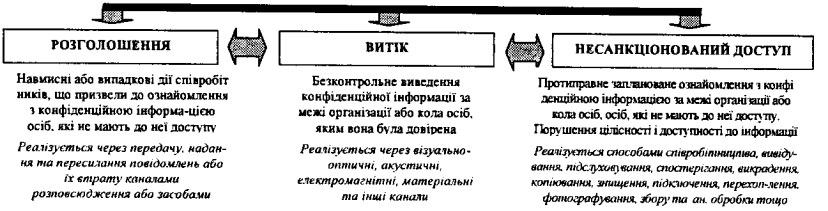


Рис. 1.7. Способи нанесення збитку інформаційній безпеці

Методи (рис. 1.8) завдяки яким цьому можна запобігти та забезпечити відповідний рівень ІБ доцільно класифікувати на:

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

інженерно-технічні методи (ставлять своєю метою забезпечення захисту інформації від витоку по технічних каналах);

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

теоретичні методи забезпечення (вирішують задачі формалізації різного роду процесів, пов'язаних із забезпеченням ІБ).

Рис. 1.8. Основні методи забезпечення інформаційної безпеки

Характерними ознаками, які нині уособлюють поняття **кібербезпеки** (рис. 1.9)

Рис. 1.9. Складові кібернетичної безпеки

– стану захищеності кіберпростору держави в цілому або окремих об'єктів його 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 та/або національним інтересам [1, 3–9] *є сукупність активних захисних і розвідувальних дій, що в процесі інформаційного протиборства зусиллями поодиноких інсайдерів або організованих кіберугруповань розгортаються навколо IP, ІКТ і ІТС* (рис. 1.10).

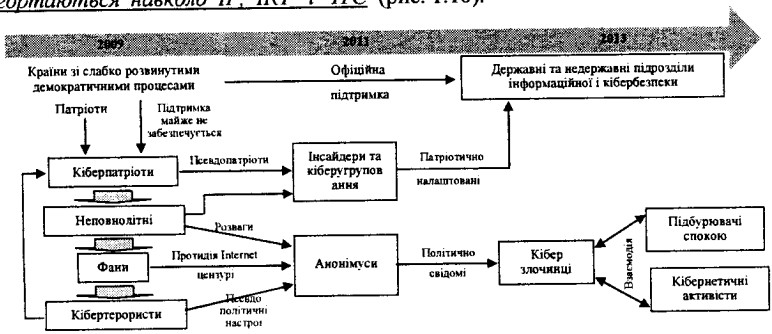


Рис. 1.10. Взаємозв'язки і мотивація здійснення кібервпливів

Такі дії спрямовані 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).

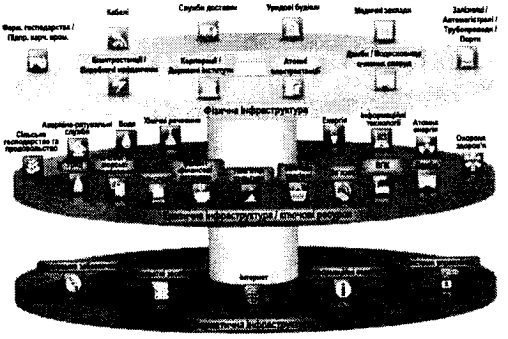


Рис. 1.11. Критично важливі складові фізичної, інформаційної та кіберінфраструктур

При цьому проблемами забезпечення кібернетичної безпеки нині є:

відсутність чіткого усвідомлення ролі та значення кібербезпекової складової у системі забезпечення національної безпеки держави;

дифініційна, термінологічна та нормативно-правова невизначеність у сфері кібербезпеки;

залежність держави від програмних та технічних продуктів іноземного виробництва;

відсутність належної координації діяльності відповідних відомств та як наслідок неузгодженість дій зі створення окремих елементів системи кібербезпеки;

складнощі із методичним забезпеченням та кадровим наповненням відповідних структурних підрозділів.

Комплексна сутність кібербезпеки за таких умов може бути виражена схемою, поданною на рис. 1.12.

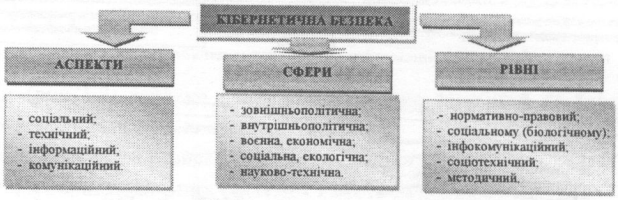


Рис. 1.12. Сутність кібернетичної безпеки

Впродовж останніх років Україна, як і більшість інших країн світу, робить певні кроки у напрямку розбудови інформаційного суспільства, забезпечення інформаційної і кібербезпеки, а також боротьби з кіберзлочинністю. Нормативно-правову базу у цих сферах діяльності складає:

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 ключова роль у забезпеченні кібербезпеки покладається на:

1) Закон України "Про захист інформації в інформаційно-телекомунікаційних системах", який регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та ІТ систем;

2) Закон України «Про Основні засади розвитку інформаційного суспільства

України на 2007-2015 роки» [23] у запропонованих змінах до якого указується на необхідність 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 запроваджено низку термінів, пов'язаних із кібербезпекою.

Практичними кроками щодо реалізації існуючої нормативно-правової бази стало створення у 2007 році 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 (СБ) 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. Усвідомлюючи ступінь та динаміку поширення комп'ютерних інцидентів теренами України у 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.

Зважаючи на певні труднощі з якими фахівці з кіберзахисту від ДССЗЗІ, СБ та МВС України стикаються в процесі роботи та неможливість самотужки розібратися з усіма проявами внутрішніх і зовнішніх загроз національній безпеці України в інформаційному і кіберпросторах, з плином часу постала гостра потреба у пошуку ними шляхів співробітництва з аналогічними організаціями світового суспільства. Фактично програмним документом для нашої держави на підтвердження такому став вислів Першого заступника Секретаря РНБО України, Співголови Спільної робочої групи Україна – НАТО з питань воєнної реформи, згідно якому "... суттєво підвищити рівень безпеки кіберпростору..." сучасного інформаційного суспільства можна лише "... завдяки тісній міждержавній співпраці, використовуючи для цього всі наявні можливості і механізми, які є в розпорядженні кожної з країн ..." [25]. При цьому одним із головних напрямків такої діяльності на його думку має стати *нарощування темпів співпраці передусім з організацією НАТО.*

Вагомим поштовхом для активізації зусиль у цьому напрямку стало прийняття організацією НАТО програмного документу 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 головним елементом політики НАТО у сфері кіберзахисту є принцип, згідно якого держави-члени Альянсу несуть пряму відповідальність за захист власних національних комунікацій та інформаційних систем. При цьому НАТО повинна мати спроможність для підтримки союзників, які стали жертвою кібератак міжнаціонального значення. Окрім цього в документі зазначається, що головні цілі співробітництва НАТО з державами-партнерами у сфері кіберзахисту перш за все полягають у покращенні спроможності 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 заходів з підтримки у випадках кібератак. Відповідно до основних положень документу країни-партнери закликаються до вжиття необхідних заходів з метою гармонізації національного законодавства у сфері кібернетичної безпеки з відповідними міжнародними нормами (зокрема, такими як Конвенція Ради Європи з питань кіберзлочинності) шляхом дотримання таких головних принципів:

1) співпраця між НАТО та країною-партнером має бути взаємовигідною у тому сенсі, що Альянс може надати країні-партнеру інформацію та підтримку у сфері кібербезпеки за умови дотримання останньою аналогічних умов взаємодії;

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

3) країни-партнери можуть звертатися з пропозицією щодо співпраці у сфері кіберзахисту та отримання підтримки з боку НАТО у випадках кібератак національного значення;

4) НАТО і партнери повинні уникати дублювання зусиль, що вживаються у рамках інших міжнародних організацій, які залучаються до захисту ІС від кібератак;

5) наявність Угоди про безпеку між НАТО та країною-партнером визначатиме обсяги допомоги та інформаційного обміну. Разом з цим, інформація, яка стосується захисту критичної інфраструктури національних комунікаційних та інформаційних систем, буде позначена та передана належним чином лише у разі потреби ознайомлення з нею.

Документ визначає також сфери співробітництва НАТО з державами-партнерами у сфері кіберзахисту, а саме: узагальнений обмін інформацією щодо

політики та доктрин; обговорення технічних засобів захисту комунікаційної та інформаційної інфраструктури (може бути передбачений на більш змістовному рівні співробітництва). Окремо у документі наголошується про те, що: по-перше, країни-партнери можуть звертатися з пропозиціями щодо проведення консультацій з питань кібернетичного захисту у форматі "28+1" або "28+n"; по-друге, процес планування та оцінки сил, а також Річні національні програми мають слугувати головними інструментами щодо прив'язки співробітництва з державами-партнерами у питаннях кіберзахисту з їхніми індивідуальними потребами та обставинами (загальна кількість Цілей партнерства у рамках ППОС, схвалених для України – 96, з них: на Збройні Сили України покладено 70 Цілей партнерства, на МВС України – 8, на МЗС України – 6, на СБУ – 11 та на Мінфін України – 1) й, 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" та Комітету з планування цивільного зв'язку може використовуватися країнами-партнерами у плані підготовки відповідного персоналу.

Враховуючи таке основними напрямами подальшого співробітництва України з НАТО у сфері кіберзахисту й, як наслідок, створення загальнодержавної системи кібернетичної безпеки українською стороною вважаються:

1) формування культури та проведення інформаційно-пропагандистської кампанії про значимість проблематики кібербезпеки держави шляхом:

забезпечення активного інформування про кібернетичні втручання і загрози, а також потенціальні уразливості ІТ систем і мереж та способи їх компенсації;

розширення співпраці державних органів з ІТ-компаніями, некомерційними організаціями тощо з метою популяризації і впровадження практик безпечної поведінки у кіберпросторі;

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

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

організації профілактичної роботи з потенційними жертвами кіберзлочинів, керівниками малого і середнього бізнесу тощо;

2) створення механізму моніторингу кібернетичних втручань і загроз, а також своєчасного прийняття рішень щодо реагування на їх прояви за рахунок:

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

2.2) формування критеріїв (на кшталт прогнозованих людських втрат,

масштабів нанесення економічних збитків, імовірної загрози дестабілізації суспільства тощо) віднесення об'єктів інформаційного та кіберпросторів до критичної інформаційної і кіберінфраструктури;

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

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 передачі даних та радіонавігації, систем телефонного і супутникового зв'язку, а також систем зв'язку з рухомими об'єктами;

2.4) 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;

забезпечення безпеки механізмів електронної міжвідомчої взаємодії;

мінімізації кількості шлюзів, що з'єднують державні інформаційні системи з мережею Internet для максимізації їх безпеки тощо;

4) підвищення надійності критичної кіберінфраструктури за рахунок:

створення механізмів моделювання і прогнозування кібервтручань та кіберзагроз;

впровадження системи обміну інформацією щодо захисту об'єктів критично важливої інформаційної і кіберінфраструктури;

забезпечення прийнятної автономності кореневої інфраструктури Internet;

розроблення механізмів протистояння використання Internet у терористичних цілях тощо;

5) підтримка вітчизняних виробників програмно-апаратного забезпечення шляхом:

5.1) 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 мережевого доступу;

проектування та створення систем виявлення атак і захисту від них;

виділення ресурсів, ранжирування обраних контрзаходів за ступенем важливості, реалізації та тестування найбільш пріоритетних;

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

5.2) 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 в області 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 реалізації єдиної науково-технічної політики щодо захисту державних інформаційних ресурсів та ІТ інфраструктури від деструктивного кібернетичного впливу шляхом:

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

цільового фінансування, підтримки і проведення НДДКР з кібербезпеки тощо;

8) реалізація механізмів партнерства держави, бізнесу і громадян у сфері кібербезпеки за рахунок:

впровадження механізмів обміну інформацією державних ситуаційних центрів і центрів реагування на прояви стороннього кібервпливу з бізнесом і суспільством;

підвищення ефективності взаємодії провайдерів Internet-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 тощо;

9) вдосконалення національного нормативно-правового та понятійно-термінологічного апарату кібербезпеки шляхом:

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

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

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

9.4) внесення змін до низки існуючих 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:

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

10.2) вдосконалення механізмів надання взаємодопомоги у технічних і методологічних аспектах випереджувального виявлення джерел, фіксації та оперативного обміну інформацією про факти здійснення кібератак, а також запобігання їх деструктивного впливу на ІР;

10.3) вдосконалення організаційно-правових норм міжнародної взаємодії з питань боротьби з кіберзлочинністю і кібертероризмом та внесення змін і доповнень до низки існуючих міжнародних нормативно-правових документів, а саме до:

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

по-друге, "Рекомендацій Міжнародного союзу електрозв'язку" (серія X: Мережі передачі даних, взаємозв'язок відкритих систем та безпека. Безпека електрозв'язку. Огляд кібербезпеки. X.1205), в яких вперше визначений зміст термінів "кіберсередовище" і "кібербезпека";

по-третє, положень Женевських і Гаагських конвенцій, стисла характеристика яких наведена у табл. 1.2 [1] (з урахуванням нових меж кібервоєн конкретні пропозиції щодо корегування Положень запропоновані у лютому 2011 року фахівцями з Нью-Йоркського інституту EastWest [1] на щорічній конференції Munich Security Conference) тощо.

Таблиця 1.2

Стисла характеристика Женевських і Гаагських 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	64 (56 у додатках)
Женевський протокол	Про заборону застосування на війні ядушливих, отрутних та інших подібних газів і бактеріологічних засобів	1925 р.	-

Продовження табл. 1.2

Документ	Назва	Дата	Кількість статей
Женевська конвенція I	Про поліпшення участі поранених і хворих у діючих арміях	1864 р. (н.ред. 1949 р.)	77 (13 у додатках)
Женевська конвенція II	Про поліпшення участі поранених, хворих та осіб, які потерпіли при кораблекрушіннях, зі складу збройних сил на морі	1949 р.	63
Женевська конвенція III	Про поводження з військовополоненими	1929 р., (н.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 й про їхнє знищення	1975 р.	15
Протокол I	Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів	1977 р.	102
Протокол II	Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв збройних конфліктів неміжнародного характеру	1977 р.	28
Протокол III	Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується прийняття додаткової відмітної емблеми	2005 р.	17

Реалізація перелічених вище заходів має здійснюватись у декілька етапів при неухильному дотриманні таких принципів: по-перше, верховенства права, законності та пріоритеті додержання прав і свобод людини і громадянина; по-друге, партнерства держави та приватного сектору з метою вироблення нових, більш оптимальних рішень; по-третє, пріоритетного розвитку та підтримки вітчизняного кібернетичного (або інформаційного) сектору; по-четверте, відповідальності суб'єктів забезпечення кібернетичної безпеки за захист національної інформаційної інфраструктури, дієвості, комплексності і постійності заходів забезпечення кібербезпеки держави й, по-п'яте, участі інституцій громадянського суспільства у забезпеченні кібернетичної безпеки держави тощо. При цьому на першому етапі враховуючи досвід іноземних країн та особливості українських реалій має бути вдосконалено понятійно-термінологічний та нормативно-правовий апарат, створено ключові елементи Єдиної загальнодержавної системи кібербезпеки, проведено заходи із підготовки структурних підрозділів спецпризначення та ЗС України до ведення дій в умовах кібервійни, сформовано базис підготовки спеціалізованих кадрів, створено міжвідомчі і центральні органи, а також удосконалено підрозділи власної інформаційної (кібер) безпеки державних установ (відомств) та комерційних організацій (структур). На другому етапі – вдосконалено міжнародні правила поведінки держав у кіберпросторі та відповідне нормативно-правове підґрунтя, впроваджено програми підтримки вітчизняної інноваційної продукції щодо протидії сторонньому кібернетичному впливу, розгорнуто мережі CERTів по усій Україні тощо. На третьому етапі – проведено коригування Стратегії на

основі оцінки ефективності її реалізації та нових викликів.

Тим не менш нині існує ціла низка проблем, які заважають Україні створити дієздатну систему протидії внутрішнім і зовнішнім загрозам власному інформаційному і кіберпросторам. Найсуттєвішими з них є [1]:

складність структури ІКТ та національного кіберпростору;

наявність якісних відмінних рис кіберзброї від зброї звичайної;

ускладненість щодо розмежування воєнних і цивільних об'єктів критичної інфраструктури держави у кіберпросторі;

можливість недержавних суб'єктів та неавторизованих (індивідуальних) користувачів виступити у ролі гравців в кіберпросторі та проблематичність щодо їх виявлення;

можливість скритного (прихованого) проведення протиборчими сторонами кібератак та кібероперацій у кіберпросторах один одного;

значна уразливість інфосфери України через надмірно широке впровадження до неї 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 і силовими структурами України, що спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення кваліфікованими фахівцями з цих питань;

відсутність єдиного понятійно-термінологічного поля кібербезпеки України, як головної складової безпеки інформаційної та системних нормативно-правових документів, які б регламентували діяльність зазначених відомств, правоохоронних і силових структур у сфері кіберзахисту;

відсутність у вітчизняному законодавстві визначень перш за все таких термінів, як "кібервійна", "кіберзахист" та "кібербезпека" (на відміну від інформаційної безпеки, сутність якої викладена у ст. 17 Конституції України), "комп'ютерна злочинність" і "комп'ютерний тероризм" (певним чином знайшли відображення у законі України "Про основи національної безпеки" та доктрині ІБ України, а також у статті 1.1.5 проекту Річної національної програми України);

відсутність загальнонаціонального координаційного центру, який був би спроможним узгоджувати і координувати діяльність зазначених вище правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпросторам України та керувати проведенням

комплексних навчань з проблеми забезпечення кібернетичної безпеки держави в інфосфері на кшталт навчань "Cyber Storm", які проводяться в США та/або "Cyber Europe", що проводяться у ЄС тощо (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 її критично важливої інформаційної і кіберінфраструктури, виникнення техногенних катастроф тощо. Саме тому найбільш пріоритетним напрямом керівництво України вважає нині реформування власної інформаційної безпеки за рахунок створення дієвої системи кібербезпеки, розбудова якої вимагає вирішення різних завдань як соціального і техногенного, так і передусім організаційного характеру. Найбільш актуальними серед них нині є [26]: чітке визначення функцій суб'єктів забезпечення кібернетичної безпеки та розподілу повноважень між ними, забезпечення належної координації діяльності як загальних суб'єктів забезпечення кібернетичної безпеки, так і відповідних спеціальних суб'єктів, розробка та впровадження найсучасніших підходів, форм і методів забезпечення кібернетичної безпеки, а також запровадження 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 варіанту реагування на кібернетичні втручання і загрози

З розвитком ІКТ, ІТС та глобальної мережі Internet світове суспільство крім отримання значних можливостей щодо обміну інформацією стало надто уразливим від стороннього кібернетичного впливу [3, 4, 9], а саме від *фактично неприхованих спроб впливу протиборчих сторін на інформаційний і кіберпростори один одного за рахунок використання засобів сучасної обчислювальної та/або спеціальної техніки й відповідного програмного забезпечення* (так званих **кібервтручань**) та інших *проявів їх дестабілізуючого негативного впливу на певний об'єкт, що реалізуються за рахунок використання технологічних можливостей інформаційного і кіберпросторів, створюючи при цьому небезпеку як для них самих, так й для свідомості людини у цілому* (так званих **кіберзагроз**). Нині, з метою уникнення багатозначності у трактуванні запропонованих термінів, інструктивні матеріали Інтерполу поділяють їх на такі групи:

власне комп'ютерні інциденти, що полягають, наприклад, у втручанні в роботу обчислювальних систем, порушенні авторських прав на програмне забезпечення, а також розкраданні даних і комп'ютерного часу тощо;

інциденти "пов'язані з комп'ютерами", що супроводжують головним чином протиправні дії за напрямом фінансового шахрайства;

мережеві інциденти, що сприяють здійсненню незаконних угод.

Під **інцидентами** у сфері високих технологій будемо розуміти *події, що полягатимуть в реалізації певної загрози та порушенні встановленого рівня безпеки інформаційно-комунікаційних систем* (рис. 1.13). Під **процесом управління інцидентами** – *процес реєстрації інформації про стан безпеки і рівноваги ІКС, передавання інформації у пункти накопичення й переробки, проведення її аналізу, прийняття рішення та формування певного керуючого впливу на об'єкт управління.*

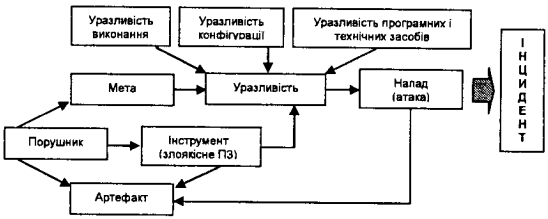


Рис. 1.13. Діаграма виникнення інцидентів у сфері високих технологій

Інша класифікація таких дій визначає сім основних їх груп, які, скоріше, можна віднести до способів або методів, використовуваних зловмисниками для здійснення нападу, а саме: перехоплення паролів інших користувачів; "соціальна інженерія"; використання помилок ПЗ й програмних закладок; використання помилок механізмів ідентифікації користувачів; використання недосконалості протоколів передачі даних; одержання інформації про користувачів стандартними засобами операційних систем; блокування сервісних функцій системи, що атакується.

Найбільший же інтерес з позицій класифікації кібернетичних втручань і загроз у цей час становить схема, пропонована Конвенцією Ради Європи 2001 року по боротьбі з кіберзлочинністю [9]. У ній говориться про чотири можливі групи таких дій:

1) *інциденти, спрямовані проти конфіденційності, цілісності й доступності комп'ютерних даних і систем*, що реалізуються через:

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

втручання в дані (протиправну зміну, ушкодження, видалення, перекручування або блокування комп'ютерних даних та керуючих команд шляхом проведення кібератак на інформаційні системи, ресурси та мережі державного і військового управління тощо);

втручання в роботу системи (протиправне порушення або створення перешкод функціонуванню комп'ютерної системи шляхом розробки та поширення вірусного програмного забезпечення, застосування апаратних закладок, радіоелектронного та інших видів впливу на технічні засоби та системи телекомунікацій і зв'язку, обробки та передачі інформації, системи захисту IP, систем і мереж, програмно-математичне забезпечення, протоколи передачі даних, алгоритми адресації та маршрутизації тощо);

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

незаконне використання комп'ютерного й телекомунікаційного встаткування (виготовлення, придбання для використання, поширення або інші способи зробити доступними: пристрої, включаючи ПЗ, розроблені або пристосовані для здійснення кожного зі злочинів першої групи; комп'ютерні паролі, коди доступу, інші подібні дані, що забезпечують доступ до комп'ютерної системи або її частини) або його повне вилучення;

2) *шахрайство та підробка, пов'язані з використанням комп'ютерів*, що полягають у:

підробці документів із застосуванням комп'ютерних засобів (протиправному навмисному внесенні, змінюванні, видаленні або блокуванні комп'ютерних даних, що приводять до зниження вірогідності документів);

шахрайстві із застосуванням комп'ютерних засобів (втручанні у функціонування комп'ютерної системи з метою навмисного протиправного одержання економічної вигоди для себе або для інших осіб);

3) *інциденти, пов'язані з розміщенням у мережах протиправної інформації (наприклад, поширенням дитячої порнографії тощо)*;

4) *інциденти відносно авторських і суміжних прав*.

При цьому, наприклад [3, 4], у США згідно законодавству цієї країни до таких дій відносять: 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; навмисне одержання

або видозміна повідомлень, що зберігаються в пам'яті комп'ютера, а також за створення перешкод для санкціонованого доступу до таких повідомлень. У Великобританії [9] до протиправних дій у сфері ІТ технологій відносять: навмисний протизаконний доступ до комп'ютера або комп'ютерної інформації, що циркулює в ньому; розголошення персональних даних, виготовлення й поширення порнографічних матеріалів (у т.ч. з використанням ЕОТ). У ФРН [9] такими протиправними діями є: неправомірний доступ до комп'ютерної інформації, її несанкціонована модифікація, підробка, утаювання 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 [9] протиправними діями у сфері ІТ технологій, як правило, вважають: перехоплення, розкрадання, використання або надання розголосу повідомлень, переданих засобами зв'язку; незаконний доступ до автоматизованої системи обробки даних; порушення або запобігання 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 обробка даних незаконним способом; зберігання певних даних понад установлений законом строк; несанкціоноване використання даних; знищення, псування або розкрадання будь-якого документа, техніки, спорудження, устаткування, установки, апарата, технічного пристрою або системи автоматизованої обробки даних або внесення в них змін; збір або передачу інформації, що міститься в пам'яті ЕОМ або картотеці іноземній державі; знищення, розкрадання, вилучення або копіювання даних, що носять характер секретів національної оборони, що втримуються в пам'яті ЕОМ або в картотеках, а також ознайомлення із цими даними сторонніх осіб; терористичні акти, пов'язані з діяннями в області інформатики тощо.

Представлені переліки не є вичерпними, але вони дають можливість [1, 9]:

умовно об'єднати зазначені вище типи дій у дві укрупнені категорії – втручання і загрози, спрямовані безпосередньо на порушення нормального функціонування ІТС та підключених 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 ж схемою), що або пов'язані з комп'ютером (computer related), або вчинені за його допомогою (computer facilitated);

зробити висновок про те, що зазначені та ним подібні дії у кіберпросторі вийшли за межі окремих країн й набули при цьому істотну фінансову підтримку та якісні комунікації;

формалізувати зазначені вище типи дій, представивши їх моделлю, яка міститиме три головні етапи – етап вивчення певного об'єкта, етап проведення

нападу на нього й етап приховування слідів нападу та, як мінімум, по дві стадії в кожному з етапів – стадію інформаційного обміну й власне стадію здійснення нападу на соціальному (біологічному), інфокомунікаційному та соціотехнічному рівнях. Останні, у свою чергу, складатимуться з, по-перше, операцій щодо обміну даними, рекогносцировки, сканування й складання карти – характерні для інформаційного обміну й, по-друге, з операцій одержання доступу, розширення повноважень, крадіжки інформації, зомбування, знищення слідів, створення "чорних ходів" і відмови в обслуговуванні – характерні для стадії здійснення нападу.

З урахуванням такого узагальнена модель системи управління інцидентами ІБ матиме вид:

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

де *INC* – управління інцидентами (внутрішніми та зовнішніми); *SEC* – мета;

CRI – критерії оцінювання стану безпеки; *X* – вхідні впливи;

KBS – база знань про внутрішні та зовнішні інциденти;

Y – реакція на внутрішні та зовнішні інциденти; *S* – стан системи;

DMF – функція прийняття рішення (реагування). Складається з двох етапів: прийняття рішення про включення елемента *ARS* в набор *TRS* й потім (на підґрунті першого етапу) – прийняття рішення про включення елемента *ARS* в набор *IRS*;

AGT – множина програмно-реалізованих мобільних інтелектуальних агентів;

ARS – набір ресурсів інформаційної безпеки, які доступні агентам;

TRS – тестовий набор ресурсів інформаційної безпеки;

IRS – інцидентно-орієнтовані набори ресурсів;

MST – стратегія управління інцидентами; *T* – час; *SYN* – самоорганізація.

При цьому під **внутрішнім** розумітимемо інцидент, джерелом якого є порушник, безпосередньо пов'язаний з постраждалою стороною (рис. 1.14). Серед найпоширеніших системних подій такого типу можна виділити: витік конфіденційної інформації; неправомірний доступ до інформації; видалення інформації; компрометацію інформації; саботаж; шахрайство за допомогою ІТ; аномальну мережеву активність; аномальне поводження бізнес-додатків; використання активів установи в особистих цілях або в шахрайських операціях. Під **зовнішнім** – інцидент, джерелом якого є порушник, безпосередньо не пов'язаний з постраждалою стороною. Серед системних подій такого типу можна виділити: шахрайство в системах електронного документообігу; атаки типу "відмова в обслуговуванні" (DoS), у тому числі розподілені (DDoS); перехоплення й підміну трафіка; неправомірне використання бренда установи в мережі Інтернет; фішинг; розміщення конфіденційної */провокаційної/ інформації в мережі Інтернет; злом або спробу злому мережевих вузлів,*

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

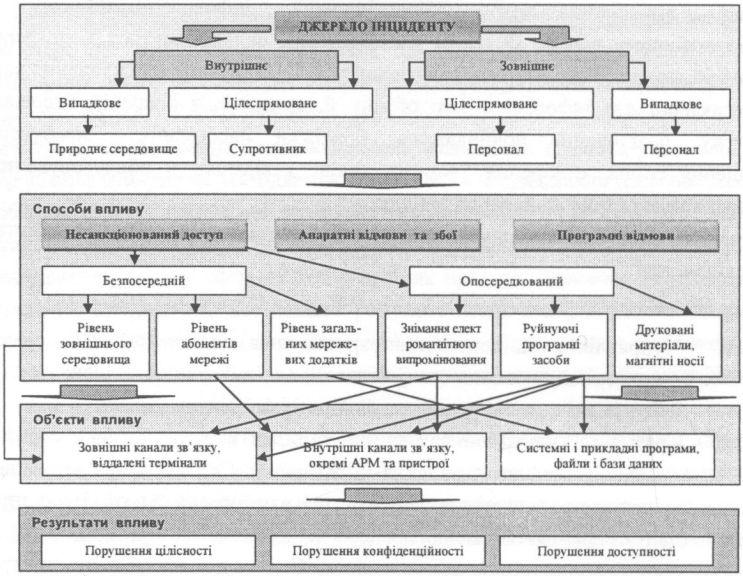


Рис.1.14. Класифікація джерел інцидентів, а також способів, об'єктів та результатів їх впливу

Усі вони згідно кодифікатору, використовуваному Міжнародною кримінальною поліцією «Інтерпол» 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 із програмами уведення виводу;

QFP - шахрайства із платіжними засобами;

QFT - телефонне шахрайство;

QFZ - інші комп'ютерні шахрайства;

4) QR - незаконне копіювання ("піратство"):

QRG - комп'ютерні ігри;

QRS - інше програмне забезпечення;

QRT - топографія напівпровідникових виробів;

QRZ - інше незаконне копіювання;

5) QS - ккомп'ютерний саботаж:

QSH - з апаратним забезпеченням;

QSS - із програмним забезпеченням;

QSZ - інші види саботажу;

6) QZ - Інші комп'ютерні злочини:

QZB - з використанням комп'ютерних дощок оголошень;

QZE - розкрадання інформації, що становить комерційну таємницю;

QZS - передача інформації конфіденційного характеру;

QZZ - інші комп'ютерні злочини.

Зважаючи на неготовність більшості організацій до обробки цих та ним подібних подій, які потенційно створюють небезпеку їх бізнесу, а також на ускладненість у відновленні їх нормального функціонування після таких подій нагально необхідним стає процес управління інцидентами інформаційної безпеки. Його складовими частинами при цьому є аналізування рівнів ІБ, оцінювання ефективності заходів безпеки, впровадження корегуючих, попереджуючих або інших заходів (рис. 1.15).

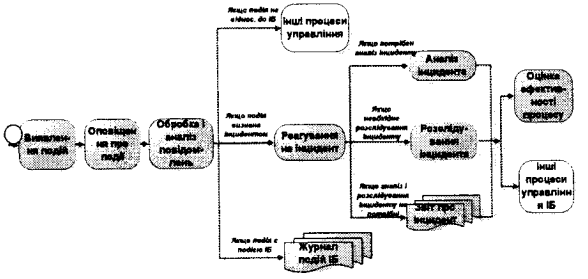


Рис. 1.15. Процес управління інцидентами ІБ

Найбільшу небезпеку серед відомих нині інцидентів становлять [27]:

1) пошукова оптимізація (SEO – Search Engine Optimization), що застосовується зловмисниками для поширення шкідливих програм. Використовуючи технології SEO та уразливості програмного забезпечення зловмисники піднімають позиції своїх попередньо заражених web-сторінок й таким чином спонукають користувачів зробити запит щодо певної новини у пошуковій системі, отримати результат, перейти по одному із самих верхніх посилань на сторінку зловмисника й запустити на своїй ПЕОМ шкідливу програму;

2) експлуатація уразливостей у клієнтському програмному забезпеченні (ПЗ), розробленому третьою стороною, наприклад, уразливостей так званої «нульової доби» що застосовуються зловмисниками для призупинення виконання певних виробничих процесів. Все частіше з цією метою використовуються уразливості в офісних програмах (Word, Excel і PowerPoint) та мультимедіа-програвачах (Real Player, iTunes, QuickTime), а також спеціальні утиліти для перегляду документів (наприклад, Adobe Reader);

3) цільовий фішинг (Spear Phishing), що застосовується зловмисниками для примушування користувача до виконання певної деструктивної дії на кшталт установлення шкідливого ПЗ на сервері компанії. Для цього зловмисники направляють певним людям у компанії ретельно підготовлені цільові повідомлення, у спробі переконати жертву відкрити шкідливе вкладення або перейти по посиланню на сайт, що містить експлойти для злому програм на стороні користувача;

4) перехоплення браузера (browser hooking), що застосовується зловмисниками для розміщення на web-сайтах контенту, який містить шкідливі скрипти (сценарії). Відкриваючи такий сайт користувач фактично запускає на своїй ПЕОМ скрипти й таким чином 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 застосовуються зловмисниками для: крадіжки конфіденційних даних з окремих web-додатків і баз даних; зміни вмісту баз даних, які будуть відображатися на web-сайтах; зміни web-контента й розміщення на сайті шкідливих скриптів для атаки на браузери відвідувачів, а також інших експлойтів, що використовують уразливості ПЗ на стороні користувача тощо;

6) атаки на адміністративні web-інтерфейси, що застосовуються зловмисниками для здійснення контролю за певними системами або інфраструктурами (ERP-системами, системами управління HVAC і електропостачанням тощо) за рахунок перехоплення браузера або експлуатації уразливостей ПЗ на стороні користувача;

7) атаки на сайти соціальних мереж (Facebook, LinkedIn, Twitter та інші), що застосовуються зловмисниками для: збору критичної інформації про діяльність компанії й технологіях, використовуваних її співробітниками; поширення експлойтів і скриптів з метою перехоплення браузера користувача;

8) атаки типу «передача хеша» (pass-the-hash), що застосовуються зловмисниками для одержання доступу у корпоративний домен за рахунок інтегрованих у Windows-системах пакетах для проведення атак (таких, як, наприклад, Metasploit і Nmap). При цьому викрадені хеші використовуються зловмисниками для аутентифікації замість паролів;

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

Не зважаючи 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]. Проте їх поява, починаючи з кінця минулого тисячоліття, вже неодноразово зафіксована [1, 28] й дає підстави стверджувати про стійку тенденцію щодо збільшення їх кількості. Такий стан справ простежується останнім часом перш за все у сфері комп'ютерних та Internet-технологій де лише за період з 2002 по 2010 рік кількість викритих внутрішніх і зовнішніх інцидентів збільшилася приблизно у 2,5 рази.

Таблиця 1.3

Кількість IT-інцидентів, що підлягали розслідуванню у різних країнах світу з грудня 2010 по квітень 2012 року

Approximate Number of Investigations, Searches, and Arrests During the Past 15 Months

Country	Total	Under age 18	18 to 28 years	Over age 28	Unknown age
United States	107	5	24	8	70
Turkey	32	8			24
Italy	15	5	10		
United Kingdom	16	6	9	1	
Argentina	10				10
Spain	7	1			6
Chile	6	2	4		
Netherlands	6	1	1		4
Colombia	5				5
France	3	1		1	1
Greece	3	2	1		
Poland	1		1		

Конкретними прикладами такому є [1, 28–31]:

1) події червня 1982 року, коли шляхом активації програмного забезпечення,

отриманого радянськими розвідниками в Канаді, та у яке, як з'ясувалось пізніше, американці попередньо ввели помилкові дані, була проведена кібератака проти сибірського газопроводу. Після одержання команди ззовні програма перевищила режим роботи газопроводу настільки, що він вибухнув;

2) події 1995 року, коли з банку "Україна" шляхом проникнення в його мережу було викрадено майже 4 мільйони доларів, 1997 року, коли на декілька годин була заблокована робота Internet-провайдера "Глобал Юкрейн", 2000 року, коли була зафіксована інформаційна диверсія проти Internet-провайдера "ukr.net", лютого 2012 року, пов'язані з масованим кібернападом на державні IP в ході виборчої кампанії в Україні (рис. 1.16);

Рис. 1.16. Динаміка деструктивних інцидентів у відношенні державних інформаційних ресурсів в Україні

3) події 2009 року, коли була виявлена цілеспрямована атака GhostNet з центром управління в Китаї, орієнтована на більш ніж сотню країн. Вторгнення відбувалися за допомогою повідомлення електронної пошти при відкритті якого запускалася шкідлива програма із прикріпленого файлу. Після установки вірус завантажував хакерський інструментарій Ghost Remote Administration Toolkit для дистанційного управління системами. Управляючий сервер у Китаї потім міг відправляти вірусу команди на передачу інформації з комп'ютерів жертв. У тому ж таки 2009 році почалася операція «Аврора», яка, по слухах, також виходила з Китаю й була спрямована на крадіжку інтелектуальної власності й закритої інформації з баз даних високотехнологічних компаній та національних відомств забезпечення безпеки і оборони. Атакуючі використовували уразливість класу use-after-free в Internet Explorer, що приводила до псування пам'яті об'єктів HTML. Це дозволяло атакуючому впровадити код в область пам'яті, що вивільнялась об'єктом при його видаленні. Для цього відразу після видалення об'єкта на його місці сторонній код створював новий. Атака здійснювалась методом попутного завантаження (drive-by download), що відбувалось без відома користувача, у результаті чого машина користувача заражалася вірусом;

4) міждержавні інциденти 2010–2012 років, спричинені мережевими черв'яками

Duqu, Flame та Stuxnet. Останній був розроблений групою фахівців з Ізраїлю і США за участю представників Німеччини та Великобританії. Наслідком його деструктивних дій стало гальмування ядерної програми Ірану. Цьому сприяло виявлення вірусом програмованих логічних контролерів (ПЛК) у автоматизованій системі управління технологічними процесами станції (Supervisory Control And Data Acquisition), а також можливість використання (для впровадження особливого коду у "залізо" ПЕОМ АЕС) чотирьох, невідомих раніше уразливостей "нульової доби" ("zero-day") у діючих версіях ОС Windows та двох дійсних сертифікатів від компаній Realtek і JMicron. Саме наявність останніх надавала можливість Win32/Stuxnet тривалий час уникати антивірусних радарів (рис. 1.17).

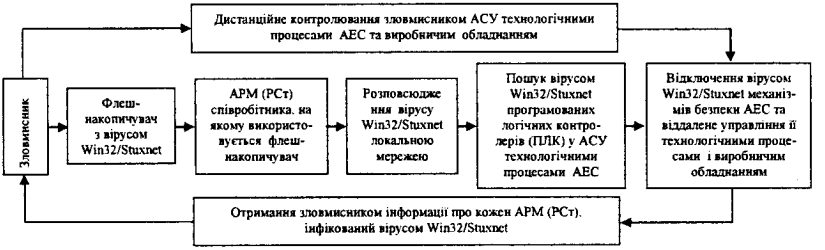


Рис. 1.17. Схема функціонування вірусу Win32/Stuxnet

У ході детального вивчення Win32/Stuxnet фахівці "Лабораторії Касперського" прийшли до невтішного висновку, що поява цієї шкідливої програми фактично знаменувала собою початок нової ери – ери кібервійни. За висловлюванням Є. Касперського – співзасновника і генерального директора "Лабораторії Касперського", цей програмний засіб призначений не стільки "... для крадіжки грошей, розсилання спама або знищення особистих даних ...", скільки створений для "... виведення з ладу заводів та ушкодження промислових систем ...".

Мережевий черв'як Worm.Win32.Flame, виявлений у 2012 році фахівцями "Лабораторії Касперського", був розроблений західними програмістами, як з'ясувалось, виключно для ведення кібершпигунства. Його основними функціями є:

розповсюдження за допомогою знімних дисків та локальних мереж;

зараження лише визначених ПЕОМ;

перехоплення мережевих пакетів, виявлення мережевих ресурсів та збір переліку уразливих паролів;

сканування диска інфікованої системи щодо наявності визначених розширень та контента;

копіювання зображень з екрана користувача в разі активності визначених процесів;

використання мікрофона інфікованої системи для запису звуків з навколишнього середовища;

передача інформації на сервери зловмисників;

використання понад 10 доменів для прийому команд з серверів управління;

встановлення безпечного з'єднання з 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 обумовлюється наявністю прихованого алгоритму дії та широкого спектру "бойових" можливостей (табл. 1.4).

Таблиця 1.4

Характеристик троянських вірусних програм "Stuxnet", "Duqu" та "Flame"

Можливості / тип	Вірусна програма		
	"Stuxnet"	"Duqu"	"Flame"
Дата застосування	червень - вересень 2010 року	вересень 2011 року	травень 2012 року
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 індустр. об'єктів	Цілеспрямований систематичний збір даних (офісні документи, креслення тощо), можливість модифікації інформації
Географія поширення	Іран, Норвегія, країни Близького Сходу	Близький Схід	
Спосіб розповсюдження	Мережа Інтернет, знімні носи інформації типу USB Flash Drive		
Мови програмування	Асемблер, С, С++	С, програмна архітектура Microsoft Visual C++	С, С++, ША
Обсяг файлу	до 0,5 Мб	від 0,06 до 0,23 Мб	понад 20 Мб
Розмір програмного коду	Близько 10 тис. рядків	6-8 тис. рядків	750 тис. рядків (базовий модуль - 650 тис. рядків /6 Мб/, найменший модуль -70 тис. рядків (170-зашифров.)
Принцип дії	Заснований на використанні вразливостей (помилок) ОС сімейства 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		

Нині такі та ним подібні дії займають чільне місце у геополітичній конкуренції переважної більшості країн світу, що, в свою чергу, обумовлює нові завдання їх ЗС й виводить на перший план проблеми так званих інформаційних і кібервоєн та інформаційного протиборства. Серед 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 та підривних дій в інформаційному і кіберпросторах;

створення та застосування спеціальних сил і засобів негативного впливу на критично важливу інформаційну і кіберінфраструктуру;

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 тощо.

Комплекс захисних заходів, що дозволять користувачеві попередити такі дії, заблокувати НСД зловмисників до мереж і систем компанії або ж мінімізувати збиток, який може бути завданий, зобразимо такою схемою (рис. 1.18).

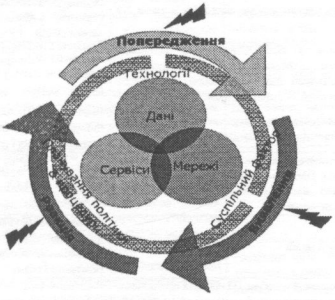


Рис. 1.18. Комплекс захисних заходів

Найбільш критичними серед них на сьогодні згідно з рекомендаціями американської ІТ-компанії "SANS" є двадцять основних заходів (рис. 1.18) [27], які за своєю суттю відповідають заходам захисту інформації, що в Україні в ході створення КСЗІ в ІТС регламентується системою нормативних документів з технічного захисту інформації (далі – НД ТЗІ, [9-22]). В табл. 1.5 наведено заходи захисту інформації (мереж і систем) від кіберзагроз, а також їх зміст відповідно до вимог Рекомендацій та вимог НД ТЗІ. При цьому показано, що заходи захисту інформації реалізуються шляхом впровадження відповідних функціональних послуг безпеки (далі – ФПБ) структура і семантичне позначення яких наведені в НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу".

Таблиця 1.5

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

№ з/п	Рекомендації американської IT-компанії "SANS" щодо захисту інформаційних ресурсів, мереж і систем від кіберзагроз		Зміст заходів захисту відповідно до вимог НД ТЗІ України
	Захід захисту	Зміст заходу	
1.	Інвентаризація дозволених для підключення пристроїв, а також пристроїв підключених не санкціоновано		Реалізація функціонального профілю безпеки (ФПБ) "Автентифікація отримувача" забезпечує захист від відмови від одержання і однозначно встановити факт одержання певного об'єкта певним користувачем
2.	Інвентаризація дозволеного до встановлення програмного забезпечення (ПЗ), а також ПЗ встановленого 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 установка систем, повинні бути попередньо налаштовані для забезпечення необхідного рівня захисту і протестовані	Реалізація ФПБ "Самотестування" дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ІТС
4.	Безпечне настроювання мережних пристроїв	Налаштовування міжмережевих екранів, маршрутизаторів, комутаторів і т.п.	Реалізація ФПБ "Самотестування" дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ІТС
5.	Захист периметра мережі	Забезпечуваний міжмережевими екранами, проксі, DMZ і системами IPS рівень захисту мережі має бути перевірений сканерами уразливостей	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 даної послуги ранжируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень
7.	Безпека прикладного ПЗ	Розроблене й придбане ПЗ має бути протестоване за допомогою автоматизованих засобів аналізу або ручного тестування на проникнення	Реалізація ФПБ "Самотестування" дозволяє комплексу засобів захисту інформації перевіряти і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій ІТС
8	Контроль використання адміністративних привілеїв	Проведення моніторингу використання й відслідковування 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 даної послуги ранжируються на підставі вибірковості керування можливостями користувачів і адміністраторів

Продовження табл. 1.5

е п	Рекомендації американської IT-компанії "SANS" щодо захисту інформаційних ресурсів, мереж і систем від кіберзагроз		Зміст заходів захисту відповідно до вимог НД ТЗІ України
	Захід захисту	Зміст заходу	
	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 адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування
0.	Постійний аналіз уразливостей й їхнє усунення	Впроваджування ефективних засобів для сканування, які дозволяють порівнювати отримані результати з результатами попереднього сканування для визначення змін, що відбулися	Реалізація ФПБ "Аналіз прихованих каналів" забезпечує виявлення та усунення потоків інформації, які існують, але не контролюються іншими ФПБ
1	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 даної послуги ранжируються залежно від кількості задіяних механізмів автентифікації
2.	Захист від шкідливого коду	Використовування адміністративних функцій або корпоративних систем забезпечення безпеки кінцевих точок з метою перевірки функціонування засобів захисту від шкідливих програм і системи IPS/IDS рівня хоста на всіх ПЕОМ мережі	
3.	Обмеження й контроль мережних портів, протоколів і служб	Відключення невикористовуваних служб і протоколів, блокування непотрібних для роботи портів, встановлення міжмережевих екранів рівня хоста для підвищення захисту	Реалізація ФПБ "Аналіз прихованих каналів" забезпечує виявлення та усунення потоків інформації, які існують, але не контролюються іншими ФПБ
4.	Захист і контроль бездротових пристроїв	Застосовування спеціалізованих ДЗ. Проведення сканування й моніторингу для виявлення працюючих бездротових мереж	Реалізація ФПБ "Конфіденційність при обміні" та "Цілісність при обміні" дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією або її модифікації, що міститься в них, під час їх експорту/імпорту через незахищене середовище
5.	Запобігання витоків даних	Використовування рішень DLP для виявлення спроб виводу критичних даних за межі мережі компанії, а також іншої підозрілої активності	Реалізація ФПБ "Аналіз прихованих каналів" забезпечує виявлення та усунення потоків інформації, які існують, але не контролюються іншими ФПБ

Продовження табл. 1.5

№ з/п	Рекомендації американської IT-компанії "SANS" щодо захисту інформаційних ресурсів, мереж і систем від кіберзагроз		Зміст заходів захисту відповідно до вимог НД ТЗІ України
	Захід захисту	Зміст заходу	
16	Забезпечення безпеки мережі	Застосовування кращих практик в області безпеки при проектуванні мережі, при настроюванні маршрутизаторів, комутаторів, критичних серверів, міжмережевих екранів, компонентів безпеки й груп клієнтських ПЕОМ	Реалізація ФПБ "Аналіз прихованих каналів" забезпечує виявлення та усунення потоків інформації, які існують, але не контролюються іншими ФПБ
17	Тестування на проникнення	Наслідування дій комп'ютерних зловмисників при визначенні границь 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) є обов'язковими етапами при створенні КСЗІ в ІТС. Вимоги до випробувань визначаються "Критеріями гарантій"
18	Організація реагування на інциденти	Періодичне проведення навчань й практичне відпрацьовування процедур реагування на інциденти на основі сценаріїв	Однією з обов'язкових умов створення та функціонування КСЗІ в ІТС є наявність служби захисту інформації в ІТС на яку покладаються питання організації та координації робіт, пов'язаних із захистом інформації в ІТС, підтримка необхідного рівня захищеності інформації та ресурсів ІТС
19	Організація можливостей відновлення даних	Впроваджування надійних і безпечних процедур резервного копіювання важливих даних	Реалізація ФПБ "Відкат" забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ранжируються на підставі множини операцій, для яких забезпечується відкат
20	Оцінювання навичок по безпеці, проведення необхідних тренінгів	Оцінювання знань і навичок співробітників з питань безпеки. При необхідності проведення додаткове навчання	Однією з функцій служби захисту інформації в ІТС є організація професійної підготовки та підвищення кваліфікації користувачів ІТС з питань захисту інформації, проведення заліків та контрольних перевірок

З метою адекватного і швидкого реагування на можливі інциденти у сфері високих технологій доцільно застосовувати так звану карту кіберзагроз (рис. 1.19), яка містить ключові елементи притаманні будь-якій кібератаці та дозволяє обрати раціональні варіанти дій для захисту від таких атак. Як приклад на рис. 1.19 подано три варіанта атак: викрадення банківських карток та фінансової інформації, APT-атаки та пошукова оптимізація (SEO). Головними умовами досягнення успіху при цьому є:

використання ліцензійного загального і спеціального, наприклад, антивірусного ПЗ з їх постійним (регулярним) оновленням;

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

"зменшення" прав процесів, які ініційовані виконавчими програмами у системі;

використання можливостей ОС щодо шифрування файлів і папок тощо.

У випадку фіксації порушень кібербезпеки на ОІД співробітникам служби безпеки компанії (організації, установі) необхідно [9, 32]:

1) ідентифікувати інцидент і переконатися, що він дійсно має місце бути;

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 консультації;

6) створити групу з розслідування інциденту, скласти план робіт зі збору доказів і відновлення систем та вести протокол подій;

7) забезпечити схоронність і належне оформлення доказів:

зняти енергозалежну інформацію з працюючої системи;

зібрати у реальному часі інформацію про інцидент;

відключити від мережі живлення;

8) у присутності третьої незалежної сторони зробити вилучення й опечатування носіїв інформації з доказовою базою, а також зняття образів та іншої інформації для її наступного аналізу і збереження:

оформити протоколом всі операції з носіями інформації;

задокументувати процес на фото- або відеокамеру;

провести детальний опис об'єктів з інформацією, даних, що витягаються, а також місць їхнього збереження;

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

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

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

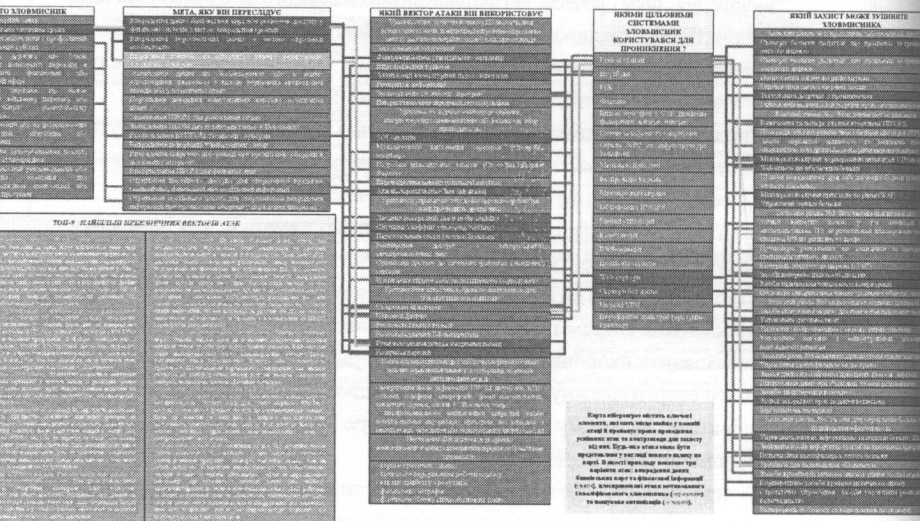


Рис. 1.19. Типова карта кіберзагроз

11) при проведенні розслідування забезпечити коректну взаємодію з зацікавленими підрозділами і зовнішніми організаціями;

12) по завершенні розслідування оформити відповідний звіт та скласти рекомендації зі зниження ризиків виникнення подібних інцидентів у майбутньому.

Окрім цього слід своєчасно налаштовувати ПЗ АРМ (РСт) та програми міжмережевого екрану (Firewall) для безпечного доступу до мережевих ресурсів Internet і ЛОМ, заборонити копіювання та запуск на виконання невідомих програм або програм, які були отримані з несертифікованих джерел, обмежувати права доступу користувачів до об'єктів файлової системи та запуску системних програм, керувати розмежуванням доступу тощо.

Це лише привентівні мірі. Чітких же правил поведінки при атаках кіберзлочинців на сьогодні на жаль не існує. Наприклад, Міжнародна організація по стандартизації тільки готовить новий стандарт ISO 27037 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence, який буде присвячений опису й систематизації процесу збору доказів під час розслідування комп'ютерних інцидентів. Саме тому найбільш пріоритетним напрямом керівництво України вважає нині реформування власної інформаційної безпеки, доктрина якої затверджена Указом Президента України №514/209 від 8 липня 2009 року. Одним з головних завдань доктрини визначено забезпечення конфіденційності, цілісності та доступності до інформації в державних інформаційних ресурсах шляхом створення надійної системи захисту людини, суспільства та держави у цілому від впливу внутрішніх і зовнішніх, навмисних та/або випадкових кібернетичних втручань і загроз та реагування на їх прояви. Останнє при цьому окрім відповідного нормативно-правового забезпечення [32] має включати низку організаційних та інженерно-технічних заходів. При цьому, наприклад, до основних напрямів удосконалення організаційного забезпечення системи кібернетичної безпеки України слід віднести [26]:

створення сприятливих зовнішньополітичних умов для прогресивного розвитку національного сегменту кіберпростору;

забезпечення повноправної участі України в загальноєвропейській та регіональних системах кібернетичної безпеки;

зосередження ресурсів і посилення координації діяльності правоохоронних, розвідувальних і контррозвідувальних органів України для боротьби у кіберпросторі з проявами організованої злочинності та кібертероризму;

забезпечення максимальної ефективності Збройних Сил у кіберпросторі та їх

здатності давати адекватну відповідь реальним і потенційним кіберзагрозам Україні;

посилення державної підтримки розвитку пріоритетних напрямів науки і техніки як основи створення високих інформаційних технологій;

забезпечення необхідних умов для реалізації прав інтелектуальної власності у національному сегменті кіберпростору;

створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури і ресурсів.

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

Останнім часом деструктивні інциденти у сфері високих технологій проводяться протиборчими сторонами, як відомо [1], з метою:

порушення або блокування роботи інформаційних систем (ІС) і мереж стратегічно важливих галузей (об'єктів) інфраструктури, в тому числі фінансового, енергетичного, промислового, транспортного та військового секторів;

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

Нині, як стверджують західні експерти, такі дії на кшталт різного роду кібератак (КбА), несанкціонованого доступу (НСД) до чужих сайтів, створення «сайтів-двійників» тощо – вийшли за межі окремих країн й за темпами росту випереджають всі інші види організованої злочинності. Більш того, за останні 5 років вони набули істотну фінансову підтримку та якісні комунікації й, до того ж, розповсюдились на всі види злочинів, учинених в ІТ сфері [1]. Тим не менш чіткого визначення цих понять й передусім такого поняття, як «кібератака» не існує. Враховуючи таке проведемо аналіз існуючих підходів до його трактування. Так, наприклад:

В. Харченко із співавторами у роботі [2, 33] визначає КбА як заходи, що здійснюються для підриву безпеки систем чи реалізації загрози характеристикам безпеки ресурсам ІС шляхом використання їх уразливостей;

автори Д. Дубов та М. Ожеван як КбА кваліфікують цілеспрямовані дії, що реалізуються в КбП (або за допомогою його технічних можливостей), та 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 з метою пошуку та використання кібернетичних уразливостей інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем [2, 35];

відповідно до роботи С. Мельника, О. Тихомирова та О. Лєнкова [2, 7] КбА – це використання технічних недоліків механізмів безпеки сучасного кіберпростору з метою дезорганізації роботи його елементів тощо

Узагальнюючи опрацьований матеріал, можна сформулювати таке визначення цьому поняттю: **кібератака** це *сукупність узгоджених за метою, змістом і часом дій або заходів* – так званих кібератакцій, *спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережності та/або авторства циркулюючої в ньому інформації з урахуванням її уразливостей, а також порушення роботи його IT систем та мереж* [1]. Нині достеменно невідомо, скільки видів кібератак та методів їх застосування до цього часу розробило людство [1]. Комплексні статистичні дослідження з цього приводу на жаль не проводились. Але ще у 1984 році Фред Коен (F. Cohen) у своїй роботі "Computer Viruses: theory and experiments", описуючи математичні основи вірусної технології, довів, що оскільки кількість злоякісних кодів, які є підмножиною множини кібератак, нескінченна, то й кількість самих атак, загальну структуру яких подано на рис. 1.20, є також нескінченна.

Характерною особливістю кібератак є проведення їх в обмежені терміни (протягом секунд, хвилин тощо). Виходячи з такого їх класифікують за такими ознаками:

1) за метою впливу на об'єкт атаки, що може бути спрямований, наприклад, на порушення цілісності (integrity) або конфіденційності (confidentiality) інформації, її захищеності від несанкціонованого доступу (authentication), а також забезпечення живучості (survivability) системи та надійності (availability) її функціонування. Закордонний і вітчизняний досвід показує, що для вирішення цих завдань використовують методи криптографії в поєднанні з перевіреним і ліцензованим програмним забезпеченням (ПЗ), а також надійні інтелектуальні носії важливої інформації (матеріал ключа). При цьому саме живучості (здатності системи вчасно виконувати свої функції в умовах фізичного руйнування, часткової втрати ресурсів, відмов і збоїв елементів, несанкціонованого втручання в систему управління), яка визначає мобілізаційну 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, приділяють останнім часом найбільшу увагу;

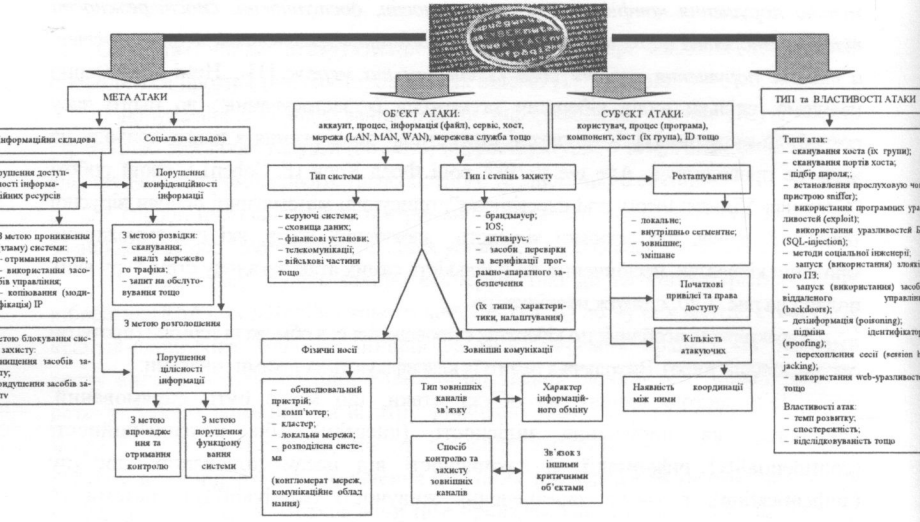


Рис. .1.20. Загальна структура кібернетичної атаки

2) за принципом впливу на об'єкт атаки:

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

використання 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 саме на систему в цілому; на дані і програми, що знаходяться на зовнішніх (дисководи, мережеві пристрої, термінали) або внутрішніх (оперативна пам'ять, процесор) пристроях системи, а також у каналах передачі 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 шляхом перехоплення пакетів на ретрансляторі мережі, або ж прослуховування з використанням прихованих каналів;

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

Зважаючи на те, що нині переважну кількість кібератак на практиці не застосовують, більш життєздатною вважається класифікація, запропонована компанією Internet Security Systems Inc. Скоротивши число можливих категорій кібератак до п'яти, фахівці компанії умовно поділили їх на такі, що:

1) сприяють збору інформації (Information gathering);

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

3) сприяють відмові в обслуговуванні (Denial of service);

4) імітують підозрілу активність (Suspicious activity);

5) забезпечують вплив на операційні системи (System attack).

За міркуваннями фахівців компанії перші чотири категорії відносяться до вилучених (можливо віддалених) кібератак, а остання – до локальних (реалізується на вузлі, що атакується). Разом з тим всі вони можуть бути як автоматизованими, так і неавтоматизованими (рис. 1.21).

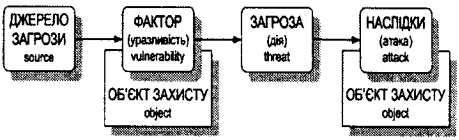


Рис. 1.21. Механізм формування кібератаки

При цьому об'єктами їх впливу можуть виступати системи і канали зв'язку, канали передачі даних, АРМ (РСт) – тобто системи, що знаходяться у взаємодії з інформаційним середовищем. Суб'єктами – джерела несанкціонованих дій (рис. 1.22), спрямованих на об'єкт кібератаки.

Рис. 1.22. Джерела НСД

Найбільш розповсюдженим видом кібератак за висновками Ф.Коена та інших незалежних експертів нині є комп'ютерні віруси. На відміну від інших П.Нойман [36] пропонує сконцентрувати увагу на двадцяти шести типах таких дій (табл. 1.6).

Таблиця 1.6

Основні типи кібернетичних атак згідно класифікації П.Ноймана

Тип атаки		Спосіб здійснення	Результат
Зовнішні		Візуальне спостереження	Спостереження за клавіатурою або монітором
		Омана	Омана операторів або користувачів
		Вилучення сміття	Вилучення інформації із 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 привілей, 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 розповсюдженими способами їх здійснення він вважає sniffer пакетів та IP-спуфінг, DoS і DDoS атаки, парольні атаки, атаки на рівні додатків типу логічних бомб і троянських коней, вірусні атаки та так звані Ін'єкції (табл. 1.7).

Таблиця 1.7

Основні способи здійснення кібернетичних атак

Type of attack	Description
Denial of service	Атака з поодинокого джерела. Блокує авторизованим користувачам доступ до того або іншого комп'ютера-жертви шляхом "переповнення" легального трафіку зовнішніми повідомленнями
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"
Exploit tools	Привселюдно доступні засоби проникнення в системи різного рівня складності з метою пошуку в тій або іншій кіберсистемі уразливих місць і одержання доступу до комп'ютера-жертви
Logic bombs	Форма саботажу, коли програміст уводить спеціально сконструйований код, що викликає деструктивну роботу виконуваної програми, у тому числі її повне припинення

Продовження табл. 1.7

Type of attack	Description
Phishing	Створення й подальше використання спеціальних електронних повідомлень і web-сайтів подібних легальним, що є добре відомими користувачам. Використовується з метою дезорієнтації користувачів, провокування їх до розкриття своїх персональних даних
Sniffer	Програма, що перехоплює й фільтрує інформаційний трафік, вишукуючи в ньому спеціальну інформацію про користувача, наприклад, передані паролі
Trojan horse	Комп'ютерна програма, що містить неявні шкідливі коди. Трояни за звичай маскуються під звичайні корисні програми, які користувач може використовувати
Virus	Програма, що інфікує комп'ютерні файли шляхом включення до них спеціальних команд. Ці команди виконуються, як правило, при завантаженні інфікованого файлу в оперативну пам'ять комп'ютера. На відміну від комп'ютерних "черв'яків", розмноження вірусів вимагає втручання (хоча найчастіше й неусвідомленого) людини-користувача
Vishing	Різновид фішинга, який використовує дешеві Internet-технології для передачі звукових (у тому числі голосових) файлів. Дає можливість шахраям створювати власні телефонні "колцентри" і звідти (від імені легальних користувачів) посилати потенційним жертвам голосові або електронні повідомлення з проханням виконати певні деструктивні дії
War driving	Метод одержання несанкціонованого доступу до комп'ютерних мереж, що використовують ноутбуки. Для виходу в Internet застосовує антени і бездротові мережеві адаптери, що містять контрольовані локатори
Worm	Незалежні комп'ютерні програми, що поширюються за допомогою копіювання по Internet самих себе з одного комп'ютера в інший. На відміну від комп'ютерних вірусів, черв'яки не вимагають для свого розмноження втручання людини
Zero-day exploit	Спосіб випередження кіберзахисту. Загроза реалізується того самого дня, коли громадськості стає відомо про наявність у системі безпеки уразливих місць, що не мають

При цьому, наприклад, **сніфер пакетів** – програма, яка використовує мережевий інтерфейс, функціонує у так званому нерозбірливому (promiscuous mode) режимі, перехоплює мережевий трафік, призначений для інших вузлів та здійснює його подальший аналіз (рис. 1.23). Результати застосування програми дають можливість: виявити паразитний, вірусний і закільцьований трафік; виявити в мережі шкідливе і несанкціоноване ПЗ (мережеві сканери, флудери, троянські програми тощо); перехопити будь-який, призначений для користувача, незашифрований, а деколи і зашифрований трафік з метою отримання паролів та іншої інформації; локалізувати несправність мережі або помилку конфігурації мережевих агентів).

Для зниження загрози сніффінгу пакетів потрібно вживати таких заходів:

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

створити комутуючу інфраструктуру (у разі використання комутуючого Ethernet протоколу це дозволить хакерам отримати доступ лише до трафіка, що поступає на порт, до якого вони підключені);

встановити антисніфери або ПЗ, що розпізнають сніфер пакетів, функціонуючий у визначеній 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 sniffer пакетів. Якщо канал зв'язку є криптографічно захищеним, то хакер перехоплює не повідомлення, а зашифрований текст (тобто незрозумілу послідовність бітів).

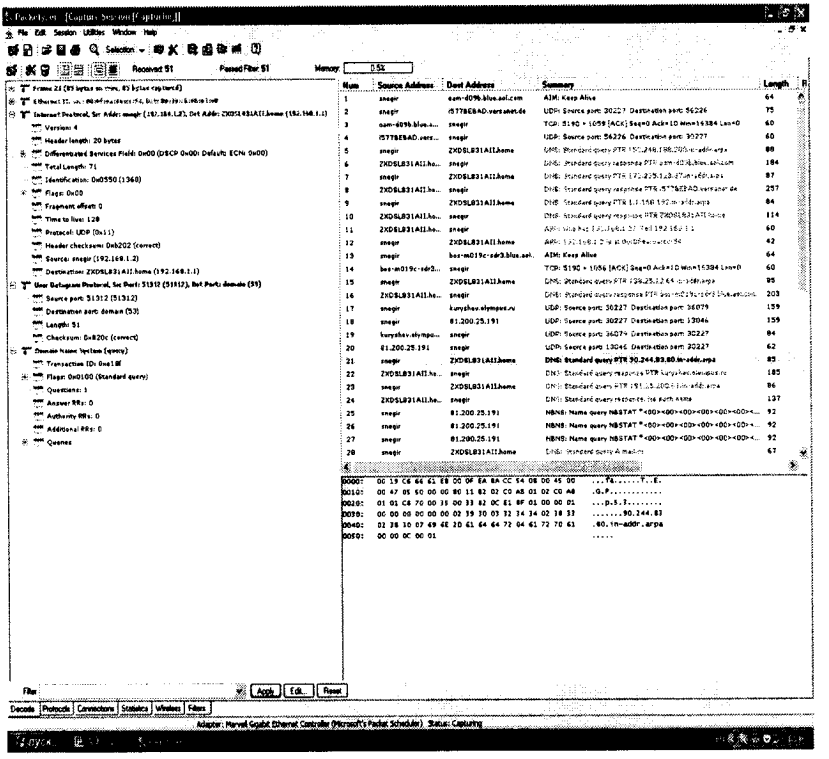


Рис. 1.23. Інтерфейс програми-сніфера Network Chemistry Packetyzer

IP-спуфінг (spoof – обман, містифікація, підроблення) – вид хакерської атаки (рис. 1.24) з якою використання чужої IP-адреси, тобто введення в оману системи безпеки або приховування реальної адреси атакуючого для того, щоб відправити/надіслати відповідний пакет на потрібну адресу чи атакованого (зловмисник, який перебуває всередині корпорації/установи або поза нею, видає себе за санкціонованого користувача). Часто використовується як складова частина комплексної атаки. Типовий приклад – DDoS атака, для здійснення якої хакер розміщує відповідну програму за чужою IP-адресою, щоб приховати власну.

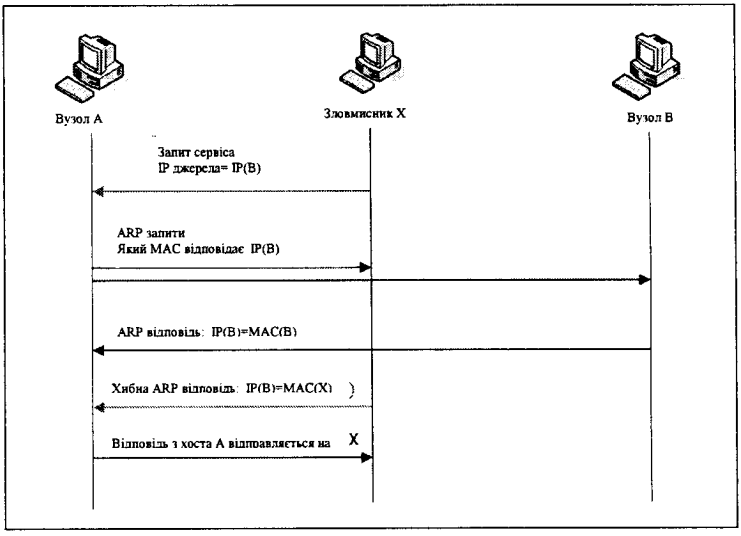


Рис. 1.24. Застосування IP-спуфінгу для отримання НСД до ресурсу

Послабити загрозу IP-спуфінгу, а кібератаку зробити абсолютно неефективною можна завдяки:

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

застосуваннюя фільтрації RFC 2827 (передбачає заборону будь-якого трафіка, вихідна адреса якого не є однією з IP-адрес певної установи);

упровадженню додаткових заходів аутентифікації, а саме створенню системи криптографічного захисту.

Відмова в обслуговуванні (Denial of Service – DoS) – атака на комп'ютерну систему з метою зробити комп'ютерні ресурси/мережу недоступними для користувачів внаслідок перевищення припустимих меж функціонування мережі, операційної системи або додатка; підвищення витрат ресурсів процесора та зменшення пропускної можливості каналу зв'язку (рис. 1.25). Найвідомішими різновидами DoS атак є такі: Flood, ICMP flood, Identification flood, TCP SYN flood, Ping of Death, Tribe Flood Network, Trinco, Stacheldracht, Trinity та багато інших. Серед них лише атаку TCP SYN flood, що полягає у надсиланні великої кількості запитів на ініціалізацію TCP-з'єднань з вузлом-мішенню, якому в результаті доводиться витрачати всі свої ресурси на те, щоб відстежувати ці частково

відкриті з'єднання, – фахівці відзначають найбільш ефективною. Вона є найвідомішим способом переповнення інформаційного каналу SYN-пакетами, внаслідок якого сервер не відповідає на запити користувачів.

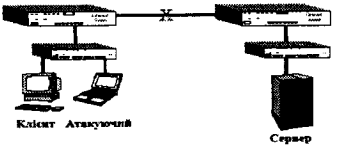


Рис. 1.25. Схема DoS атаки

Під час Flood ("затоплення") та ICMP flood (flood ping – "потік пінгів") атак на систему надсилається відповідно велика кількість ICMP (найчастіше) або UDP-пакетів, які не несуть корисної інформації та так званих ехо-запитів ICMP (пінг системи). У результаті відбувається зменшення перепускної смуги каналу, незначне завантаження комп'ютерної системи аналізом "сміття", що надійшло, та генерацією на нього відповідей (довідково: ICMP-пакети не аналізуються системою за умовчанням, а відповіді на них не займають багато CPU-time). Атака Identification flood (запит ідентифікації системи) 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). Зважаючи на те, що аналіз цих запитів і генерування на них відповідей потребують більше процесорного часу, ніж при пінгах, така атака вважається більш ефективною. Результатом атаки Ping Of Death є зависання ОС системи, включаючи мишу й клавіатуру. Це, як правило, є відповіддю системи на надходження сильно фрагментованого ICMP пакету великого обсягу (64Kb). На даний час майже не використовується. UDP flood (User Datagram Protocol) та TCP flood атаки полягають у відправленні на адресу системи-мішені безлічі пакетів UDP та TCP, що призводить до "зв'язування" мережевих ресурсів. На сьогодні вони вважаються найменш небезпечними. Це пояснюється їх легким виявленням зважаючи на застосування при обміні пакетами головного контролера й агентів нешифрованих протоколів TCP і UDP.

Загрозу DoS атак можна послабити у результаті:

правильної конфігурації на маршрутизаторах і міжмережевих екранах функцій антиспуфінга (впровадження фільтрації RFC 2827) та функцій антиDoS;

обмеження обсягу некритичного трафіка (non-critical traffic – визначає імовірність того, що мережа зв'язку відповідає заданому та узгодженому трафіку), що проходить мережею. Типовим прикладом такого є обмеження обсягів трафіка ICMP, що використовується тільки для діагностичних цілей.

Розподілена DDoS атака (Distributed Denial of Service) – це підтип DoS атаки,

що здійснюється одночасно з великої кількості IP-адрес (комп'ютерів) на систему об'єкта атаки та має за мету зробити мережу недоступною для звичайного використання (рис. 1.26). Для цього створюються так звані ботнети (інакше бот-мережі або зомбі-мережі) із групи заражених шкідливими програмами комп'ютерів, які одночасно надсилають запити до ресурсу, що атакується (рис. 1.27). У результаті сервер не справляється з навантаженням, і доступ до атакованого ресурсу ускладнюється або взагалі стає неможливим.

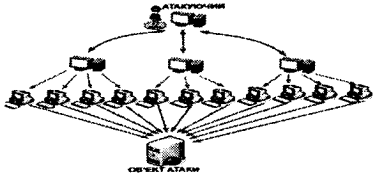


Рис. 1.26. Схема DDoS атаки

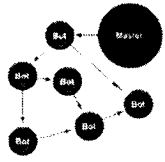


Рис. 1.27. Загальна схема організації бот-мережі

Найбільш відомими різновидами DDoS атак є TCP SYN flood (рис.1.28), TCP flood (рис. 1.29), SYN flooding, UDP flood, Smurf та ICMP flood атаки. При цьому найнебезпечнішими є програми, що використовують одночасно кілька видів описаних атак, наприклад, TFN і TFN2K .

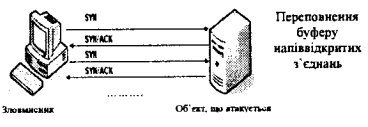


Рис. 1.28. TCP SYN flood атака

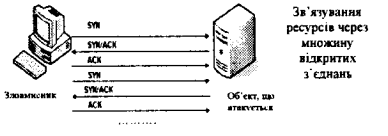


Рис. 1.29. TCP flood атака

Для створення програм у хакера має бути високий рівень підготовки. Однією з останніх програм для організації DDoS-атак є Stacheldracht, що дозволяє організовувати всілякі типи атак і лавини широкомовних ping-запитів із шифруванням обміну даними між контролерами й агентами. З погляду інформаційного захисту, DDoS-атаки є однією з найскладніших мережевих загроз, тому вживання ефективних заходів протидії є винятково складним завданням для організацій, діяльність яких залежить від Internet. Основними методами протидії DDoS атакам є такі:

профілактика причин, що спонукають тих або інших осіб організовувати DDoS атаки. Дуже часто атаки є наслідками особистої образи або політичних, релігійних розбіжностей;

розосередження або побудова розподілених і резервних систем, які не

припинять обслуговувати користувачів, навіть якщо деякі їхні елементи стануть недоступними;

фільтрація трафіка на маршрутизаторах (міжмережеві екрани та спеціалізовані antiflood засоби фільтрації – найбільш ефективний, але й найбільш дорогий метод. За можливості їх встановлюють 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 піддаються впливу разом з безпосередньою ціллю;

нарощування ресурсів системи (якщо flood спрямований на вичерпання ресурсів, то примітивнішим 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:

сканери портів – збирають інформацію, що передається мережею, через відповідний принтерний, модемний або інший порт комп'ютера (найбільш відомою серед них є, наприклад, програма Neo Trace);

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

модемні та мережеві кіберрозвідники – автоматично записують телефонні розмови у режимі диктофона, програвання записів 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, встановленої на ПЕОМ, обсяг пам'яті та процесор, здійснюють моніторинг адрес електронної пошти, відстежують масиви інформації, передані всередині мережі, відвідувані сайти та інформацію з них, а також розділи, які викликають інтерес у користувачів.

Алгоритм реалізації КбА подано на рис. 1.30.

Останнім часом складність кібератак, а також їх кількість і частота поступово збільшується. Свого апогею вони досягли нині у глобальній мережі Internet [37–43], яка з часом почала впливати на розвиток усієї планети та стала незамінним депозитарієм загальнолюдського знання. За нинішніх умов Internet взагалі може бути як предметом (метою) злочинних посягань та середовищем, в якій скоюються правопорушення. За висновками, зробленими експертами з дослідницького

інституту *United States Institute for Peace* (*USIP*), саме *Internet* на сьогодні є «… ідеальним середовищем для діяльності терористів …». Це пояснюється тим, що доступ до цієї глобальної мережі надто легкий. В ній «… надзвичайно легко забезпечити анонімність користувачів …», вона «… ніким не управляється і не контролюється …», у ній «… не діють закони та не існує поліції …» [44].

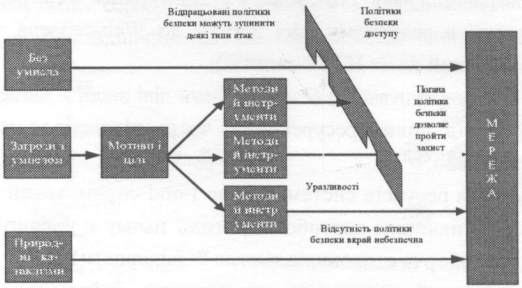


Рис. 1.30. Алгоритм реалізації кібератаки

Підтвердженням такому висновку стали результати досліджень Institute for Security Technology Studies At Dartmouth College (США) [45], метою яких було прогнозування ситуації в Internet у результаті 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", опублікованого 22 вересня 2001 року, фахівцями інституту були проаналізовані політичні конфлікти, що стимулювали зростання кількості атак на ресурси Internet, а саме конфлікти між Індією й Пакистаном, Ізраїлем і Палестиною, NATO і Сербією, США та Китаєм тощо. Фахівці інституту, як наслідок, констатували, що фізичні атаки на елементи критично-важливої інфраструктури провідних країн світу супроводжуються останнім часом обов'язковим зростанням кількості кібератак, перш за все на сервери та активне мережне устаткування, що підключене до цієї глобальної мережі. Представники інституту System Administrator and Network Security (США) та Центру із захисту національної інфраструктури при ФБР (США) взагалі зробили спільну заяву про те, що здійснення кібератак поступово стає потужним засобом ведення інформаційних воєн між державами, а Internet за їх розумінням – потужним "інструментом кіберпланування" [46], який забезпечує сучасним терористам анонімність, можливість управляти і координувати дії при підготовці та здійсненні терактів. Тобто, за твердженням [44–46] та інших фахівців, тероризм останнім часом зробив якісний крок у своєму розвитку й еволюціонує у напрямку, який можливо назвати "мережною війною" (netwar). Підтвердженням такому є вислів директора

ЦРУ Леона Панетта який вважає, що для США «майбутній Пірл-Харбор, скоріш за все, буде комп'ютерною атакою». За його думкою цьому не в останню чергу сприятиме (рис. 1.31):

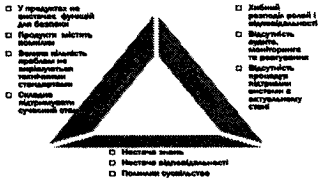


Рис. 1.31. Фактори, що впливають на інформаційну безпеку

стрімкий розвиток глобальної мережі Internet, що з часом стала незамінним депозитарієм людського знання і на цей час налічує понад 550 мільярдів документів, розміщених більш ніж на 39 мільйонах серверів, поєднуючи при цьому понад мільярд користувачів;

поява можливості високошвидкісного бездротового доступу зловмисників до всього спектра існуючих і перспективних послуг мережі Internet за доступними цінами й у будь-якій точці світу за рахунок використання WiMAX, 4G й інших сучасних IT-технологій;

небувалий сплеск виходу на світовий ринок злоякісного програмного забезпечення (троянських програм всілякого призначення, вірусних програм для смартфонів, комунікаторів і КПК, великої кількості вірусних програм для операційних систем Linux, Mac OS тощо) та можливість здійснення з його допомогою електронних нападів;

поява нових та вдосконалювання 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 тощо.

Необхідно відзначити, що тероризм є постійним супутником людства. Ще у I столітті нашої ери в Іудеї діяла секта сикаріїв (сика – кинджал або короткий меч), що знищувала представників єврейської знаті, які співробітничали з римлянами. У середні віки представники мусульманської секти ассошафінів убивали префектів і каліфів. У ці ж часи політичний терор практикували деякі таємні суспільства в Індії та Китаї. На територіях сучасного Ірану, Афганістану й деяких інших країн звірячий страх на своїх супротивників з мусульманської сунитської знаті та правителів наводила могутня й гранично закрита секта ісмаїлітів, що використовувала у своїй боротьбі доведені до досконалості

способи фізичного усунення неугодних осіб. Нині терористичні дії спрямовують не лише проти певних індивідуумів з політичних міркувань, а й проти цивільних і військових об'єктів з метою підриву економічної безпеки або обороноздатності противника. При цьому діяльність сучасних терористів характеризує:

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

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

3) спроможність ефективного використання конфліктних і кризових ситуацій у своїх цілях (впровадження в поточну політичну кон'юнктуру проявів інформаційного тероризму).

Такий стан справ у свою чергу призвів до появи принципово нового різновиду терористичних дій у віртуальному просторі, який кінець-кінців отримав у ЗМІ загальну назву – **кібертероризм** (КбТ). Власне як термін це поняття в ІТ лексиконі з'явилось приблизно у середині 80-х років. Саме тоді одним із наукових співробітників США Беррі Коліном він був вперше уведений 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 і дані, виражені у застосуванні насильництва відносно до цивільних цілей з боку субнаціональних груп або тайних агентів". У 1998 році біля половини із 30 терористичних організацій, внесених США в список «Іноземних терористичних організацій», мали власні Web-сайти, до 2000 року практично всі терористичні групи виявили свою присутність у мережі Інтернет. Протягом 2003-2004 років було виявлено біля 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, так характеризує ситуацію, що склалася сьогодні: "... у світі сформувалась нова форма тероризму – *кібертероризм*, який використовує комп'ютер та мережі зв'язку для руйнування частин національної інфраструктури та досягнення власних цілей" [47].

Але на порядку денному світового співтовариства проблема КбТ постала лише після 2010 року, коли в Іранському Центрі по збагаченню урану був виявлений вірус «Stuxnet», що привело до виходу з ладу ядерних центрифуг (розділ 1.1 підручика). Якщо раніше питання безпеки в Інтернеті зводилися, переважно, до захисту особистої інформації й 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 стали розуміти, що і їхні внутрішні об'єкти можуть бути піддані небезпеці. У

результаті цього почалося активне обговорення, які форми може приймати *кібертероризм*, які існують методи боротьби з ним і яким може бути міжнародне співробітництво в цій сфері, щоб знизити можливі ризики.

Відповідно до Конвенції Ради Європи 2001 року по кіберзлочинам засобами кібертероризму є: комп'ютерна система, комп'ютерні дані, послуги ТКС, а також дані трафіку. Збиток від їх застосування в основному може бути зв'язаний з:

1) людськими жертвами або матеріальними втратами, викликаними деструктивним використанням елементів мережної інфраструктури;

2) можливими втратами (у тому числі загибеллю 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, викликаними діями по її руйнуванню або ушкодженню;

4) моральним збитком як власника мережної інфраструктури, так і власного інформаційного ресурсу;

5) іншими можливими втратами від несанкціонованого використання інформації з високим рівнем таємності.

Тим не менш й до цих пір чіткого визначення такого поняття як «кібертероризм» не існує. Враховуючи таке проведемо аналіз існуючих підходів до його трактування. Так, наприклад [2]:

1) переважна кількість науковців, а саме 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 вважати виключно використання компонентів КбП у якості засобів або середовища для реалізації терористичних дій (Instrument). У їх визначеннях присутні усі ознаки традиційного тероризму, реалізованих за допомогою сучасних інформаційних та комунікаційних технологій (це класичний випадок КбТ = «тероризм» + «КбП»);

2) певна частина науковців, а саме В. Голубєв, М. Політ, Д. Деннінг, В. Пилипчук, О. Дзьобань, Ю. Гаврилов та Л. Смирнов притримуються думки, що КбТ – це дії, пов'язані з використанням елементів КбП як предмету (Subject) злочинних посягань, які реалізуються шляхом різного роду КбА та спрямовані на нанесення шкоди конкретним об'єктам критичної інформаційної інфраструктури з певних характерних тероризму мотивів);

3) у роботах К. Колмена, С. Мельника, О. Тихомирова, О. Федорова та Є. Роговського чітко прослідковується гіпотеза про те, що терористичні угруповання використовують КбП перважно у суміжних цілях (AdjTarget) – з метою зв'язку із суспільством, проведення інформаційно-психологічного впливу, створення

пропагандистських сайтів, збирання необхідної для реалізації терактів інформації засобами Інтернет;

4) деякі із відомих авторів у своїх роботах [37, 42, 43, 47] під КбТ взагалі розуміють синтез дій, визначених зокрема у пп. 1 та 2 – це О. Корченко, Дж. Левіс, Д. Малишенко, К. Керр, С. Гавриш та К. Вілсон.

Ґрунтовний аналіз існуючих визначень терміну КбТ дав можливість сформувати таблицю 1.8 та констатувати, що жодне із них одночасно усі вказані у таблиці критерії не задовольняє.

Таблиця 1.8

Багатокритеріальний аналіз визначень поняття КбТ

№	Дефініція	Базовий критерій		
		Instrument	*Subject*	*AdyTarget*
1.	В. Харченко, О. Корченко та ін.	+	-	-
2.	О. Корченко та ін.	+	+	-
3-4	В. Голубєв	-	+	-
5.	М. Погіт	-	+	-
6.	О. Довгань та В. Хлань	+	-	-
7.	К. Кольєн	-	+	+
8.	Націон. центр захисту інфраструктури США	+	-	-
9.	Д. Деннінг	-	+	-
10.	Дж. Левіс	+	+	-
11.	Ю. Трявінков	+	-	-
12.	Націон. конф. державної законотворчості, США	+	-	-
13.	О. Клімчук 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. Пістинчук та О. Дьяобань	-	+	-
22.	М. Девост, Б. Хьютом та Н. Похлард	+	-	-
23.	Ю. Гавриков та Л. Сьєрчиков	-	+	-
24.	К. Вілсон	+	+	-
25.	Є. Рогозинський	+	-	+

З огляду на це варто сформулювати таке ґрунтовне визначення поняття КбТ. **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 сплановані й політично вмотивовані кібератаки на ІТС з використанням високих технологій* (рис. 1.32).

Рис. 1.32. Індустрія сучасного кібертероризму

Спектр прояву КбТ достатньо широкий – від прийняття хибних рішень або розповсюдження паніки, до проникнення в канали і системи зв'язку та навігації тощо. Його результатом може бути, наприклад, введення хибного IP або порушення цілісності існуючого, дезорганізація роботи критично важливих елементів інформаційної та/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. До його основних особливих рис нині відносять:

високу ефективність кібератак;

просторово-часову невизначеність джерела кібератаки та його віддаленість від об'єкта атаки;

часову невідповідність між власне кібератакою й процесом її підготовки; можливість організації складних кібератак одночасно на різні ІТС з різних напрямів тощо.

Виступаючи з проблем світових загроз директор ЦРУ США Джордж Тенет зробив заяву, що кібертероризм, розповсюджуючись світом, може з часом набути значно більших ніж очікувалося масштабів й, як результат, стати реальною загрозою для національної безпеки будь-якої держави. За його твердженням вже зараз більшість терористичних угруповань на кшталт Hizbollah, HAMAS, the Abu Nidal organization і Bin Laden's al Qa'ida («Аль-Каїда») та інших ним подібних структур, для підтримки своєї протиправної діяльності використовують останні досягнення інформаційних технологій та комп'ютерного прогресу – "…комп'ютерні файли, електронну пошту і шифрування (криптографію та стеганографію) …". Підтвердженням такому є той факт, що на сьогодні абсолютно всі відомі терористичні групи публікують власні матеріали щонайменше на 40 різних мовах та у своїй діяльності застосовують здебільшого такі прийоми, як [48, 49]:

завдання збитків окремим елементам інформаційного та кіберпростору;

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

крадіжка або знищення інформаційних, програмних і технічних ресурсів інформаційного та кіберпростору, що мають суспільну значимість шляхом подолання їх систем захисту, впровадження вірусів та різного роду закладок;

вплив на програмне забезпечення та інформацію з метою їхнього перекручування або модифікації;

розкриття та загроза опублікування або власне саме опублікування закритої інформації про функціонування інформаційної інфраструктури

держави, суспільно значимі військові інформаційні системи, коди шифрування та принципи роботи шифрувальних систем;

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

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

проведення інформаційних і психологічних операцій тощо.

Найбільш характерним прикладом "продуктивної роботи" кібертерористів нині вважають так званий кіберджихад, який ведуть один проти одного хакери Пакистану та Індії за Кашмір [44, 50]. Пакистанські хакери зламують Web-сайти індійських державних установ. У свою чергу, індійська хакерська група (Indian Snakes) у якості "віртуальної помсти" поширює мережевий черв'як "Yaha-Q". Головне завдання цього вірусу полягає у здійсненні DDoS атак на деякі пакистанські ресурси, серед яких – Internet-провайдери, сайт фондової біржі в Карачі та урядові ресурси. Ще одним досить відомим прикладом є 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, наприклад, 6 жовтня 2000 року було уражено 40 ізраїльських сайтів і принаймні 15 палестинських. Програмний засіб проведення розподілених атак з відмовою в обслуговуванні став головним інструментом, використовуваним ізраїльтянами. Пропалестинські хакери за можливості руйнували будь-який тип ізраїльських сайтів, змінюючи їхній зміст повідомленнями під рубрикою "За вільну Палестину" або "Вільний Кашмір". Організація "Hezbollah" взагалі виробила цілу стратегію завдання збитків ізраїльському уряду, його військовим і діловим колам [54]. Першою фазою, на думку лідерів "Hezbollah", повинна стати дестабілізація урядових органів Ізраїлю. Друга буде сконцентрована на краху фінансових інститутів. А в ході третьої та четвертої – має відбутися 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. Перш за все це пояснюється тим, що зазначений різновид кіберзагроз не має державних кордонів, а його потенційні представники здатні рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі. Разом з тим наведені приклади дають можливість зробити висновок про те, що сучасний тероризм еволюціонує у напрямку, який нині можна назвати "мережевою війною".

Нині тероризм у мережі Інтернет взагалі вийшов на якісно новий рівень – здійснення кібератак під неформальною егідою й при фінансуванні провідних держав світу, спрямованих проти політичних режимів окремих країн або на збір персональних даних громадян. Нещодавно, переважно завдяки світовим ЗМІ, стало відомо про програми секретних служб Великобританії – Центра урядового зв'язку (UK Government Communications HeadQuarters) під кодовою назвою «Tempora», а також про програму Агентства національної безпеки (АНБ) США «Prism», ініційованих президентами Дж. Бушем і Б. Обамой. Зазначені програми спрямовані на стеження за громадянами будь-яких країн світу за допомогою всесвітньої мережі Інтернет. Зокрема, програма британських спецслужб «Tempora» спрямована на збір і передачу в США даних, переданих через 46 трансатлантичних ліній, і розрахована на обробку щодня біля 20 петабайт інформації. До відома, всі архіви Інтернету, за станом на кінець 2012 р., становлять 10 петабайт даних. Факт стеження за іноземними громадянами в рамках програми «Prism» визнав навіть глава національної розвідки АНБ США Джеймс Клеппер. Так, відповідно до «Prism», найбільші світові Інтернет-компанії (у т.ч. 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. Мова йде 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 [*чит. Проект постанови «Про створення Тимчасової спеціальної комісії Верховної Ради України з питань з'ясування рівня загрози для національної безпеки України, що являють собою програми по збору й пошуку даних, які застосовуються спеціальними службами США» від 24.07.2013 №3020*]. Крім того, американські спецслужби мають можливість відслідковувати транзакції по кредитних картках, електронній переписці, інформацію про підключення користувачів до тих або інших сайтів, дані мобільного зв'язку. Крім Інтернет-корпорацій, у програмі «Prism» задіяний і такий відомий виробник комп'ютерної техніки, як американська компанія «Dell». З цією метою АНБ США використовує програму інтелектуального аналізу даних «Bovndtess informant» призначену для систематизації даних про країни, у яких ведеться «електронне стеження». Завдяки даній програмі була створена цифрова карта із вказівкою країн-об'єктів для електронної розвідки. Судячи із цієї карти, активніше всього спецслужби діють в тому ж таки Ірані, Пакистані та Йорданії.

Кібертероризм, як головна складова ***кіберзлочинності***, займає 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 жодної уяви;

3) темпи комп'ютерізації (кількість комп'ютерів в Україні щорічно зростає приблизно у 1,5–2 рази) та збільшення кількості користувачів Internet (з 500 тисяч у 2000 році до 5 мільйонів 800 тисяч – у 2005).

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

недостатню увагу з боку державних органів до проблем інформатизації, незважаючи на потенційну економічну рентабельність національного сегменту Internet;

відсутність достатньої державної фінансової підтримки фундаментальних і прикладних вітчизняних досліджень у сфері попередження і боротьби з кіберзлочинністю;

відставання вітчизняного законодавства в інформаційній галузі від розвинутих 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 БД;

посилення можливостей для негативного інформаційного впливу на людину, суспільство і державу за допомогою нових комп'ютерно-телекомунікаційних засобів і технологій, що постійно розвиваються і поширюються;

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

Враховуючи це пріоритетним напрямом для керівництва України на сьогодні є організація взаємодії і координація зусиль правоохоронних органів, спецслужб і судових органів передусім СБ та Служби зовнішньої розвідки (СЗР) України, ДССЗЗІ та МВС України, спрямованих на забезпечення безпеки національного інформаційного простору, здійснення заходів з кіберзахисту власної ІТ-інфраструктури та протидію внутрішнім і зовнішнім кібернетичним загрозам. Тим не менш 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, яке призначено для обробки зібраної інформації тощо) в

умовах інтенсифікації діяльності кіберзлочинців Україні з дня на день стає все важче. Цьому в першу чергу сприяє:

складність організації захисту міжмережевої 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 з сучасних мережевих протоколів;

наявність помилок у конфігурації систем і засобів забезпечення безпеки, "економія" або взагалі повне ігнорування необхідності їх впровадження тощо.

Саме це пояснює ефективність кібератак, майже кожна з яких досягає очікуваного результату та робить надзвичайно актуальними завдання як їх виявлення, так і попередження їх наслідків. Головними кроками, що цьому сприятимуть є вивчення слабких місць прикладних програм за даними корпорацій Bugtrad (http://www.securityfocus.com) і CERT (http://www.cert.com), застосування крім системного адміністрування систем розпізнавання атак (IDS технологій) додаткового ПЗ, що дасть можливість відстежувати всі пакети, які проходять через визначений мережевий інтерфейс, проведення аналізу спеціальних аналітичних додатків із застосуванням лог-файлів операційних систем та мережевих лог-файлів, застосування евристичних механізмів захисту, антивірусних програм та персонального Firewall тощо.

Питання для самоконтролю

1. Дайте визначення поняттям «інформаційний» і «кібернетичний» простір. Назвіть основних дійових осіб кіберпростору.

2. Що таке «кіберборотьба»? Які основні риси їй притаманні?

3. Дайте визначення поняттю «інформаційна безпека». Назвіть основні загрози, які на неї впливають та методи, завдяки яким цьому можна запобігти.

4. Дайте визначення поняттю «кібернетична безпека». Назвіть головні ознаки, які його уособлюють.

5. Які документи регламентують діяльність із забезпечення інформаційної і кібербезпеки в Україні? Наведіть приклади внеску у реалізацію цих процесів державних підрозділів спецпризначення.

6. За якими принципами мають розвиватися взаємовідносини між Україною та НАТО у сфері інформаційної і кібербезпеки? Назвіть основні напрями співробітництва Україна–НАТО у сфері кіберзахисту.

7. Що впливає на прагнення України створити дієздатну систему інформаційної і кібербезпеки?

8. Дайте визначення поняттям «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 провідні країни світу: США, Німеччина, Франція, Великобританія та інші?

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

12. Дайте визначення «внутрішньому» і «зовнішньому» інцидентам. Наведіть приклади їх класифікації згідно кодифікатору Інтерполу.

13. Які із вдомих інцидентів становлять нині найбільшу небезпеку?

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

15. Назвіть найбільш критичні заходи захисту інформації від кіберзагроз.

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

17. Перелічте основні кроки, які мають бути дотримані співробітниками служб безпеки у випадку фіксації порушень інформаційної і кібербезпеки.

18. Дайте визначення поняттю «кібератака». Наведіть приклади його трактування 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 снiфінгу?

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 поняттю «кібертероризм». Наведіть приклади його трактування 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 – початку XXI сторіччя свідчить, що незважаючи на потужні зусилля світової спільноти щодо врегулювання міждержавних протиріч мирним шляхом кількість і гострота збройних конфліктів сучасності з року в рік фактично не знижуються. Більш того, останнім часом вони охоплюють не тільки традиційні сфери збройної боротьби – зокрема землю, море і повітря, а й поступово просуваються у такі новітні сфери, як простори інформаційний та кібернетичний [54, 55]. Про їх важливість нині свідчить:

1) створення більшістю країн світу, як було відмічено у розділі 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 її військово-політичне керівництво, а також захисту своїх інформаційних об'єктів від подібного впливу* та **кіберборотьби** [56];

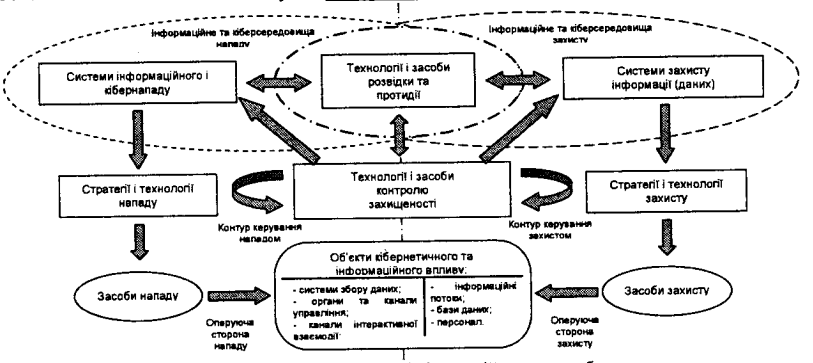


Рис. 2.1. Концептуальна схема інформаційного протиборства

2) змінювання відношення цих країн до власної **інформаційної** й, як наслідок, **кібернетичної безпеки**.

Основними сферами впливу протиборчих сторін при цьому є соціальна, когнітивна, інформаційна та фізична сфери (рис. 2.2), а головними формами інформаційного протиборства – інформаційний і кібертероризм, інформаційна і кіберзлочинність та

заходи із забезпечення власної інформаційної і кібербезпеки (рис. 2.3).

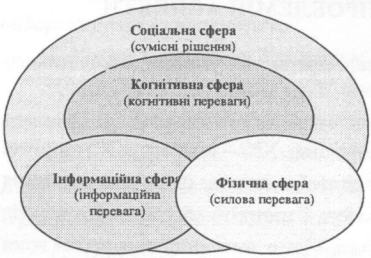


Рис. 2.2. Сфери впливу інформаційного протиборства

Рис. 2.3. Основні форми інформаційного протиборства

Останнім часом такі дії займають чільне місце у геополітичній конкуренції переважної більшості країн світу, що, в свою чергу, обумовлює нові завдання їх ЗС й виводить на перший план проблеми так званих **інформаційних** – *інформаційне протиборство, що охоплює весь інформаційний простір конфліктуючих сторін та може приймати форми як дипломатичної, так економічної і збройної боротьби* (рівні та форми яких наведені на рис. 2.4) і передусім

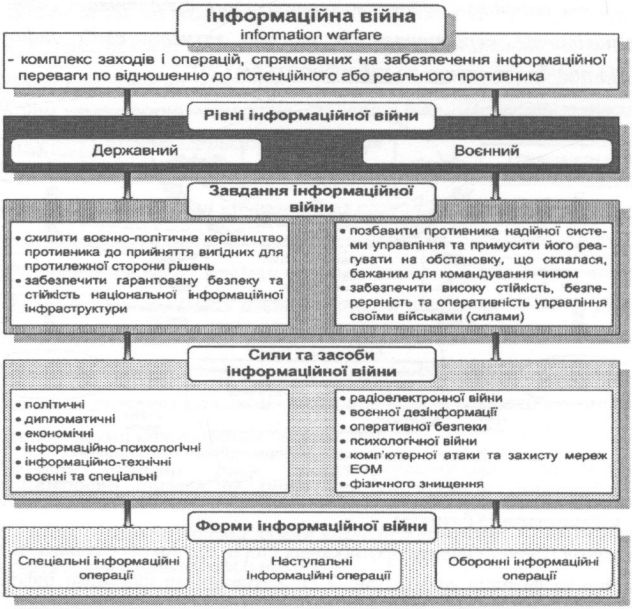


Рис. 2.4. Рівні та форми інформаційної війни

кібервоєн – *активне протистояння між державами, політичними групами, соціальними утвореннями, приватними і комерційними установами та іншими державними і позадержавними суб'єктами, метою якого є заподіяння шкоди один одному в ІТ сфері за рахунок проведення як оборонних /махист власних АТС від деструктивного впливу/, так і наступальних /встановлення контролю над ІТС протиборчої сторони/ дій* [1, 56].

Серед причин такої ситуації можна назвати:

1) відсутність або недосконаліть нормативно-правової бази, яка б:

1.1) забороняла застосування **інформаційної** – *різновид зброї, яка визначає сукупність засобів інформаційного впливу, призначених для нанесення протиборчими сторонами в процесі інформаційного протиборства збитку елементам інформаційної інфраструктури один одного* (рис. 2.5) і передусім

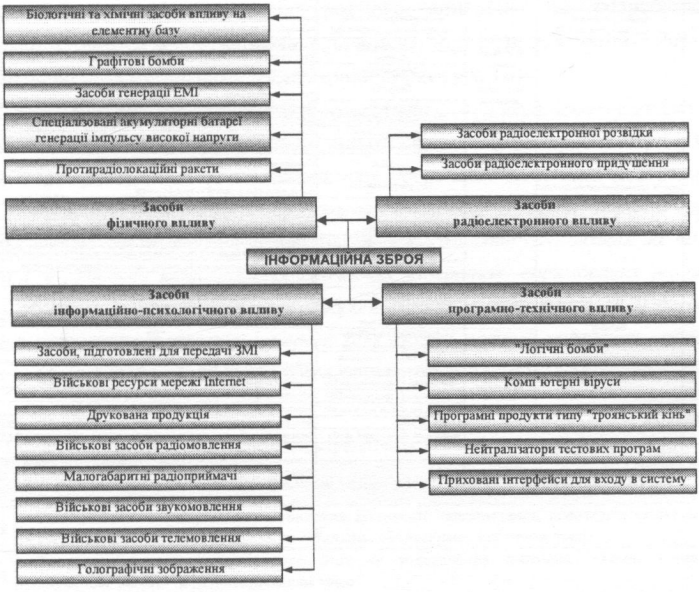


Рис. 2.5. Засоби передачі (доставки) та застосування інформаційної зброї

кіберзброї (табл. 2.1) – *спеціальні атакові та оборонні засоби ураження, що дають можливість цілеспрямовано змінювати, знищувати, копіювати і блокувати інформацію, долати системи захисту, обмежувати доступ законних користувачів, порушувати функціонування носіїв інформації для дезорганізації роботи технічних засобів ІТ систем і мереж,* перевага яких

Таблиця 2.1

Загальна характеристика основних видів наступальної і оборонної кіберзброї

...ови види НОКЗ за ...особом реалізації впливу на ІТС	Засоби реалізації	Класифікаційні ознаки	Типи	Призначення, властивості та функціональні особливості
АЛГОРИТМІЧНА	Існуючі уразливості математичних алгоритмів ПЗ		Експлойти (англ. *exploit* - експлуатувати, розробляють)	Несанкціонований доступ до інформаційних ресурсів шляхом використання "недокументованих" можливостей програмного забезпечення
ПРОГРАМНА	Комп'ютерні віруси	За об'єктом впливу	Завантажувальні	Уражання завантажувальних секторів оперативної пам'яті
			Файлові	Зараження файлової системи у разі запуску програми, яка містить вірус
			Макровіруси	Здійснення трансляції даних до конкретних несанкціонованих адресатів
		За способом зараження	Резидентні	Залишають свою резидентну частину (перехоплює 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 функціями	З деструктивними функціями	Властивість до самодублювання
			Безпекові	Справжність за конкретно програми
	Засоби несанкціонованого доступу		Несертифіковане ПЗ	Подолання систем захисту інформації та проникнення до інформаційних систем, вплив на протоколи передачі 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 програмного забезпечення
			Програмні пастки	Опосередкований вплив на функціонування системи шляхом використання помилок програмного забезпечення
			Програмні черв'яки	Маскуються під системні засоби пошуку вільних інформаційних ресурсів
		За місцем створення	Дослідники	Виявлення уразливих місць в системах
			Перехоплювачі	Несанкціоноване відтворення та отримання даних
			Рубіжники	Спотворення та знищення коду програм
			Активні хвости	Порушення нормального режиму функціонування конкретної програми або операційної системи
		За способом доставки до системи	Асоційовані з програмно-апаратним середовищем	Впроваджена у BIOS та активізація при завантаженні системи
			Асоційовані з програмним середовищем	Активізуються при завантаженні активних розділів дискового простору (MasterBoot та RecordBoot - сектори)
			Асоційовані з завантажувальною ОС	Впроваджуються при завантаженні системи та ініціалізації драйверів
			Асоційовані з прикладним ПЗ	Вбудовані в програми тестування, утиліти та драйвери
			Модулі, що містять код закладки	Впроваджуються у 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 і розважального призначення
АПАРАТНА	Апаратні закладки, що вбудовані у комплектуючі частини електронно-обчислювальної техніки та периферійного обладнання			Закладки, що маскуються під звичайні пристрої мікроелектроніки, призначені для збору, обробки та передачі інформації

порівняно з іншими видами зброї забезпечується перш за все їх:

універсальністю (не залежать від кліматичних і географічних особливостей місцевості ведення військових дій);

прихованістю (можливість приховати свої наміри нападати на супротивника);

економічною ефективністю (невеликі затрати);

можливістю застосування для вирішення широкого кола завдань (можна застосовувати на будь-яких етапах війни, на різних суб'єктів);

масштабністю застосування (можливе здійснення впливу на стаціонарні і мобільні елементи системи наземного, морського, повітряного і космічного базування);

наявністю ефекту "ланцюгової реакції" (вплив на одиничний елемент системи може привести до виведення з ладу інших елементів, сегментів і системи цілком);

складністю здійснення міжнародного контролю за розробкою і застосуванням (може бути надійно прихована від розвідок інших держав, різних міжнародних організацій, їх контролюючих органів);

1.2) забороняла проведення **інформаційних** – *сукупність узгоджених та взаємозв'язаних за метою, завданнями, місцем і часом інформаційних акцій, ударів та заходів, що проводяться як послідовно, так і одночасно за єдиним замислом та планом з метою забезпечення національних інтересів в одній обраній сфері життєдіяльності держави* та **кібероперацій** – *сукупність узгоджених за часом, глибиною і завданнями відносно короткочасних кібератак, спрямованих на певну кількість об'єктів впливу протиборчої сторони з метою одержання НСД до їх IP, порушення роботи їх IT систем і мереж або взагалі повного виведення обраних об'єктів з ладу* (основні методи проведення яких приведені у табл. 2.2);

Таблиця 2.2

Основні методи проведення кібератак, стратегічних та спеціальних кібероперацій

Рівень завдань	Основні методи проведення
Тактичний	Ускладнення чи вибіркове призупинення діяльності телекомпаній, операторів стільникового зв'язку, провайдерів Internet, відомчих локальних обчислювальних мереж тощо.
Тактичний	Тимчасове призупинення, дезорганізація чи ускладнення діяльності систем управління транспортом, енерго- й газопостачанням тощо. Вибіркове призупинення та порушення діяльності систем управління об'єктами критичної інфраструктури, включаючи банківську сферу, підприємств атомної, хімічної, нафтопереробної промисловості тощо.
Стратегічний	Розкриття державних кодів та шифрів, перехоплення та дешифрування листування вищих посадових осіб держави. Несанкціонований доступ до державних баз даних, у 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, провайдерів Internet, відомчих комп'ютерних мереж, систем централізованого управління енерго- і газопостачанням, зв'язком.

Продовження табл. 2.2

Рівень завдань	Основні методи проведення
Стратегічний	Завдання програмної або апаратної шкоди комп'ютерним системам на атомних електростанціях, підприємствах хімічної, нафто- і газопереробних галузей тощо.
Спеціальний	Несанкціонований доступ у системи управління стратегічною зброєю та імітація примусового запуску окремих елементів ракетної чи іншої зброї. Блокування систем управління військами, передача 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 їх польотного завдання й навіть перенацілювання на інші об'єкти у суміжних країнах тощо.

1.3) встановлювала б відповідальність протиборчих сторін за здійснення злочинів в **інформаційній сфері** – *сукупність суб'єктів, що приймають участь в інформаційній взаємодії та інформації, призначеної для використання цими суб'єктами, а також технологій, що забезпечують цю взаємодію з точки зору обробки, зберігання й обміну інформацією між суб'єктами* (рис. 2.6);

Рис. 2.6. Структура інформаційної сфери

2) формування окремими державами власних доктрин і стратегій наступальних та підривних дій в інформаційному і кіберпросторах;

3) створення та застосування спеціальних сил і засобів негативного впливу на критично важливу інформаційну і кіберінфраструктуру;

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

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

Зважаючи на таке, забезпечення інформаційного суверенітету більшості держав світу й України зокрема (згідно із Законами України "Про основи національної безпеки України" та "Про Основні засади розвитку інформаційного

суспільства в Україні на 2007–2015 роки"), потребує розгортання **власних систем кібернетичної безпеки** [9] за рахунок підвищення рівня координації діяльності державних органів щодо виявлення, оцінювання і прогнозування загроз інформсфері, запобігання таким загрозам та забезпечення ліквідації їх наслідків, а також здійснення міжнародного співробітництва з цих питань. Конкретними кроками для вирішення ними цих завдань має бути поетапне (рис. 2.7):

Рис. 2.7. Методологія формування державної системи кібернетичної безпеки

по-перше, удосконалення методів, засобів та способів отримання суспільно значущої інформації з відкритих, відносно відкритих і закритих електронних джерел, оцінювання рівня захищеності власних ІТ систем і мереж від впливу внутрішніх та зовнішніх кібернетичних втручань і загроз, а також злому систем захисту протиборчих;

по-друге, формування власних систем захисту національної інфосфери від стороннього кібервпливу та вдосконалення існуючої нормативно-правової бази;

по-третє, забезпечення автоматизації процесів пошуку та збору інформації (ІРМ, відомостей, даних та знань) у відкритих і відносно відкритих та її добування із закритих електронних джерел, а також накопичення і оброблення такої інформації та обміну нею.

Нині це потребує додаткового дослідження світового досвіду щодо побудови ІТС та їх складових підсистем, ключовим елементом яких є зокрема моделі **системи захисту інформації** (рис. 2.8),

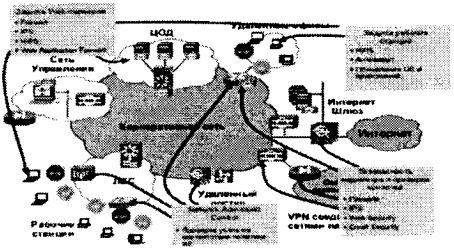


Рис. 2.8. Модель системи захисту інформації в ІТС

а математичним забезпеченням – моделі процесів кібернападу (КБн) і кіберзахисту (КБз) від стороннього кібервпливу (рис. 2.9).

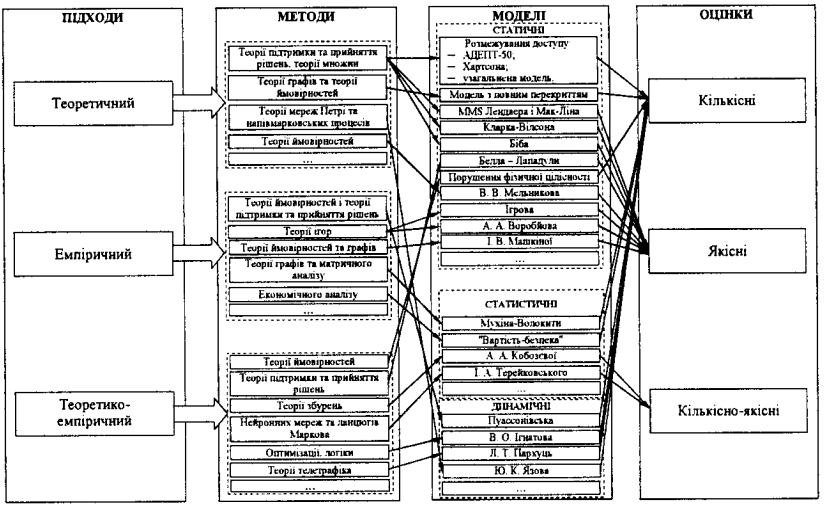


Рис. 2.9. Методи та моделі процесів кібернападу і кіберзахисту

У низці відомих закордонних наукових публікацій такими моделями, як відомо [57], є 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-графова модель TAKE-GRANT тощо);

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-імовірнісні моделі (Гогена-Месигера (GM- модель));

захисту від загроз відмов в обслуговуванні (модель розподілення ресурсів Мілена (MPP));

контролю цілісності (модель Біба, модель Кларка-Вілсона) тощо.

Базисом для них виступає математичний інструментарій [1, 57], в основу якого покладено теоретичний, емпіричний та теоретико-емпіричний підходи. При цьому теоретичний підхід ґрунтується передусім на методах теорії підтримки і прийняття рішень, теорії графів, теорії ймовірностей, теорії мереж Петрі та напівмарковських процесів тощо. Моделі КБн і КБз, розроблені на їх базі, дають можливість отримати головним чином якісні оцінки рівня захищеності (РЗ). Науково-методичним базисом емпіричного підходу є методи теорії ймовірностей, теорії підтримки та прийняття рішень, теорії ігор, мереж Петрі, теорії графів та матричного аналізу, економічного аналізу тощо. Статичні, стохастичні та динамічні моделі, розроблені на основі емпіричного підходу, дозволяють отримати окремо систему як якісних, так і кількісних показників оцінювання РЗ. Синтез теоретичного і емпіричного підходів ґрунтується на групі математичних методів, які їм відповідають. Особливістю даного підходу є включення до набору математичного інструментарію методів теорії збурень, нейронних мереж та ланцюгів Маркова, методів теорії логіки та оптимізації, теорії трафіка тощо. На відміну від двох попередніх підходів відомі на сьогодні моделі на базі теоретико-емпіричного підходу дозволяють отримувати не тільки кількісні, а й кількісно-якісні оцінки РЗ.

Особливої уваги, а у деяких випадках й докорінного перегляду при підготовці й проведенні інформаційних і кібервоєн сучасності та найближчого майбутнього потребують погляди на **систему розвідувального забезпечення** усіх, супутніх цьому заходів. Головним чином це пояснюється появою нових комунікаційних можливостей та постійно зростаючим інформаційним ресурсом, які останнім часом значно

розширюють кількість потенціально-можливих джерел для такого прогресивного виду розвідки, як **розвідка ІТ систем** (рис. 2.10) – *комплексу заходів, спрямованих на систематичний і цілеспрямований пошук, збір та добування з автоматизованих ІТС (СІТС), комп'ютерних мереж і систем зв'язку цивільного та/або військового призначення інформації стосовно протиборчої сторони (конкурента), її вивчення та обробку, а також формування на цій підставі уявлення про реальні та/або потенційно можливі джерела стороннього кібернетичного впливу* [1, 58, 59].

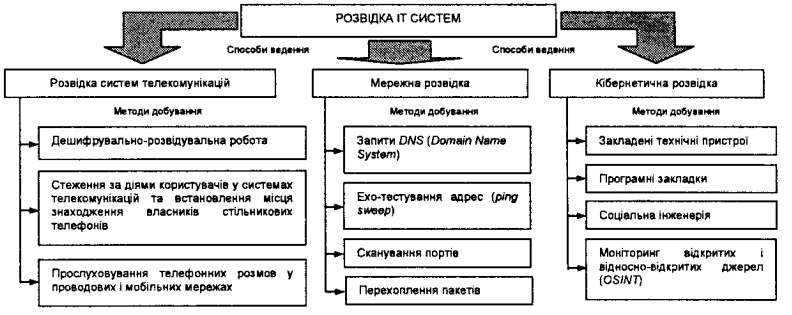


Рис. 2.10. Способи та методи ведення розвідки ІТ систем

Від інших видів розвідка ІТС відрізнятиметься перш за все механізмами (способами), а також силами і засобами, що задіяні у процесах добування розвідувальної інформації (РІ). У цьому контексті під **силами розвідки** слід розуміти підрозділи (особовий склад), що задіяні в процесі добування, аналітичної обробки та збереження інформації. Під **засобами розвідки** – спеціальну техніку (у тому числі й бойову), пристрої, спорядження, тобто все те, за допомогою чого особовий склад виконує завдання розвідки ІТС. Під **РІ** – інформаційні й розвідувальні матеріали та відомості, які надійшли від засобів різних видів розвідки або різнотипних відкритих, відносно відкритих і закритих джерел. При цьому під відносно відкритими розуміються електронні ресурси, що вимагають реєстрації для наступної роботи в них (форуми, більшість з мережевих сервісів тощо) або люди, що спілкуються за допомогою соціальних мереж, чатів, засобів швидкого обміну повідомленнями або електронною поштою, а під відкритими – ресурси, що можуть бути отримані офіційним шляхом без залучення органів добування та порушення норм міжнародного права і національного законодавства. До них, як правило, належать:

засоби комунікації – інформаційні агентства, друковані ЗМІ (газети, журнали тощо), аудіовізуальні ЗМІ (радіо, телебачення), електронні ЗМІ, інформаційні ресурси мережі Internet тощо;

суспільна інформація – урядові повідомлення, фінансові плани, демографічні

дані, законотворчі акти, матеріали прес-конференцій, промови, презентації, результати опитувань тощо;

наукові і професійні дані – академічні дослідження, НДДКР, матеріали наукових конференцій, семінарів та круглих столів, наукові публікації тощо;

геоінформаційні матеріали – карти, атласи, географічні відомості щодо визначених об'єктів;

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

Головними способами ведення розвідки ІТС слід вважати:

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

мережеву розвідку – *комплекс заходів, спрямованих на систематичний та цілеспрямований пошук і добування інформації про ІТС об'єкта розвідки, їх ресурси, засоби захисту, пристрої та ПЗ, що в них використовується, їх уразливі місця та межі проникнення, а також подальшого вивчення цих даних та їх обробки;*

кібернетичну розвідку – *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 накопиченням, наступною верифікацією та аналітичною обробкою, оцінювання на підставі отриманої інформації можливих загроз (ризиків) власному кіберпростору, виявлення їх ознак та прогнозування їх можливого прояву, а також планування та, у разі потреби, здійснення впливу на кіберпростір ворогуючої сторони.*

Ним у свою чергу властиві специфічні, з різним рівнем можливостей щодо розвідки кібервтручань і кіберзагроз та притаманні лише кожному конкретному способу, методи. Так, наприклад, у своїй повсякденній діяльності розвідувальні органи переважної більшості країн світу використовують головним чином методи **дешифрувально-розвідувальної роботи** (ДРР), методи **соціальної інженерії** (СІ) – *комплекс заходів, спрямованих на одержання неавторизованим користувачем НСД до інформації про призначення, структуру, встановлені права доступу, систему захисту, реєстраційні імена і паролі, а також іншої конфіденційної інформації про об'єкт атаки – людину або їх групу, використовуючи його слабкість, некомпетентність, непрофесіоналізм або недбалість та керуючи його*

діями, а також методи **моніторингу відкритих і відносно-відкритих джерел** (МВВВД) – *процес постійного збору з таких джерел широкого спектра інформації про одне й те ж явище, подію чи об'єкт розвідки, її обробки та приведення у структуровану і логічно обґрунтовану систему просторово-часових, причинно-наслідкових та інших залежностей для підготовки оперативних і виважених рішень за визначеною тематикою*), що властиві відповідно розвідці систем телекомунікацій та кібернетичній розвідці. Серед них саме методи соціальної інженерії або інакше соціального інжинірингу (СІ), застосування яких завдяки домінуючому людському чиннику в умовах стрімкого розвитку мережі Internet сприяє подоланню таких відомих технологій безпеки, як міжмережеві екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережевих атак тощо – набувають останнім часом особливої актуальності. Західні і вітчизняні фахівці практикують їх останнім часом як самостійно, без застосування технічних засобів [60], так і використовують в якості інструмента під час планування та проведення інших видів атак на об'єкт розвідки.

Існує багато прикладів тому, що результати ДРР, СІ та МВВВД є несуперечними й, за висновками експертів, здебільшого доповнюють один одного. Підтвердженням такому є досвід практичної діяльності структурних підрозділів спецпризначення, результати проведених навчань і тренувань, які за оцінками вітчизняних і західних фахівців дозволяють стверджувати, що у сучасних умовах силами й засобами, наприклад, ДРР про об'єкти розвідки добувається від 5 до 8% інформації (матеріалів, відомостей, даних та знань). Разом з цим, шляхом проведення моніторингу відкритих і відносно-відкритих джерел та соціального інжинірингу, навпаки – про об'єкти розвідки добувається від 35 % до 95 % розвідувальних даних, які інколи не тільки не відрізняються від військових і державних таємниць, але й часто можуть перевершувати їх за своєю цінністю.

Інші методи розвідки ІТС світовою розвідувальною спільнотою розглядаються як надзвичайно ризиковані. Це пояснюється тим, що їх ведення потребує цифрового проникнення у мережі та комп'ютери, які знаходяться на балансі інших держав, корпорацій або приватного сектору й передбачає пряму взаємодію з їх певними організаційними структурами та механізмами збору РІ. Легітимність застосування цих методів може бути визначена на наш погляд лише після детального аналізу відповідними фахівцями їх правових, технічних, організаційно-штатних та інших особливостей на предмет відповідності діючому вітчизняному законодавству й, особливо, міждержавним угодам.

Зважаючи, що функціонування високотехнологічних галузей промисловості,

Збройних сил у цілому, а також сил і засобів розвідки зокрема, характеризується на сучасному етапі розвитку інформаційного суспільства постійним зростанням обсягів інформації, яка циркулює мережею Internet, жорстким дефіцитом часу на її пошук, збір, добування та первинну обробку, накопичення інформації, її систематизацію за певними класифікаційними ознаками, подальший аналіз, синтез, узагальнення та доведення до споживачів, а також перетворення інформації у синтезовані висновки і рекомендації та підготовку на їх підставі пропозицій для розроблення і прийняття певних управлінських рішень актуальними стають завдання щодо **автоматизації усіх заходів, супутніх цим процесам** [61–63]. Це у свою чергу потребує впровадження у діяльність державних структур сучасної системи інформаційного забезпечення, що має відповідати вимогам щодо:

якості (стислості і чіткості формулювань, своєчасності надходження);

цілеспрямованості (задоволення конкретних потреб);

точності та вірогідності (правильного відбору початкових матеріалів і відомостей, безперервності їх збору, накопичення та оброблення, оптимальності систематизації інформації, а також її доведення/передавання).

У підрозділах спеціального призначення (ПСП) України, що являють собою комплекси з великою кількістю повсякденно пов'язаних та взаємодіючих підрозділів, саме точність і вірогідність інформаційного забезпечення є першорядними і неодмінними факторами їх надійного та ефективного функціонування. Задовольнити ці вимоги можна шляхом впровадження сучасної ЕОТ та новітніх ІТ технологій у процеси діяльності таких структур, а також оснащення останніх сучасними програмними і програмно-апаратними засобами. Одним з можливих способів розв'язання цього завдання є створення та розгортання за певними напрямами підпорядкування уніфікованих спеціальних програмно-апаратних комплексів розвідки, й передусім кіберрозвідки (СПАКР) як такої, що відповідатимуть вимогам до систем підтримки прийняття рішень та являтимуть собою систему організаційно-технічних мір, засобів і заходів, призначених для забезпечення автоматизації процесів розвіддіяльності у кіберпросторі, підвищення їх ефективності, якості і оперативності, а також автоматичного математично-аналітичного розв'язання нагальних управлінських задач, мінімізації витрат робочого часу споживачів при роботі з інформацією (інформаційними і розвідувальними матеріалами, відомостями, даними) та документами, оцінювання на їх підставі можливих загроз (ризиків) власному кіберпростору, виявлення їх ознак та прогнозування їх можливого прояву, а також комплексного захисту власних масивів

розвідувальної інформації та процесів інформаційного обміну між підсистемами і компонентами СПАККР та здійснення, у разі потреби, кібернетичних атак (нападів) на кіберпростір протилежної сторони тощо.

З функціональної точки зору перспективний СПАККР має:

а) розглядатися як система, що складаються з низки взаємозалежних підсистем та їх окремих компонент, орієнтованих на виконання відповідних функцій шляхом розв'язання певного комплексу завдань (рис. 2.11);

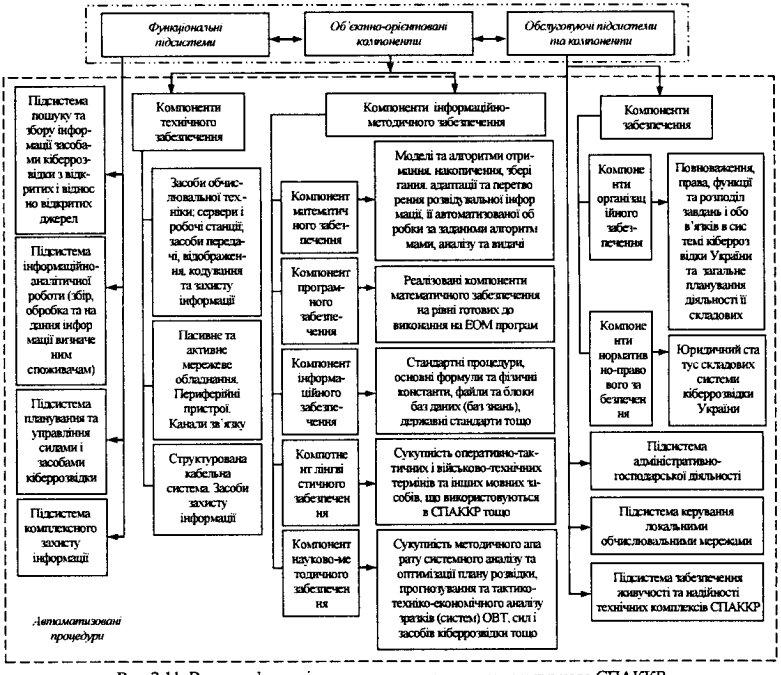


Рис. 2.11. Взаємозв'язок підсистем та компонент перспективного СПАККР

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

в) оснащуватись сучасними програмними і 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 і засобами, комплексного захисту інформації в системі, – тобто функціональні підсистеми основного призначення, а також підсистеми обслуговування і забезпечення, одним з елементів

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

Таким чином, стислий аналіз стану боротьби провідних держав світу за володіння світовим ІР дає можливість зробити висновок, що Україна, як суверенна та незалежна держава, знаходиться нині на початкових етапах цього складного шляху. Тим не менш застосування проти нашої держави розвиненими країнами світу, що мають необхідний промисловий та інтелектуальний потенціал, низки кібератак і кібероперацій вже зараз може призвести до серйозних проблем, пов'язаних із забезпеченням безперебійного функціонування головних елементів її інфраструктури, цілісності та конфіденційності інформації, а також її збереження, тобто всього того, з чим вже зіштовхнулась більшість розвинених країн Заходу.

Одним з найбільш ефективних засобів профілактики, протидії та боротьби з найрізноманітнішими кібернетичними втручаннями і загрозами на теренах нашої держави, поступово перетворюючись з діяльності щодо своєчасного викриття ознак підготовки імовірного противника до збройного нападу в діяльність, орієнтовану на досягнення та/або утримання над ним певної інформаційної переваги невдовзі стане розвідка ІТ систем. Значне підвищення її результативності у сучасних умовах може бути досягнуто шляхом активізації зусиль за напрямом розвідки систем телекомунікацій (РСт), мережевої (МР) і кіберрозвідок (КР). Завдяки раціональному поєднанню чотирьох основних процедур – пошуку, збору, обробки та подання інформації в інтересах певних сил, найбільш дієвим і, можливо, найбільш потужним способом ведення розвідувальної діяльності у відкритих і відносно відкритих електронних джерелах на найближчу перспективу залишатиметься саме КР, завдяки ж можливості використання уразливостей в певних криптографічних алгоритмах та/або протоколах, застосування сучасних криптографічних методів захисту інформації та проведення криптоаналітичних атак РСт, як така, вважатиметься найбільш результативним способом добування інформації із закритих електронних джерел.

Вирішення завдань розвідувальної діяльності на сучасному етапі розвитку ІКТ та ІТС неможливе, як відомо, без автоматизації заходів з пошуку, збору та/або добування інформації про об'єкт розвідки, їх подальшої обробки, аналізу і синтезу. Цьому сприятиме створення за певними напрямами підпорядкування спеціальних програмно-апаратних комплексів зокрема таких, як СПАККР. Підвищення продуктивності, відмовостійкості, сумісності, розширюваності, масштабованості та ефективності існуючих і перспективних систем обробки даних, а також їх інформаційної й кібербезпеки неможливе без розгортання спеціальних ІТ систем.

2.2. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки

В епоху глобальної інтенсифікації інформаційних процесів та їх проникнення в усі сфери діяльності людини (соціальну, політичну, економічну тощо), коли практично кожній особі доводиться вирішувати завдання оцінки та прогнозування ефективності роботи встаткування або інших людей, надійної взаємодії з різними елементами IT інфраструктури тощо – збільшення залежності кожного індивідума від інформаційних систем і мереж, а також його уразливості від стороннього кібернетичного впливу постійно зростає. Це, як результат, сприяє перевантаженню психіки людини та може спонукати її до розголосу інформації з обмеженим доступом (ІзОД), а також створює передумови для проведення соціальними інженерами атак на заздалегідь визначені потенційні жертви. Такими у сучасних організаціях (установах, компаніях тощо) можуть бути адміністратори, начальники, користувачі та власне знайомі будь-кого із наведених вище категорій, які можуть мати різні права досту до IP або взагалі не мати жодних прав щодо доступу до інформаційної системи. Особистісно-професійні характеристики їх поведінки, що можуть привести до розголосу ІзОД, якою вони оперують у своїй службовій діяльності, а також можливі дії соціальних інженерів приведені на рис. 2.12.

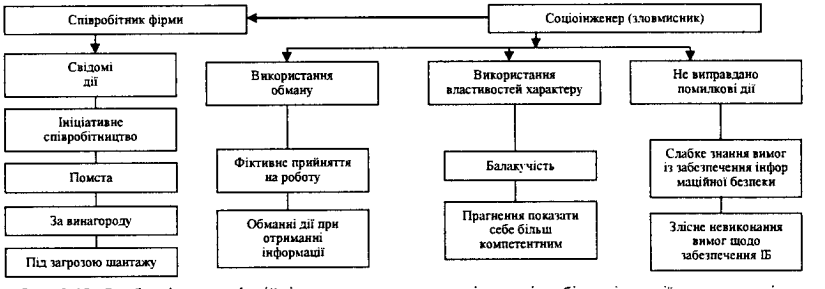


Рис. 2.12. Особистісно-професійні характеристики поведінки співробітників та дії зловмисників, що сприяють реалізації загроз інформаційної і кібербезпеки

У таблиці 2.3 показано можливий ступінь одержання доступу соціального інженера (1 – низький; 2 – середній; 3 – високий) з рівнем підготовки новачок, аматор та професіонал до різних засобів застосування, на різних рівнях взаємовідносин та до різних категорій персоналу організації. При цьому його дії засновані передусім на особливостях прийняття людьми рішень, відомих як когнітивні упередження. Вони використовуються в різних комбінаціях, з метою створення найбільш підходящої стратегії обману в кожному конкретному випадку.

Але загальною рисою всіх цих методів є саме введення в оману, з метою примушення людини зробити певну дію, яка необхідна соціальному інженерові.

Таблиця 2.3

Імовірність одержання доступу різних рівнів та категорій персоналу

Клас атаки / підготовленість зловмисника	Новачок	Аматор	Професіонал
Засоби застосування			
Телефон	3	3	3
Електронна пошта	2	3	3
Звичайна пошта	1	3	3
Розмова по Internet	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 поставленого результату соціальним інженером використовується цілий ряд усіляких тактик, а саме:

видавання себе за іншу особу;

відволікання уваги;

нагнітання психологічної напруги тощо.

Для цього соціальний інженер граючи на симпатіях жертви, її страхах, реактивності і довірі використовує такі психологічні інструменти, як:

входження в певну роль (соціальний інженер звичайно демонструє кілька характерних ознак тої ролі, яку він грає);

примушення жертви відігравати певну роль (соціальний інженер часто змушує свою мішень відігравати незвичну роль, наприклад, примушуючи її до підпорядкування своїй агресивній поведінці або призиваючи до жалості);

збивання жертви з думки (соціальні інженери прагнуть вступити в контакт із мішенями, коли ті перебувають у режимі роздумів, і втримувати їх там);

створення із жертвою моменту згоди (соціальні інженери створюють момент згоди, роблячи цілу серію запитів, починаючи із зовсім необразливих);

формування у жертви потреби в допомозі (люди випробовують позитивні емоції, коли допомагають іншим).

Незважаючи на те, що співробітники фірми (організації, установи) можуть

бути джерелом загрози, її керівництво часто відмовляється це визнавати. Існує кілька причин, що пояснюють таке поводження:

довіра керівництва до співробітників, заснована на особистій симпатії;

упевненість керівництва в порядності і відданості співробітників;

упевненість керівництва в силі впливу корпоративної етики.

Тим не менш факти розголошення ІзОД мають місце практично у кожній фірмі (організації, установі). Причинами такого може бути (рис. 2.12):

прагнення людини до самоствердження, популярності й слави;

невідповідність адміністративних мір покарання за розголошення ІзОД збитку, що наноситься її розголошенням;

випадкове розголошення ІзОД у бесідах з іншими особами, засобах масової інформації й т.д.;

прагнення співробітників одержати фінансову вигоду;

відсутність служби безпеки компанії;

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

психологічні конфлікти між співробітниками, між співробітниками й керівництвом.

На мотивацію людини до розголошення можуть впливати також і певні надзвичайні ситуації (НС) соціального характеру, приведені на рис. 2.13.

Рис. 2.13. Надзвичайні ситуації соціального характеру

Разом з тим на лояльність співробітників впливають наступні фактори [64]:

матеріальна винагорода;

цікава робота;

кар'єрні перспективи;

перспективи професійного росту;

репутація компанії;

психологічна атмосфера в колективі;

умови роботи;

корпоративна культура;

особистість начальника;

поводження начальника.

З наведеного переліку на перші місця претендують передусім такі незадоволені людські мотивації, як – заробітна плата, цікава робота, кар'єрні перспективи, перспективи професійного росту, репутація компанії. Варто згадати, що заробітна плата стоїть на другому місці й у п'ятиступеневій ієрархічній градації мотивацій американського соціолога А. Маслоу [65–66], після проблем біологічного виживання людини, таких як їжа, питво, світло, повітря. Оцінка мотивації психологічного клімату в колективі (шосте місце) свідчить, насамперед, про якісь безладдя в колективах. Саме простір між 1 і 6-ою незадоволеними мотиваціями є простором для негативного. прояву людського фактора: нелояльності й зрадництва інтересів фірми (організації, установи).

Таким чином, як видно, схоронність ІзОД на 80% залежить від правильного підбора, розміщення і виховання кадрів, персоналу, відданого фірмі (організації, установі) [67–68]. Єдино вірним шляхом, який дозволить запобігти розголошення ІзОД – є ретельний підбір персоналу та обмеження його доступу до такої інформації. Для цього керівництвом фірми (організації, установи) має дотримуватись певний алгоритм прийняття на роботу, який може полягати:

в проведенні аналізу робочого місця (оцінюванні наявних інформаційних, фінансових і людських ресурсів, складанні портрета ідеального співробітника характеристики якого повністю відповідають вимогам робочого місця, визначенні майбутніх перспектив компанії й формуванні програми їхньої реалізації тощо);

у відборі майбутніх співробітників за критеріями освіти, комунікабельності, досвіду, уміння приймати рішення в екстремальних ситуаціях тощо;

у проведенні попередньої бесіди по відбору та заповненні бланка заяви;

у перевірці рекомендацій і зобов'язань перед іншими фірмами;

в ухваленні рішення.

В подальшому керівництвом фірми (організації, установи) мають бути реалізовані шляхи із унеможливлення розголосу ІзОД за рахунок, наприклад:

підписання угоди про нерозголошення ІзОД при прийнятті співробітника на роботу і його звільнення (психологічно це діє дуже добре: більшість людей боїться порушувати підписані домовленості);

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

застосування системи відеоспостереження.

формування ради по безпеці з представників від кожного відділу;

матеріального стимулювання співробітників, що працюють із ІзОД;

проведення заходів, що підвищують лояльність співробітників;

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

проведення комплексної перевірки співробітника, що звільняється. Пропонування йому залишитися в фірмі (організації, установі) на посаді консультанта або стати одним з акціонерів тощо.

Разом з цим керівництво фірми (організації, установи) повинно вживати реальних заходів по захисту ІзОД. До таких мір належать: забезпечення умов захисту й безпеки; забезпечення планування дій, спрямованих на забезпечення безпеки; завчасне рішення питань по забезпеченню безпеки, не чекаючи того моменту, коли щось відбудеться. Неуважність керівництва до проблеми людських відносин, нерозв'язаність проблеми може стати причиною розголосу ІзОД. Основною мотивацією щодо попередження таких дій може стати: зростання продуктивності праці та прибутків, помітне поліпшення життєвого рівня співробітників, нормалізація психологічного клімату в колективі, поява в співробітників почуття причетності до спільної справи, зменшення або ліквідація плинності кадрів, зниження негативних наслідків людського фактора в системі забезпечення комплексної безпеки, зменшення числа ймовірних порушників правил і норм безпеки серед персоналу компанії тощо.

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

Останнім часом Інтернет став улюбленою зброєю в руках незадоволених споживачів та співробітників, за допомогою якої вони успішно атакують фірми (організації, утанови), їхню продукцію і керівництво. Розміщення в мережі негативної інформації може здійснюватися ними різними способами, а саме:

1) шляхом створення спеціалізованих сайтів таких як, наприклад, сайт "Суспільної думки", на яких споживачі виражають невдоволення на адресу певного виду продукції або послуг (consumer opinion sites);

2) шляхом поширення "електронних пліток" й іншої недостовірної інформації;

3) шляхом створення різних груп у соціальних мережах, блогах, форумах.

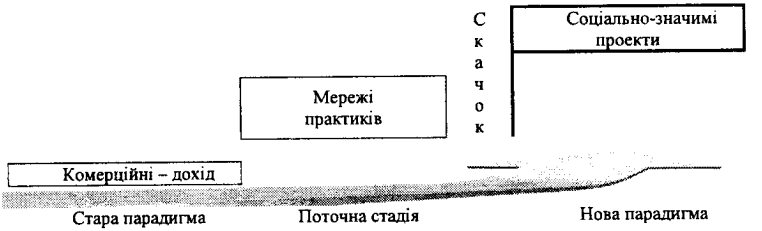
Під **соціальною мережею** в цьому сенсі розуміють *множину акторів (точок, вершин, агентів – індивідуумів і організацій) які можуть вступати у взаємодію один з одним*. Вона є результатом розвитку інформаційних технологій, частиною соціальної структури суспільства та цікавим соціотехнічним об'єктом,

який відображає різні зв'язки між акторами через різноманітні соціальні взаємини в термінах вузлів та зв'язків, починаючи з випадкових знайомств і закінчуючи тісними родинними узами. Вузли є відособленими акторами в мережах, а зв'язки відповідають стосункам між акторами. У сучасний момент можна спостерігати 3 види або класу соцмереж, а саме [69]:

комерційні, орієнтовані на дохід;

мережі практиків, орієнтовані на навчання;

«нова парадигма», орієнтовані на соціально-значимі проекти.



Перспективними напрямами розвитку соціально-мережних технологій є мережі Практиків (поточна стадія), а також некомерційні соціально-орієнтовані мережні проекти і ресурси (нова парадигма). З формальної точки зору такі мережі зручно представляти графо-аналітичними моделями виду $G(N,E)$ [70], застосовуючи для їхнього подальшого аналізу розвинені імовірнісно-реляційні та реляційно-алгебраїчні моделі. При цьому у графі $G(N,E)$ (рис. 2.14) $N=\overline{1,n}$ – кінцева множина вершин, у якості яких витупають програмно-технічні пристрої H (хости) та користувачі інформаційної системи A (агенти); E – множина ребер, що відбивають взаємодію кожного окремого агента A з хостом H та зв'язки між пристроями й між користувачами.

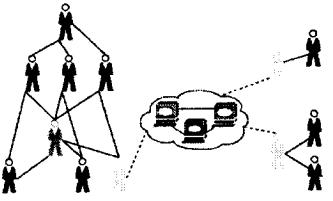


Рис. 2.14. Приклад відображення схеми зв'язків у соціальних мережах

Поводження агентів може залежати при цьому від таких факторів (рис. 2.15):

індивідуального – внутрішньої схильності (переваг) агента вибирати ту або іншу дію за відсутності будь-якого зовнішнього впливу;

соціального – обумовленого взаємодією (взаємовпливом) з іншими агентами;

адміністративного – результату впливу на нього з боку керуючого органа (центра).

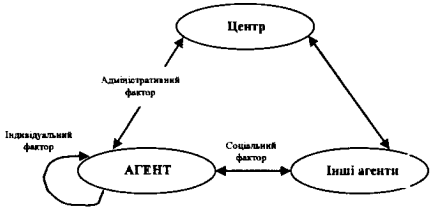
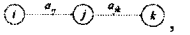


Рис. 2.15. Фактори, що впливають на актора у соцмережі

Агенти, які піддані описаним факторам, називаються залежними (від одного або декількох факторів). Агентів, на які не впливають перераховані вище фактори називаються незалежними. При цьому, наприклад, агент позначений блакитним кольором (рис. 2.14), має найбільше зв'язків в середині своєї соціальної мережі. В ідеальній ситуації, він мав би бути лідером або керівником групи (організації). Агенти, позначені зеленою фарбою мають зв'язки із іншими соціальними групами, і можуть виступати в ролі передавачів інформації між мережами. Їх вплив один на одного можна зобразити таким чином:



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

Моделям користувачів ІС, асоційованим з вершинами описаного графа (рис. 2.14), співставлені наступні атрибути (позначки) [71, 72]:

множина пристроїв, до яких у даного користувача є доступ (даний пункт також має на увазі доступ до конфіденційної інформації, що зберігається на даних пристроях);

права доступу користувача до конфіденційної інформації;

посада користувача;

права доступу користувача до контрольованих зон;

профіль уразливостей користувача, що містить рівень їх виразності.

Моделям хостів (програмно-технічних пристроїв) ІС, асоційованим з вершинам описаного графа (рис. 2.14), співставлені наступні атрибути (позначки):

критичні документи, що зберігаються на пристроях;

програмно-технічні характеристики пристроїв;

місце розташування програмно-технічних пристроїв (хостів) відносно контрольованих зон інформаційної системи.

Реляційно-алгебраїчна модель на додачу до результатів графо-аналітичної використовується з метою аналізу захищеності користувачів ІС від соціотехнічних атак. Її складовими елементами є: I – критична інформація, що циркулює у системі; H – хости, що характеризуються програмно-технічним наповненням і зв'язками; A – користувачі, що характеризуються відповідним профілем уразливості; U – атакуючі дії зловмисників; R – ресурси зловмисників. В моделі оцінюванню можуть бути піддані декілька видів декартових добутків виду $U \times A$, $H \times A$ та $A \times I$ над якими задані відношення й імовірнісні оцінки переходів.

На відміну від реляційно-алгебраїчної моделі, імовірнісно-реляційна враховує стохастичний характер успішності соціоінженерного атакуючого впливу зловмисника на користувачів ІС. В рамках цієї моделі профіль уразливостей користувача містить рівні вираженості цих уразливостей і формалізуються як тривимірний масив. Залежно від рівня вираженості уразливостей користувача його відповідні реакції на соціоінженерні атакуючі впливи зловмисника мають різну імовірність, яку позначають через p_{ijk}, де k – конкретний користувач ІС, i – конкретна уразливість цього користувача, j – конкретний соціоінженерний атакуючий вплив зловмисника, спрямований на визначену уразливість користувача. Враховуючи таке імовірність досягнення атокою вузла, який містить інформацію I користувачем a може бути знайдена з виразу:

$$P_I(a,I) = \sum_{\substack{h_u \in A \\ (P_{ijk}, h_u) \in A_H}} P_A(a, p_{ijk}) P_H(h_u, I)$$

де $P_{IH}(h,I) = \sum_{\{h_i\}_m} \left[\prod_{\substack{j, h_j, h_{j-1} \in \{h_i\} \\ (h_u, I) \in H_I}} P_H(h_j, h_{j-1}) \right] P_A(a, p_{ijk}) P_H(h_u, I)$ – імовірність досягнення атакою вузла, який містить інформацію I у випадку, якщо початковою точкою розповсюдження атаки зловмисника є користувач, який має доступ до хоста h.

Соціальна мережа це складний соціотехнічний об'єкт, у трактуваннях кібернетики – «велика система». Її характерними закономірностями є [73]:

1) наявність власних міркувань агентів;

2) змінювання думки під впливом інших членів соцмережі;

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

4) різна степінь піддання агентів впливу (конформізм, стійкість думок);

5) існування побічного впливу у мережі соцконтактів, зменшення побічного впливу із збільшенням відстані;

6) існування лідерів міркувань (агентів із максимальним впливом),

формалізація індексів впливу;

7) існування порогу чутливості до зміни міркувань оточуючого середовища;

8) локалізація груп (по інтересам, з близькими міркуваннями);

9) наявність специфічних соціальних норм;

10) врахування факторів соціальної кореляції (загальних для груп агентів);

11) існування зовнішніх факторів впливу (реклама, маркетингових акцій) та зовнішніх агентів (засобів масової інформації, виробників товарів тощо);

12) наявність стадій – характерних етапів динаміки міркувань соцмережі (наприклад, процесу дифузії інновацій);

13) лавиноподібні ефекти (каскади);

14) вплив структурних властивостей соцмереж на динаміку думок:

чим більше у агентів зв'язків, тим у нього більше, з одного боку, можливостей впливу через власне оточення на усю мережу, а з іншого – ступінь уразливості від чужого впливу;

чим вище щільність зв'язків активних агентів-сусідів, тим більше імовірність змінювання стану зв'язаного з ними агента (ефект кластеризації);

чим більше проміжне значення агента, тим, з одного боку більше його значення у розповсюдженні міркування/інформації з одної частини мережі в іншу, а з іншого – менше його вплив на агента-сусіда;

15) активність (цілеспрямованість поведінки) агентів;

16) можливість утворення угруповань, коаліцій;

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

18) нетривіальна взаємна інформованість агентів;

19) ігрова взаємодія агентів;

20) оптимізація інформаційних впливів;

21) інформаційне управління у соціальних мережах.

Області застосування й напрями розвитку класичних соціальних мереж наведені в табл. 2.4 [74].

Під віртуальною (онлайновою) соціальною мережею розуміється соціальна структура Інтернет-середовища, вузли якої становлять організації або окремих людей, а зв'язки між ними позначають установлені взаємодії (політичні, корпоративні, службові, сімейні, дружні, по інтересах і т.д.). Інтернет забезпечує зростання інтенсивності інтелектуальної взаємодії на кілька порядків, появу нових якостей за рахунок емерджентних властивостей складної соціотехнічної «великої системи». При цьому на відміну від класичної соціальної групи, скажемо, учених, інженерів, лікарів, соціальне співтовариство, що діє в Інтернет середовищі допускає

оперативне вивчення, вимір і класифікацію.

Таблиця 2.4

Області застосування й напрями розвитку соціальних мереж

	Можливість	Тренд	Приклади	Прим.
СУСПІЛЬСТВО	Слабка	Мережа Партії Регіонів		Дезинтегрированість
ОСВІТА	Можливо *(У проектах)*	Підтримка дистанційного навчання	Мережа творчих учителів - www.IT-N.ru	АПК і ППРО за підтримкою MicroSoft
НАУКА і ТЕХНІКА	Можливо *(Приклади)*	Мережі проф.співтовариств	Мед. Мережа www.wurman.ru	Миколаєнко Євген Іванович
ДІЛОВА СФЕРА	Реально	Мережі Практиків	Автолюбителі, напр.	www.Avto.ru
КУЛЬТУРА	З'являються	Взаємопроникнення	Соціальна мережа художників	*www. algonet.ru/ ?ID=637620*

Розвиваючи системотехнічний підхід, віртуальна мережа розглядається сьогодні з позицій суспільної мети і корисності, соціальної значимості і можливостей впливу на суспільство. Її відмінними рисами є топологія, розмаїтість, поширеність, складність, стійкість, а також наявність групової динаміки в поводженні. Організація внутрішньомережної міжособистісної взаємодії з комунікаційної точки зору, дає оцінку потужності такого об'єднання за принципом "багато з багатьма", як 2 у степені N, де N – число учасників мережі. Тоді як у класичній трансляційній мережі, де поширення інформації забезпечується за широкомовним принципом від "одного до багатьох" – потужність пропорційна числу точок (учасників). Соціальна орієнтованість мережних об'єднань супутня розвитку її емерджентних властивостей (emergence – незвідність властивостей системи до властивостей окремих елементів і не ідентичність), зокрема виникненню "ройових ефектів". Останнім при цьому властиві такі характерних ознаки:

відсутність централізованого управління;

самостійність субодиниць;

висока подключаємість субодиниць;

павутинна нелінійна обумовленість впливу.

У своєму розвитку віртуальні соціальні мережі проходить ряд типових етапів:

етап становлення, коли спостерігається приплив енергії, обумовлений людською цікавістю, ностальгією й бажанням знайти старих і нових знайомих;

етап стабільності, коли процеси, що відбуваються усередині мережі стають ізоенергетичними;

етап стагнації, коли цікавість до соціальної мережі поступово зменшується.

Корисну інформацію для пояснення цих процесів дає графік росту числа користувачів соціальної мережі Facebook, наведений на сайті Співтовариства.ру (рис. 2.16) [75, 78]. Загальним для більшості мереж буде початкова зона першої

версії проекту, «сплеск розголосу», деякий спад - «площина тих, хто сумнівається», що прийшли завдяки розголосу або за компанію, але не побачили подальшого інтересу до соціально-мережного життя. Далі відбувається планомірне зростання числа учасників мережі до її «насичення», зона стабільної роботи й неминуче вмирання проекту із заміною його новим, більш модним, технологічним, актуальним, сучасним і т.д. Інтерес для дослідника представляє початковий етап - «сплеск розголосу» і зона зростання кількості тих, хто витримав, обумовлені як зовнішніми керуючими впливами власників проекту й можливо, що більш цікаво, внутрішніми процесами самоорганізації і формуванням груп.

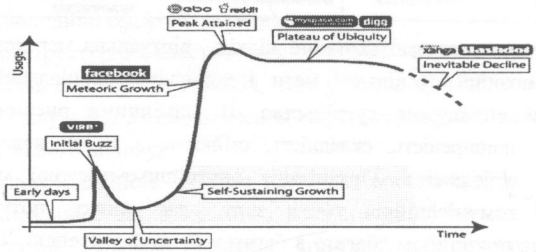


Рис. 2.16. Графік росту числа користувачів

Віртуальні соцмережі [76] можуть бути дуже різними залежно від причин і цілей їхнього виникнення. Наприклад, соціальна мережа друзів в університеті схожа на гніздо (рис. 2.17), а соціальна мережа знайомств виглядає зовсім інакше (рис. 2.18).

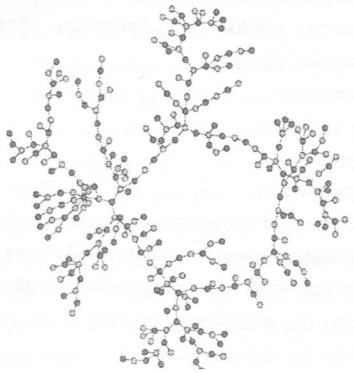


Рис.2.17. Граф соцмережі Університету

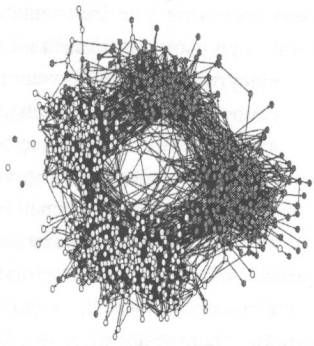


Рис. 2.18. Граф соцмережі знайомств

Їх велика частина – це комерційні, професійно і суспільно-орієнтовані соціальні мережі. Рейтинг найбільш популярних з них наведений на рис. 2.19.

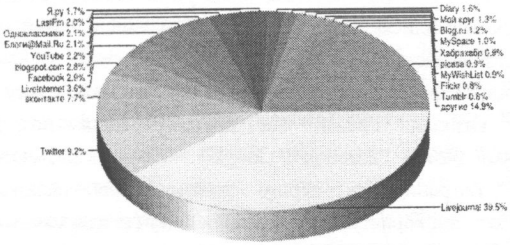


Рис. 2.19. Рейтинг популярності соціальних мереж

Віртуальні соцмережі стартували у 1995 році з порталу у США **Classmates.com** («Однокласники» - його російський аналог). Проект став початком бума соцмереж у 2003-2004 роках, коли були запущені LinkedIn (для ділових контактів), MySpace и Facebook (для самовираження особистості). Нині на підґрунті таких соцмереж, як **Facebook** та **Twitter** почали формуватися локальні соціопростори (рис. 2.20) [77–79].

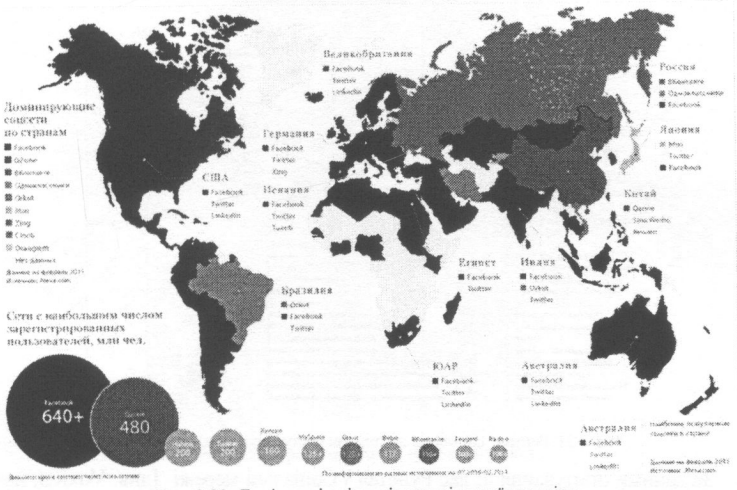


Рис. 2.20. Домінуючі оціальні мережі у країнах світу

Згідно даним дослідження, проведеного Globalwebindex, лідерство серед них сьогодні як і раніше належить Facebook. На друге місце вийшла соціальна мережа Google+, що обігнала YouTube і Twitter. На п'ятому місці перебуває соціальна мережа "None of the Above"-"Проти всіх". Далі йдуть підряд 8 китайських соцмереж. Між ними в середину потрапила ділова соціальна мережа LinkedIn, вона

очолює другу двадцятку. Російська соціальна мережа Вконтакте займає 21-е місце. Одноклассники розмістилися на передостанньому місці. 16-е місце зайняла соціальна мережа знайомств Badoo.com [80].

Самою швидко зростаючою соціальною платформою світу дослідники з GlobalWebIndex визнали Twitter. На другому місці по темпах росту користувальницької бази - Facebook і Google+. «Вконтакте», «Одноклассники» і Pinterest також потрапили в першу десятку. Для складання рейтингу підраховувалися активні користувачі з 31 країни світу (ті, хто хоча б раз за останній місяць використовували мережу). За твердженням дослідників, ці дані релевантні для 90% дорослого інтернет-населення земної кулі. При цьому, зрівнялися показники II і IV кварталів минулого року. База користувачів Twitter виросла на 40% за зазначений період, а в порівнянні з липнем 2009 року – це більш, ніж семиразовий ріст у числі активних користувачів. Повністю першу десятку формують такі мережі, як Twitter, Facebook, Google+, «Вконтакте», Sonico (Мексика), LinkedIn, Mig33 (Індонезія), Pinterest, «Одноклассники», 51.com (Китай).

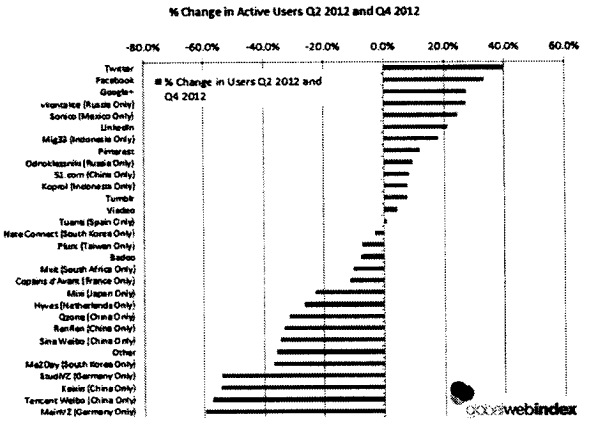


Рис. 2.21. Рейтинг соцмереж по темпах росту користувальницької бази

За даними опитування «Глас Рунета» \ Соціальні мережі [див. VoxRU, дані від 2007 року], у якому взяли участь більше 2000 активних користувачів Рунета, у тому числі, 86% проживаючих у Росії й 14% за кордоном, більшість (66%) опитаних знають про існування в Інтернеті соціальних мереж і користуються їхніми можливостями. Причому найбільшу популярність і поширення даний сервіс придбав серед жителів Москви й Санкт-Петербурга, Києва та обласних центрів України. Серед тих, хто знає про існування соціальних мереж, лише 10% не користуються ними. Серед тих

користувачів Рунета, хто користується соціальними мережами, найбільш популярними ресурсами є Одноклассники (74%), Мій мир (40%), Вконтакте (37%), Моє коло (27%), Rambler Планета (24%), LovePlanet (22%). На частку інших сайтів, позиціонуючих себе як соціальні мережі, доводиться 10-20% користувачів Рунета, що відвідують такі ресурси. Близько 25% респондентів серед тих, хто користується соціальними мережами, протягом тижня щодня не більше однієї години часу приділяють цьому заняттю. У цілому ж, тривалість користування соціальними мережами в робітники (навчальні) дні трохи нижче, ніж у неробочі (вихідні) дні [77].

В Україні перше місце залежно від попиту користувачів отримала соцмережа Connect.ua. Вона об'єднала у собі більше 760 тисяч українців (вузлів), що становить 1,65% населення України й більше 10 мільйонів зв'язків (рис. 2.22). У ньому для більшої наочності більш сильні зв'язки були розміщені в центрі графа, а більш слабкі – з боків.

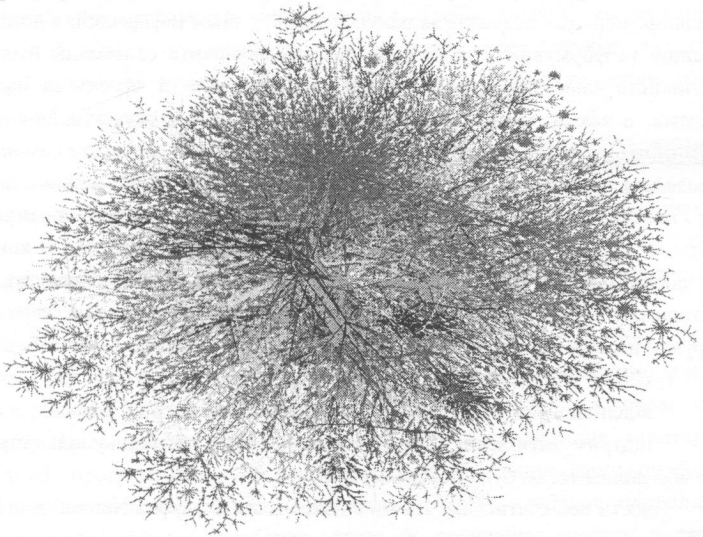


Рис. 2.22. Граф соціальної мережі Коннект

Одна з перших українських політичних соціальних мереж, що має назву *Politiko.com.ua* і поєднує політиків, експертів, журналістів, лідерів партій і виборців України в рамках одного співтовариства посіла друге місце. На третьому місці розташувалось співтовариство професіоналів *Profeo*, що займається налагодженням ділових і особистих контактів, розвитком фахівців, підвищенням їхнього професійного рівня. Profeo.ua є універсальною платформою для розвитку

майбутніх професіоналів. *Tuse.ua* перебуває на четвертому місці й уважається незамінним засобом спілкування, що відбиває у свою чергу стан душі людини, його спосіб життя, сприяє зближенню людей і допомагає зробити життя прекрасніше. На п'яте місце потрапив інтерактивний портал про Риболовлю й полювання. Дана соціальна мережа rybalka.com - не тільки форум для рибалок, він також уміщає GPS карти рік і озер України, а також фотозвіти про риболовлю й полювання. Наступні п'ять місць, що залишилися, зайняли [77]:

Autovisio.com.ua, що зібрала актуальну інформацію про автомобільні новини;

Prweb.com.ua, представлений співтовариством журналістів і пиарщиків.

People.ukrhome.net (соціальна мережа jiteli.net);

Science-community.org – сайт для вчених;

Cafe.beeline.ua – соціальна мережа, призначена для абонентів Beeline.

Регулярне відстеження (моніторинг) інформації у цих та інших подібних соціальних мережах дозволяє за рахунок аналізу такої інформації, відстеження тенденцій та формування зворотного зв'язку, визначити своє місце й оцінити ефективність своєї діяльності, заздалегідь виявити й зрозуміти можливі проблеми, а також мінімізувати негативні наслідки. Зважаючи на таке під **моніторингом соціальних мереж (SMM)** будемо розуміти *спеціально організоване, систематичне спостереження за станом соціальних мереж, явищ і процесів, що відбуваються у даних середовищах, з метою їхньої оцінки, контролю й прогнозу*. Його проведенням окрім спеціальних SMM-компаній нині займаютьсяі як стражі порядку (ЦРУ в США й МВС України), так і роботодавці. У цих цілях вони використовують безліч стартапів, серед яких лідируючі позиції займають:

1) сервіс Trendrr [80], що дозволяє:

відслідковувати кількість завантажень додатків для Facebook;

підтримувати велику кількість відео sharing сайтів (яку кількість відео з тим або іншим тегом було переглянуто);

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

2) сервіс Trackur [81], що дозволяє відслідковувати потоки інформації по багатьох онлайнових проектах (сервіс збирає всі типи інформації, відображаючи її в максимально зручному виді);

3) сервіс Sentiment Metrics [82], що дозволяє аналізувати й обробляти дані, представляючи їх у доступному й зрозумілому виді. SentimentMetrics - система, що має інформацію про бренд, яка надходить із різних блогів, форумів, новин, прес-релізів.

Моніторинг соціальних мереж в Інтернеті через занадто великий потік інформації не проводиться вручну. Процес відбувається автоматизовано з використанням спеціальних on-line сервісів або програмного забезпечення, як платного, так і безкоштовного. Сервіс реагує на появу на будь-якому сайті згадування назви компанії, імен ключових фігур, конкурентів, посилання на ваш сайт, а також ключових слів, важливих для вашої індустрії й, як результат, висилає менеджерові повідомлення про такий факт.

Нині виділяють наступні види моніторингу соціальних мереж:

регулярний моніторинг – дозволяє постійного відслідковувати інформацію, що з'являється в соціальних мережах, допомагає зрозуміти тенденції зміни думки, реакцію на ту або іншу інформацію й навіть скорегувати інформаційну політику;

первинний моніторинг – призначений для компаній, які тільки починають використовувати нові інтернет media у своїй комунікаційній активності. Він дозволить визначити «гарячі теми», місця присутності цільової аудиторії та лідерів думок, що, як результат, сприятиме створенню основи комунікаційної стратегії компанії в інтернет;

конкурентний моніторинг – дозволяє визначити положення конкурентів у мережі, їхню активність і promo компанії;

репутаційний моніторинг – проводиться, як правило, за період не менш 6 місяців й дозволяє визначити імідж компанії та її продукції, що зложився в інтернеті в цілому. Результати аналізу - це образ компанії, що складається в споживачів, які шукають інформацію в безмежних просторах мережі.

Починати моніторинг слід насамперед з аналізу ключових слів, які потрібно відслідковувати в Інтернеті (назва компанії, продукту, сервісу, послуги, назва компанії-конкурента, посилання, важливі ключові слова індустрії). Весь цей матеріал необхідний для настроювання моніторингу сервісів або програм. По-друге, необхідно здійснити пошук площадок (сайтів, блогів), які висвітлюють потрібну індустрію. По-третє, необхідно попрацювати з негативними постами, особливо, якщо їх посилання входять у топ 20 пошукових результатів по важливих ключових словах, почати спробу усунення негативної інформації, навести контакти із власниками сайтів тощо. І, як результат, варто провести роботу із блогом або сайтом компанії (продукту, сервісу, послуги) з метою виведення його на перші місця по важливим і значимим пошуковим запитам. При цьому завжди важливо пам'ятати, що офіційність, підготовленість відповідей і коментарів – це те, що не працює в соціальному Інтернеті. Інтернет побудований за принципом спілкування

людини з людиною у рамках єдиних, багатокористувальницьких веб-платформ, де головне правило – індивідуальний підхід до кожного. Ці платформи надали можливість користувачам спілкуватися з друзями, читати новини, дивитися фільми, слухати музику, ділитися цим з іншими учасниками, брати участь в обговореннях, поєднуватися по інтересах, створювати співтовариства тощо.

Подальші дослідження соцмереж мають бути зосереджені на (рис. 2.23):

формуванні математичних моделей топології Інтернет та механізмів розповсюдження інформації у ньому;

формуванні математичних моделей управління семантичним простором;

розробці систем негласного контролю Інтернет ресурсів;

розробці моделей псі-впливу тощо.

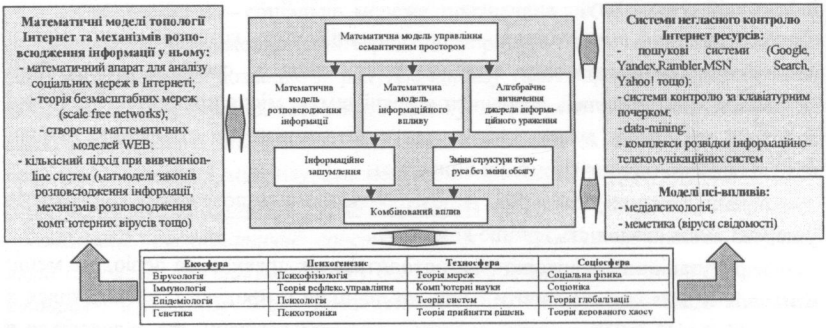


Рис.2.23. Напрями дослідження соціальних мереж

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

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

Під **системою** взагалі слід розуміти, як відомо [83–86], *цілісність взаємопов'язаних елементів та взаємозв'язків між ними, яким притаманні певні властивості, мета, цілі та функції*. Систему, як правило, характеризує структура, що відбиває взаємодію між її елементами і випливає з властивостей останніх або оточення; а також функціонал, що регламентує відношення певного елемента до системи у цілому та можливість управління нею. Якщо в системах існують не тільки однобічні причинно-наслідкові залежності, то говорять про комплексні, або

інакше про складні системи. Їх основними властивостями як правило є [87]:

інтегративність – *визначає* фактори, які утворюють і зберігають систему;

комунікативність – степінь зв'язку з зовнішнім середовищем;

рівновага – це здатність зберігати деякий стан при відсутності збурень;

стійкість – здатність системи повертатись до попереднього стану, після того як вона була з нього виведена;

адаптація – здатність системи до цілеспрямованого пристосування.

Вони визначаються як зворотними зв'язками системи, так і властивостями окремих її елементів.

Серед множини діючих складних систем можна виділити нині *технічні, ергатичні, технологічні, економічні, соціальні, організаційні та управлінські* системи. Так, наприклад, еволюційний розвиток **соціальних систем** можна зобразити схемою, поданою на рис. 2.24.

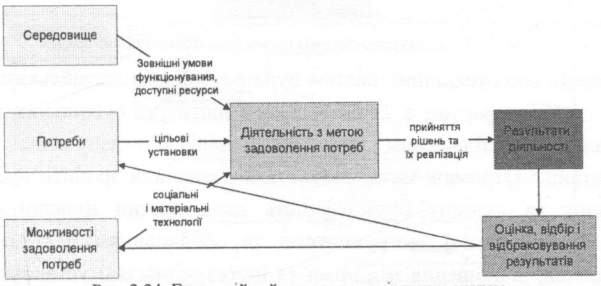


Рис. 2.24. Еволюційний розвиток соціальних систем

Вони включають ті елементи «людського фактора», які впливають: на кожного окремого індивідуума та їх групи, а також на їх відношення 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 вирішують заздалегідь визначені завдання*. Вони включають такі змінні у технології роботи: коли і де повинно виконуватися завдання, як завдання повинно виконуватися, який взаємозв'язок між виконуваними завданнями. Складні **ергатичні** або інакше **соціотехнічні системи** – *це системи, складовим елементом яких є людина-оператор, знання, уміння, настрої, ціннісні переваги та відношення до виконуваних обов'язків якої у взаємодії з технічним пристроєм в процесі, наприклад, виробництва матеріальних цінностей, управління певними процесами, обробки інформації тощо сприяють підвищенню ефективності вирішення визначених завдань або поліпшенню їх результативності* (рис. 2.25).

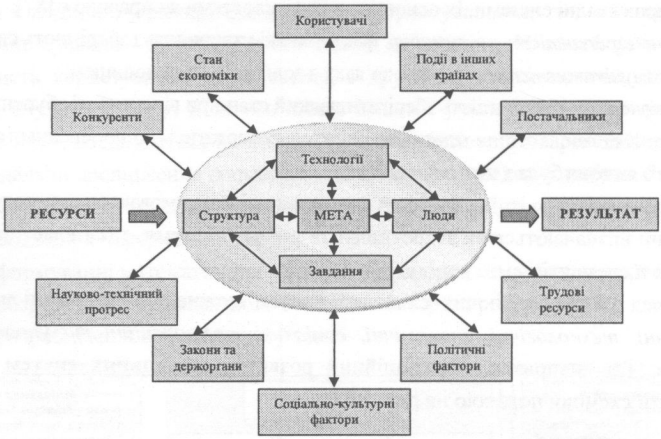


Рис.2.25. Структурно-логічна схема соціотехнічної системи

Концепція соціотехнічних систем була розроблена англійськими вченими Е.Трістом та К.Бемфортом з Тевістокського інститута суспільних відношень, які займались дослідженням процесів механізації добування вугілля у Великобританії. Отримані ними результати дозволили зробити висновок про взаємозв'язок та взаємну обумовленість двох частин цілісної системи – технічної, представленої інструментами та обладнанням й соціальної, яка включає людей, відношення міх ними та інституціональні установки, а також характеристики соціотехнічної системи, головними серед яких є:

1) організаційна філософія, що базується на розумінні працівниками своїх цілей і призначення підприємства, їхня постійна готовність розділити з адміністрацією всю повноту відповідальності за результати господарської діяльності;

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

3) новий підхід до розробки робочих місць і роль виконавця в процесі прийняття управлінських рішень;

4) нова схема розміщення встаткування, що відповідала б потребам перспективної форми організації праці й забезпечувала б прискорення матеріальних потоків на виробництві;

5) нові форми й методи підготовки й перепідготовки кадрів, більш гнучка кадрова політика, спрямована на гарантування зайнятості;

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

Одним із найбільш відомих загальнометодологічних принципів створення складних соціотехнічних систем є **системний підхід** [88–91] – *напрямок методології наукового пізнання, в основі якого лежить розгляд явищ (процесів, об'єктів), як систем* (рис. 2.26). Сукупність методологічних принципів і теоретичних положень системного підходу дозволяють:

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

простежувати зміни, що відбуваються у системі в результаті зміни окремих її ланок;

вивчати специфічні системні якості;

робити обґрунтовані висновки щодо закономірностей розвитку системи;

визначати оптимальний режим її функціонування.

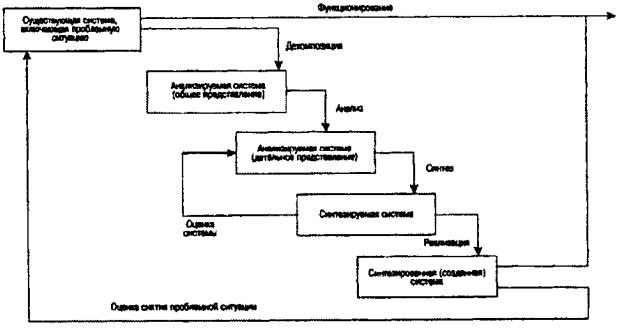


Рис. 2.26. Системний підхід до рішення проблемної ситуації

Основні етапи системного підходу:

формування проблеми;

виділення цілі або сукупності цілей;

визначення альтернативних засобів, за допомогою яких можна досягти цілі;

визначення ресурсів, необхідних при використанні кожної системи;

побудування математичної моделі, тобто ряду залежностей між цілями й альтернативними засобами їхнього досягнення;

визначення критеріїв вибору кращої альтернативи.

Основні принципи системного підходу:

принцип системності або *єдності* (вимагає розгляду, вивчення об'єктів досліджень як систем. Передбачає сумісний розгляд системи і як цілого, і як сукупності компонентів – елементів, підсистем, системотворчих відношень);

принцип кінцевої мети (зводиться до абсолютного пріоритету кінцевої або глобальної мети – основної функції, основного призначення тощо);

принцип зв'язності (довільна компонента системи розглядається сумісно з її зв'язками з оточенням);

принцип модульності (у багатьох випадках в системі доцільно реалізувати декомпозицію на складові різного ступеня загальності та розглядати її як сукупність певних модулів і зв'язків між ними);

принцип ієрархічності пізнання (в більшості випадків в системі доцільно реалізувати ієрархічну побудову та/або впорядкування її складових за важливістю). Принцип вимагає трирівневого вивчення об'єкту, а саме: вивчення самого об'єкту ("власний" рівень); вивчення цього ж об'єкту як елементу більш складної системи ("зовнішній" рівень); вивчення цього об'єкту у відповідності з його складовими ("нижчий" рівень);

принцип функціональності (вимагає спільного розгляду структури і функцій об'єкту з пріоритетом функцій над структурою. На практиці принцип функціональності зокрема означає, що у випадку надання системі нових функцій корисно переглянути її структуру, а не намагатися втілити нову функцію в стару схему реалізації системи);

принцип розвитку (повинен закладатися при побудові штучних систем як здатність до вдосконалення, розвитку системи за умови збереження якісних особливостей. Межі розширення функцій та модернізації повинні бути чітко усвідомленими творцями штучної системи, тому що існують доцільні межі її універсальності. Можливості для розвитку закладаються шляхом надання системі властивостей до самонавчання, самоорганізації, штучного інтелекту);

принцип децентралізації (в управлінні системою співвідношення між централізацією та децентралізацією визначається призначенням та метою системи. Загальним у цьому випадку має бути таке: ступінь централізації повинен бути мінімальним, що забезпечить досягнення остаточної мети);

принцип невизначеності (стверджує, що в багатьох випадках ми працюємо з системою, про яку або не все знаємо, або не все розуміємо у її поведінці. Тому невизначеності та випадковості повинні братися до уваги при визначенні стратегії та тактики розвитку системи);

принцип формалізації (підкреслює, що системний підхід націлений на отримання кількісних характеристик, створення методів, що звужують неоднозначність понять, визначень, оцінок тощо);

принцип інтеграції (відображає спрямованість системного підходу на вивчення інтегративних властивостей та закономірностей системи, розкриття

базисних механізмів інтеграції цілого).

Основними інструментами системного підходу є **системний аналіз** та **синтез**. Аналіз і синтез – загальнонаукові методи, без яких не може обійтися жоден акт наукового дослідження, є протилежно спрямованими (аналіз – від цілого до частини, синтез – від частин до цілого) і разом з тим нерозривно зв'язаними способами пізнання [90, 91].

Системний аналіз – це *методологія дослідження таких властивостей та відношень в об'єктах, які важко спостерігаються та важко розуміються, за допомогою представлення цих об'єктів у вигляді окремих складових частин, елементів, ознак і протилежностей цілеспрямованих систем, вивчення властивостей і взаємних відношень цих систем як відношень між цілями та засобами їх реалізації.*

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

враховує принципову складність об'єкта, що досліджується;

бере до уваги розгалужені та стійкі взаємні зв'язки його з оточенням;

враховує неможливість спостереження ряду властивостей об'єкта та оточуючого середовища;

реальні явища, їх властивості та зв'язки з оточенням переводяться далі в абстрактні категорії теорії систем;

ґрунтуючись на відомих властивостях складних систем дозволяє виявити нові конкретні властивості та взаємні зв'язки конкретного об'єкта дослідження;

на відміну від інших методів, в яких точно визначені об'єкти, включає як один з важливих етапів визначення об'єкта, його знаходження чи конструювання;

орієнтується не на розв'язання «правильно сформульованих» задач, а на створення правильної постановки задачі, вибір відповідних методів для її розв'язання.

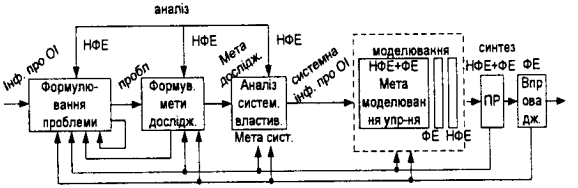


Рис. 2.27. Взаємозв'язок основних етапів системного аналізу

Основне в системному аналізі – знайти шлях, яким можна перетворити складну проблему в простішу, яким чином не лише складну до розв'язання, але й для розуміння, проблему перетворити в послідовність задач, для яких існують

методи їх розв'язання. Системний аналіз завжди конкретний – завжди має справу з конкретною проблемою, конкретним об'єктом дослідження, є продуктивним тоді, коли застосовується до розв'язання завдань певного типу. Він, як правило, спрямований на розв'язання складних слабко структурованих проблем, в яких переважають якісні, маловідомі і невизначені сторони, обумовлені:

неясністю розуміння проблеми;

складністю класифікації проблем і, як наслідок, вибором неадекватних засобів їх розв'язання;

спотвореною оцінкою проблем (близькі, але дрібні проблеми затуляють великі, але віддалені);

неправильною оцінкою значимості проблем внаслідок вузькопрофесійної точки зору;

складнощами постановки проблем на віддалену перспективу;

змішуванням цілей, які необхідно досягнути, з засобами їх досягнення.

Метою застосування системного аналізу до конкретної проблеми є підвищення ступеня обгрунтованості рішення, що приймається. Його основна функція полягає у виділенні таких ознак події, що могли б бути прийняті як підстава для об'єднання, систематизації фактів, розташування їх у відповідному порядку (хронологічному, функціональному, структурному і т.п.), який тим чи іншим чином характеризує визначену сторону розвитку досліджуваної події. За допомогою системного аналізу встановлюються протилежні властивості, тенденції події, що є сторонами визначених протиріч і дозволяють розкрити внутрішнє джерело розвитку події. Потреба в ньому виникає, коли:

формулюється (визначається) нова проблема, а її розв'язання потребує координації цілей з множиною засобів їх досягнення;

сформульована проблема має розгалужені зв'язки, що викликають віддалені наслідки в різних галузях, і прийняття рішення в таких випадках потребує врахування сукупної ефективності та повних затрат;

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

створюються нові складні системи або здійснюється вдосконалення (модернізація) існуючих, а важливі рішення повинні прийматися на достатньо віддалену перспективу за наявності невизначеності і ризику тощо.

Для забезпечення успіху системного аналізу потрібно:

застосовувати його у тих випадках, для яких він призначений;

мати потребу в його проведенні, уявляти мету та (або) його призначення;

відчувати відповідальне ставлення до нього як аналітиків, так і замовника;

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

відображати в результатах системного аналізу реальний стан справ та реальні шляхи розв'язання проблем, а не "обгрунтування" суб'єктивних рішень;

мати відповідні ресурси (кваліфікованих експертів, обладнання, гроші);

враховувати в роботі можливий вплив сторонніх побічних факторів (прогноз наукових відкриттів, винаходів, політичної ситуації).

Невід'ємною складовою системного аналізу є моделювання – процес дослідження реальної соціотехнічної системи (рис. 2.28), побудова її моделі (об'єкта, який має схожість с прототипом і є засобом опису, пояснення, прогнозування його поведінки), дослідження її властивостей та перенесення отриманих відомостей на систему, що моделюється.

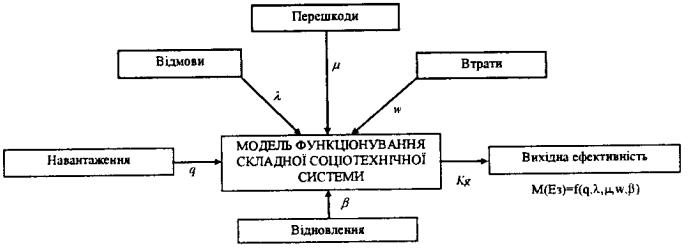


Рис. 2.28. Процес моделювання складної соціотехнічної системи

де

де

q – *параметри потоку навантажень*

λ – *параметри потоку відказів*

μ – *параметри перешкод*

w – *параметри втрат*

β – *параметри відновлення*

$K_г$ – *коефіцієнт готовності*

} *показники надійності*

Математична модель СТС в даному випадку має створюватись на принципах функціонального об'єднання моделей елементів і підсистем в єдиний комплекс програмно реалізованих алгоритмів, які здійснюють імітацію відповідних процесів для будь-яких вхідних умов і поточних станів.

Нині існує значна кількість різноманітних методологій та методів опису складних соціотехнічних систем. Найбільш відомими серед них є методи специфікації систем, що базуються на теоріях відносин і графів та відображають структури досліджуваних систем. Враховуючи таке під час опису СТС доцільно розглядати функціональні, технічні, організаційні, документальні, алгоритмічні, програмні, інформаційні та інші види структури таких систем (рис. 2.29).

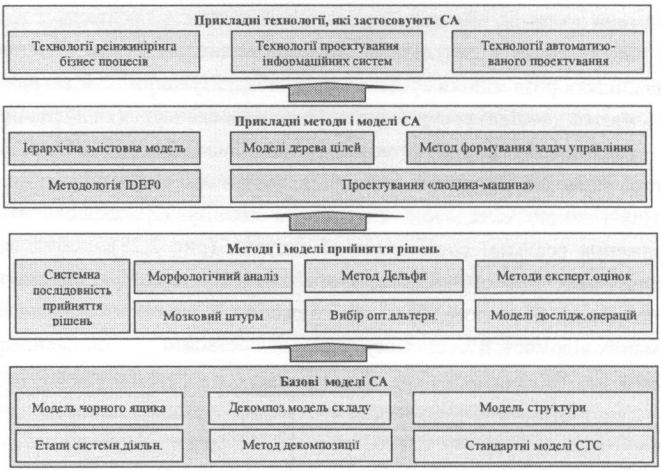


Рис. 2.29. Класифікація моделей і методів системного аналізу

Вони відрізняються між собою типами використовуваних елементів та зв'язками між ними (табл. 2.4).

Таблиця 2.4

Вид структур, їхні елементи й зв'язки.

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

Альтернативою зазначеним методам можуть служити методології сімейства IDEF. З їхньою допомогою можна ефективно відображати і аналізувати моделі діяльності широкого спектра складних систем у різних розрізах. При цьому широта й глибина обстеження процесів у системі визначатиметься самим розроблювачем.

Від інших методології сімейства IDEF відрізняються тим, що вони:

є простими в освоєнні;

дають специфікації, що графічно доступні для огляду;

дозволяють відобразити різні взаємозалежні й необхідні для проектування аспекти побудови системи;

допускають покрокове уточнення специфікацій;

не залежать від прикладної області системи.

У цей час до сімейства IDEF можна віднести такі стандарти:

по-перше, методологію функціонального моделювання – IDEF0. За допомогою наочної графічної мови IDEF0 досліджувана система з'являється 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 моделювання інформаційних потоків усередині системи – IDEF1, яка дозволяє відображати й аналізувати структуру та взаємозв'язки інформаційних потоків;

по-третє, методологію динамічного моделювання розвитку систем – IDEF2. У зв'язку з досить серйозними складностями аналізу динамічних систем від цього стандарту практично відмовилися, і його розвиток призупинився на самому початковому етапі. Однак у цей час присутні алгоритми і їхні комп'ютерні реалізації, що дозволяють перетворювати набір статичних діаграм IDEF0 у динамічні моделі, побудовані на базі "розфарбованих мереж Петрі" (CPN - Color Petri Nets);

по-четверте, IDEF3 - методологію документування процесів – IDEF3, що відбуваються в системі. За допомогою IDEF3 описуються сценарій і послідовність операцій для кожного процесу. IDEF3 має прямий взаємозв'язок з методологією IDEF0 - кожна функція (функціональний блок) може бути представлена у вигляді окремого процесу засобами IDEF3;

по-п'яте, методологію побудови об'єктно-орієнтованих систем – IDEF4. Засоби IDEF4 дозволяють наочно відображати структуру об'єктів і закладені принципи їхньої взаємодії, тим самим дозволяючи аналізувати й оптимізувати складні об'єктно-орієнтовані системи;

по-шосте, методологію онтологічного дослідження складних систем – IDEF5. За допомогою методології IDEF5 онтологія системи може бути описана з використанням певного словника термінів і правил, на підставі яких можуть бути сформовані достовірні твердження про стан розглянутої системи в деякий момент часу. На основі цих тверджень формуються висновки про подальший розвиток системи й виробляється її оптимізація.

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

У функціональній моделі система представляється у вигляді ієрархії функцій

(процесів, рішень, діяльностей). Для кожної з функцій вказуються: які об'єкти надходять на її входи, а які виробляються на її виходах; керуючі впливи та механізми реалізації функції. Функціональна модель повинна давати відповіді на такі питання про систему:

що представляє із себе система в цілому?;

яка декомпозиція функцій у системі?;

що перетворює функції системи та що є результатом їхнього виконання?;

що керує виконанням функцій?;

що необхідно для виконання функцій (які механізми)?;

як зв'язані функції та об'єкти?

Послідовно даючи відповіді на перераховані питання, можна побудувати функціональну модель будь-якої складної соціотехнічної системи.

Для інформаційних об'єктів функціональної моделі може бути побудована інформаційна модель. Вона описує відносини між елементами системи в вигляді структур даних (склад та взаємозв'язки) і у спрощеному варіанті вона будується 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, по яких розрізняються їхні екземпляри в межах кожного типу сутностей.

Інформаційна модель дає опис форм існування і представлення інформації в системі та операцій її перетворення.

Сучасні СТС забезпечують великий спектр форм представлення інформації та методів її перетворення і переведення з однієї форми в іншу залежно від характеру виконуваних задач, наприклад, в формі формалізованих і неформалізованих текстів на природній мові, формалізованих і неформалізованих графічних зображень, реляційних відношень, аудіо- повідомлень, відео- зображень тощо. Опис форм представлення інформації в цілому визначає характер взаємодії людини-оператора з інформаційною моделлю та її структуру. Динамічна модель відбиває часові характеристики системи й послідовність взаємодії функцій у часі. Тобто вона описує інформаційні процеси (динаміку функціонування), та оперує такими поняттями, як стан системи, події, перехід із одного стану в інший, умови переходу, послідовність подій. Динамічна модель будується за чотири кроки:

крок 1 - визначення діяльностей на які витрачається час;

крок 2 - визначення черг, де витрачається час на обслуговування;

крок 3 - визначення ресурсів, необхідних для виконання діяльностей;

крок 4 - завдання статистичних параметрів моделі, її входів і виходів.

Таким чином, дана сукупність моделей дозволяє описати як існуючу, так і майбутню соціотехнічну систему.

Системний синтез – *процес установлення зв'язків між виділеними елементами, ознаками, протилежностями, з'єднання їх і відтворення досліджуваної події в його істотних ознаках і відносинах.* Необхідною умовою його проведення є здатність дослідника бачити об'єкт у русі й тим самим відтворювати зв'язки між дійсним, минулим і майбутнім. Саме ці категорії виражають часову структуру образу пізнання, здатність дослідника відображати систему в процесі її розвитку. *Основна функція синтезу* – встановлення зв'язків між фактами й об'єднання їх у класи, групи, підгрупи і т.п. по виділених ознаках. За його допомогою простежуються відносини між фактами, характер взаємозв'язку між ними, розкриваються причини, функціональна залежність, з'ясовується послідовність етапів, ступенів, тенденцій розвитку досліджуваної події. Встановлюючи зв'язок фактів, синтез дає можливість визначити місце і роль кожного з них у загальному ланцюзі розвитку події, простежити дійсне положення речей. Синтез систем (складних проектів і програм) проводиться в чотири етапи. На першому з них здійснюється вибір методу синтезу і розробка математичної моделі оптимізації (математична модель оптимізації являє собою сукупність математичної моделі функціонування системи і моделі, що реалізує обраний метод оптимізації на ЕОМ). На другому – розроблення технічного завдання на програмування і налагодження. На третьому – перевірка адекватності моделі, й на четвертому – рішення задачі, корекція і реалізація результатів синтезу.

Системний синтез може здійснюватися трьома методами:

1) *аналітичним* – характеризується тим, що задача формулюється математично суворо та з урахуванням цього реалізується на ЕОМ;

2) *імітаційним* – сприяє отриманню статистичних даних про найбільш доцільні напрями оптимізації системи залежно від зміни її функціонування. У загальному випадку імітаційний синтез характеризується такими обставинами:

по-перше, його можна розглядати як експериментальне визначення статичних характеристик випадкового процесу за допомогою машинного експерименту, що дуже часто включає оптимізацію;

по-друге, його можливо трактувати як синтез за допомогою варіаційних розрахунків. Імітаційне моделювання може проводитись такими методами: методом варіантних розрахунків; методом статистичних іспитів; методом на основі множини досяжності тощо;

3) *евристичним* – застосовується для синтезу систем, які формалізовані недостатньо суворо, а також не можуть бути чітко виражені математично та

вирішені за допомогою аналітичного методу або шляхом імітації.

Вони дають можливість об'єднати математичні і неформальні методи, суворі способи дослідження формалізованих моделей з експериментом та евристичними прийомами. При цьому аналітичний та імітаційний методи головним чином базуються на відомих методах оптимізації. Так, наприклад, залежно від типу моделі (статистична або динамічна) задачу оптимального синтезу доцільно вирішувати методом математичного програмування або варіаційним методом.

Одним із різновидів складних соціотехнічних систем при створенні яких повною мірою реалізується теорія системного підходу є **інформаційно-телекомунікаційні системи.** Вони являють собою сукупність **інформаційних** – *організаційно-технічних систем, в яких реалізовані технології обробки інформації з використанням технічних і програмних засобів й які забезпечують вироблення певних управлінських рішень* та **телекомунікаційних** – *власне 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 інший спосіб* **систем**, *які у процесі обробки інформації, призначеної для забезпечення реалізації певних інформаційних потреб, діють як єдине ціле та орієнтовані на виконання визначених (спеціальних) функцій і завдань.* За рахунок впровадження і реалізації сучасних **ІКТ** – *методів і засобів функціональних, змістовних та забезпечувальних компонент інформаційно-комунікаційної структури які, будучи об'єднаними засобами ЕОТ, підтримують процеси циркуляції і переробки інформації, визначають хід використання інформації та впливають на надійність і оперативність виконання 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 і значущості;

подання інформації у зручному для користувачів вигляді та організації зворотного зв'язку з нею;

використання інформації для оцінювання тенденцій, розробки прогнозів, оцінювання альтернатив рішень і дій, вироблення стратегій тощо.

Виходячи з такого мета створення будь-якої ІТС полягає в тому, щоб у гранично короткі терміни створити систему обробки інформації, яка має задані споживчі якості, а саме продуктивність, відмовостійкість, сумісність, розширюваність, масштабованість і ефективність та характеризується властивостями:

1) *загальності і абстрактності* (як системи розглядаються предмети,

явища природи, різні процеси);

2) *множинності* (кожна сукупність елементів, яка може бути підмножиною різних систем, відрізняється системотворчими властивостями та конкретними відношеннями елементів один з одним);

3) *цілісності* (система поводить себе 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 їх властивості суттєво визначаються всією системою. В свою чергу, система визначається властивостями елементів, але не зводиться до їх суми. Вона має деякі нові визначальні 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 в той же час вона є системою зі своїми елементами і зв'язками. Відомо, що досліджувана складна система будується з елементів завдяки існуванню зв'язків між ними. Сукупність усіх зв'язків та їх певний порядок складає структурну організацію системи, яка може мати ряд рівнів і специфічних "зрізів", що знаходяться у відношеннях субординації та координації між собою. В організації таких систем дуже важливе значення мають прямі та зворотні зв'язки, а також структури, що забезпечують процес управління);

6) *синергізму* (ефективність функціонування кожної системи є вищою за сумарну ефективність ізольованого функціонування її елементів. Відомо, що кожний елемент системи та система в цілому певним чином проявляють себе, діють на інші елементи і систему, на зовнішнє середовище, тобто здійснюють деякі функції. Ці функції закономірно пов'язані з структурою системи і зовнішнім впливом на неї. Установивши зв'язки між структурою і функціями, між "входами" та "виходами" системи, можна докорінно змінювати її стан).

Довільна модель складної ІТС, що поєднує соціальну та технічну складові, які врівноважуються між собою за рахунок так званих модераторів (ролей у системі кожного працівника, цілей узгодження бажань працівників із технічними можливостями, умінь працівників та їх здатностей) подана на рис. 2.30.

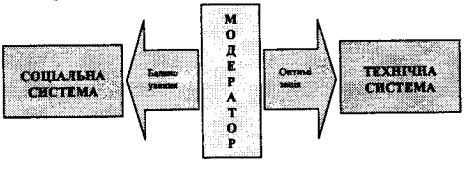


Рис. 2.29. Соціотехнічна модель складної ІТ системи

Моделі ІТС складаються з підсистем і компонент. До їх найбільш визначальних **підсистем** – *виділених за деякими признаками частин глобальної системи, що виконують завдання з прийому та передачі даних від інших підсистем і компонентів, їх обробки та збереження*, згідно [92–97], належать **телефонні** – *призначені для передачі мовної інформації*, **радіо** – *призначені для передачі мовної інформації і даних*, **комп'ютерні** – *призначені для передачі даних у будь-якій формі*) та **телевізійні** – *призначені для передачі мовної інформації та зображення* мережі. Їх лідируюча роль у сучасному інформаційному суспільстві визначається такими взаємозалежними чинниками:

1) потребою держав світу в одержанні найрізноманітнішого економічного, наукового, культурного та іншого ІР;

2) рівнем телефонізації держав світу, розвиненістю їх систем електрозв'язку та їх інтегрованістю з міжнародними мережами;

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

4) наявністю у державах світу досить розгалуженої системи загальнодоступних баз даних та різних довідкових служб;

5) злиттям технологій радіо, телефонних та інших ІТ мереж тощо.

Зазначені 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, але й бойові платформи, і в першу чергу такі, що є носіями засобів вогневої поразки. Їх складовими можуть бути також засоби розвідки, контррозвідки та спостереження, системи інформаційного забезпечення операцій, дипломатичних заходів та соціальних процесів.

Під **компонентами ІТС** – технічною, інформаційно-методичною, організаційною, нормативно-правовою тощо, згідно [92–97], розуміють *елементи засобів забезпечення, що виконують визначені програмно-технічні функції в тій або іншій її підсистемі.* При цьому, наприклад, технічна компонента може включати до свого складу пристрої для прийому, передачі, обробки і зберігання інформації. Інформаційно-методична компонента об'єднує, як правило, низку споріднених компонент лінгвістичного, математичного, програмного, інформаційного та інших видів забезпечення. При цьому, наприклад, компонента лінгвістичного забезпечення має включати термінологічні словники, правила формалізації даних та засоби діалогової взаємодії посадових осіб з технічними і програмними засобами СІТС. Компонента математичного забезпечення – загальне та спеціальне математичне

забезпечення (математичні методи, моделі/процедури та алгоритми). Компонента програмного забезпечення повинна включати:

1) 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 тощо;

2) спеціальне програмне забезпечення (СПЗ) – програмно-апаратні засоби, що дозволять вирішувати специфічні задачі управління, які не можуть бути вирішені програмами загального програмного забезпечення;

3) програмну документацію.

Компонента власне інформаційного забезпечення має складатися з комплексу спеціалізованих системних програм, що призначені для пошуку, збору, добування та обміну інформацією й включати відомості про користувачів, систему форм і шаблонів електронних документів, системні та інші журнали, що необхідні для відслідковування етапів функціонування системи та здійснення відповідного контролю інших компонент і сервісів тощо. Організаційна та нормативно-правова компоненти повинні включати: базу даних нормативно-правових актів законодавства України; методичний апарат організації та ведення роботи; розподіл повноважень, прав, завдань та обов'язків; режимні правила та обмеження згідно чинного законодавства.

Структурно ІТС в цілому та її функціональні підсистеми включають до себе: технічні засоби; інформаційні канали; оточуюче середовище та обслуговуючий персонал. До обслуговуючого персоналу відноситься весь персонал, який будь-яким чином пов'язаний з існуючою ІТС (оператори, адміністратори, техніки тощо). До оточуючого середовища – будинки, службові приміщення, шахти в яких знаходяться елементи ІТС тощо. Інформаційні канали в даному випадку являють собою систему взаємопов'язаних елементів інформаційної середи. У результаті їх взаємодії створюються поля, що переносять ІР та забезпечують його передачу в середу розповсюдження у заданому напрямку. Під середою розповсюдження у цьому випадку розуміють, як правило, частину простору в якій інформація переміщується. Вона визначається набором фізичних параметрів, основними з яких є часові і частотні характеристики, а також характеристики перепускної спроможності та параметри навантаження.

У цей час системний підхід до створювання складних ІТС грунтується на однокритеріальному або багатокритеріальному оцінюванні альтернатив. Найбільш відомий варіант системного аналізу зв'язаний з однокритеріальним оцінюванням за показниками вартості та ефективності (критерій "ефективність-

вартість"). В цьому випадку вибір раціональної ІТС (раціонального зразка ОВТ, раціонального проекту) проводиться за максимумом цільової функції при заданій вартості. За цільову функцію обирається критерій ефективності використання коштів, що були витрачені, наприклад, на розробку нового (проведення модернізації існуючого) зразка (системи) ОВТ. Суть даного критерію полягає у визначенні того, який бойовий (потенціальний) ефект очікується від зразка в конкретних умовах застосування, при конкретних витратах на його розробку та серійне виробництво: $K=E/C$, де K – критерій "ефективність-вартість"; E – показник ефективності зразка озброєння; C – показник вартості зразка озброєння, що забезпечує задану ефективність.

Методи багатокритеріального оцінювання альтернатив є більш універсальними. Існуючу їх множину можна об'єднати в ряд таких груп: 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 виникають дві основні проблеми, а саме: по-перше, як одержати оцінки за окремими критеріями; по-друге, як об'єднати ці оцінки в загальну оцінку корисності альтернативи.

Для формування багатокритеріальної оцінки складної ІТС (СІТС) нині використовується така система показників [1]:

а) коефіцієнт результативності K_p – визначає міру вкладу (ефекту) СІТС у результативність певних завдань. Визначається через продуктивність ІТС – швидкість виконання нею регламентованих дій. У загальному випадку коефіцієнт результативності визначається співвідношенням:

$$K_p = \sum_{n=1}^{H_0} P_n B_n \Pi_n \Big/ \sum_{n=1}^{H_0} P_n B_n \qquad (2.1)$$

де Π_n – продуктивність СІТС за певний період часу; P_n – імовірність появи інформації n-ї категорії; B_n – коефіцієнт важливості інформації n-ї категорії; H_0 – загальна кількість введених категорій важливості;

б) коефіцієнт ефективності K_e – визначає міру відношення ефекту застосування СІТС до витрат на його досягнення і характеризує її результативність;

в) коефіцієнт новизни K_n – визначає міру рівня та ступеня використання нових ідей і технічних рішень при проведенні модернізації (оновлювання) СІТС. Характеризує відносний рівень підвищення результативності K_p, який можуть забезпечити на момент початку модернізації нові ідеї та нові технічні рішення. Визначається за формулою:

$$K_н = K_{рн} K_{ор} K_{свп}, \tag{2.2}$$

де $K_{рн}$ – показник рівня новизни ідей; $K_{ор}$ – показник об'єму реалізації нових ідей; $K_{свп}$ – показник ступеня впливу нових ідей і нових технічних рішень на результативність зразка техніки. При цьому значення показників $K_{рн}$, $K_{ор}$ та $K_{свп}$ визначаються експертним оцінюванням;

г) коефіцієнта перспективності $K_п$ – визначає міру рівня морального старіння елементів СІТС на момент завершення їх розробки. Характеризує відносний рівень результативності $K_р$, який очікується на момент закінчення розробки певної СІТС за рахунок нових ідей і технологічних рішень. Величина $K_п$ визначається експертним оцінюванням;

д) коефіцієнт технологічності $K_Т$ – визначає міру науково-технічного рівня технології проектування та виробництва СІТС на момент початку її розробки. Характеризує технологічні можливості із забезпечення початкового рівня результативності (на початку модернізації СІТС) з використанням реалізованих ідей і технічних рішень. Практично визначає потенційний рівень результативності попереднього покоління техніки, як відправну точку для розробки нового або оновлювання існуючого. Величина $K_Т$ визначається експертним оцінюванням;

ж) коефіцієнт технічного (воєнно-технічного) ризику $K_{втр}$ – визначає міру бажаних наслідків при невдалій реалізації заданих тактико-технічних вимог (ТТВ). Визначає імовірність невиконання ТТВ:

$$K_{втр} = 1 - P_{кр}, \tag{2.3}$$

де $P_{кр}$ – імовірність того, що отримане значення коефіцієнта результативності знаходиться у заданому інтервалі допущень.

Величина $P_{кр}$ визначається експертним оцінюванням, а її верхні і нижні межі задаються у технічному завданні (ТЗ);

з) коефіцієнт технологічного ризику $K_{тр}$ – визначає міру невдач при завершенні розробки нового або модернізації існуючої СІТС у визначені терміни. Визначається як імовірність того, що реалізована тривалість $T_р$ її розробки (оновлювання) виявиться поза межами заданого інтервалу допущень:

$$K_{тр} = 1 - P_{тр}, \tag{2.4}$$

де $P_{тр}$ – імовірність того, що величина $T_р$ знаходиться у заданих межах які задаються у ТЗ. Величина $P_{тр}$ визначається експертним оцінюванням.

Означена система показників у цілому може бути представлена при цьому таким чином:

$$K = \left\{ K_{\kappa\kappa} \quad \updownarrow \quad k = \overline{1, kk} \right\} \tag{2.5}$$

де k – порядковий номер показника; kk – загальна кількість показників, що використовуються у кожній конкретній експертизі.

Питання для самоконтролю

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

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

3. Дайте визначення поняттям «інформаційна» та «кібер» зброя. Чим обумовлюється їх перевага порівняно з іншими видами зброї?

4. Дайте визначення поняттям «інфосфера», «інформаційна» та «кібер» операція.

5. Назвіть напрями діяльності по створенню дієвої системи кібербезпеки.

6. Що є базисом для розробки моделей кібернападу і кіберзахисту? Наведіть приклади моделей, що є найбільш відомими.

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

8. Дайте визначення поняттю «розвідка інформаційно-телекомунікаційних систем» та основним способам її ведення: розвідці систем телекомунікацій, мережевій і кіберрозвідкам.

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

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

11. Яким вимогам має задовольняти система інформаційного забезпечення кібернетичної безпеки? Перелічте основні вимоги до програмно-апаратних комплексів кіберрозвідки.

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

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

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

15. Дайте визначення поняттю «соціальна мережа». Які класи соцмереж Вам відомі? Чим регламентується поведінка агентів у мережі?

16. Назвіть основні відмінні риси 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 відомі Вам його основні різновиди.

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

20. Дайте визначення складним технічним і соціотехнічним системам. Перелічте їх основні характеристики

21. Що Ви розумієте під системним підходом до створення складних соціотехнічних систем? Назвіть основні принципи та етапи системного підходу.

22. Назвіть основні інструменти системного підходу. Дайте їм визначення.

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

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

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

26. Якими методами системний синтез забезпечується?

27. Дайте визначення поняттю «інформаційно-телекомунікаційна система» та її складовим. Перелічте основні властивості ІТС.

28. Наведіть приклад моделі складної ІТС. Дайте визначення поняттям «підсистема» та «компонента» ІТС.

29. Якими чинниками обумовлюється лідируюча роль ІТС у розвитку інформаційного суспільства?

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

31. Перелічте показники, які використовуються для багатокритеріальної оцінки ІТС. Розкрийте їх сутність.

Розділ 3
МЕТОДИ І ЗАСОБИ СОЦІАЛЬНОГО ІНЖИНІРІНГУ

Глибинні зміни у відношенні більшості держав земної кулі (зокрема і України) до власної інформаційної й, як наслідок, кібернетичної безпеки фактично зумовлюють необхідність розроблення рекомендацій щодо коротко- та довгострокових пріоритетів трансформації їх безпекового сектору за напрямами пошуку і збору інформації з відкритих та відносно відкритих та її добування із закритих електронних джерел й обміну такою, а також захисту власного ІР від стороннього кібервпливу. Зазначені проблеми в певних аспектах висвітлено у багатьох публікаціях зарубіжних і вітчизняних авторів. Найвідомішими серед них є роботи В.В. Домарєва, Дж. Козіола [98], М. Кузнєцова [99], Кр. Касперськи [100], К. Митника, І. Симдянова та інших фахівців. Певною мірою вони також знайшли відображення у розділі 2 цього підручника. Проте проведений аналіз першоджерел свідчить, що комплексного дослідження процесів розвідувальної діяльності у ІТ середовищі й передусім поведінки у ньому так званого когнітивного базису [101] – звичайних користувачів, професійних шпигунів та/або хакерів (порушників тощо) та способів і методів які вони застосовують до цього часу нажаль не проводилось. Саме тому викладення основних понять і особливостей соціального інжинірингу, як одного із можливих методів розвідки ІТС нині є завданням найбільш актуальним.

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

Від інших видів розвідка ІТС, структуру якої надано на рис. 2.10, відрізняється насамперед механізмами – способами і методами, а також силами і засобами, що задіяні у процесах збору та/або добування інформації [59, 102]. Головними способами її ведення слід вважати розвідку систем телекомунікацій (РСт), мережеву (МР) і кіберрозвідку (КР) які, як зазначено у розділі 2, спрямовані на систематичний пошук, збір та/або добування:

інформації про об'єкти розвідки у ІТ системах її передавання, випромінювання і приймання та захищених криптосистемах – РСт, а також у відкритих і відносно відкритих електронних джерелах – КР;

даних про ресурси, засоби захисту, пристрої та програмне забезпечення (ПЗ), що використовується в ІТС об'єкта розвідки, їх уразливі місця та межі проникнення (МР), – з подальшим обліком та накопиченням такої інформації, її верифікацією, вивченням та аналітичною обробкою.

Зважаючи на те що силами і засобами РСт та МР добувається відповідно до

5–8 % та до 7 % інформації, яка необхідна протиборчим сторонам одна про одну, останнім часом надзвичайно розвинувся такий спосіб розвідки ІТС, як КР. Її силами і засобами нині може добуватися від 35 % до 95 % інформації про об'єкти розвідки, яка має властивість не тільки не відрізнятися від військових і державних таємниць, але й часто перевершувати їх за своєю цінністю. Залежно від важливості та специфіки покладених завдань, наявних ресурсів, а також за методами, що застосовуються для пошуку і збору інформації [59], кіберрозвідка ІТС поділяється на (рис. 3.1) технічний і програмний методи її ведення, метод так званої соціальної інженерії (СІ), а також метод, що передбачає моніторинг відкритих і відносно відкритих електронних джерел (аналог відомої OSINT розвідки).

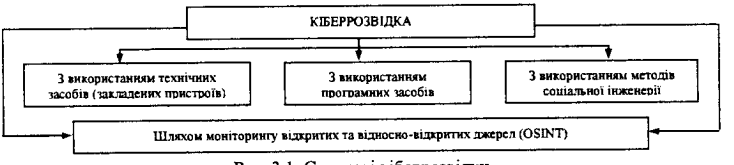


Рис. 3.1. Складові кіберрозвідки

Враховуючи, що саме завдяки людському чиннику в умовах стрімкого розвитку мережі Internet можуть бути подолані такі відомі технології безпеки, як міжмережеві екрани, пристрої ідентифікації, засоби шифрування, системи виявлення мережевих атак тощо, західні і вітчизняні фахівці [98–103, 109–119] вважають нині СІ одним із найбільш перспективних методів розвідки ІТС й передусім такого її різновиду, як кіберрозвідка (КР). Основними цілями методу вони вважають отримання неавторизованим користувачем (хакером, порушником тощо) інформації про призначення, структуру, встановлені права доступу, систему захисту, реєстраційні імена і паролі, а також іншої конфіденційної інформації про об'єкт атаки (розвідки) шляхом несанкціонованого доступу до ресурсів Інтернет, використовуючи для цього слабкість або некомпетентність, непрофесіоналізм або недбалість людину (або групи людей) та керуючи її (їх) діями.

Тобто, суть СІ – заставити людину здійснити певні дії, які йому не вигідні, але необхідні атакуючому. Типологія інформаційних джерел для діяльності соціоінженера може бути представлена при цьому такими ресурсами:

соціальними закладками (social bookmarking), які створюють список закладок або популярних web-сайтів та використовуються для пошуку користувачів із спільними інтересами (Delicious);

соціальними каталогами (social cataloging), які орієнтовані на наукову сферу для роботи с базами даних, цитатами з наукових статей (Academic Search Premier, LexisNexis, Academic University, CiteULike, Connotea);

соціальними бібліотеками, які містять посилання на книги, аудіозаписи тощо з системою рейтингів и т. п. (discogs.com, IMDb.com);

соціальними мережами web-майстрів, які містять посилання на пости, звернення тощо. Часто мають рейтинги або рекомендації;

багатокористувальницькими мережевими іграми (Massively Multiplayer Online Games), які імітують віртуальні світи з різними системами переможців і переможених (World of Warcraft);

геосоціальними мережами, які містять дані про геолокації, наприклад GPS для визначення місця розташування користувача, а також створюють про файли місць, де вони зараз;

професійними соцмережами для пошуку роботи, розвитку ділових зв'язків (LinkedIn, MarketingPeople тощо);

віковими та гендерними соцмережами для відповідних користувачів.

Для пошуку та збирання з них інформації про об'єкт атаки соціоінженери користуються нині, як правило, механізмами претекстінгу, фітингу, бейтінгу та ним подібними, де:

1). ПРЕТЕКСТИНГ (готовь сценарий) A → B → C → !!! — *- дії, що в ході атаки, здійснюваної зазвичай по телефону або по «Skype», відпрацьовуються порушником за заздалегідь сформованим сценарієм і мають на меті забезпечити його входження у довіру до жертви*

Для одержання інформації Pretexting припускає використання зловмисником голосових засобів зв'язку (телефон, Skype і т.п.) з метою представлення себе третьою особою або особою, яка потребує допомоги. Найкраща стратегія – використання спочатку невеликих запитів і згадування імен реальних людей в організації, звичайно керівного складу. У процесі розмови зловмисник пояснює, що він потребує допомоги (більшість людей готові виконати невеликі завдання, які не сприймаються ними як підозрілі запити). Як тільки довірчий зв'язок установлений, зловмисник може попросити щось більш істотне й з великим успіхом.

Метод Pretexting особливо ефективний стосовно нетехнічних користувачів, які можуть володіти корисною інформацією.

2). ФИШИНГ (РЫБАЛКА ;) Забросил удочку и ожидай рыбку — *- дії, що в ході атаки, здійснюваної порушником через e-mail, вимагають від потенціальної жертви розголосити певну конфіденційну інформацію про себе – логіни, паролі тощо шляхом її так званої перевірки*

Метою більшості фішингових листів є спроба примусити користувача нажати щось і записати 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 електронного повідомлення під конкретного користувача, нібито отриманого з

надійного джерела, збільшує ймовірність того, що користувач прочитає пошту або навіть зробить дії згідно наведених рекомендацій, позначених у тексті повідомлення.

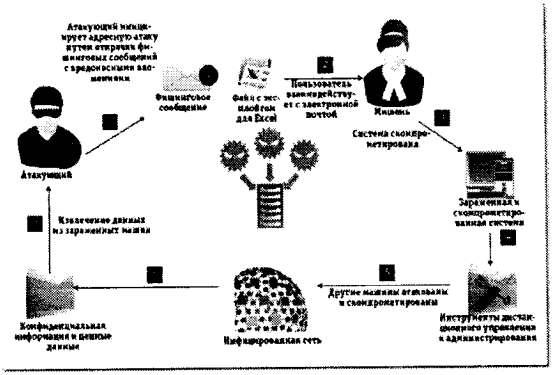


Рис. 3.2. Адресна атака з фішинговим повідомленням

За оцінками фахівців, більше 70% фішингових атак у соцмережах є успішними. Фішинг стрімко набирає свої оберти, а оцінки збитку сильно відрізняються: за даними компанії «Gartner», у 2008 році жертви фішерів втратили 2,4 мільярди доларів США, в 2009 році – збиток склав 2,8 мільярди доларів, в 2010 – 3,2 мільярди (табл.3.1).

Таблиця 3.1

Економічні показники атак масованого і цільового фішингу на типову установу

Типова установа	Атака масованого фішинга	Атака цільового фішинга
Витрати на проведення	2 000$	10 000$
Загальна кількість направлених повідомлень	1 000 000	1000
Доля заблокованих повідомлень	99%	99%
Доля відкритих повідомлень	3%	70%
Доля повідомлень з використаними посиланнями	5%	50%
Доля успіху	50%	50%
Дохід від одної жертви	2 000$	8 000$
Загальний прибуток	14 000$	150 000$

Відносно окремої установи економіка цільового фішинга може бути набагато цікавішою. Не зважаючи на те, що витрати на проведення такої операції значно вище порівняно із масовим фітингом (за оцінками Cisco SIO - приблизно у п'ять разів), але й вищими може бути як дохід, так і прибуток. Це пояснюється якістю отримання адрес, орендованого ботнета, а також вартістю засобів генерації повідомлень електронної пошти, придбаного злоякісного ПЗ, створеного сайта,

засобів управління установою, базової інфраструктури обробки заказів, послуг провайдерів з реалізації та вивчення даних користувачів тощо.

БЕЙТИНГ *(а-ка троян)* 3). *В отличие от трояна – целевой*	- запуск злоякісного ПЗ, наприклад, троянських програм (бекдорів, руткітів, кейлогерів, клікерів та проксі-троянів) як відповіді на e-mail запит порушника або через інфікований CD (флеш-накопичувач)

Злоякісне ПЗ створюється з використанням широкого класу технологій і поступово стає дедалі більш серйозною проблемою. Його метою може бути:

закачування або скачування файлів;

копіювання помилкових посилань, що ведуть на підроблені веб-сайти, чаты або інші сайти з реєстрацією;

створення перешкод роботі користувача;

викрадення даних, що представляють цінність або таємницю, у тому числі інформації для аутентифікації, для НСД до ресурсів;

поширення інших шкідливих програм, таких як віруси;

знищення даних (стирання або переписування даних на диску, ушкодження файлів) і встаткування, виведення з ладу або відмови обслуговування комп'ютерних систем, мереж;

збір адрес електронної пошти й використання їх для розсилання спама;

шпигунство за користувачем і таємне повідомлення третім особам яких-небудь відомостей;

реєстрація натискань клавіш із метою крадіжки інформації такого роду як паролі й номери кредитних карток;

дезактивація або створення перешкод роботі антивірусних програм і файєрвола.

Діє злоякісне ПЗ відповідно до схеми, представленої на рис. 3.3,

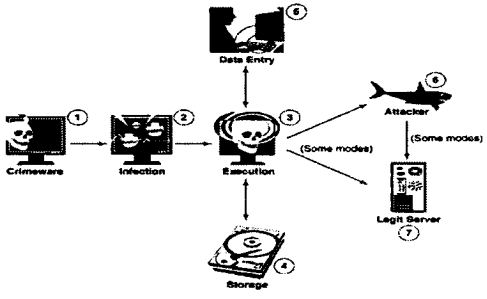


Рис. 3.3. Структурно-логічна схема організації бейтинг-атак

де 1 – етап розповсюдження злоякісного ПЗ засобами соціального інжинірінгу;

2 – етап інфікування ПЕОМ;

3 – етап запуску злоякісного ПЗ шляхом проведення одноразової атаки або за рахунок реконфігурування системи (впровадження руткітів);

4 – сканування пам'яті системи на наявність у ній конфіденційних даних;

5 – крадіжка конфіденційних даних з пам'яті системи;

6 – пересилання конфіденційних даних за визначеною адресою;

7 – отримання сервером конфіденційних даних або від злоякісного ПЗ, або від атакуючого.

Більшість випадків поширення злоякісного ПЗ ґрунтується на соціальних пастках і проводиться спеціально для одержання фінансової вигоди.

4). QUI PRO QUO *(что-либо вместо чего либо) Представился другом – рассказут секрет ;)* - несанкціоноване надання додаткових прав і можливостей зареєстрованим користувачам системи.

Цей вид атаки передбачає дзвінок соціального інженера в організацію по корпоративному (внутрішньому) телефону. У більшості випадків соціальний інженер представляється співробітником технічної підтримки, що робить опитування на виникнення технічних проблем. Під час процесу «рішення» технічних проблем, соціальний інженер «змушує» користувача вводити команди, які дозволяють йому запустити або встановити шкідливе ПЗ на його комп'ютер.

Прикладом застосування означених підходів можуть слугувати троянський proxy-сервер "Mitglieder" та ICQ-черв'як "Bizex", що з'явилися у 2004 році [100, 104]. Перший з 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. Таким чином, заражені машини утворювали мережу машин-зомбі (ботнет), якими можна було керувати віддалено. Для поширення ICQ-черв'яка "Bizex" порушники використовували масове несанкціоноване розсилання по ICQ повідомлення "http://www.jokeworld.biz/index.html:)) LOL". Одержавши таке повідомлення об'єкт атаки, що нічого не підозрював, відкривав зазначену сторінку й у випадку, якщо використовувався браузер Internet Explorer з незакритою уразливістю, на комп'ютер завантажувалися файли черв'яка, а в деяких випадках і супутнього йому троянa. Після установки в систему "Bizex" закривав запущений ICQ-клієнт і, підключившись 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 прийняття рішень звичайними користувачами, професійними шпигунами та/або хакерами, яких у західних інформаційних джерелах нині називають когнітивним базисом [59].

Ще одним із механізмів, використовуваних порушниками для одержання спеціальної інформації з ІТС, нині вважається створення підставних профілів. Найбільш відомим прикладом цьому було створення Томасом Райаном з Provide Security підставного профілю молодої симпатичної дівчини 25 років, яка за легендою була фахівцем з 10-річним стажем роботи в 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 на додавання в друзі 300 чоловікам і жінкам із числа військових, співробітників секьюриті-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 самостійно додавати в друзі інші люди – колеги тих, кому "спеціалістка у сфері безпеки" нав'язала своє спілкування першою. У такий спосіб Томас Райан одержав доступ до великої кількості особистої інформації (персональних даних), фотографій, а також розкрив зв'язки спілкування певних фахівців, що становили для нього певний інтерес.

Але, як виявляється, СІ не вичерпується одними лише соціальними мережами. Прикладом цьому став конкурс, проведений на одній з конференцій Defcon, у ході якого всім бажаючим було запропоновано за один дзвінок тривалістю у 25 хвилин витягнути максимум інформації, що сприяла б організації успішної кібератаки. Один з учасників конкурсу зумів за допомогою всього двох телефонних дзвінків ввести в оману співробітника технічної підтримки компанії British Petroleum та змусити його видати інформацію, яка б допомогла в організації кібератаки 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 установлені на цих комп'ютерах. Крім того, переможець примусив співробітника British Petroleum відвідати сайт Social-Engineer.org, завдяки чому заробив ще декілька додаткових балів. Крім цього доволі відомими є випадки, коли хакери отримували нагоду проникнути до ІТС об'єкта розвідки за результатами вивчення вмісту сміттєвих ящиків, наприклад, у Нью-Йоркській телефонній компанії, або ж шляхом виявлення слабких місць у системі мережної безпеки. Одним з таких місць у мережі банку BABank (США) виявилось закриття порта технічного обслуговування паролем, встановленим виробником [101]. Як результат хакери отримали всі права

доступу до системи. У подальшому внаслідок використання на поштовому сервері застарілої версії Unix хакери встановили над цим сервером контроль і отримали змогу взаємодіяти 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", метою якого було 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 Германії з'ясували, що:

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

по-друге, 43 % з опитаних визнали, що у певні моменту часу бізнес структури, які вони представляли зазнали цільових атак методом СІ, кожна з яких потенціальній жертві обійшлася приблизно у 25–100 тисяч доларів. При цьому майже 70 % усіх порушень, пов'язаних з безпекою інформації, здійснювалось саме співробітниками цих структур;

по-третє, майже третина з досліджених бізнес структур була атакована 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 % досліджених структур), а основними методами їх роботи є розсилання фішингових листів (47 % респондентів), вплив через соціальні мережі (39 % респондентів), а також через незахищені мобільні пристрої (12 % респондентів).

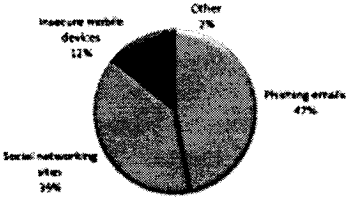


Рис. 3.4. Джерела проектування соціальних загроз

Найбільш сприйнятливими до таких дій на думку опитаних є нові співробітники (60 %), підрядники (44 %) та виконавчі помічники (38 %). При цьому 40 % відсотків респондентів усю відповідальність за можливі витоки покладають саме на персонал (рис. 3.5). Для унеможливлення ризику впливу на нього методами СІ частина учасників дослідження, а саме 26 % з них засвідчила, що регулярно проводять

відповідні тренінги для персоналу або планують розроблення відповідної програми (19 %), а 34 % респондентів констатувала, що взагалі не приділяють уваги щодо підготовки персоналу для попередження збитків від застосування методів CI.

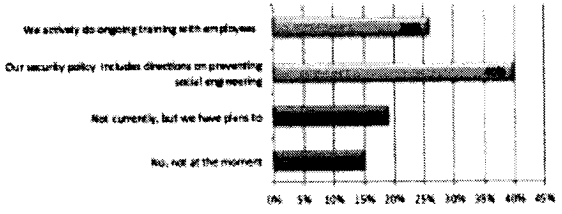


Рис. 3.5. Результати реагування на соціальні атаки

Для захисту користувачів від CI 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. Їх перевага обумовлюється можливістю вирішення 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 потенціальні канали витоку інформації (генератори шуму, мережеві фільтри, скануючі радіоприймачі тощо). Їх переваги обумовлюються 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, видалення тимчасових файлів тощо. Їх переваги полягають в універсальності, гнучкості, надійності, здатності до модифікації і розвитку. Недоліки обумовлюються 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 з давніх-давен. Так, наприклад, «нічні демони» в Японії, або ніндзя, вельми активно використовували властивості людського розуму наряду з гіпнозом. 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 їх імені, вони, використовуючи вигідні аргументи, підлещування або завуальовану дезінформацію, вели дипломатичні переговори й були здатні вирішити певні питання не тільки особистого, а й державного рівня. СІ завжди була головною зброєю і у середовищі шпигунів (розвідників). Так, наприклад, агенти КДБ СРСР та ЦРУ США вміли, видаючи себе за іншу особу, вивідати державні таємниці. Тобто в усі часи спрацьовувала приказка: "… найслабкіша ланка системи безпеки – людина …".

У сучасному розумінні поняття СІ з'явилось досить недавно. Вперше 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

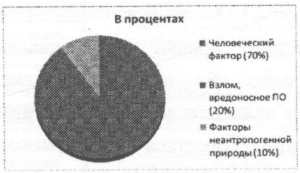


Рис. 3.7. Загрози інформаційної і кібербезпеки у відсотках

застосовувати можливості соціального інжинірингу для (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 Internet шляхом ведення діалогу з нею або з її оточенням у службах обміну миттєвими повідомлення (messenger), наприклад, ICQ;

одержання закритої (конфіденційної) інформації про об'єкт атаки (розвідки) або інформації, що становить для порушника певний інтерес, наприклад, номери телефонів потенційної жертви, адресу її прописки/проживання, реальне ім'я і прізвище та іншої подібної інформації шляхом встановлення контакту з нею та/або уведення її в оману;

одержання інформації про об'єкт атаки (розвідки), що необхідна для забезпечення НСД до системи, а саме пароля, яким користується потенційна жертва, серії й номеру її паспорта та інших відомостей про неї шляхом входження до жертви у довіру;

примушення об'єкта атаки (розвідки) до дій, необхідних порушнику шляхом нав'язування такому об'єкту нової моделі поведінки.

Рис.3.7. Основні області застосування СІ

Зважаючи на можливі прояви безвідповідальності або недбалості (співробітник цілеспрямовано або випадково може зробити деякі дії по компрометації інформації), наявності у певної частини співробітників корисних інтересів (співробітник намагатиметься цілеспрямовано перебороти систему захисту для доступу до інформації підприємства, яка є закритою), їх намагання самоствердитись (співробітник затіває свого роду гру «користувач проти системи». І хоча наміри можуть бути нешкідливими, буде порушена сама практика безпеки), , а також враховуючи можливість стресів і психологічних впливів у колективах (можуть бути викликані необхідністю виконання співробітником вимог режиму таємності, тобто діяти в рамках обмеження своєї волі) та плинність кадрів (завдяки переманюванню талановитих співробітників підприємства, до того ж обізнаних у секретах, конкурентами) техніки СІ нині спрямовані на:

співробітників, які мають безпосереднє відношення до діяльності компанії (установи, підприємства): керівників і начальників відділів, персоналу відділу кадрів, секретарів а персональних помічників тощо;

нових і тимчасових співробітників, які незадоволені роботою в компанії (установи, підприємства) або які звільняються тощо.

При цьому соціоінженери (неавторизовані користувачі) застосовують підходи, які за ознаковим принципом (рис. 3.8) доцільно поділити на методи за взаємодією з політикою безпеки та дистанційністю, за ініціалізацією та маніпулюванням, за порушенням характеристик безпеки, за реляційними ознаками, за ступінем важкості, типом джерела та типом доступу. Зазначені методи можуть практикуватись як самостійно, без застосування технічних засобів [112], так і бути інструментом під час планування або проведення інших видів атак на об'єкт розвідки із застосуванням закладених пристроїв та/або програмних закладок.

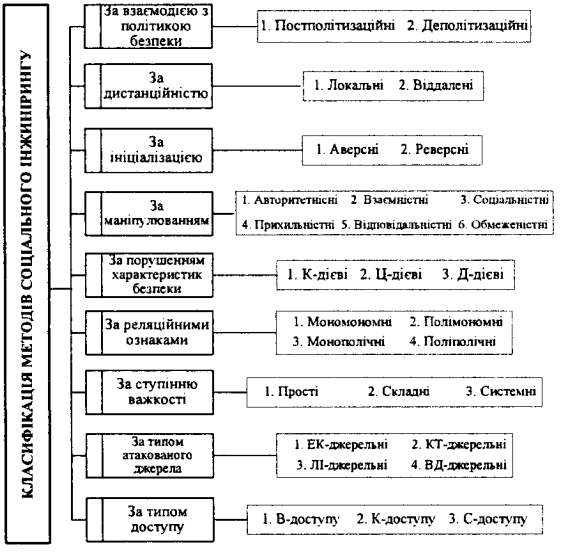


Рис. 3.8. Узагальнена класифікація МСІ

При цьому за **взаємодією з політикою безпеки** методи соціальної інженерії (МСІ) можуть бути постполітизаційними та деполітизаційними.

Постполітизаційні МСІ засновані на використанні недоліків у вже існуючій політиці безпеки. Наприклад, такими недоліками можуть бути: неправильно побудовані правила розмежування доступу; використання програмних і апаратних засобів з недостатнім рівнем захищеності; прорахунки у блокуванні каналів витоку інформації з обмеженим доступом; заборона видачі імен та телефонів персоналу джерелу (здійснюючого запит), яке достовірно не ідентифіковане тощо.

Деполітизаційні атаки пов'язані з помилками і недбалістю, які мають місце при реалізації заходів із забезпеченням вже існуючої політики безпеки.

Це, в першу чергу, пов'язано з людським чинником і залежить від недостатньої адміністративної підтримки, коректності виконання функцій захисту, своєчасності реагування на нештатні ситуації (тобто, коли створюються умови, які не описані в політиці безпеки і працівники не реагують на них з урахуванням відповідних заходів безпеки) тощо. Прикладом нештатної ситуації може бути неврахована поведінка персоналу при проханні найвищого керівництва компанії отримати секретну інформацію.

За **дистанційністю** МСІ поділяються на локальні та віддалені.

Локальні МСІ реалізуються шляхом безпосереднього індивідуального 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. Дані МСІ реалізуються за допомогою засобів комунікації, такими, як телефон, факс, електронна пошта, віртуальна комп`ютерна мережа тощо.

Т-віддалені МСІ базуються на використанні телефону, що є найбільш поширеним підходом у проведенні соціотехнічних атак. Володіючи навичками маніпулювання основними рисами людської натури, атакуючий може добувати потрібну йому інформацію видавши себе за іншу особу та переконавши в цьому атакованого (це є особливо дієвим методом у великих корпораціях, оскільки знати всіх співробітників та слідкувати за прийомом нових достатньо складно). Соціотехніки звертають особливу увагу на те, як створити досконале психологічне середовище для атаки. Незалежно від методу, що використовується, основна мета полягає в тому, щоб переконати людину (що розкриває інформацію) в тому, що соціотехнік і є таким об`єктом, якому можна довірити відповідну інформацію. Для цього використовуються маскарадингові технології [109]. Наприклад, соціотехнік може представитися співробітником віддаленого офісу і просити локального доступу до пошти, новим співробітником, що просить про допомогу, постачальником або виробником ПЗ та пропонувати його оновлення.

МТ-віддалені МСІ базуються на використанні мережевих технологій, наприклад, електронної почти, широкого спектру вірусного та іншого шкідливого ПЗ, Інтернет-ресурсів тощо. У разі використання електронної пошти жертві може бути відправлений запит або прохання на виконання певної дії від імені керівництва, співробітників, знайомих тощо. Прикладом такого типу може бути відправлення запиту відділу фінансів надання звіту за місяць

керівництву, який потрібно відіслати на підставлену соціотехніком електронну поштову скриньку. Іншим випадком МТ-віддаленого МСІ може бути відправлення разом з листом або прикладним ПЗ вірусів чи шкідливого ПЗ, або адреси Інтернет-ресурсу на них. Це може бути здійснено шляхом відправлення вкладення до листа на електронну поштову скриньку, прикріплення шкідливого ПЗ до завантажувальної програми тощо. Також соціотехнік може надіслати атакованому лист з повідомленням, що винайдена нова корисна утиліта, яку можна отримати за певною адресою, де атакуючий розміщує шкідливу програму або вірус. Соціотехнік також може відправити тільки адреси Інтернет-ресурсу на відомі джерела з дуже схожою, але відмінної від справжньої, адресою. Оскільки атакуючим створено достатньо схожий графічний інтерфейс, то жертва не підозрюючи може зареєструватись, залишивши свій ідентифікатор, пароль чи адресу електронної поштової скриньки, або спробувати увійти як вже зареєстрований користувач. Соціотехнік може здійснити МТ-віддалену атаку шляхом використовування фальшивого pop-up вікна (небажане вікно, яке з`являється під час роботи з Інтернет-ресурсами), де можуть бути розміщені на перший погляд корисні, проте небезпечні, адреси Інтернет-ресурсів, форми для додаткової реєстрації, вікна завантаження шкідливого ПЗ під виглядом корисних додатків тощо.

За **ініціалізацією** МСІ поділяються на аверсні і реверсні.

Аверсними (прямими) є МСІ, при яких соціотехнік звертається до атакованого зі своєю проблемою, переконуючи його в своїй авторизованності та просить про допомогу. Аверсні соціотехнічні атаки також можуть бути реалізовані за допомогою шкідливого ПЗ та використання неуважності атакованого. Наприклад, соціотехнік може, представившись адміністратором комп`ютерного відділу і залетефонувавши на вихідних додому одному із службовців, який займається розробкою важливого проекту, з повідомленням (ніби в знак вічливості) 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 пов`язані з тим, що соціотехнік створює ситуацію, в якій атакований стикається з певною проблемою і звертається до атакуючого для її розв`язання. Інша форма реверсної соціальної інженерії полягає в перенаправленні дій на атакуючого, тобто ціль (соціотехнік) розпізнає атаку і використовує різні методи (психологічні прийоми) для отримання максимально можливої інформації про атакуючого. Наприклад,

представившись робітником технічної допомоги провайдера (компанії, які надають послуги доступу до мережі Інтернет), соціотехнік може повідомити жертві про можливі проблеми з доступом до глобальної мережі ближчим часом і дати свій номер телефону, за яким потрібно звернутися для швидкої ліквідації проблеми (в даному прикладі жертва є новим співробітником або знаходиться в філіалі компанії, де немає адміністратора). Після чого атакуючий телефонує провайдеру та представляючись начальником фірми просить відключити доступ вище згаданого філіалу у зв`язку із ремонтними роботами в офісі. Соціотехніку залишається тільки чекати, коли жертва залетефонує в надії отримати допомогу, після чого атакуючий може сам приїхати на місце знаходження жертви та отримати доступ до робочої станції.

За **маніпулюванням** рисами людської натури МСІ поділяються на авторитетністні, прихильністні, взаємністні, відповідальністні, соціальністні та обмежувальністні, які відповідно назвемо АВ-, ПР-, ВМ-, ВП-, СЦ- та ОБ-маніпулюванням. Такі ознаки визначені шляхом узагальнення результатів соціальних досліджень щодо впливів (маніпуляцій) на людей, де виділено шість рис людської натури, які можна використовувати для отримання потрібної інформації.

Методи ***АВ-маніпулювання*** ґрунтуються на тому, що людям властиве бажання зробити (задовольнити запит) послугу особі з авторитетом (владою) і соціотехнік отримує необхідні дані, якщо атакований сприймає його як авторитетне чи компетентне джерело. Наприклад, соціотехнік може використовувати маскарадні технології вигляді ствердження, що телефонує керівництво, представитись як правоохоронні органи тощо.

Методи ***ПР-маніпулювання*** засновуються на вмінні викликати у атакованого схильність до себе. Це пов`язано з тим, що люди зазвичай задовольняють запит суб`єкта, який викликає прихильність до себе, має схожі інтереси, проблеми тощо, наприклад, перед з`ясуванням необхідних даних шляхом здійснення ключового запиту соціотехнік з`ясовує інтереси жертви і представляє їх як свої, або повідомляє, що вони з атакованим з однієї ж школи, міста тощо.

Методи ***ВМ-маніпулювання*** пов`язані зі схильністю людини машинально надавати інформацію у відповідь на певну взаємність (бажання відплатити), наприклад, матеріальну річ, пораду, допомогу тощо і це особливо ефективно тоді, коли атакований не чекає цього. Найефективніший шлях до взаємності (тобто отримання інформації) – неявно піднести подарунок, який би зобов`язав жертву. Наприклад, представитись співробітником департаменту інформатизації і сказати, що деякі комп`ютери компанії, інфіковані новим особливо небезпечним вірусом [109], який не виявляється наявними засобами

захисту і пропонує розв'язати зазначену проблему. Далі (на свою користь) соціотехнік просить атакованого протестувати нову утиліту, що дозволяє користувачу змінити паролі.

Методи ***ВП-маніпулювання*** грунтуються на звичках виконувати обіцяне, щоб не здаватися людиною, яка не заслуговує довіри. Наприклад, соціотехнік радить новому відповідальному співробітнику (відповідно до підписаної ним угоди) ознайомитися з процедурами і правилами політики безпеки, виконання яких надають законних повноважень щодо коректності користування ресурсами інформаційних систем компанії. Після обговорення декількох положень безпеки соціотехнік запитує пароль співробітника (для підтвердження виконання ним угоди) з метою перевірки його протистояння вгадуванню і далі надає рекомендації формування пароля в наступному разі. Атакований погоджується слідувати порадам, оскільки це відповідає політиці компанії і соціотехнік підтверджує його згоду слідувати угоді.

Методи ***СЦ-маніпулювання*** пов`язані з належністю атакованого до певної авторизованої (соціальної) групи, а дії в ній інших є гарантом істинності в питанні поведінки. Тобто, необхідно виконувати те, що виконують інші. Наприклад, соціотехнік видає себе за перевіряючого із служби безпеки і називає імена інших людей з відділу атакованого, які вже пройшли відповідну процедуру перевірки. Жертва вірить цьому, що дозволяє атакуючому задавати різні питання, аж до визначення ідентифікатора і пароля, які використовує жертва.

Методи ***ОБ-маніпулювання*** грунтуються на ліміті так званого "безкоштовного сиру", тобто віри в те, що об`єкт ділиться частиною інформації, на яку претендують інші, або ця інформація доступна тільки у даний момент. Наприклад, соціотехнік розсилає електронні листи з повідомленням про те, що ті, хто зареєструються на новому розважальному сайті до кінця тижня, отримають безкоштовно електронний альбом будь-якого виконавця. В процесі реєстрації ніщо не підозрюючий співробітник зазначає свій ідентифікатор, пароль, електронну пошту тощо. А як відомо люди часто, щоб не забувати паролів і ідентифікаторів, використовують однакові у всіх системах. Скориставшись цим, соціотехнік може отримати доступ до службових або приватних інформаційних ресурсів атакованого.

Якщо в процесі атаки використовуються різні риси людської натури, то результуючим буде комбінований тип на основі вище згаданих, наприклад, АВВД-маніпулювання використовує авторитетнісну та відповідальнісну риси.

За **порушенням характеристик безпеки** МСІ поділяються на К-, Ц- та Д-дієві.

К-дієві методи спрямовані на порушення такої характеристики безпеки, як конфіденційність. Тобто, наприклад, внаслідок дій соціотехніка конфіденційна інформація стає відомою йому або будь-кому іншому при забороні доступу до неї.

ПРИКЛАД 3.1. Розроблення К-дієвої атаки, спрямованої на отримання доступу до важливої документації організації (установи).

Етап 1. На сайті компанії знаходимо ім'я директора, телефон приймальні директора компанії і телефон служби підтримки. Зробивши дзвінок в службу підтримки і запропонувавши послуги по наданні інтернету, дізнаємося провайдера, який обслуговує компанію.

Етап 2. Зробивши дзвінок до служби підтримки вдруге, вже від імені провайдера в зв'язку з терміновою справою, дізнаємося номер телефону і ім'я чергового адміністратора

Етап 3. Оскільки компанія велика і рядовий адміністратор може не знати особисто директора, дзвонимо по наданому у службі підтримки телефоні і від імені директора скаржимося на погано продуктивність праці секретарки черговому адміністратору. В результаті просимо заблокувати доступ із комп'ютера секретарки до розважальних сервісів (youtube, соцмережі). Потім дзвонимо в приймальню директора і від імені мережевого адміністратора, просимо перевірити в секретарки робото спроможність інтернету, перейшовши на сайт youtube.com або vk.com. Оскільки вони заблоковані, повідомляємо, що це якийсь новий вірус, який вразив цілу мережу компанії і потрібно негайно зробити резервну копію цінних документів. Під почуттям відповідальності секретарка погоджується допомагати. Оскільки вірус вразив і засоби віддаленого доступу, поянюємо секретарці де скачати і як встановити TeemViewer. Після цього просимо вказати де знаходиться 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) при виявленні несправностей в ПК або мережі дії користувачів мають бути чітко регламентовані;

3) в організації має дотримуватись чітка організація ієрархічної моделі видання наказів (директор -> керівник відділу-> працівник) та створені чіткі правила по роботі із цінними для неї документами.

Ц-дієві методи спрямовані на порушення цілісності інформації. Наприклад, якщо соціотехніку в результаті проведення атаки вдалось 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 телефон служби підтримки. Дзвонить в службу підтримки і пропонує свої послуги по певному питанню, які ніби-то є дуже вигідними. Йому пропонують зв'язатися з менеджером компанії. Таким чином соціотехнік отримує електронну пошту менеджера, щоб надіслати йому всі умови надання послуги.

Етап 2. За отриманою електронною адресою соціотехнік здійснює пошук акаунтів жертви на різноманітних соцмережах. По вмісту інформації в акантах виділяє основні звички чи вподобання жертви.

Етап 3. Жертві на електронну пошту соціотехнік надсилає листа, в якому ідеться про розробку супер сучасного браузера інтегрованого з безліччю функцій залежно від уподобань жертви (наприклад, інтегрована панель для прослуховування улюбленої радіостанції, чи інтеграція із соцмережами).

Соціотехнік пропонує взяти участь у тестуванні бета-версії браузера і отримати абсолютно безкоштовну ліцензію. Авторизація браузера проходить по електронній адресі, в результаті чого в процесі установки буде запит на введення паролю. Після того, як пароль введено, він передається по інтернету соціотехніку, а встановлення браузера закінчується помилкою. Після цього, як правило, користувач забуває про інцидент.

Рекомендації щодо захисту від Ц-дієвих атак:

1) ніколи не встановлювати ПЗ з ненадійних джерел;

2) не вводити жодних авторизаційних даних, коли не підтверджено надійність ресурсу чи ПЗ;

3) для робочих і особистих потреб мати дві різні електронні адреси. При виникненні інциденту, або при найменшій підозрі на можливість інциденту одразу змінити пароль до електронної пошти.

Д-дієві методи це такі МСІ, внаслідок яких порушується доступність інформації. Прикладом є відмова мережевого сервеНа які складару в результаті отримання соціотехніком ідентифікатора та пароля адміністратора безпеки.

ПРИКЛАД 3.3. Розроблення Д-дієвої атаки, спрямованої на блокування доступу до інформаційної бази 1С:Бухгалтерії.

Етап 1. На сайті компанії соціотехнік знаходить телефон менеджера компанії. Дзвонить до менеджера і пропонує свої послуги по впровадженні 1С:Бухгалтерії. Дізнається, що жертву обслуговує інша компанія. Поміж словом дізнається назву цієї компанії.

Етап 2. Після дзвінка до компанії-постачальника послуг1С під виглядом

потенційного користувача, соціотехнік дізнається ім'я директора та те, що за кожним клієнтом закріплений працівник постачальника.

Під час другого дзвінка в компанію-постачальник соціотехнік каже, що знайомі порадили йому певного працівника постачальника, який їх обслуговує, а він забув його ім'я. В результаті цього він отримує ім'я працівника, що обслуговує потенційну жертву.

Етап 3. Під виглядом працівника постачальника, соціотехнік з'являється із метою оновлення конфігурації, яка необхідна для нормального функціонування 1С після виявленого багу. При цьому повідомлює, що звичний працівник компанії захворів. Від головного бухгалтера він отримує пароль до ІБ із адміністративними правами. Для оновлення блокує доступ до бази, і ніби-то під час оновлень, змінює у всіх облікових записах бази пароль. Після закінчення повідомляє, що доступ до бази був заблоковано і відновиться через певний час. Після цього соціотехнік спокійно покидає компанію.

Рекомендації щодо захисту від Д-дієвих атак:

1) при певних, наперед не повідомлених змінах в обслуговуванні, цікавитися про їх легітимність в керівництва компанії, яка надає певні послуги;

2) після виконання технічного обслуговування, вимагати продемонструвати працездатність системи. При роботі працівника технічного обслуговування, обов'язково слідкувати за його діями;

3) цікавитися легальністю встановлюваного оновлення.

Якщо в процесі атаки порушуються різні характеристики безпеки, то результуючим буде комбінований тип на основі вище згаданих, наприклад, МСІ КЦД-дії порушують конфіденційність, цілісність та доступність інформації.

За **реляційними ознаками** МСІ поділяються на мономономні, полімономні, монополічні та поліполічні.

Мономономні МСІ спрямовані для здійснення атаки у напрямку від одного атакуючого до одного атакованого. Наприклад, здійснення дзвінка до співробітника з запитом на отримання потрібної інформації.

Полімономні МСІ це такі, при яких атака реалізуєтсья спрямованими діями від двох та більше атакуючих до одного атакованого. Прикладом може слугувати відправлення електронної пошти від декількох соціотехніків (які, наприклад, будуть видавати себе за знайомих жертви) до одного отримувача. При цьому атакованого спробують переконати відкрити надану адресу Інтернет-ресурсу, де, наприклад, його спіткає можливість завантажити шкідливе ПЗ.

Монополічні МСІ реалізуються направленими діями від одного атакуючого на два чи більше атакованих. Наприклад, якщо потрібно отримати інформацію, яка

не може бути надана одним співробітником під загрозою викриття, соціотехнік може телефонувати в різні дні або різним людям для отримання потрібних даних.

Поліполічні МСІ це такі, що об`єднують в собі полімономні та монополічні технології, при яких атака реалізується спрямованими діями від двох та більше атакуючих до двох та більше атакованих. Група соціотехніків зможе більш ефективно отримати потрібну інформацію від групи людей, яку достатньо складно одержати вище перерахованими МСІ, що класифікуються за реляційними ознаками.

За **ступенем важкості** МСІ бувають прості, складні та системні.

Прості МСІ реалізуються невеликою кількістю кроків. Наприклад, при необхідності дізнатись імена службовців потрібного відділу на підприємстві, соціотехнік може використати наявні інформаційні ресурси компанії (наприклад, Web-сайт), дізнатись номер телефону служби підтримки і, зателефонувавши туди, дати запит на потрібну йому інформацію.

Складні МСІ здійснюються шляхом комбінування нескладних алгоритмів для виявлення потрібної інформації. Наприклад, якщо необхідно дізнатись паролі користувачів, то можна реалізувати таку послідовність: спочатку визначити, чиї паролі потрібні (тобто дізнатись імена), потім дізнатись, яке джерело може дати потрібну інформацію, після цього дія спрямовується на отримання пароля будь-яким із методів.

Системні МСІ реалізуються на основі використання складного алгоритму (розгалудженого, зі зворотніми зв`язками та циклічними процесами) для отримання інформації, яку не можливо дістати простими чи складними методами. Системні атаки можуть використовуватися для отримання кодів нових продуктів ПЗ, доступу до серверів систем безпеки тощо.

За **типом атакованого джерела** МСІ поділяються на: ЕК-, ЛГ-, КН- та ВП-джерельні. Фактично тип джерела пов`язаний із рівнем інформованості атакованого.

ЕК-джерельні атаки направлені на експерта, чиї професійні знання і контакти (як робота, так і хобі) забезпечують високу орієнтацію в питанні, що підлягає розробці соціотехніком. Експерт може видати як базові матеріали, так і вивести на невідомі джерела інформації. Загальна надійність отримуваних при цьому даних найчастіше є високою.

ЛГ-джерельні атаки спрямовані на легковажну особу, що виказує потрібні факти в діловій, дружній, компанійській або інтимній бесіді. Така випадкова інформація може бути надзвичайно цінною, хоча загалом не виключена як звичайна брехня, так і навмисна дезінформація.

КН-джерельні атаки спрямовані на людей (контактерів), які будь-яким

чином контактують або колись контактували з об'єктом, що вивчається соціотехніком (людиною, групою, організацією тощо). Це можуть бути випадкові ділові партнери, родичі або знайомі, працівники сервісу тощо. Разом з повідомленням певних фактів вони можуть сприяти в підході до об'єкту або ж брати участь у прямому вилученні у нього інформації.

ВП-джерельні атаки спрямовані на випадкового індивіда, який не розглядається як потенційний інформатор, проте є носієм важливої інформації. Зважаючи на випадковість і непередбачувальність на таку людину соціотехніки не покладаються, але намагаються отримати як найбільше потрібних даних.

Якщо в процесі атаки використовуються різні типи атакованих джерел, то результуючим буде комбінований тип на основі вище згаданих, наприклад, ЕККН-джерельна пов'язана з експертом та контактером.

За **типом доступу** до інформації МСІ поділяються на методи В-, К- та С-доступу.

Методи ***В-доступу*** пов'язані з доступом до інформації, яка відображена у відкритих джерелах, наприклад, друковані періодичні видання, Інтернет-ресурси, засоби масової інформації, дзвінки в службу підтримки тощо.

Методи ***К-доступу*** орієнтовані на отримання доступу до конфіденційної інформації, тобто до такої, яка є не секретною, проте доступ до неї контролюється особами, які несуть за неї відповідальність. Наприклад, імена, номери телефонів, поштові адреси, посади і т. ін.

Методи ***С-доступу*** пов'язані з отриманням доступу до інформації, що має гриф секретності та привілеї на яку має обмежене коло довірених осіб. Такою інформацією можуть бути, наприклад, секретні коди доступу, новітні розробки, секретні матеріали тощо.

Якщо соціотехнічні атаки пов'язані з реалізацією доступу до різних типів інформації, то результуючим буде комбінований метод, який окрім методів, перелічених вище, міститиме до того ж й певну сукупність засобів та «параметрів оточення». Прикладом такому може бути атака ВК-доступу, орієнтована приміром на відкриту та конфіденційну інформацію. Такий підхід дає можливість існуючу множину кібератак з використанням соціальної складової умовно поділити на такі категорії:

1) атаки по засобам застосування, а саме, з використанням при спілкуванні телефону, електронної пошти, Інтернету (в реальному часі), звичайної пошти або особистої харизми в ході зустрічі;

2) атаки за рівнем соціального відношення до об'єкта розвідки: офіційним, товариським або дружнім;

3) атаки за ступенем доступу об'єкта до ІКС: адміністратор – високий

ступінь доступу, начальник – середній, користувач – низький.

Реалізація в нихбудь-якого з наведених вище методів дозволить:

провести пошук необхідної інформації у відкритих джерелах;

отримати пароль або коди доступу до системи;

надіслати безкоштовне програмне забезпечення (ПЗ) або патч жертві для установки, вірус або троянського коня в якості додатку до електронного листа;

дослідити вміст сміттєвих контейнерів компанії (установи, організації, підприємства);

відвідати компанію під виглядом клієнта, співробітника постачальника або виробника загального і спеціального програмного забезпечення, представником партнерської компанії або законодавчого органу;

проникнути до компанії під виглядом нового керівника або співробітника, обслуговуючого персоналу, знайомого або родича;

зробити начебто помилкові дзвінки в компанію або її певним співробітникам під виглядом довіреної людини або співробітника з метою отримання необхідної інформації;

налагодити персональні стосунки із співробітниками компанії;

працевлаштуватися в компанію (установу, організації, підприємство) тощо.

3.3 Алгоритм соціотехнічної атаки: етапи проведення, супутні уразливості та основні ризики

Як було зазначено вище головна мета соціотехнічних атак – одержати доступ до захищених ІКС з метою крадіжки інформації, паролів, персональних даних і т.п. Для цього [120] неавторизовані користувачі згідно із схемою Шейнова (рис. 3.9) повинні:

Рис. 3.9. Алгоритм дій порушників методом соціальної інженерії

1) визначити мету – тобто те, за якого роду інформацією саме йде полювання й де вона знаходиться;

2) зібрати інформацію про об'єкт розвідки – тобто вивчити жертву (джерелом інформації може служити практично все: аналіз трафіка, пошти, навіть касових чеків тощо. Під «об'єктом» розуміється жертва, на яку націлена атака неавторизованого користувача);

3) розробити план дій, провести моральну підготовку і тренування (опрацювати сценарій, зіставити його кожне слово з психологічною моделлю вивченої жертви);

4) виявити найбільш привабливі мішені впливу;

5) створити умови необхідні для впливу соціального інженера на об'єкт розвідки, тобто примусити (attrahere – залучати, притягати) жертву до таких дій, які йому потрібні. Прикладом такому може стати потреба співробітника у грошах про що соціальний інженер дізнається на етапі збору інформації. Заходи СІ з атракції повинні примусити співробітника терміново шукати гроші.

6) сформувати звіт і подати його замовнику.

Узагальнений алгоритм соціотехнічної атаки, який дозволить реалізувати 2-й етап схеми Шейнова наведений на рис. 3.10. У ньому дії соціотехніків представлені одновимірним масивом $Д[i]$, який позначає необхідну додаткову інформацію, де $i=\overline{1,n}$, а n - кількість додаткової інформації. Алгоритм передбачає обов'язкове дотримання таких етапів [121, 122] (Додаток В):

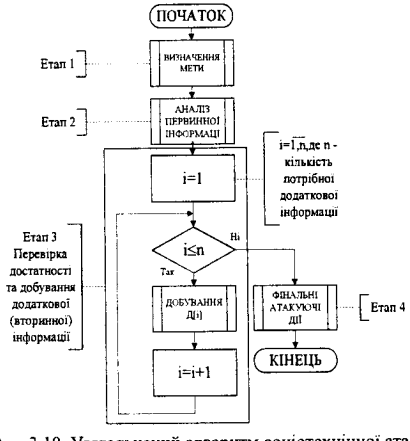


Рис. 3.10. Узагальнений алгоритм соціотехнічної атаки

Етап 1. Визначення мети.

Етап 2. Аналіз джерел, з яких є можливість добути інформацію, потрібну на початковому етапі. У першу чергу розглядаються відкриті джерела, оскільки

немає режиму обмеження доступу до них.

Етап 3. Перевірка достатності добутої інформації для здійснення атаки. Якщо необхідні додаткові дані, те соціотехнік визначає кроки та реалізацію добування потрібної інформації, а якщо її кількість достатня для здійснення атакуючих дій, те соціотехнік переходити до наступного етапу.

Етап 4. Фінальні атакуючі дії.

Природно, що при проведенні будь-якої атаки з використанням соціального інжинірингу (шляхом видавання себе за іншу особу; відволікання уваги; нагнітання психологічної напруги й т.д.) так само, як і у ході виконання звичайних атаках, одним з обов'язкових атрибутів є класифікація ступеня доступу до інформації при успішно проведеній атаці. Цей ступінь залежить від рівня підготовленості соціального інженера й того, ким є жертва (таблиця 2.3). У подальшому, розробивши сценарій атаки, соціоінженери використовують такі основні компоненти ПЗ, як, наприклад, повідомлення, яке в свою чергу складається з інформаційного наповнення, відомостей про відправника й довідкового посилання на злоякісне ПЗ та засіб доставки (електронну пошту, службу миттєвих повідомлень та/або однорангові мережі).

ПРИКЛАД 3.4. Розроблення соціотехнічної атаки спрямованої на отримання кредитної картки та мобільного телефону начальника проекту нової продукції фірми ***A*** для конкурентної фірми ***B***.

З урахуванням наведених у табл. 2.3 обмежень алгоритм здійснення такої атаки з використанням можливостей МСІ може бути поданий схемою, приведеною на рис. 3.11. Він складається з таких етапів.

Етап 1. Визначення номеру кредитної картки та мобільного телефону начальника проекту нової продукції фірми ***A*** для конкурентної фірми ***B***.

Етап 2. Пошук шляхів виходу на сайт компанії ***C***, де міститься телефон служби підтримки (довідкової служби). З цією метою представники фірми ***B*** обрали саме підприємство ***C***, де жертва є постійним клієнтом.

Етап 3. З'ясовування номеру телефону та імені потрібного службовця відділу клієнтів. Для цього соціотехнік має знати процедуру видачі інформації про клієнтів. Зателефонувавши до служби підтримки компанії ***C***, соціотехнік представляється клієнтом, повідомляє про випадок крадіжки кредитної картки у людини, яка є клієнтом фірми ***C***, та здійснює запит потрібної йому інформації (які дані надає клієнт і яким чином та чи надійно вони зберігаються). На поданий запит соціотехнік отримує відповідь, що кожен клієнт має власний порядковий номер, а його імена, номери контактних телефонів, кредитних карток тощо надійно зберігаються в базі компанії. Тим не менш таким чином соціотехнік дізнається про

те, куди потрібно зателефонувати та як зробити запит номеру кредитної картки і мобільного телефону начальника проекту нової продукції фірми **С**, щоб не викликати підозри. Разом з тим соціотехніку для здійснення атаки необхідно себе певним чином ідентифікувати. Знаючи структуру компанії **С** (інформація з сайту) він вибирає регіональне відділення в іншому місті. Телефонуючи у службу підтримки, соціотехнік дізнається ім'я та телефон працівника відділу рахунків.

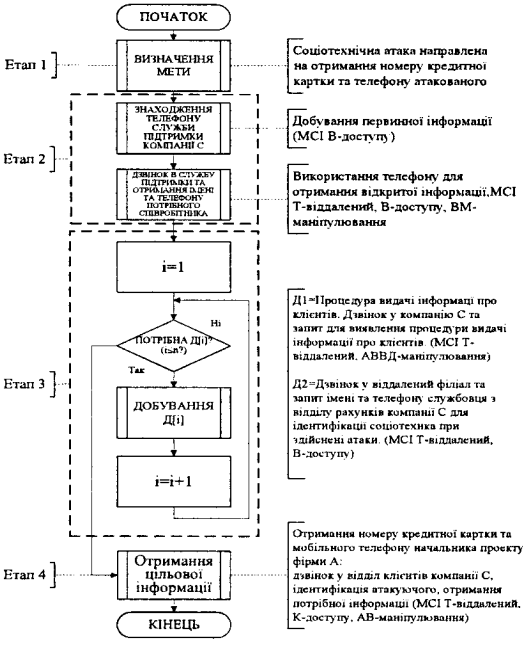


Рис. 3.11. Приклад алгоритму здійснення соціотехнічної атаки

Етап 4. Фінальним кроком є дзвінок у відділ клієнтів компанії ***С***. Соціотехнік представляється службовцем відділу клієнтів регіонального відділення, називає ім'я й повідомляє про зараження його комп'ютера вірусом та що він на даний момент не може відкрити базу, щоб задовольнити запити серйозного клієнта. Після чого просить надати йому потрібну інформацію, даючи лише ім'я клієнта [122].

Як видно, головними ризиками при успішній реалізації соціотехнічної атаки, спрямованої на отримання номерів кредитної картки та мобільного телефону начальника проекту нової продукції фірми ***А*** для конкурентної фірми ***В*** можуть бути [4–6]: витік конфіденційної інформації (ВКІ); нанесення збитку репутації організації (НЗРО); пониження працездатності організації (ППО); перевитрата

ресурсів (ПрР) та фінансові втрати (ФП). На результат такої атаки можуть суттєво вплинути уразливості, що сконцентровані в таблиці 3.2 [123].

Таблиця 3.2

Уразливості корпоративної мережі, що сприяють проведенню атаки

Напрямок атаки	Нинішнє положення справ	Коментарі
Мережні атаки		
Електронна пошта	На комп'ютерах всіх співробітників установлена програма Microsoft Outlook	У кожного співробітника свій електронний ящик, що не дозволяє здійснювати контроль за вхідною поштою
Інтернет	Співробітники використовують інтернет у робочих і особистих цілях	Користування інтернетом в особистих цілях не дозволяє здійснювати контроль за діями співробітників
Спливаючі додатки		На сучасний момент жодні технічні засоби захисту від спливаючих додатків в організації не використовуються
Служба миттєвого обміну повідомленнями	Прийняті в організації методи роботи допускають 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 необхідно зробити системними
Пошук інформації в смітті		
Внутрішнє сміття	Кожне відділення позбувається від власного сміття самостійно	
Зовнішнє сміття	Сміттєві контейнери розташовуються на території організації. Вивіз сміття здійснюється по четвергах	
Особистісні підходи		
Безпека офісів	Всі офіси залишаються незамкненими протягом усього робочого дня	
Співробітники, що працюють будинки	Письмові стандарти забезпечення безпеки систем співробітників, що працюють удома, відсутні.	
Інші напрямки атак і уразливості, специфічні для компанії		
Підрядники, що працюють на об'єктах		Немає жодної інформації про спів робітників компанії та не прийняті для них політики безпеки

З використанням таблиці уразливостей корпоративної мережі, що допускають проведення неавторизованими користувачами атак такого виду й спрямованості можна визначити вимоги політик безпеки, типи й рівні ризику для фірми *А* (таблиця 3.3) [124, 125].

Таблиця 3.3

Форма для визначення вимог до забезпечення безпеки та оцінювання факторів ризику

Напрямок атаки	Можливі вимоги політик	Тип ризику	Рівень ризику	Дія
	Викласти ПБ захисту від загроз, заснованих на методах соц.інжинірингу, у письмній формі			
	Внести пункт про необхідність дотримання ПБ у стандартний контракт із співробітником			

Продовження табл. 3.3

Напрямок атаки	Можливі вимоги політик	Тип ризику	Рівень ризику	Дія
	Внести пункт про необхідність дотримання ПБ у стандартний контракт із підрядником			
Мережні атаки				
Електронна пошта	Прийняти ПБ, що регламентує дії співробітників при одержанні вкладень конкретних типів	УКІ ЗЗРО ФП	3	Розроблена ПБ використання електронної пошти, створений єдиний поштовий клієнт-сервер
Спливаючі додатки	Включити в політику використання інтернету явні вказівки із приводу того, що варто робити з появою спливаючих діалогових вікон	УКІ ПрР ФП	3	Розроблено політику використання комп'ютерів
Інтернет	Прийняти ПБ, що регламентує використання інтернету	УКІ ППО ПрР ФП	4	Розроблено політику використання інтернету
Служба миттєвого обміну повідомленнями	Прийняти політику, що визначає підтримувані й припустимі клієнтські програми миттєвого обміну повідомленнями	УКІІ ППО	2	Розроблено правила по роботі зі службами миттєвих повідомлень
Телефонні атаки				
Корпоративна телефонна станція	Прийняти політику керування обслуговуванням корпоративної телефонної станції	УКІ ФП	2	Розроблено політику роботи при телефонних переговорах
Служба підтримки	Прийняти політику, що регламентує надання доступу до даних	УКІ Прр	2	Розроблено політику управління доступом
Пошук інформації в смітті				
Паперове сміття	Прийняти політику утилізації паперового сміття	УКІ НЗРО ФП	3	Розроблено інформаційну ПБ
Електронне сміття	Прийняти політику утилізації електронного сміття	УКІ НЗРО ФП	3	Розроблено інформаційну ПБ
Особистісні підходи				
Фізична безпека	Прийняти політику роботи з відвідувачами	УКІ ФП	2	Розроблена ПБ роботи з відвідувачами
Безпека офісів	Прийняти політику управління ідентифікаторами й паролями користувачів	УКІ НЗРО ФП	3	Розроблена ПБ ідентифікації і аутентифікації
Співробітники, що працюють поза об'єктом	Прийняти політику використання мобільних комп'ютерів поза організацією	УКІ НЗРО ФП	3	Розроблена ПБ роботи поза організацією
Інші напрямки атак і уразливості, специфічні для організації				
Підрядники, що працюють на об'єктах організації	Прийняти політику перевірки співробітників сторонніх організацій	УКІ НЗРО ТР ФП	4	Підписується угода про нерозголошення відомостей

Як результат, за ознаковим признаком варіант наведеної вище соціотехнічної атаки може бути класифікований як: деполітизаційна, Т-віддалена, аверсна, АВВМ-маніпульована, К-дієва, монополічна, складна та ЕК-джерельна атака Вк-доступу.

3.4 Загрози соціального інжинірингу

Останнім часом при організації і проведенні атак соціоінженери застосовують такі інструменти (канали) нападу, як [126, 127]:

електронна пошта (e-mail);
телефонний зв'язок;
аналіз сміття;
особистісні підходи;
реверсивна соціальна інженерія.

Використовуючи відносну анонімність Internet це дає їм можливість дібратися до об'єкта атаки й скористатися його системними ресурсами.

3.4.1 Загрози з використанням електронної пошти (e-mail)

Техніка застосування електронної пошти для розповсюдження фішинг-повідомлень з деструктивним інформаційним наповненням вперше була докладно описана у 1987 році, а сам термін – «фішинг-атака» з'явився 2 січня 1996 року в новостній групі «alt.online-service.America-Online» мережі «Usenet». На сьогодні це мабуть найпопулярніша схема соціального інжинірингу в процесі реалізації якої соціоінженери використовують такі методи нападу, як:

атаки типу "людина посередине " (Man-in-the-middle);
атаки, що використовують кроссайтові сценарії (Cross-site Scripting);
атаки з підміною URL та інші.

Одними з перших можливості фішингу наприкінці минулого століття реалізували розробники вірусів "Melissa" та "LoveLetter". Через e-mail віруси надсилали власні копії користувачам, адреси яких вибирались з адресної книги інфікованої ПЕОМ, з ознакою важливого повідомлення та певним змістом (рис. 3.12).

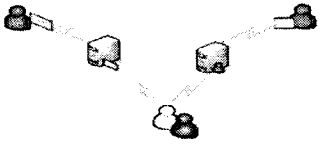


Рис. 3.12. Структурно-логічна схема дій порушника з використанням можливостей електронної пошти (e-mail) та служби миттєвих повідомлень (IM)

На рисунку показано, як працює імітація при використанні e-mail та IM. Зловмисник (на рисунку виділений червоним кольором) виконує роль відомого користувача й посилає електронну пошту або IM-повідомлення виходячи з того, що

одержувачі приймуть їх за повідомлення від когось, кого вони знають. Знайомство послабляє користувальницьку захищеність. У результаті дій так званих «phishing kit» – утиліт, які дозволяють у короткий термін створювати фішинг-сайти, інфікованими виявляються, як правило, всі ПЕОМ, власники яких зацікавились цим повідомленням.

Нині, за даними звіту компанії APWG (Anti-Phishing Work Group), щомісяця виявляється понад 20 000 фішингових розсилань та біля 12 000 фішерських web-сайтів. Так, наприклад, лише у першому півріччі 2006 року фішери відправили 157 тисяч унікальних листів, що на 81 відсоток перевищило їх кількість зафіксовану у другому півріччі 2005 року. На сучасному етапі розвіттку IT-індустрії без цього вже не обходиться жодний витік персональних даних. Фішингові розсилання (рис. 3.13) з відомостями, що викликають тривогу (наприклад, містять загрози щодо закриття банківських рахунків), пропонують занадто гарні угоди (наприклад, для того, щоб бути правдою), благають про пожертвування (наприклад, від імені благодійних організацій), обіцяють великі грошові вигоди з мінімальними зусиллями тощо є передтечею нападу на клієнтів банків і електронних платіжних систем. Метою фішерів все частіше стають користувачі соціальних мереж.

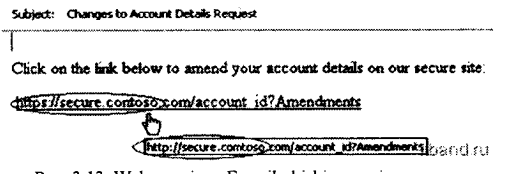


Рис. 3.13. Web-сторінка E-mail phishing повідомлення

На рис. 3.13 відображено зовні припустиме посилання на сайт управління облікового запису Contoso. Однак при уважному розгляді можна знайти такі розходження:

а) з тексту повідомлення (використовуючи https) видно, що сайт безпечний. Однак на екрані показано, що сайт фактично використовує http;

б) назва компанії в пошті – "Contoso", а у посиланні – "Comtoso".

Камуфляж, використовуваний у подібних випадках, змушує електронну пошту здаватися більш правдоподібною. У листі часто міститься пряме посилання на сайт, який зовні неможливо відрізнити від справжнього (рис. 3.14). При цьому кожен phishing-лист маскується під запит про користувальницьку інформацію, що нібито повинно полегшити користувачеві установку відновлення або забезпечити додаткове обслуговування (рис. 3.15).

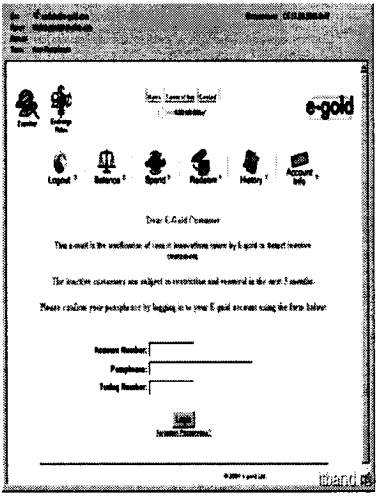


Рис. 3.14. Зразок фішингового листа з підробленою mail-адресою відправника

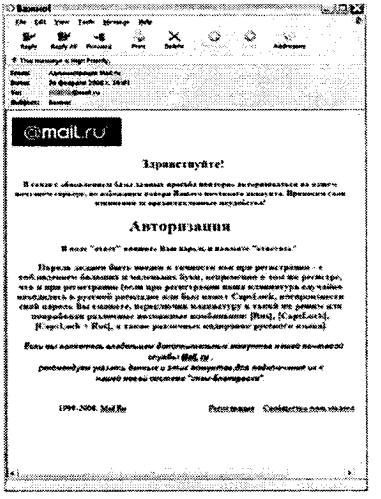


Рис.3.15. Зразок фішингового листа користувачам пошти Mail.ru

З'явившись на такому сайті, користувач може повідомити зловмисникам цінну інформацію, яка дозволить їм одержати доступ, наприклад, до акаунтів і банківських рахунків. Головні правила, яких він повинен дотримуватись з тим, щоб успішно протистояти фішинг атакам:

не відкривати підозрілі посилання, отримані навіть у повідомленнях від знайомих вам людей;

не встановлювати й не запускати ігри й 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.

У липні 2006 року з'явився новий різновид фішинга, що відразу одержав назву «**вішинг**». Атака заснована на використанні системи попередньо записаних голосових повідомлень, метою яких є відтворення «офіційних дзвінків» від банківських і інших IVR (англ. Interactive Voice Response) систем, принцип дії яких показаний на рис. 3.16. Звичайно, жертва одержує запит (найчастіше через фішинг електронної пошти) про необхідність зв'язку з банком для підтвердження або відновлення якої-небудь інформації. Система вимагає аутентифікації користувача за допомогою уведення PIN-коду або пароля.

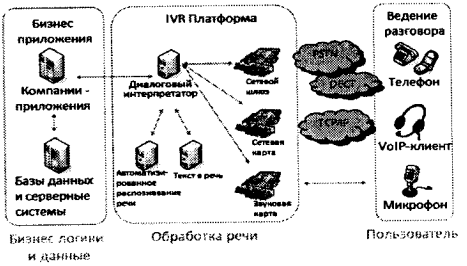


Рис. 3.16. Принцип дії IVR систем

Основна відмінність фішинга й **«вішинга»** у тім, що у випадку вішинга в повідомленні міститься прохання подзвонити на певний міський номер. При цьому зачитується повідомлення, у якому потенційну жертву просять повідомити свої конфіденційні дані. Власників такого номера знайти не просто, тому що 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 «war dialler» (автонабирач), що набирає номера в певному регіоні й при відповіді на дзвінок відбувається наступне:

автовідповідач попереджає споживача, що з його картою здійснюються шахрайські дії, і дає інструкції – передзвонити за певним номером негайно;

коли за цим номером здійснюють дзвінок, на іншому кінці проводу відповідає типово комп'ютерний голос, який повідомляє, що людина повинна пройти звірення даних і ввести 16-значный номер карти з клавіатури телефону;

як тільки номер уведений, вішер стає власником всієї необхідної інформації (номер телефону, повне ім'я, адреса);

потім, використовуючи цей дзвінок, можна зібрати й додаткову інформацію, таку, як PIN-код, термін дії карти, дата народження, номер банківського рахунку тощо.

Якими не є небезпечними фішинг і вішинг, однак у мережі нині існує ще більш серйозна загроза – **фармінг**. Фармінг (pharming) – перенапрямок жертви за помилковою (хибною) адресою. Для цього може використовуватися деяка навігаційна структура (файл hosts, система доменних імен – domain name system, DNS). Механізм фармінга має багато спільного зі стандартним вірусним зараженням. Жертва відкриває поштове послання або відвідує якийсь web-сервер, на якому виконується скрипт-вірус. При цьому спотворюється файл hosts. У результаті жертва попадає на один з помилкових сайтів.

Механізмів захисту від фармінга на сьогодні просто не існує.

Ще один різновид phishing-атак – **spear-phishing** (переклад: вилов риби за допомогою списа/дротика). Це вузько спрямовані й координовані атаки на організацію або конкретного користувача з метою одержання критично важливих даних. У цьому випадку 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 й описів (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 одержати інформацію компанії.	Конфіденційна інформація. Ділова довіра.
Викрадення фінансової інформації	Хакер використовує phishing, vishing, pharming або spear-phishing методи, щоб запросити конфіденційну інформацію (наприклад подробиці облікового запису).	Гроші. Конфіденційна інформація.
Завантаження mailware	Хакер обманює користувача й, за допомогою відкриття гіперпосилання або відкриття вкладення, інфікує мережі компанії	Доступність
Завантаження хакерського ПЗ	Хакер обманює користувача й, за допомогою відкриття гіперпосилання або відкриття вкладення, завантажує шкідливе ПЗ	Атака на ресурси. Доступність. Гроші.

Щоб більш ефективно протидіяти хакерським нападам, які використовують соціальну інженерію треба ставитися зі скептицизмом до чого-небудь несподіваного у вашій поштовій скриньці. Щоб підтримувати цей підхід в організації, необхідно включити в політику безпеки посібник з використання електронної пошти, який охоплює питання використання: вкладень у документах; гіперпосилань у документах; запитів про персонал або інформацію компанії зсередини компанії; запитів про персонал або інформацію компанії зовні компанії тощо.

ПРИКЛАД 3.5. Спливаючі додатки й діалогові вікна

Більшість співробітників компанії переглядає Internet з особистих причин. Ці дії можуть принести небезпеку контакту зі зловмисниками, що використовують соціальну інженерію. Хоча зловмисники можуть й не переслідувати мету нападу саме на вашу компанію, однак вони можуть використовувати ваш персонал для одержання доступу до її ресурсів. Одна із самих популярних цілей полягає в тому, щоб впровадити поштовий сервер у межах вашої комп'ютерної мережі, через який зловмисник зможе почати

phishing або інші поштові напади (табл. 3.5) на інші компанії або фізичні особи.

Існує два найпростіших методи спокусити користувача перейти по посиланню в діалоговому вікні – це надіслати користувачеві попередження про проблему, що виглядає як відображення реалістичної операційної системи або прикладного повідомлення про помилки та пропозиції додаткових послуг, наприклад, безкоштовного завантаження, що нібито змусить комп'ютер користувача працювати швидше. Захист користувачів від спливаючих додатків, полягає насамперед у розумінні того, що це прозорий обман й що вони за жодних обставин не повинні натискати посилання на спливаючих вікнах, не порадившись, наприклад, із персоналом служби підтримки. Однак при цьому персонал повинен бути впевнений, що штат підтримки не буде поверхово ставитися до прохань користувачів про допомогу, якщо користувач переглядає Internet. Ці довірчі відносини можна передбачити вашою політикою безпеки по роботі в Internet.

Таблиця 3.5

Он-лайн атака за допомогою спливаючого додатка й діалогового вікна

Мета нападу	Опис	Спрямованість
Викрадення персональної інформації	Хакер запитує персональну інформацію співробітника	Конфіденційна інформація Гроші
Завантаження mailware	Хакер обманює користувача, за допомогою відкриття гіперпосилання або відкриття вкладення, інфікує мережі компанії	Доступність
Завантаження хакерського ПЗ	Хакер обманює користувача, за допомогою відкриття гіперпосилання або відкриття вкладення, завантажує хакерське ПЗ	Атака на ресурси. Доступність. Гроші.

ПРИКЛАД 3.6. Instant Messaging

Миттєва передача повідомлень (IM) – відносно нове середовище зв'язку й разом з тим ідеальне середовище для нападів з використанням соціальної інженерії. Саме безпосередність і дружелюбний інтерфейс IM роблять його ідеальним засобом для нападів, адже користувачі розцінюють дану службу як телефон і не зв'язують її з потенційними загрозами ПЗ. Основні атаки, що використовують IM, це гіперпосилання на malware і розсилання злоякісного ПЗ (таблиця 3.6). Їх результативності сприяє невимушеність IM, які разом з опцією надання прізвиська значно розширюють можливості для атаки.

Таблиця 3.6

Напади IM передачі повідомлень

Мета нападу	Опис	Спрямованість
Запит про конфіденційну інформацію компанії	Хакер, виконуючи роль колеги, використовує IM імітацію, щоб запросити ділову інформацію	Конфіденційна інформація Довіра

Продовження табл. 3.6

Мета нападу	Опис	Спрямованість
Завантаження malware	Хакер обманює користувача, за допомогою відкриття гіперпосилання або відкриття вкладення, інфікує мережі компанії	Доступність
Завантаження хакерського ПЗ	Хакер обманює користувача, за допомогою відкриття гіперпосилання або відкриття вкладення, завантажує хакерське ПЗ	Атака на ресурси. Доступність. Гроші.

Якщо існує потреба у використанні зручності миттєвої передачі повідомлень (ІМ), необхідно включити ІМ-безпеку у політику безпеки установи. Для цього доцільно встановити наступні п'ять правил використання:

увести стандарт на єдину ІМ платформу;

визначити параметри настроювання безпеки розгортання;

рекомендувати користувачам не використовувати настроювання за замовчуванням;

установити стандарти пароля;

забезпечити посібник з використання.

ПРИКЛАД 3.7. Зламування поштової скриньки

Саме 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 скрипт, що буде копіювати ці файли й поставити його на автозавантаження. Скрипт у купі з фільмами, музикою або іграми необхідно записати на флешку та підкинути потенційній жертві, яка при спробі прочитати інформацію з флеш-пам'яті попутно запустить і скрипт.

```
[autorun]
open=нужный скрипт.vbs
```

Для зламування поштової скриньки можна використовувати також і кейлогери – програми, що записують всі натискання клавіш. Дії зловмисника у при цьому такі ж, як і у 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 з паролем, які відразу перешлються зловмиснику.

3.4.2 Загрози при використанні телефонного зв'язку

Телефон також пропонує унікальний спосіб нападу для хакерів. Це знайоме середовище. У цей час можливість злому телефонного зв'язку, здійснюваного по IP-

протоколу Internet (VoIP) є головною загрозою для компанії, а VoIP-імітація стає настільки ж широко розповсюдженим явищем, як e-mail та IM-імітація.

У процесі організації й проведення ***phreaking***-атак як правило:

просять надати певну інформацію, імітуючи законного користувача, щоб або звернутися до телефонної системи безпосередньо або одержати вилучений доступ до комп'ютерних систем;

одержують доступ до "вільного" використання телефону;

одержують доступ до системи комунікацій.

Самий звичайний підхід хакера – симулювання ролі телефонного інженера, як показано на рисунку 3.17.

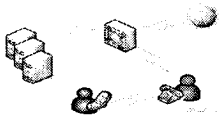


Рис. 3.17. Схема атаки на офісну АТС

Запити про інформацію або доступ по телефону – відносно не ризикована форма атаки. Якщо адресат стає підозрілим або відмовляється виконувати запит, хакер може просто покласти трубку. Але такі атаки більш складні, чим атака хакера, який просто дзвонить у компанію й просить надати ідентифікатор або пароль користувача. Звичайно використовується сценарій, коли просять або пропонують довідку (таблиця 3.7), перш ніж майже машинально відбувається запит про особисту або ділову інформацію.

Таблиця 3.7

Телефонні напади

Мета нападу	Опис	Спрямованість
Запит інформації компанії	Хакер виконує роль законного користувача щоб одержати конфіденційну інформацію	Конфіденційна інформація Ділова довіра
Телефонний запит інформації	Хакер причиняється телефонним майстром, щоб одержати доступ до офісного АТС, і потім робити зовнішні запити	Ресурси Гроші
Використовуючи офісну АТС, звернутися до комп'ютерних систем	Хакер зламує комп'ютерні системи, використовуючи офісну АТС, захоплює або управляє інформацією, заражає malware.	

З цією метою зловмисник працює за таким алгоритмом:

1) вибирає мету по телефонній книзі – організацію, де є телефон секретаря;

2) здійснює дзвінок секретареві й з'ясовує ім'я персони, з якою можна проконсультуватися з приводу деяких проблем, пов'язаних з роботою системи;

3) здійснює дзвінок будь-якій іншій людині, чий номер телефону є в книзі, припускаючи, що вона має доступ до системи;

4) представляється (зрозуміло, вигаданим ім'ям) як помічник тієї персони, ім'я якої він довідався з першого дзвінка. Говорить, що у зв'язку з переінсталяцією системи адміністратор дав завдання поміняти паролі всім користувачам;

5) довідується ім'я входу, колишній пароль, говорить новий пароль.

У тому випадку, якщо доступ до системи відбувається за допомогою телефонних ліній, дзвонить секретареві, говорить, що не виходить додзвонитися до системи, і просить назвати правильний номер телефону.

ПРИКЛАД 3.8.

Відомо, що адміністратору доволі часто приходиться стикатися з ситуацією, коли користувач, який тривалий час «не входив» у систему окрім свого «імені» нічого іншого із службової інформації, необхідної для цього не пам'ятає. У таких випадках користувач користується телефонним правом.

Змоделюємо такий випадок на прикладі UNIX-системи.

Дзвінок адміністраторові.

Хакер: Здрастуйте, ви адміністратор?

Адміністратор: Так.

Х.: Вибачите, що відволікаю. Не могли б ви мені допомогти?

А.: (Ну що ще йому треба?) Так, звичайно.

Х.: Я не можу у своєму каталозі виконати команду **ls**.

А.: (Начебто йому це треба!) У якому каталозі?

Х.: /home/anatoly.

А.: (От аджже дурний юзер!) Зараз подивлюся. (Заходить у цей каталог і набирає команду ls, що успішно виконується й показує наявність нормальних прав на каталог.)

А.: Усе у вас повинне працювати!

Х.: Хммм... Почекайте. О! А тепер працює. Дивно...

А.: (Хмммм!!!) Так? Добре!

Х.: Спасибі величезне. Ще раз вибачаюся, що відірвав ВАС від справ.

А.: (Ну нарешті!) Так немає за що. До побачення.

Кінець розмови.

Начебто нічого особливого. Але що ж відбулося насправді?

У каталозі /home/anatoly серед множини інших файлів лежав змінений варіант програми **ls**. Саме його-то адміністратор і запустив. Вся справа в тому, що при виконанні цього файлу у адміністратора були усі права на систему, і, відповідно, всі програми, які він запускає, можуть робити із системою практично все, що завгодно. Що було в цьому файлі, крім можливості показувати список файлів у каталозі, тепер тільки зломщикові й відомо.

Головну складність при використанні телефонного зв'язку представляє голос. Якщо об'єкт знайомий з тим, ким представився нападаючий, то необхідно зробити так, щоб їх голоса майже не відрізнялися.

3.4.3 Аналіз сміття

Незаконний аналіз сміття – надзвичайно цінна діяльність. Ділові паперові відходи неоціненні для тих хакерів (зловмисників), які використовують СІ, адже це допоможе їм при атаці видавати себе за співробітників компанії.

Так, наприклад, якщо в компанії відсутні правила утилізації відходів, які включають позбавлення від несправних використаних цифрових носіїв – жорстких дисків, компакт-дисків тощо вони можуть стати неоціненними носіями усіх видів інформації про діяльність установи (табл. 3.8). Враховуючи таке політика безпеки компанії повинна включати положення про управління життєвим циклом носіїв, включаючи процедури руйнування або стирання.

Таблиця 3.8

Атаки на сміття

Мета нападу	Опис	Спрямованість
Паперові відходи в зовнішніх урнах	Хакер бере папір із зовні розміщеної урни зі сміттям, щоб заплучити будь-яку доречну інформацію компанії	Конфіденційна інформація Атака на довіру
Паперові відходи у внутрішніх урнах	Хакер бере папір із внутрішніх офісних урн, роблячи обхід будь-яких рекомендацій захисту	Конфіденційна інформація Атака на довіру
Електронні відходи цифрових носіїв	Хакер отримує інформацію з викинутих електронних носіїв. Хакер також краде самі носії	Конфіденційна інформація Атака на довіру Ресурси

Як видно з таблиці персонал компанії повинен розуміти значення викинутих паперових або електронних носіїв. Атаку на сміття не можна вважати правопорушенням, тому ви повинні гарантувати, що персонал знає, як утилізувати непотрібні матеріали. Тобто необхідно завжди знищувати паперові відходи й витирати або знищувати електронні носії. Для цього необхідно:

1) розробити процедури знищення сміття й розмістити ємності для відходів усередині периметра, що захищається, щоб вони були недоступні;

2) управляти внутрішніми відходами. Політика безпеки часто пропускає цю проблему, оскільки передбачається, що кожен хто одержує доступ до ресурсів компанії, повинен заслуговувати довіри;

3) визначити категорії інформації й яким чином персонал повинен з нею поводитись. При цьому категорії могли б включати:

конфіденційну інформацію (необхідно знищувати всі папери, що мають

даний шифр у спеціальних знищувачах паперу (шредерах));

приватну інформацію (необхідно знищувати всі папери, що мають даний шифр у спеціальних знищувачах паперу);

відомчу інформацію (необхідно знищувати всі папери, що мають даний шифр у спеціальних знищувачах паперу перед викиданням у загальнодоступні урни);

публічну (загальнодоступну) інформацію (бажано позбуватися від загальних документів у будь-якій урні або використовувати їх як чернетки).

3.4.4 Особистісні підходи

Для хакера найпростіший шлях одержання інформації – попросити про це безпосередньо. Цей підхід може здаватися грубим, але це основа шахрайства. Існує чотири різновиди такого підходу:

1) залякування (може використовувати уособлення повноважень, щоб примусити адресат виконати запит);

2) переконання (самі звичайні форми переконання включають лестощі);

3) використання довірчих відносин (вимагає більш тривалого терміну, протягом якого підлеглий або колега формують відносини, щоб одержати довіру й інформацію від адресата);

4) допомога (цей підхід пропонує надання хакером допомоги адресатові, що буде вимагати від останнього оприлюднення особистої інформації).

Безсумнівно, **довіра** – одна з головних цілей хакера. Захист від **залякування** – розвиток культури "відсутності остраху через помилку". Якщо нормальне поводження – увічливість, то успіх залякування зменшується. **Переконання** завжди було важливим людським методом. Ви можете впровадити сувору інструкцію яка визначає, що персонал повинен і не повинен робити. Створена атмосфера розуміння в компанії й політика паролів – кращий захист. Для більшості компаній середнього розміру головна загроза – **«колеги».** Штат відділу кадрів повинен проявляти передусім обережність при найманні контрактного персоналу. Якщо хакер, який використовує соціальну інженерію, одержує постійну роботу в компанії, то кращий захист – розуміння персоналу і їхня прихильність правилам політики безпеки. Нарешті, атака **«допомога»** може бути скорочена, якщо ви маєте ефективну сервісну підтримку. Внутрішній помічник – часто результат втрати довіри до існуючих послуг служби підтримки компанії. Для реалізації кожного зі згаданих вище підходів хакери повинні здійснити віртуальний або ж вийти на менш розповсюджений, але більше ефективний особистий контакт із адресатом.

Сьогодні існують наступні види віртуального контакту (табл. 3.9):

за допомогою електронного поштового повідомлення;

за допомогою повідомлення, що спливає у вікні браузера.

Обсяг одержуваної пошти й використання «троянців» дозволяють віднести процедури віртуального контакту до найбільш привабливих навіть із мінімальною величиною успіху. Для запобігання атак, побудованих на особистісному підході необхідно:

визначити в політиці безпеки компанії, що служба підтримки – єдине місце, куди потрібно повідомляти про проблеми;

гарантувати, що служба підтримки має погоджений процес відповіді в межах установленого рівня обслуговування;

регулярно перевіряти виконання сервісних робіт щоб упевнитися, що користувачі одержують підходящий рівень відповідей і рішень.

Таблиця 3.9

Фізичні напади

Мета нападу	Опис	Ціль
Викрадення ідентифікатора мобільного користувача	Хакер спостерігає за законним користувачем, що набирає ім'я й пароль для входу в систему	Конфіденційна інформація
Викрадення ідентифікатора домашнього користувача	Хакер зображує із себе ІТ для одержання 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, зображуючи із себе інженера підтримки.	Конфіденційна інформація Ділова довіра Ділова доступність Ресурси Гроші
Зовнішній доступ до домашньої мережі працівника	Хакер одержує доступ до широкополосного каналу Internet через незабезпечену домашню мережу	Ресурси
Несупроводжуваний доступ до офісу компанії	Хакер одержує доступ під видом авторизованого користувача компанії	Конфіденційна інформація Ділова довіра Ділова доступність Ресурси Гроші
Звертання до людини в офісі компанії	Хакер звертається до людини, щоб використовувати комп'ютерне встаткування або паперові ресурси	Конфіденційна інформація Ділова довіра Ділова доступність Ресурси, Гроші

3.4.5 Реверсивна соціальна інженерія (reverse social engineering)

Обернена соціальна інженерія (ОСІ) описує ситуацію, у якій адресат із числа персоналу звертається до хакера за допомогою в усуненні своїх проблем і пропонує хакеру ту інформацію, яку він хоче продати (рис. 3.20). Цьому, як правило, передує дрібна диверсія, у ході якої хакер (можливо інженер компанії) ініціює неполадку в роботі комп'ютера, підключеного в мережу. Розрахунок на те,

щоб користувач уявляв собі масштаб нещастя не таким вже і безнадійним, але при цьому усунути його власними силами він не міг. Далі вже справа соціальної техніки – як правило, десь поблизу (наприклад у списку ICQ контактів) виявляється «гарний знайомий» когось із співробітників (уже днів 10 як спілкується) який володіє потрібними знаннями, або оголошення розташованого неподалік «центра комп'ютерної швидкої допомоги», або повідомлення про вигідну акцію підвищення користувальницької грамотності. Головне, що все швидко, дешево (швидше за все задурно), і «не вимагає» обов'язкового оповіщення колег і топ-менеджерів про ганебну IT-безграмотність конкретної особистості.

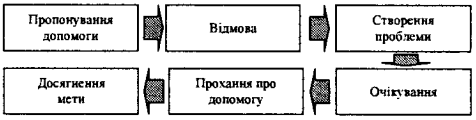


Рис. 3.20. Метод оберненої СІ

Такий сценарій може здаватися малоймовірним, однак він здійснюється все частіше. Зовсім очевидно, що дрібна поломка буде успішно й оперативно усунута, співробітник компанії буде щасливий продовжити спілкування з власним комп'ютером, а хакер одержить заповітні зачіпки за допомогою яких він зможе знов-таки відшліфовувати свою майстерність і знаходити нові жертви.

Обернений соціальний інжиніринг будується на трьох факторах (табл. 3.10):

створенні ситуації, що змушує людину звернутися по допомогу;

рекламуванні своїх послуг та надання допомоги;

випередженні надання допомоги іншими людьми тощо.

Таблиця 3.10

Обернена соціальна інженерія

Мета нападу	Опис	Спрямованість
Викрадення ідентифікаційних даних	Хакер одержує користувальницький ідентифікатор і пароль уповноваженого користувача	Конфіденційна інформація; гроші Ділова довіра та ділова доступність
Викрадення інформації	Хакер використовує ідентифікатор уповноваженого користувача й пароль, щоб одержати доступ до файлів компанії	Конфіденційна інформація; гроші; ресурси. Ділова довіра та ділова доступність
Завантаження malware	Хакер обманює користувача, підсуваючи йому гіперпосилання або вкладення в e-mail. Коли завантаження закінчене, імітуєма проблема зникає й користувач продовжує працювати, не звертаючи увагу на факт, що він порушив захист і завантажив malware-програму. У такий спосіб відбувається інфікування мережі компанії	Ділова доступність та ділова довіра
Завантаження хакерського ПЗ	Хакер обманює користувача, підсуваючи йому гіперпосилання або вкладення в e-mail, відбувається використання ресурсів компанії	Ресурси, гроші Ділова довіра

Захист від атак СІ є, безсумнівно, одним із найбільш складних у розробці заходів. Його не можна побудувати винятково технічними методами, які можуть і повинні бути використані для запобігання небажаних витоків інформації шляхом соціального інжинірингу. Для побудови системи протидії таким атакам, безсумнівно, варто залучати професійних консультантів, а не намагатися будувати захист самотужки. При цьому варто враховувати існуючі тактики вторгнення й дотримуватися стратегій, що рекомендуються, їхнього попередження (табл. 3.11).

Таблиця 3.11

Стандартні тактики вторгнення та стратегії їх запобігання

Область ризику	Тактика хакера	Стратегія запобігання
Телефон (допомоги)	Уособлення і переконання	Поповніть співробітників ніколи не видавати паролі або іншу конфіденційну інформацію по телефону
Проникнення в будівлю	Неавторизований фізичний доступ	Сувора перевірка ідентифікаційних карт, навчання службовців і наявність служби охорони
Офіс	Підглядання через плече	Не набирайте паролі в присутності кого-небудь (а якщо доводиться, робіть це швидко!)
Телефон (допомоги)	Уособлення при дзвінку на телефон допомоги	Всі співробітники повинні мати PIN для використання телефону допомоги
Офіс	Блукання по коридорах у пошуках відкритих офісів	Необхідно, щоб усіх гостей супроводжували
Комп'ютерна кімната / телефонний вузол	Спроба отримати доступ, видалити устаткування, та / або постановка пристрої для перехоплення секретних даних	Тримайте комп'ютерні / телефонні кімнати весь час закритими і регулярно оновлюйте опис обладнання
Телефон та АТС	Дзвінки за рахунок компанії	Контроль за міжміськими і міжнародними дзвінками, відстеження дзвінків, заборона на пере адресацію
Сміттєві корзини	Копання в смітті	Зберігайте весь мотлох у захищених місцях, важливі дані знищуйте в Шредері, стирайте інформацію з викидаються магнітних носіїв
Внутрішня мережа і Інтернет	Створення та впровадження троянських коней для викрадення паролів тощо	Безперервне інформування про системних і мережевих змінах, навчання використання паролів
Офіс	Крадіжка важливих документів	Помітьте документи як конфіденційні і зберігайте в закритому місці
Звичайна – психологічна	Уособлення і переконання	Підтримуйте компетентність службовців за допомогою регулярного інформування та програм навчання

Використання класичних систем запобігання витоків інформації може зробити неоціненну послугу в раннім виявленні й блокуванні подібних спроб компрометації чутливих даних. Засоби контролю знімних носіїв і зовнішніх пристроїв допоможуть захистити інтелектуальну власність організації в тому випадку, якщо хтось із її співробітників став випадковою жертвою підкинутого пристрою із привабливим умістом.

Однак найбільш дієвою буде програма навчання питанням інформаційної безпеки. Співробітники мають бути навчені тому, що електронна пошта компанії призначена передусім для ведення бізнесу, тим самим обмежуючи

можливе влучення адрес електронної пошти користувачів в Інтернет. Співробітники також повинні бути обережні при роботі із вкладеннями з незнайомих джерел. Організації також повинні мати формальну політику безпеки для використання соціальних мереж, що забороняє або обмежує інформацію, яку співробітники можуть розміщати на своїх особистих сторінках. Сайти соціальних мереж являють собою відмінний інструмент для соціального інжинірингу. Регламентування даних про компанію, розташовуваних співробітниками на сайтах соціальних мереж, буде сприяти підвищенню рівня загальної інформаційної безпеки компанії.

Питання для самоконтролю

1. На що спрямовані перспективні способи і методи розвідки ІТС? Дайте визначення та наведіть приклади ефективності розвідки систем телекомунікацій, мережевої і кіберрозвідок.

2. Дайте визначення соціальній інженерії, як одному із найбільш перспективних методів кіберрозвідки. До яких ресурсів Інтернет застосування СІ забезпечує доступ.

3. Розкрийте сутність соціальної інженерії. Які тонкощі людського характеру сприяють роботі соціального інженера?

4. Якими механізмами користуються зловмисники в процесі ведення соціального інжинірингу? Стисло розкрийте їх сутність.

5. Перелічте основні заходи та засоби організаційного, програмного та технічного забезпечення захисту інформації.

6. За рахунок чого можна зменшити негативні наслідки соціальної інженерії на рівні програмного забезпечення?

7. Що сприятиме підвищенню результативності роботи соціального інженера?

8. Назвіть основні області застосування технологій СІ. Наведіть відомі Вам приклади.

9. Наведіть узагальнену класифікацію методів СІ. Розкрийте сутність методів СІ, що грунтуються на взаємодії з політикою безпеки.

10. Розкрийте сутність локальних і віддалених, аверсних і реверсних методів СІ, а також відомих Вам методів маніпулювання в ході соціального інжинірингу.

11. На які складові поділяються методи СІ за порушенням характеристик безпеки та реляційними ознаками, за ступенем важкості, типом джерела та

типом доступу?

12. Які категорії кібератак з використанням соціальної інженерії Вам відомі? Які суттєві питання дозволить розв'язати їх реалізація?

13. Опишіть алгоритм дій зловмисників методом соціальної інженерії. Наведіть відомі Вам приклади.

14. Що може вплинути на успіх у реалізації соціотехнічної атаки?

15. Покажіть 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 в якості інструмента соціальної інженерії.

18. Назвіть спільні й відмінні риси відомих Вам фішингових і вішингових атак. У чому полягає механізм фармінгу? Наведіть приклади.

19. Поясніть сутність використання телефонного зв'язку в якості інструмента соціальної інженерії. Наведіть приклади.

20. Поясніть сутність використання незаконного аналізу сміття в якості інструмента соціальної інженерії. Наведіть приклади.

21. Які особистісні підходи використовуються соціальними інженерами для одержання інформації від працівників фірми-конкурента?

22. Назвіть основні переваги та недоліки реверсивної соціальної інженерії. На яких основних факторах вона базується?

23. Назвіть основні стратегії запобігання стандартним тактикам вторгнення.

Розділ 4
ЗАХИСТ ІНФОРМАЦІЇ ВІД СОЦІОТЕХНІЧНИХ АТАК

За своїм правовим режимом інформація поділяється нині на конфіденційну і таємну. Згідно закону України "Про інформацію" конфіденційна інформація – це відомості, які знаходяться 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 таємницю (банківську, комерційну, службову, професійну, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству і державі.

У свою чергу конфіденційна інформація може бути такою, яка є власністю держави або яка не належить державі. Саме вона, а точніше право власника на її захист є однією із меж реалізації права на інформацію. При цьому засоби, призначені для захисту інформації можуть бути поділені на:

пасивні – фізичні (інженерні), технічні та програмні засоби тощо;

активні – джерела безперебійного живлення, шумогенератори, скремблери, програмно-апаратні засоби маскування інформації тощо.

4.1 Канали несанкціонованого доступу до інформації

Під каналами несанкціонованого одержання інформації (КНОІ) розуміються такі дестабілізуючі фактори, під дією яких особами або процесами, які не мають на це законних повноважень може бути одержана або створена небезпека одержання інформація, що захищається. Об'єктивна необхідність формування повної множини потенційно можливих КНОІ така, як і для причин порушення цілісності інформації (ППЦІ). У той же час, труднощі формування повної множини КНОІ значно більші, ніж при вирішенні аналогічної задачі для ППЦІ. Пояснюється це тим, що несанкціоноване одержання інформації пов'язане переважно зі злочинними діями людей, які надто важко піддаються структуризації. Враховуючи таке формування якомога повної множини КНОІ доцільно за критерієм відношення до стану інформації, що захищається та критерієм ступеня взаємодії зловмисника з її елементами. За першим критерієм можна розрізнити два стани: безвідносно до обробки (несанкціоноване одержання інформації може мати місце навіть у тому випадку, якщо вона не обробляється, а просто зберігається) і в процесі безпосередньої обробки. Повна структуризація другого критерію може бути здійснена виділенням таких його значень [178]:

перше – без доступу (тобто непряме одержання інформації);

друге – з доступом, але без зміни їхнього стану або змісту;

третє – з доступом і зі зміною змісту інформації або стану.

Враховуючи таке класифікаційна структура КНОІ матиме вигляд, приведений у 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 по методу розподілу цілого на частини.

Таким чином, уся множина потенційно можливих КНОІ може бути розділеною на шість класів [178].

Таблиця 4.1

Класифікаційна структура КНОІ

Ознака класифікації		*Відношення до стану інформації, що захищається*	
		Безвідносно до обробки інформації **А – канали**	*Виявляються в процесі обробки* **В – канали**
Без доступу	**К – канали**	*1 – КЛАС* *АК – канали*	*2 – КЛАС* *ВК – канали*
З доступом	*Без зміни* **П – канали**	*3 – КЛАС* *АП – канали*	*4 – КЛАС* *ВП – канали*
	Зі зміною **Пи – канали**	*5 – КЛАС* *Апи – канали*	*6 – КЛАС* *ВПи – канали*

Наступним кроком на шляху вирішення розглянутої задачі є обґрунтування більш повного переліку КНОІ в межах кожного із шести класів. Отриманий перелік буде виглядати таким чином:

КНОІ першого класу – канали, що виявляються безвідносно до обробки інформації і без доступу зловмисника до інформації:

1. Розкрадання носіїв на заводах, де відбувається їхній ремонт;
2. Підслуховування розмов осіб, що мають відношення до інформації;
3. Провокування на розмови осіб, що мають відношення до інформації;
4. Використання зловмисником візуальних засобів;
5. Використання зловмисником оптичних засобів;
6. Використання зловмисником акустичних засобів.

КНОІ другого класу – канали, що виявляються в процесі обробки інформації без доступу зловмисника до неї:

1. Електромагнітні випромінювання пристроїв відображення;
2. Електромагнітні випромінювання процесорів;
3. Електромагнітні випромінювання зовнішніх запам'ятовуючих пристроїв;
4. Електромагнітні випромінювання апаратури зв'язку;
5. Електромагнітні випромінювання ліній зв'язку;
6. Електромагнітні випромінювання допоміжної апаратури;
7. Електромагнітні випромінювання пристроїв введення;

8. Електромагнітні випромінювання пристроїв підготовки даних;
9. Паразитні наводки в комунікаціях електропостачання;
10. Паразитні наводки в системах водопостачання і каналізації;
11. Паразитні наводки в мережах теплопостачання і вентиляції;
12. Паразитні наводки в шинах заземлення;
13. Паразитні наводки в ланцюгах газифікації;
14. Паразитні наводки в ланцюгах радіофікації;
15. Паразитні наводки в ланцюгах телефонізації;
16. Паразитні наводки в мережах живлення по ланцюгу 50 Гц;
17. Паразитні наводки в мережах живлення по ланцюгу 400 Гц;
18. Підключення генератора завад;
19. Підключення апаратури, що реєструє;
20. Огляд відходів виробництва, що потрапляють за межі контрольованої зони.

КНОІ третього класу – канали, що виявляються 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 четвертого класу – канали, що виявляються в 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 в 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 враженості програмного забезпечення "вірусом".

КНОІ п'ятого класу – канали, що виявляються 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. Включення в програми блоків типу "троянський кінь", "бомба" тощо.
12. Читання залишкової інформації в ОЗП після виконання санкціонованих запитів.

КНОІ шостого класу – канали, що виявляються в процесі обробки інформації з доступом зловмисника до інформації та застосуванням її:

1. Незаконне підключення до апаратури;
2. Незаконне підключення 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'ятовуючих 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, уніфікованності та безперервності. Домінантним чинником, як за ефективністю захисту, так і за ресурсовитратами у кожній із характеристик безпеки є комплексність. Комплексний захист від соціотехнічних атак ефективний лише при системному підході [103, 109, 115, 128], який у свою чергу грунтується на принципах:

законності (полягає у додержанні відповідності заходів, що плануються до реалізації в галузі забезпечення інформаційної і кібербезпеки, чинному законодавству);

невизначеності (обумовлюється неясністю поводження суб'єкта, тобто невизначеністю того хто, коли, де і яким чином може порушити безпеку об'єкта захисту);

неможливості створення ідеальної системи захисту (обумовлюється принципом невизначеності й залежить від обмеженості ресурсів засобів захисту);

мінімального ризику й мінімального збитку (ґрунтуються на тезі щодо неможливості створення ідеальної системи захисту. Відповідно до них необхідно враховувати конкретні умови існування об'єкта захисту для будь-якого моменту часу);

безпечного часу (ґрунтується на необхідності урахування як абсолютного (часу, протягом якого необхідне збереження об'єктів захисту), так і відносного часу (проміжку часу від моменту виявлення злочинних дій до досягнення мети зловмисником));

«захисту всіх від всіх» (полягає в організації захисних заходів проти всіх форм загроз для ОІД, що є наслідком принципу невизначеності);

персональної відповідальності (припускає персональну відповідальність кожного співробітника ОІД за дотримання режиму безпеки в рамках своїх повноважень, функціональних обов'язків і діючих інструкцій);

обмеження повноважень (припускає обмеження повноважень суб'єкта на ознайомлення з інформацією, до якої він не має доступу, а також введення заборони доступу до об'єктів і зон, перебування в яких не обумовлено родом його діяльності);

взаємодії й співробітництва (припускає культивування довірчих відносин між співробітниками, відповідальними за інформаційну і кібербезпеку та персоналом, а також налагодження співробітництва з усіма зацікавленими організаціями й особами);

комплексності та індивідуальності (ґрунтується на доцільності проведення комплексних, взаємозалежних і дублюючих один одного заходів для забезпечення безпеки об'єкта захисту, реалізованих з індивідуальною прив'язкою до конкретних умов);

послідовних рубежів безпеки (передбачає якомога раннє оповіщення про кібернапад на об'єкт захисту або інші несприятливі події з метою збільшення ймовірності того, що завчасний сигнал тривоги засобів захисту забезпечить службам безпеки можливість вчасно визначити причину тривоги й організувати ефективні заходи щодо протидії);

рівноміцності й рівнопотужності рубежів захисту (ґрунтуються на відсутності незахищених ділянок у рубежах захисту ОІД (рівноміцність) і відносно однаковій величині їх захищеності відповідно зі ступенем загроз

(рівнопотужність)).

Дотримання визначених принципів дозволить сформувати низку вимог до комплексної системи протидії соціотехнічним атакам і захисту від них, уникнути проблем пов'язаних з занадто високою вартістю реалізації цих вимог, неможливістю ефективного контролю за їх виконанням та важкістю їх засвоєння виконавцями, повністю нівелювати ризики усіх можливих загроз для об'єкту захисту, а також розробити уніфіковану концепцію захисту інформації від соціотехніків щодо різних типів працюючого персоналу, циркулюючої інформації, інформаційних систем та умов їх використання тощо. При цьому роботи щодо захисту від соціотехнічних атак повинні проводитися безперервно на кожному етапі циркулювання інформації з урахуванням впливу персоналу.

З урахуванням [128, 129] превентивні методи захисту від соціотехнічних атак можна розділити на **правові** (законодавчі та морально-етичні), **організаційні** (організаційно-адміністративні, організаційно-технічні та організаційно-економічні) та **інженерно-технічні** (фізичні, технічні та програмні). При цьому, наприклад, законодавчі методи ґрунтуються на нормативно-правових актах, за допомогою яких регламентуються права та обов'язки співробітників, а також встановлюється відповідальність всіх співробітників та підрозділів, які мають відношення до захисту інформації від соціотехнічних атак, за порушення правил роботи з важливими даними, результатом чого може бути порушення їх захищеності. Морально-етичні – засновані на сформованих у колективі моральних норм та етичних правил, дотримання яких сприяє захисту інформації від атак соціотехніків, а їх порушення прирівнюється до недотримання правил поведінки в суспільстві або колективі.

Сутністю організаційно-адміністративних методів є:

мінімізація витоку інформації через персонал;

організація спеціального документообігу;

виділення спеціальних захищених приміщень та засобів ЕОТ;

використання сертифікованих програмних і технічних засобів;

використання зареєстрованих носіїв інформації тощо.

Найдієвішими серед них є методи *антропогенного захисту*, що полягають у:

а) залученні уваги людей до питань безпеки;

б) усвідомленні користувачами всієї серйозності проблеми й прийняття політики безпеки системи;

в) вивченні та впровадженні необхідних методів і дій для підвищення захисту інформаційного забезпечення.

Одним із прикладів такому є формування у персоналу навичок, спрямованих на розкриття соціотехнічних атак та адекватного реагування на їх

прояви. Одним із перших кроків, які має виконати працівник при спробі зловмисників анонімно (наприклад, по телефону, скапу тощо) отримати від них інформацію про установу, її керівництво або персональні дані інших працівників – знайти для себе відповідь на два ключових питання:

як дізнатися про те, що той хто звертається з проханням є саме тим, за кого себе видає?;

як дізнатися про те, що у того хто звертається з проханням на це є певне право?

Приблизний алгоритм його подальших дій подано на рис. 4.1 (Додаток Г).

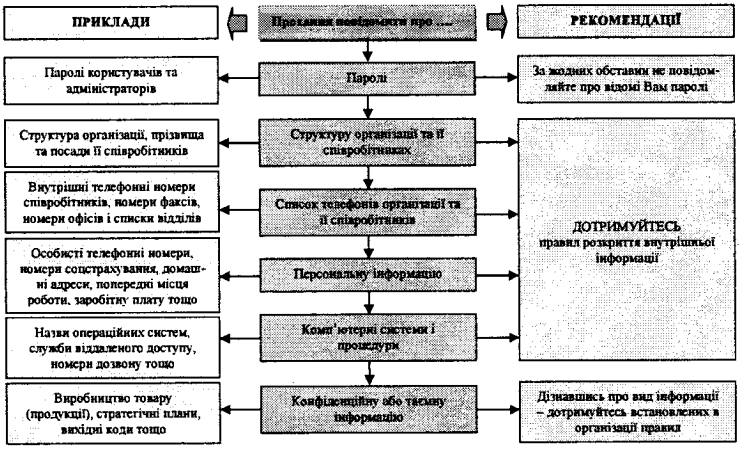


Рис. 4.1. Рекомендація з розкриття атаки спрямованої на одержання інформації

Єдиним але до того ж всеохоплюючим недоліком методів антропогенного захисту є їх пасивність.

Організаційно-технічні методи захисту реалізують через обмеження доступу до інформації сторонніх осіб, відключення від ЛОМ та Internet осіб, які мають доступ до конфіденційної інформації, передавання конфіденційної інформації лише спеціальними інженерно-технічними засобами, нейтралізацію витоку інформації електромагнітними і акустичними каналами тощо. Їх поділяють на інформаційні, процедурні, класифікаційні, застережливі, навчальні, спонукаючі [131]. *Інформаційні методи* включають локальні заходи, що реалізуються в межах організації та спрямовані на інформування персоналу щодо реалізацій соціотехнічних атак та нагадування про їх можливість. Наприклад:

розробка відповідних інформаційних статей, буклетів і брошур, календарів, пам'яток (наприклад, в конвертах із зарплатою) тощо, які поширюються в роздрукованій або електронній формі;

використання різноманітних повідомлень в системі корпоративних ресурсів, в локальній комп'ютерній мережі та інших стосовно правил поведінки з важливою інформацією (наприклад, при вході в систему користувачу з'являється повідомлення: "Якщо Ви пересилаєте конфіденційну інформацію електронною поштою, не забудьте зашифрувати її!");

оголошення через інформаційні дошки, електронні табло в громадський місцях (наприклад, у місцевому кафетерії, з часто оновлюваною інформацією про положення політики безпеки (ПБ)), спеціальні плакати, голосову пошту, місцеві гучномовці, спеціальні наклейки на телефонах (наприклад: "Телефонуючий дійсно той, за кого себе видає?") тощо

Процедурні засновані на розробці порядку дій, правил ПБ, рекомендацій, якими повинен керуватися персонал при використанні та наданні співробітникам або стороннім особам корпоративної інформації. Прикладом можуть бути:

правила ПБ, які містять в собі положення щодо соціотехнічних атак, з якими повинен бути ознайомлений персонал;

процедури при прийомі та звільнені співробітників;

порядок повідомлення працівників про зміни або нововведення в ПБ;

дії персоналу в нештатних ситуаціях;

рекомендації щодо надання важливої інформації.

Класифікаційні полягають у виборі критеріїв поділу інформації на класи та обґрунтування класифікаційної структури за вибраними критеріями. *Застережливі* методи ґрунтуються на системі заходів, що спрямовані на підвищення пильності та відповідальності персоналу на основі реалізації відповідних процедур безпеки. Наприклад: використовування різноманітних ідентифікаторів (наприклад, носіння бейджиків, включаючи тимчасові перепустки для співробітників, які забули перепускні ідентифікатори); супроводження відвідувачів; запит підтвердження особи при надходженні запиту на важливу інформацію; здійснення зворотного дзвінка при запиті важливої інформації; повідомлення адміністратору безпеки про підозрілі інциденти; при запиті від співробітників перевірити наявність його в штаті; під час нестандартного запиту задокументувати розмову, намагатися якомога більше дізнатися про атакуючого. *Спонукаючі методи* засновані на заохоченні працівників до дотримування ними методів захисту від соціотехнічних атак, наприклад, знання правил ПБ, успішне проходженнях перевірок (про які вони не знають) тощо. Прикладом такого методу є грошова винагорода, оголошення подяки, публікація найбільш надійного працівника місяця тощо. *Навчальні методи* засновані на проведенні необхідних заходів з метою придбання персоналом відповідних знань, вмінь та навичок протидії соціотехнічним атакам. Наприклад:

підвищення кваліфікації;

проведення періодичних тренінгів на робочих місцях;

використання автоматизованих систем перевірки стійкості співробітників до соціотехнічних атак, інструктажі тощо.

Перевага організаційно-технічних методів обумовлюється тим, що вони, по-перше, дозволяють вирішувати безліч різнорідних проблем, по-друге, прості в реалізації, по-третє, швидко реагують на небажані дії в мережі й, по-четверте, мають необмежені можливості модифікації і розвитку. Недоліки – висока залежність від суб'єктивних факторів, у тому числі від загальної організації роботи в конкретному підрозділі.

Організаційно-економічні методи передбачають проведення заходів з стандартизації методів і засобів захисту інформації, сертифікації засобів ЕОТ за вимогами інформаційної і кібербезпеки, страхування інформаційних ризиків, ліцензування діяльності у сфері захисту інформації тощо.

Інженерно-технічні методи (фізичні, технічні та програмні) захисту від соціотехнічних атак передбачають наряду з використанням штатними службами безпеки активних і пасивних технічних засобів протидії сторонньому кібервпливу на кшталт відключення, упакування й опечатування, а потім і належного зберігання відповідних носіїв інформації (дозволяють звести до нуля ризик знищення даних у результаті роботи шкідливих програм і дій зловмисника та забезпечити достатній рівень оцінюваної вірогідності результатів), виконання ними заходів щодо розроблення відповідних компонент системи, навчання користувачів і обслуговуючого персоналу формам і методам експлуатації ТЗ і ПЗ, а також контролю за дотриманням правил їх експлуатації. Недоліком даного підходу є висока чутливість до помилок установки і настроювання засобів захисту, складність управління.

4.2.1 Засоби та заходи фізичного, технічного і криптографічного захисту інформації з обмеженим доступом

Фізичні методи захисту від соціотехнічних атак засновані на використанні механічних, електричних, електронних та інших пристроїв і систем, які функціонують автономно створюючи різного роду завади на шляху соціотехніків. Такими можуть бути периметрові системи контролю, пропускні системи, засновані на технологіях smart-card, touch-memory тощо [130–132]. Вони забезпечують фізичну безпеку ІС – споруд та приміщень де розташована ІС (температура в приміщенні 10...26°С, вологість повітря 35...50%), самої інформаційної системи, допоміжного обладнання (принтери, сканери тощо), носіїв інформації і каналів передачі (отримання) інформації. Головними заходами фізичного захисту є 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 і його місця розташування повинні визначатися цінністю інформації, ризиком порушення безпеки та необхідністю дотримання існуючих захисних мір.

Діапазон засобів фізичного захисту, який можна застосувати для попередження катастроф або зведення їх до мінімуму, дуже великий, починаючи від самого нижнього рівня до найскладнішого. При цьому кожен рівень фізичного захисту має визначені режимні території, зони або приміщення у межах яких необхідно забезпечити належний рівень захисту. Так, наприклад, для захисту периметра можуть створюватись системи охоронної й пожежної сигналізації, системи цифрового відео спостереження, системи контролю й управління доступом (СКУД) тощо. За для цього пропонуються наступні рекомендації [178]:

режимні території, зони або приміщення повинні відповідати цінності інформації, що захищається;

периметр безпеки повинний бути чітко визначений;

допоміжне устаткування (ксерокс, факс тощо) повинно бути розміщено так, щоб зменшити ризик НСД до інформації з обмеженим доступом;

фізичні бар'єри повинні при необхідності простиратися від підлоги до стелі, щоб запобігти несанкціонованому доступу у режимні приміщення;

не слід надавати стороннім особам інформацію про те, що робиться в режимних територіях, зонах або приміщеннях без потреби;

доцільно розглянути можливість установлення заборони на роботу поодинці без належного контролю;

інформаційну систему варто розміщати у спеціально призначених для цього місцях, окремо від обладнання контрольованого сторонніми підрозділами;

у неробочий час режимні території, зони або приміщення повинні бути фізично недоступні і періодично перевірятися охороною;

у межах режимних територій, зон або приміщень використання фотографічної, звукозаписної і відео апаратури повинно бути заборонено;

на режимних територіях, у режимних зонах та приміщеннях варто установити належний контроль доступу тощо.

З метою реалізації заходів контролю необхідно:

вести облік дати і часу входу й виходу відвідувачів (відвідувачам повинний бути наданий доступ до конкретної, дозволеної інформації);

вилучати права доступу в режимні території, зони або приміщення в співробітників, що звільняються з даного місця роботи;

дотримуватись пропускного та внутрішньооб'єктового (організаційних та технічних заходів і правил щодо забезпечення режиму, встановленого в організації. Його основними завданнями є обмеження кола осіб, що допускаються до ІзОД, проведення робіт з виконавцями щодо роз'яснення вимог роботи з документами, які мають гриф обмеження доступу, забезпечення встановленого порядку користування ІзОД тощо) режимів.

Технічний захист є одним з найбільш потужних заходів захисту від соціотехнічних атак. Його основними методами є методи які заважають як добуванню інформації, так і її використанню. Технічні методи реалізуються за рахунок впровадження різних за типом пристроїв (механічних, електромеханічних, електронних й ін.), які схемно вбудовуються в апаратуру систем обробки інформації або сполучаються з нею для захисту ресурсів від вторгнення соціотехніків. Такі пристрої або перешкоджають фізичному проникненню, або, якщо проникнення все-таки відбулося, заважають несанкціонованому доступу до інформації (табл. 4.2), у тому числі за допомогою її маскування.

Таблиця 4.2

Основні методи і засоби несанкціонованого отримання інформації та її захисту

Типова ситуація	Канали витоку інформації	Методи і засоби	
		отримання інформації	захист 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
Провідному	Сигнал в лінії	Паралельний телефон, пряме підключення, електромагнітний датчик, диктофон, телефонна закладка	Маскування, скремблювання, шифрування, спецтехніка
	Наводки	Спеціальні радіотехнічні пристрої	Спецтехніка
Радіотелефону	ВЧ-сигнал	Радіоприймачі	Маскування, скремблювання, шифрування, спецтехніка
Документ на паперовому носії	Безпосередньо 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, наводки	Спеціальні радіотехнічні засоби	Екранування
Поштові відправлення	Безпосередньо 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, наводки	Спеціальні радіотехнічні пристрої	Контроль доступу, криптозахист, пошук закладок, сканування
	Електричні сигнали	Апаратні закладки	
	Програмний продукт	Програмні закладки	
Передача документа по каналах зв'язку	Електричні та оптичні сигнали	Несанкціоноване підключення, імітація зареєстрованого користувача	Криптозахист
Виробничий процес	Відходи, випромінювання тощо	Спецапаратура різного призначення	Оргтехзаходи, фізичний захист

Першу частину завдання вирішують замки, грати на вікнах, захисна сигналізація й ін. Другу – генератори шуму, мережні фільтри, скануючі радіоприймачі й безліч інших пристроїв, що перекривають витік інформації потенційними технічними каналами, або дозволяють 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 наступні 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 управляють проходженням мереженого трафіка відповідно до правил (*policies*) безпеки. Як правило, міжмережні екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;

системи виявлення вторгнень (*IDS - Intrusion Detection System*) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу "відмова в обслуговуванні" (*Cisco Secure IDS, Intruder Alert і NetProwler* від компанії *Symantec*). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;

засоби створення віртуальних приватних мереж (*VPN - Virtual Private Network*) – для організації захищених каналів передачі 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 шляхом її динамічного шифрування;

засоби аналізу захищеності – для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації (*Symantec Enterprise Security Manager, Symantec NetRecon*). Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Під технічними каналами розуміються при цьому канали сторонніх електромагнітних випромінювань і наведень (ПЕМІН), акустичні канали, оптичні канали й ін. Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;

установкою на лініях зв'язку високочастотних фільтрів;

побудовою екранованих приміщень ("капсул");

використанням екранованого устаткування;

установкою активних систем зашумлення.

Узагальнюючу схему можливих каналів витоку і несанкціонованого доступу (НСД) до інформації, оброблюваної в типовому одноповерховому офісі наведено на рис. 4.2, де:

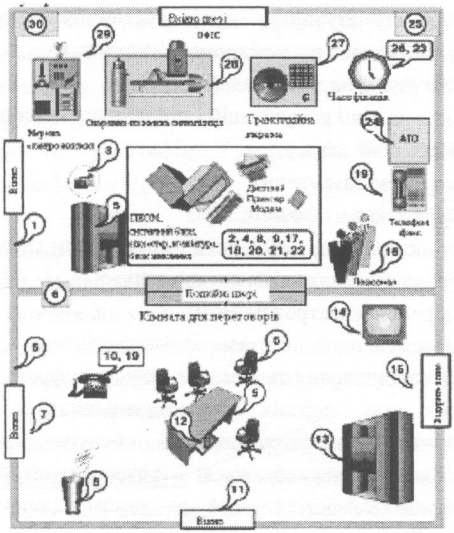


Рис. 4.2. Схема каналу витоку і НСД до інформації в типовій одноповерховій офісній споруді

1) витік за рахунок структурного звуку в стінах і перекриттях;

2) знімання інформації зі стрічки принтера, погано стертих дискет і т. п.;

3) знімання інформації з використанням відеозакладок;

4) програмно-апаратні закладки в ПЕОМ;

5) радіо-закладки в стінах і меблях;

6) знімання інформації з системи вентиляції;

7) лазерне знімання акустичної інформації з вікон;

8) виробничі й технологічні відходи;

9) комп'ютерні віруси, логічні бомби й т. п.;

10) знімання інформації за рахунок наведень і "нав'язування";

11) дистанційне знімання відео інформації (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 обслуговуючий персонал);

17) несанкціоноване копіювання;

18) витік за рахунок побічного випромінювання термінала;

19) знімання інформації за рахунок використання "телефонного вуха";

20) знімання з клавіатури й принтера акустичним каналом;

21) знімання з дисплея по електромагнітному каналу;

22) візуальне знімання з дисплея й 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 й 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 у тому числі й від соціотехнічних атак, перелік їх постачальників, а також послуг з установлення, монтажу, налагодження та обслуговування визначаються особами, які володіють, користуються і розпоряджається інформацією з обмеженим доступом самостійно або за рекомендаціями спеціалістів з технічного захисту інформації згідно з нормативними документами технічного захисту інформації. Їх вибір зумовлюється фрагментами або комплексним способом захисту інформації. При цьому фрагментний захист забезпечує протидію певній загрозі, а комплексний – одночасну протидію множині 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. З метою оцінювання стану ТЗІ, що обробляється або циркулює в ІС, комп'ютерних мережах та системах зв'язку, а також підготовки обґрунтованих виводів для прийняття відповідних рішень проводиться експертиза в сфері технічного захисту інформації. Порядок розрахунку та інструментального визначення зон безпеки інформації, реалізація заходів технічного захисту інформації, розрахунку ефективності захисту та порядку атестації технічних засобів забезпечення інформаційної діяльності, робочих місць (приміщень) установлюються нормативними документами з ТЗІ.

Переваги методів технічного захисту пов'язані з їхньою надійністю, незалежністю від суб'єктивних факторів, високою стійкістю до модифікації. Слабкі сторони – недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

Програмні методи захисту інформації у тому числі й від соціотехнічних атак засновуються на спеціальних прикладних пакетах або окремих програмах, що входять до складу програмного забезпечення (ПЗ) систем обробки даних. Вони включають програми для ідентифікації та аутентифікації користувачів, контролю та розмежування доступу до інформації, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту, аудита й моніторингу, антивірусного захисту тощо. Їх застосовують з метою забезпечення:

ідентифікації та аутентифікації користувачів, персоналу і ресурсів системи оброблення інформації;

розмежування доступу користувачів до інформації, засобів обчислювальної техніки і технічних засобів інформаційних систем;

цілісності інформації та конфігурації інформаційних систем;

реєстрація та облік дій користувачів;

маскування оброблюваної інформації;

реагування (сигналізації, відключення, зупинення робіт, відмови у запиті) на спроби несанкціонованих дій.

Найбільш ефективними методами захисту інформації від соціотехнічних атак є **криптографічні технології захисту.** Вони забезпечують нині три основних типи послуг: аутентифікацію (яка включає ідентифікацію), неможливість відмови від довершеного (*non-repudiation*) і збереження таємниці. Ідентифікація (підвид аутентификації) перевіряє, чи є відправник послання тим, за кого себе видає. Аутентифікація йде ще далі – перевіряє не тільки особистість відправника, але і відсутність змін в посланні. Реалізація вимоги неможливості відмови не дозволяє будь-кому заперечувати, що він відправив або отримав певний файл або дані (це схоже з відправкою рекомендованого листа поштою). І нарешті, збереження таємниці – це захист послань від несанкціонованого перегляду [178].

Зважаючи на таке криптографію (математичні методи перетворення даних для забезпечення безпеки) можна застосовувати для багатьох різних цілей в інформаційній безпеці, наприклад, криптографія може допомогти забезпечити конфіденційність та (або) цілісність даних, а також неспростовність проведеної ідентифікації та автентифікації. При цьому в обставинах, коли важливо зберігати конфіденційність, тобто коли інформація є надзвичайно чутливою, треба розглядати засоби безпеки, що зашифровують інформацію для зберігання чи

передавання мережею. За обставин, коли важливим є цілісність даних, що зберігаються чи оброблюються, для безпеки цих даних треба розглянути геш-функції, цифрові підписи та (або) засоби забезпечення цілісності. Засоби безпеки цілісності надають безпеку від випадкової чи зловмисної зміни, добавлення чи вилучення інформації. Засоби цифрових підписів можуть забезпечувати безпеку, схожу до засобів цілісності повідомлень, але також мають властивості, що дозволяють уможливити неспростовність. Під час вирішення питання про використання засобів шифрування, цифрових підписів чи інших засобів забезпечення цілісності треба брати до уваги відповідні державні закони і норми, вимоги до управління ключами (відповідну інфраструктуру відкритих ключів) та труднощі, які необхідно подолати для гарантування того, що справжнього поліпшення безпеки можна досягти без створення нових вразливостей.

Методи криптографії (наприклад, засновані на використанні цифрових підписів) можуть бути використанні для повідомлень, комунікацій та транзакцій з метою підтвердження чи спростування відправлення, передавання, подання, доставлення, оповіщення про отримання тощо. У ситуаціях, коли є важливою автентичність даних, для підтвердження достовірності даних може бути використаний цифровий підпис. Ця необхідність проявляється особливо, коли використовуються дані, на які посилає третя сторона, або коли велика кількість людей залежить від точності даних джерел, на які посилаються. Цифрові підписи також можна використовувати для підтвердження факту, що дані створені чи передані певною особою.

Застосовуючи криптографію треба подбати про те, щоб дотримувалися всі правові та регуляторні вимоги в цій сфері. Один з найважливіших аспектів криптографії – адекватна система управління ключами. Криптографія з відкритим ключем заснована на концепції ключової пари. Кожна половина пари (один ключ) шифрує інформацію таким чином, що її може розшифрувати тільки інша половина (другий ключ). Одна частина ключової пари – особистий ключ, відома тільки його власнику. Інша половина – відкритий ключ, розповсюджується серед всіх його кореспондентів, але пов'язана тільки з цим власником. Ключові пари володіють унікальною особливістю: дані, зашифровані будь-яким з ключів пари, можуть бути розшифровані тільки іншим ключем з цієї пари. Іншими словами, немає ніякої різниці, особистий або відкритий ключ використовується для шифрування послання; одержувач зможе застосувати для розшифровки другу половину пари. Ключі можна використати і для забезпечення конфіденційності послання, і для аутентифікації його автора. У першому випадку для шифрування послання відправник використовує відкритий ключ одержувача, і таким чином

воно залишиться зашифрованим, поки одержувач не розшифрує його особистим ключем, У другому випадку, відправник шифрує послання особистим ключем, до якого тільки він сам має доступ. При цьому слід враховувати, що процедури управління ключами залежать від використовування алгоритму наміру щодо використання ключів та політики безпеки.

Для вирішення цих завдань у 1985 році Коблиць і Міллер незалежно один від одного запропонували використовувати при побудові криптосистем алгебраїчні структури, визначені на множині точок на еліптичних кривих. Розглянемо випадок визначення еліптичних кривих над простими кінцевими полями довільної характеристики і над полями Галуа характеристики 2.

Нехай $p>3$ – просте число, $a,\ b \in GF(p)$ такі, що $4a^2+27b^2 \neq 0$. Еліптичною кривою E над полем $GF(p)$ називається множина рішень $(x,\ y)$ рівняння $y^2 = x^3 + ax + b$ над полем $GF(p)$ разом з додатковою точкою ∞, яка має назву точки нескінченності. Позначимо кількість точок на еліптичній кривій E через $\#E$. Верхня і нижня границі для $\#E$ визначаються теоремою Хассе:

$$p+1-2\sqrt{p} \le \#E \le p+1+2\sqrt{p}. \qquad (4.1)$$

Задамо бінарну операцію на E (в адитивному запису) наступними 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) $\forall (x_1,\ y_1) \in E,\ (x_2,\ y_2) \in E,\ x_1 \neq x_2,\ (x_1,\ y_1)+(x_2,\ y_2)=(x_3,\ y_3)$,

де $x_3 = \lambda^2 - x_1 - x_2,\quad y_3 = \lambda(x_1 - x_3) - y_1,\quad \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$.

(V) $\forall (x_1,\ y_1) \in E,\ y_1 \neq 0,\ (x_1,\ y_1)+(x_1,\ y_1)=(x_2,\ y_2)$,

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 утворить 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. Нехай $a,\ b \in GF(2^m),\ b \neq 0$. Еліптична крива E над полем $GF(2^m)$ називається множиною рішень $(x,\ y)$ рівняння

$$y^2 + xy = x^3 + ax + b \tag{4.2}$$

над полем $GF(2^m)$ разом з 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, $\# E$ парне.

Операція додавання на E у цьому випадку 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) $\forall (x_1,\ y_1) \in E,\ (x_2,\ y_2) \in E,\ x_1 \neq x_2,\ (x_1,\ y_1) + (x_2,\ y_2) = (x_3,\ y_3)$,

де $x_3 = \lambda^2 + \lambda + x_1 + x_2 + a,\quad y_3 + \lambda(x_1 + x_3) + x_3 + y_1,\quad \lambda = \dfrac{y_1 + y_2}{x_1 + x_2}$.

(V) $\forall (x_1,\ y_1) \in E,\ x_1 \neq 0,\ (x_1,\ y_1) + (x_1,\ y_1) = (x_2,\ y_2)$,

де $x_2 = \lambda^2 + \lambda + a,\quad y_2 = x_1^2 + (\lambda + 1)x_3 \quad \lambda = x_1 + \dfrac{y_1}{x_1}$.

У цьому випадку множина точок еліптичної кривої E із заданої в такій 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 $n = P + P + \cdots + P$, 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. Оберемо ціле число $n < \# E$. Тоді як пряму функцію виберемо добуток n. Для його обчислення по оптимальному алгоритму буде потрібно не менше $2 \cdot \log_2 n$ операцій додавання. Зворотну задачу сформулюємо в такий спосіб: по заданій еліптичної кривої E, крапці $P \in E$ і добутку n знайти n. В даний час усі відомі алгоритми рішення цієї задачі вимагають експонентного часу.

Для встановлення захищеного зв'язку два користувача A і B спільно вибирають еліптичну криву E і крапку P на ній. Потім кожен з користувачів вибирає своє секретне ціле число, відповідно a і b. Користувач A обчислює добуток a, а користувач B – b.Далі вони обмінюються обчисленими значеннями При цьому параметри самої кривої, координати крапки на ній і

значення добутків є відкритими і можуть передаватися по незахищених каналах зв'язку. Потім користувач A множить отримане значення на a, а користувач B множить отримане їм значення на b. У силу властивостей операції множення на число $a\ b = = b\ a$. Таким чином, обоє користувача одержать загальне секретне значення (координати крапки ab), що вони можуть використовувати для одержання ключа шифрування. Зловмиснику для відновлення ключа буде потрібно вирішити складну з обчислювальної точки зору задачу визначення a і b по відомим E, P, a і b.

Змішані **програмно-апаратні методи** реалізують ті ж функції, що апаратні й програмні методи окремо, і мають проміжні властивості. Одним із прикладів їх застосування є формування у персоналу навичок, спрямованих на адекватне реагування на прояви соціотехнічних атак. розкриття соціотехнічних атак та адекватного реагування на їх прояви. Одним із правил, яким має користуватися кожен працівник – не довіряти жодному без ідентифікації особи. Приблизний алгоритм його подальших дій подано на рис. 4.3 [133].

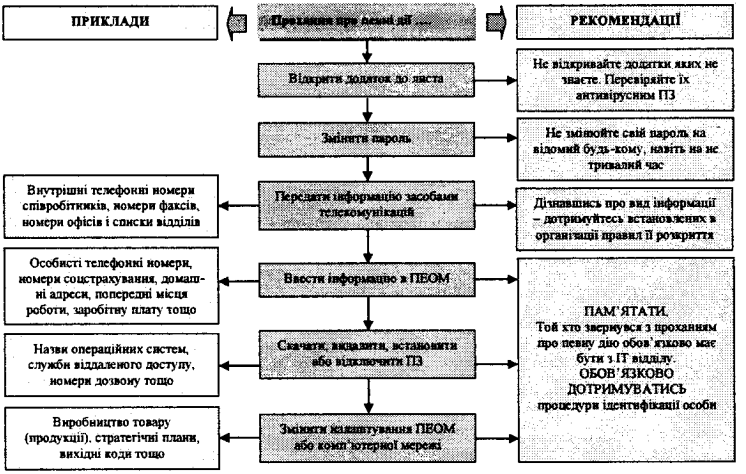


Рис. 4.3. Рекомендація з розкриття атаки спрямованої на здійснення якої-небудь дії

Переваги методів програмного захисту – універсальність, гнучкість, надійність, простота установки, здатність до модифікації й 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

З позицій впливу на інформацію та систему її обробки найбільший інтерес представляють загрози за метою реалізації. На їх підґрунті формується, 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 та НД ТЗІ 2.5-004-99) такі загрози полягають у порушенні конфіденційності інформації, її цілісності та доступності (рис. 4.4).

При цьому до загроз порушення конфіденційності інформації у ІС згідно з відносимо спроби:

несанкціонованого перехоплення електронних і акустичних випромінювань;

примусового електромагнітного опромінення (підсвічування) ліній зв'язку;

несанкціонованого застосування закладених пристроїв і програмних закладок;

відновлення тексту принтера та дистанційного фотографування;

розкрадання носіїв інформації й 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 відносяться до різних класів захищеності;

копіювання носіїв інформації з подоланням засобів захисту;

маскування під зареєстрованого користувача або під під запити системи;

використання недоліків мов програмування й операційних систем;

незаконне підключення до апаратури і ліній зв'язку;

виведення з ладу механізмів захисту;

впровадження і використання комп'ютерних вірусів тощо.

Вони можуть бути реалізовані порушником за умови подолання ним засобів:

організаційного обмеження доступу (p_{ood});

охоронної сигналізації (p_{oc});

захисту від вірусних атак ($p_{атак}$);

канального захисту від несанкціонованого доступу із телекомунікаційної мережі до ресурсів ЛОМ ($p_{кзткм}$);

управління доступу, включаючи засоби управління фізичним доступом до приміщень, системних блоків, клавіатури тощо ($p_{уфд}$);

адміністрування доступу до відповідних суб'єктів і об'єктів з використанням механізмів загального і спеціального ПЗ ($p_{ад}$).

Виходячи з такого ймовірність подолання неавторизованим користувачем зазначених засобів захисту може бути визначена з виразу:

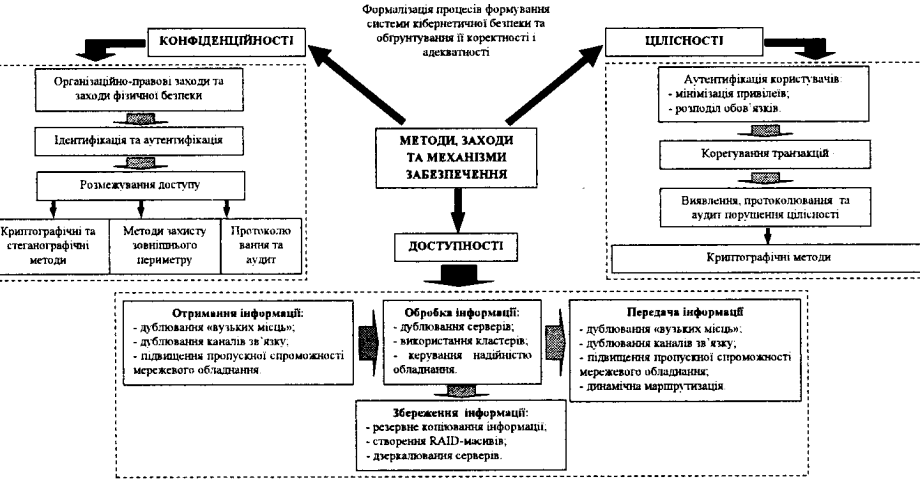


Рис. 4.4. Основні методи і заходи забезпечення безпеки інформації

$$p_{пзз} = p_{уфд} \cdot p_{ад} \cdot [1-(1-p_{ооД})\cdot(1-p_{ос})\cdot(1-p_{атак})\cdot(1-p_{кзктм})]. \quad (4.4)$$

Подальше розкриття змісту інформації з обмеженим доступом може статися лише за умови, якщо порушник після її отримання:

знає мову, якою інформація представляється (ймовірність події – $p_{мова}$);

знає і може застосовувати програмні засоби або апаратуру криптографічного перетворення (ймовірність події – $p_{пз/ктп}$);

має необхідні ключі або ключові набори для такого перетворення (ймовірність події – $p_{ключі}$).

Виходячи з такого ймовірність подолання неавторизованим користувачем засобів криптографічного захисту з урахуванням положень [1, 178–182] може бути визначена з виразу:

$$p_{кзі} = p_{мова} \cdot p_{пз/ктп} \cdot p_{ключі} \cdot \quad (4.5)$$

Тоді ймовірність порушення конфіденційності інформації з подоланням розглянутих вище засобів може бути визначена як:

$$P_{ПКІ} = p_{кзі} \cdot [1-(1-p_{пзз})]. \quad (4.6)$$

До загроз порушення цілісності інформації відносимо:

несанкціоновану модифікацію та/або видалення програм і даних;

вставку, зміну або видалення даних в елементах протоколу в процесі обміну між абонентами обчислювальної мережі;

втрату даних у результаті збоїв, порушення працездатності елементів обчислювальної мережі або некомпетентних дій суб'єктів доступу тощо.

Перелік класів і груп причин порушення цілісності інформації (ППЦІ) подамо у вигляді 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

Продовження табл. 4.3.

Найменування групи ППЦІ	Найменування ППЦІ
1.5. Відмови систем живлення	1.5.1. Аварійне відключення 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. Відключення систем кондиціонування забезпечення
	1.6.2. Зниження продуктивності систем контролю умов роботи кондиціонування апаратури
	1.6.3. Не забезпечення системою кондиціонування персоналу
	1.6.4. Відключення інших систем забезпечення нормальних умов роботи апаратури і персоналу
1.7. Відмови систем передачі даних	1.7.1. Повний вихід із ладу каналу зв'язку передачі 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 доп. 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 передачі керування
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 інформації, що відновлюється
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 відключення систем забезпечення кондиціонування
	2.6.2. Короткочасне зниження продуктивності систем кондиціонування
	2.6.3. Короткочасне відключення інших систем забезпечення нормальних умов роботи апаратури і персоналу
2.7. Збої систем передачі даних	2.7.1. Неправильне виконання функцій передачі 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. Помилки програми	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 передачі даних	3.4.1. Неправильна схема комутації каналу передачі даних
	3.4.2. Неправильна схема комутації в каналі
	3.4.3. Неправильний монтаж схеми в пристроях зв'язку

Продовження табл. 4.3.

Найменування групи ППЦІ	Найменування ППЦІ
СТИХІЙНІ ЛИХА	
4.1. Пожежа	4.1.1. Невеличка (локальна)
	4.1.2. Середня
	4.1.3. Загальна (велика)
4.2. Повінь	4.2.1. Місцевий (локальний)
	4.2.2. Середній (у межах будинку)
	4.2.3. Загальний (міський)
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. Невеличка
	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. Роздруківка масивів
5.3. Розкрадання	5.3.1. Розкрадання банків 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. Підключення	5.5.1. Підключення генератора завад
	5.5.2. Підключення апаратури, що реєструє
5.6. Поломка	5.6.1. Поломка апаратури
	5.6.2. Ушкодження програм
	5.6.3. Ушкодження елементів баз даних
	5.6.4. Ушкодження носіїв
	5.6.5. Ушкодження документів
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 випромінювання пристроїв відображення інформації
	6.1.2. Випромінювання процесорів ЕОМ
	6.1.3. Випромінювання зовнішніх пристроїв, що запам'ятовують
	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

Продовження табл. 4.3.

Найменування групи ППЦІ	Найменування ППЦІ
6.2. Паразитні наводки	6.2.1. Наводки в комутаторах загального призначення
	6.2.2. Наводки в слабкострумових ланцюгах
	6.2.3. Наводки в мережах живлення
6.3. Зовнішні електромагнітні випромінювання	6.3.1. Випромінювання біля пристроїв наочного відображення інформації
	6.3.2. Випромінювання біля зовнішніх пристроїв, що запам'ятовують
	6.3.3. Випромінювання біля друкувальних пристроїв
6.3. Зовнішні електромагнітні випромінювання	6.3.4. Випромінювання біля апаратури зв'язку
	6.3.5. Випромінювання біля процесів
	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 й при аналізі загроз конфіденційності інформації (ймовірність такої події – $p_{пзз}$ визначена раніше);

захисту цілісності від загроз у телекомунікаційних мережах ($p_{цткм}$);

захисту від спеціальних впливів на інформацію по ТКМ ($p_{сп.вп}$);

контролю та поновлення цілісності інформації ($p_{конт.ц}$).

З урахуванням можливостей попереднього підходу, ймовірність порушення цілісності $P_{ППЦІ}$ може бути знайдена з виразу:

$$P_{ППЦІ} = p_{конт.ц} \cdot \left[1 - (1 - p_{пзз}) \cdot (1 - p_{сп.вп}) \cdot (1 - p_{цткм})\right]. \qquad (4.7)$$

До загроз порушення доступності інформації відносимо:

повторення або вповільнення елементів протоколу;

придушення обміну в телекомунікаційних мережах;

використання помилок або недокументованих можливостей служб і протоколів передачі даних для ініціювання відмови в обслуговуванні;

перевитрата обчислювальних або телекомунікаційних ресурсів тощо.

Вони, як і в попередніх випадках, можуть бути реалізовані за умови подолання неавторизованим користувачем систем управління доступом до IP

ЛОМ (ідентифікації, аутентифікації, надання певних повноважень чи привілеїв, з наступною їх перевіркою під час кожної із спроб доступу до ресурсів) та фільтрації. Виходячи з такого стійкість системи управління доступом – (в розумінні ймовірності її не подолання) визначається стійкістю процесів ідентифікації та аутентифікації самого адміністратора безпеки, як користувача з найширшими повноваженнями:

$$p_{ссуд} = 1 - p_{нзз}. \tag{4.8}$$

Ця задача може вирішуватися застосуванням у ІС засобів фільтрації типу міжмережевих екранів (*firewall*, брандмауерів), сервісів-посередників (*proxyservices*) тощо. При середній тривалості обслуговування в СІТС одного запиту і пуассонівському законі розподілу ймовірностей впливу, ймовірність того, що під час звернення до ресурсу він уже використовується, дорівнює:

$$p_{вик.рес} = 1 - p_0 = 1 - \exp\left\{-t_{вик.рес} \cdot \lambda_{зап}\right\}, \tag{4.9}$$

де p_0 – ймовірність відсутності впливів (ймовірність того, що на певному часовому інтервалі виникне рівно нуль впливів);

$t_{вик.рес}$ – середнє значення часу використання ресурсу.

Враховуючи таке ймовірність порушення доступності ресурсу з дорівнюватиме:

$$P_{ПД} = 1 - \left(1 - p_{вик.рес}\right) \cdot \left(1 - p_{ссуд}\right). \tag{4.10}$$

Виходячи з наведених вище формульних залежностей комплексна величина ймовірності порушення системи захисту інформації у ІС та їх специфічному класі – ЛОМ за метою реалізації з урахуванням пропозицій [1, 178–182] може бути, як результат, знайдена з виразу:

$$P_{ПСЗІ} = 1 - \left(1 - P_{ПКІ}\right) \cdot \left(1 - P_{ПЦІ}\right) \cdot \left(1 - P_{ПДІ}\right). \tag{4.11}$$

Наряду з загрозами за метою реалізації у окремий клас загроз варто виділити події, які залежно від умов можуть вплинути на кожну з відомих складових безпеки інформації шляхом:

несанкціонованого доступу до ресурсів обчислювальної мережі без використання штатних засобів обчислювальної техніки;

несанкціонованого включення до складу комплексів засобів обробки й захисту інформації нових елементів або зміни режимів їхньої роботи;

виконання програм або дій в обхід системи захисту;

підбору, перехоплення, розголошення або використання нестійких

параметрів аутентифікації 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 і 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 передачі інформації між вузлами ІС або усередині вузла, такі події можуть бути поділені на загрози, що:

1) використовують принцип доступу суб'єкта ІС (користувача, процесу) до певного об'єкта (файлу даних, каналу зв'язку) або до прихованих каналів, тобто шляхів передачі інформації;

2) забезпечують активний або пасивний впливи на складові безпеки інформації в ІС;

3) реалізують опосередкований та безпосередній впливи, а також вплив на систему дозволів в ІС.

До перерахованих вище загроз безпеки інформації варто додати ще й такі, як:

загроза несанкціонованого обміну інформацією між користувачами;

загроза відмови від інформації, тобто невизнання одержувачем (відправником) факту її одержання (відправлення) тощо.

Якщо вести мову конкретно про загрози безпеці інформації в ІС за метою реалізації, то з метою забезпечення конфіденційності й цілісності інформації у системі за рахунок унеможливлення доступу до неї та модифікації неавторизованим користувачем її змісту, окрім заходів організаційного обмеження доступом, необхідно перш за все застосовувати засоби: адміністрування доступу, управління фізичним доступом, криптографічного перетворення, контролю цілісності та охоронної сигналізації. З метою недопущення переводу ресурсу в режим штучної відмови – порушення доступності об'єкту за рахунок унеможливлення вчасного використання того чи іншого ресурсу авторизованим користувачем, необхідно додатково передбачити механізми: запобігання постійного чи занадто тривалого використання такого ресурсу, забезпечення стійкості та відновлення процесів в умовах збоїв, резервування інформаційних об'єктів, аналізу потоків запитів від суб'єктів ЛОМ та телекомунікаційних мереж, контролю та поновленню цілісності інформаційних об'єктів (наприклад, в каналах ІС).

4.3.1 Метод визначення значень показників уразливості ІзОД

Враховуючи, що з усієї сукупності показників уразливості інформації особливе місце займають базові показники, які характеризують уразливість інформації в якому-небудь одному структурному компоненті ІС по одному якому-небудь КНОІ, відносно якогось потенційного порушника, – схема їх визначення в загальному вигляді матиме вигляд, приведений на рис. 4.5) [178].

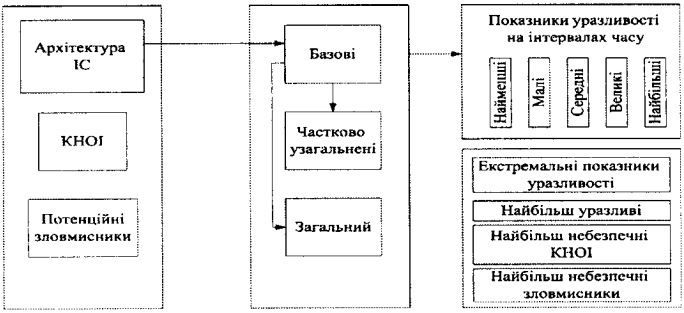


Рис. 4.5. Загальна схема визначення показників уразливості інформації

Значення базових показників визначається архітектурою ІС (від чого залежить рівень захищеності кожного її структурного компонента), множиною потенційно можливих КНОІ (від чого залежать потенційні можливості злочинних дій у структурному компоненті), а також чисельністю потенційних порушників і їхніх можливостей здійснювати злочинні дії. Потенційно можливою є та обставина, що несанкціоноване одержання інформації в сучасних ІС можливо не тільки шляхом безпосереднього доступу до даних, але і багатьма іншими шляхами, які не потребують такого доступу.

Узагальнена структурна схема потенційно можливих злочинних дій в ІС наведена на рис. 4.6.

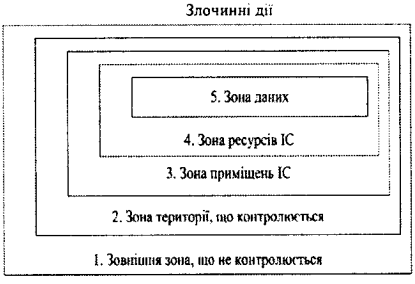


Рис. 4.6. Структурна схема потенційно можливих злочинних дій

Виділені зони характеризуються наступними особливостями.

1. **Зовнішня неконтрольована зона** – територія навколо ІС, на якій персоналом і засобами ІС не застосовуються засоби і не здійснюються жодні заходи для ЗІ.

2. **Зона контрольованої території** – територія навколо приміщення ІС, що постійно контролюється персоналом або технічними засобами.

3. **Зона приміщень ІС** – внутрішній простір тих приміщень, у яких розташовані 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 захищається.

Злочинні дії з метою несанкціонованого одержання інформації можливі в кожній із перерахованих зон. При цьому для несанкціонованого одержання інформації – необхідно одночасне настання таких подій:

порушник повинен одержати доступ у відповідну зону;

під час перебування порушника в зоні, у ній повинен з'явитися відповідний КНОІ;

відповідний КНОІ повинен бути доступний порушнику;

у КНОІ в момент доступу до нього порушника повинна знаходитися інформація, що захищається.

Відповідно до теореми можливостей, здатність несанкціонованого одержання інформації порушником k-ї категорії по j-му КНОІ в l-й зоні і-го структурного компонента ІС визначається такою залежністю:

$$P_{ijkl}^{(n,l)} = P_{ikl}^{(n,d)} * P_{ijl}^{(n,k)} * P_{ijkl}^{(j,\mu)} * P_{ijl}^{(n,u)}, \qquad (4.12)$$

де i – поточний ідентифікатор структурного компонента ІС; j – те ж для КНОІ; k – те ж для категорії потенційних порушників; l – те ж для зони злочинних дій;

P_{ikl} – можливість доступу порушника k-ї категорії в l-у 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 зоні i-го компонента за умови доступу порушника в зону;

P_{ijl} – можливість наявності інформації, що захищається в j-ому КНОІ в l-й зоні i-го компонента в момент доступу туди порушника.

Приведена залежність буде справедлива в тому випадку, коли всі події, відображені в правій частині формули, є незалежними одна від одної, тобто коли поява будь-якої з них впливає на можливість появи інших. У противному

випадку необхідно враховувати коефіцієнти між можливостями залежних подій. В даному випадку будемо вважати, що усі події є незалежними.

Для базової можливості несанкціонованого одержання інформації байдуже, в якій зоні це одержання інформації мало місце. Вона раніше визначена як можливість несанкціонованого одержання інформації в одному компоненті ІС одним порушником певної категорії й по одному КНОІ. Позначимо базову можливість як P_{ijk} й запишемо її в такому вигляді:

$$P_{ijk}^{(n,б)} = 1 - \prod_{l=1}^{5} \left[1 - P_{ijkl}^{(n,б)}\right] = 1 - \prod_{l=1}^{5} \left[1 - P_{ikl}^{(n,d)} P_{ijl}^{(n,k)} P_{ijkl}^{(n,н)} P_{ijl}^{(n,u)}\right] \qquad (4.13)$$

Значення частково узагальнених показників можуть визначатися таким чином. Нехай *{k*}* – підмножина з повної множини потенційно можливих порушників, яка нас цікавлять. Тоді можливість несанкціонованого одержання інформації зазначеною підмножиною порушників по *j-му* КНОІ в *і-ому* компоненті ІС $P_{ij}^{(r)}\{k^*\}$ визначається виразом:

$$P_{ij}^{(r)}\{k^*\} = 1 - \prod_{\forall j^*} \left[1 - P_{ijk}^{(б)}\right], \qquad (4.14)$$

де $\forall j^*$ – множення в дужках для усіх k, що входять в підмножину.

Аналогічно, якщо існує підмножина представляючих інтерес КНОІ, то уразливість інформаційному компоненту даній підмножині КНОІ щодо *k-го* порушника може бути визначена з виразу:

$$P_i^{(r)}\{j^*\}k = 1 - \prod_{\forall j^*} \left[1 - P_{ijk}^{(б)}\right]. \qquad (4.15)$$

Якщо ж *{і*}* підмножина цікавлячих структурних компонент ІС, то уразливість інформації в них по *j-му* КНОІ щодо *k-го* порушника

$$P^{(r)}\{i^*\}jk = 1 - \prod_{\forall i^*} \left[1 - P_{ijk}^{(б)}\right]. \qquad (4.16)$$

Кожен з приведених виразів дозволяє робити узагальнення по одному якомусь параметру. Для одержання комплексного виразу необхідно врахувати одночасно підмножини *{i*},{j*},{k*}*. Тоді, очевидно, загальний показник уразливості $P^{(r)}$ визначається виразом:

$$P^{(r)} = 1 - \prod_{\forall i^*} \left(1 - P_{ijk}^{Б}\right) \prod_{\forall j^*} \left(1 - P_{ijk}^{Б}\right) \prod_{\forall k^*} \left(1 - P_{ijl}^{Б}\right). \qquad (4.17)$$

Тепер визначимо вирази, що описують екстремальні показники уразливості. Як відзначалося раніше, екстремальними можна назвати показники, які характеризують найбільш несприятливі умови захищеності інформації:

найуразливіший структурний компонент ІС, КНОІ та найнебезпечнішу категорію порушників.

Зважаючи на таке позначимо через: i – найбільш уразливий структурний компонент ІС, j – найбільш небезпечний КНОІ та k – найнебезпечнішу категорію порушників. Тоді очевидно, що:

$$\bar{i} = iEp^y \to \max \forall i, \tag{4.18}$$

де i – є таке i, для якого заданий показник уразливості p^y приймає максимальне значення для всіх i.

Аналогічно:

$$\bar{j} = jEp^y \to \max \forall j \tag{4.19}$$

$$\bar{k} = kEp^y \to \max \forall k \tag{4.20}$$

Неважко помітити, що приведені вище вирази є адекватними для таких інтервалів часу, які є малими. Їх не не можна зводити до точки, але процеси, що відбуваються на цих інтервалах відносно уразливості інформації, можна вважати однорідними. При збільшення можливостей у порушника для дій та збільшенні можливостей зміни стану ІС і умов обробки інформації час, необхідний для цього також зростатиме.

Припустимо, що малий інтервал можливо розділити на дуже малі і на кожному з них визначати уразливість інформації. А оскільки процеси, що відбуваються на малому інтервалі часу однорідні, то на кожному інтервалі уразливість буде визначатися однозначно по залежності:

$$P^M = 1 - \prod_{t=1}^{N_t} \left(1 - P^T\right), \tag{4.21}$$

де P^T – уразливість у точці (на дуже малому інтервалі);

P^M – показник уразливості на малому інтервалі;

t – перемінний індекс дуже малих інтервалів, на які розбитий малий інтервал;

N_t – загальне число інтервалів.

Неважко помітити, що розглянутий підхід може поширюватися і на інші види інтервалів, тобто, великий інтервал уявити деякою послідовністю малих і т.п. Проте, приведені вирази будуть справедливі лише в тому випадку, якщо на всьому розглянутому інтервалі часу умови для злочинних дій залишаються незмінними. У реальних умовах вони можуть змінюватися, причому найбільш важливим фактором, що впливає на можливості злочинних дій, є активні дії системи ЗІ. Технологія функціонування системи ЗІ повинна бути тим сильнішою і активнішою, чим вище уразливість інформації.З урахуванням цього запишемо:

$$P^T(t) = \oint[P^T(t-1)]. \tag{4.22}$$

Тобто, значення крапкового показника в кожній точці розглянутого інтервалу є деяка функція від значення цього показника в попередній точці. Тоді вираз (5.10) можна записати в такому вигляді:

$$P^M = 1 - \prod_{t=1}^{N^t}\left\{1 - \oint[P^T(t-1)]\right\}. \tag{4.23}$$

Розглянуті моделі є аналітичними, оскільки вони дозволяють визначати необхідні значення показників уразливості шляхом аналітичних обчислень.

Проте в багатьох практичних ситуаціях конкретні значення вихідних розмірів для визначення базового показника уразливості інформації можуть змінюватися залежно від конкретних ситуацій у ІС та зовнішньому середовищі і не виражатися у вигляді конкретних формул унаслідок складності вихідних моделей. У той же час часто можна структурувати системи, що моделюються і процеси до такого ступеня, що задача може бути вирішена методом моделювання. Для складних ІС і слабоструктурованих схем функціонування систем обробки найбільш адекватним методом прогнозування показників уразливості буде статистика. Проте для того, щоб статистичним шляхом безпосередньо прогнозувати значення показників уразливості, необхідні багатопараметричні статистичні дані передісторії. В даний час статистичні дані практично відсутні, і одержання їх являє собою дуже складну проблему. З метою спрощення задачі будемо прогнозувати не безпосередні показники уразливості, а складові величини, що входять у вираз для показників якості. Як випливає з моделей оцінки показників якості, такими величинами є:

можливість прояву дестабілізуючих факторів (наявності КНОІ);

можливість наявності інформації що, захищається в місці і під час прояву дестабілізуючих факторів;

можливість несанкціонованого одержання інформації під впливом дестабілізуючих факторів, незважаючи на застосування ЗІ.

Розглянемо можливі підходи до прогнозування перерахованих величин.

Можливість прояву дестабілізуючих факторів – P_{ijz}.

При сталому процесі функціонування системи обробки інформації прояв дестабілізуючих факторів можна вважати як випадковий пуасонівський процес. Позначивши *ijz* як інтенсивність потоку *i-го* фактора в *j-му* технічному засобі (ТЗ), що знаходиться в *Z-му* стані та відповідно з властивостями пуасонівського процесу запишемо:

$$P_{ijk} = f_{tijk} * \sigma_t, \tag{4.24}$$

де σ_t, – інтервал часу, істотно менший того інтервалу, відносно якого визначена величина.

Так як для загального випадку інтервал прогнозування цій умові задовольняти не буде, величину P_{ijk} запишемо в такому вигляді:

$$P_{ijk} = 1 - \left(1 - \rho_{ijz}\right) \cdot \left(\frac{\Delta t}{\sigma_t}\right)$$

де Δt – інтервал прогнозування.

Отже, за такого підходу весь період прогнозування Δt можна розділити на менші інтервали тривалістю σ_t записавши при цьому, що:

$$\overline{j} = jEp^{y} \rightarrow max \forall j \ . \tag{4.25}$$

Тоді за умови, що $\Delta t \gg \sigma_t$, можна записати:

$$P_j^M = \frac{\sum_{\theta} \gamma_{t\theta} \Delta t}{\frac{\Delta t}{\sigma t}} = \frac{\sigma t}{\Delta t} \sum \gamma_{j\theta} \ . \tag{4.26}$$

Значення функції визначаються по технологічному графіку обробки інформації в прогнозований період часу.

Можливість несанкціонованого одержання інформації під дією дестабілізуючих факторів, незважаючи на застосування засобів ЗІ P_{ij}.

Аналогічно аналізу попереднього параметра період прогнозування будемо здійснювати на малих інтервалах часу. Введемо функцію x_{in}^{Q}, що дорівнює:

$$\begin{cases} 1 - \textit{якщо } j\textit{- ий засіб захисту на } k\textit{- му інтервалі часу активно використовується в } i\textit{ - ому ТЗ} \\ 0 - \textit{не використовується;} \end{cases} .$$

З урахуванням того, що $\Delta t \gg \sigma_t$, можна записати:

$$P_{ik}^{НП} = \prod \forall_{\eta} \left(1 - P_{ij}^{\eta}\right) \cdot \frac{\sigma}{\Delta e} \cdot \sum N_{ji}^{\theta} \ , \tag{4.27}$$

де $P_{ik}^{НП}$ – можливість того, що при використанні η *-го* засобу захисту в *j-м* ТЗ несанкціоноване одержання інформації не буде мати місце навіть при появі *i-го* дестабілізуючого фактора.

Виходячи з концепції захисту інформації як сукупності взаємозалежних організаційних заходів і технічних систем, синтезованих на основі обраних критеріїв оптимізація з урахуванням обмежень і спрямованих на захист інформації при її формуванні, передаванні, прийому, обробки і збереження з метою зберігання її цілісності, формується поняття захищеності інформації в ІС. Поняття захищеності є центральним у силу таких причин:

1. Сама мета створення системи (моделі) ЗІ є досягнення науково-технічного

рівня захищеності інформації в ІС. Таким чином, методологія оцінки захищеності інформації є по суті методологією наукового обґрунтування кількісних показників досягнення мети системи захисту.

2. Методологія оцінки захищеності інформації в ІС є, насамперед, методологією наукового обґрунтування норм ефективності ЗІ. Оптимальний або раціональний вибір одиниць виміру і кількісних значень норм ефективності визначають категорії якості системи захисту, структуру і математичний апарат синтезу, аналізу й оптимізації моделі захисту і саму якість захисту. Дійсно, завищені норми ефективності ведуть до підвищення витрат на створення системи захисту, а занижені норми просто не дозволяють досягти цілей захисту.

3. Методологія оцінки захищеності інформації в ІС є основою для реального рівня захисту інформації в конкретних системах і його порівняння з нормами ефективності захисту, а, отже, є основою для вирішення питань про методи і засоби досягнення системи захисту.

Визначаючи критерії якості захисту, структуру і математичний апарат синтезу, аналізу й оптимізації моделі системи захисту, методологія оцінки захищеності інформації визначає цілі, засоби і методологію інженерного аналізу, спрямованого на виявлення потенційних стратегій нападу на інформацію в ІС і основні характеристики стратегій нападу, визначення можливих заходів захисту і вимог до їхніх параметрів.

4.4 Доопрацювання засобів захисту інформації

Всі засоби захисту потрібно використовувати так, щоб вони функціонували і продовжували функціонувати передбачуваним і відповідним способом. Цей аспект безпеки є одним з найважливіших, однак йому часто приділяють мало уваги. Частіше система або служба вже існують, тому захист впроваджують пізніше і потім залишають без нагляду. Існує навіть тенденція ігнорувати засоби захисту, які були застосовані, а підтримці або убезпечуванню приділяти незначну увагу. Більше того, втрату ефективності засобів захисту потрібно спрогнозувати в планах, а не спостерігати вже як факт. Також необхідно перевіряти узгодженість захисту, контролювати робоче оточення, оглядати записи у журналі та обробляти інциденти для гарантії тривалості процесу убезпечування. Доопрацювання, навіть враховуючи те, що ним часто нехтують, є одним з найважливіших положень безпеки інформаційних технологій. Реалізовані засоби захисту можуть працювати ефективно, якщо вони перевірені в реальному циклі ділової активності. Потрібно бути впевненим, що їх використовують правильно і що будь-які інциденти і зміни захисту виявлені та вжито відповідних заходів. Основні задачі завершальної

діяльності полягають у тому, щоб забезпечити правильність функціонування засобів захисту. Через деякий час з'являється тенденція погіршення роботи служб чи механізмів. Доопрацювання призначено для виявлення цих погіршень і ініціювання коригувальних дій. Це єдиний спосіб підтримувати рівні засобів захисту, необхідні для забезпечення захисту системи інформаційних технологій. Управління безпекою інформаційних технологій є безперервним процесом, що не припиняється після реалізації плану безпеки інформаційних технологій [178].

Діяльність "механізму доопрацювання" охоплює:

обслуговування засобів захисту для забезпечення їхньої безперервної й ефективної роботи;

перевіряння, яке гарантує, що засоби захисту задовольняють обумовлені методики і проекти;

контролювання активів, загроз, уразливості і засобів захисту щодо відхилень, щоб виявити зміни, які впливають на ризики;

досліджування інциденту, щоб гарантувати відповідну реакцію на небажані події.

Механізм доопрацювання – тривалий процес, який повинен містити переоцінку рішень, прийнятих раніше.

Супровід

Більшість засобів захисту вимагає супроводу і підтримування керівництвом для забезпечення правильного і відповідного функціонування в процесі їхньої діяльності. Ці дії (супровід і підтримування керівництвом) мають бути заплановані і виконуватися згідно з графіком. Таким способом накладні витрати можуть бути мінімізовані і збережена цінність засобів захисту.

Для виявлення несправностей необхідна періодична перевірка. Захисний засіб, що ніколи не перевірявся, не має великої цінності, тому що неможливо визначити ступінь довіри йому. Діяльність щодо супроводу містить:

перевірку журналів;

зміну параметрів, щоб відобразити зміни і доповнення;

повторне ініціювання початкових значень або лічильників;

адаптацію до нових версій.

Вартість супроводу і підтримування керівництвом завжди треба брати до уваги під час визначання і вибирання засобів захисту, тому що витрати на супровід і керування можуть дуже відрізнятися залежно від різних засобів захисту, а це може слугувати вирішальним чинником для їхнього вибору. Взагалі, необхідно мінімізувати витрати із супроводу і підтримування керівництвом засобів захисту, тому що можливо після вибору конкретних засобів захисту вони можуть вимагати

не тільки одноразових витрат, але й подальших.

Обслуговування

Обслуговування засобів захисту, що охоплює також і управління, є важливою частиною програми безпеки організації. Всі рівні керівництва відповідальні за обслуговування, щоб гарантувати:

виділення необхідних ресурсів організації для обслуговування засобів захисту;

періодичну переатестацію засобів захисту для гарантування виконання ними своїх функцій;

модернізацію засобів захисту у разі появи нових вимог;

чітко визначену відповідальність за обслуговування засобів захисту;

незмінність визначеного рівня ефективності наявних засобів захисту під час модифікації технічного й програмного забезпечень у разі розширення системи інформаційних технологій;

запобігання новим загрозам або ураженням при модернізації технологій.

Якщо здійснено описані вище заходи з обслуговування, то засоби захисту продовжуватимуть виконувати визначені функції, що дасть змогу уникати несприятливих і збиткових уражень.

Відповідність засобів захисту

Перевіряння відповідності засобів захисту, тобто аудит чи ревізія захисту, є дуже важливим для гарантування відповідності й узгодженості з планом безпеки системи інформаційних технологій. Щоб гарантувати, що рівень безпеки інформаційних технологій залишається ефективним, важливо, щоб впроваджувані засоби захисту завжди відповідали проекту чи плану захисту системи інформаційних технологій. Це треба затверджувати на усіх етапах проходження проектів і систем, а саме на етапах проектування і впровадження, життєвого циклу експлуатації, а також етапу заміни або переміщення.

Перевіряння відповідності захисту треба планувати і об'єднувати з іншими запланованими заходами. Вибіркові перевіряння особливо корисні для визначання, чи відповідає виконавчий персонал і користувачі певним засобам захисту і процесам. Процедури перевірки необхідні для забезпечення коректності функціонування засобів захисту, правильності їхнього впровадження і використовування і, за потреби, проведення випробовування. Там, де виявлено, що засоби захисту не відповідають безпеці, повинен бути створений і реалізований план коригувальних дій з подальшим аналізом результатів. Перевіряння відповідності захисту можна використовувати у випадках:

нових систем і після впровадження служб інформаційних технологій (після того, як були реалізовані);

наявних систем чи після впровадження служб інформаційних технологій через деякі проміжки часу (наприклад щорічно);

наявних систем і служб інформаційних технологій у разі змін у методиках безпеки системи інформаційних технологій для визначання необхідних коригувань з метою забезпечення необхідного рівня засобів захисту.

Перевіряти відповідність захисту може зовнішній чи внутрішній персонал, використовуючи контрольні списки, що стосуються методики безпеки системи інформаційних технологій. При цьому власне засоби захисту, що забезпечують захист системи інформаційних технологій, можуть бути перевірені за допомогою:

проведення періодичного контролювання і випробовування;

проведення вибіркових перевірянь стану рівнів захисту і цілей у специфічних сферах критичності або важливості.

Під час будь-якого перевіряння відповідності захисту можна одержати цінну інформацію щодо дій системи інформаційних технологій за допомогою:

використання пакетів програм для фіксування подій;

використання контрольних точок для відстежування повної хронології подій.

Перевіряння відповідності захисту для підтвердження і наступні регулярні перевіряння повинні ґрунтуватись на погоджених переліках засобів захисту, отриманих в результаті останнього аналізу ризику, на методиці безпеки системи інформаційних технологій, а також на процедурах функціонування захисту інформаційних технологій, що затверджені керівництвом, включаючи звіти про інциденти. Цілі полягають в тому, щоб визначити, чи реалізовані засоби захисту, чи правильно впроваджені, чи використовуються правильно, і, де необхідно, чи перевірені. За нормального режиму функціонування системи необхідно щоденно перевіряти використовування засобів захисту. Співбесіди зазвичай теж необхідні у цьому випадку, але результати повинні бути максимально точними і перевіреними. Сказане кимсь, може бути суб'єктивним поглядом і повинно бути підтвердженим особами, з якими він (вона) працює.

Це допомагає одержати всеосяжний контрольний список і погоджені форми звіту. Контрольні списки повинні охоплювати загальну ідентифікаційну інформацію, наприклад, деталі конфігурації, важливість захисту, методичні документи, навколишнє середовище. Фізичний захист повинен стосуватися зовнішніх аспектів, таких як зовнішні споруди, включаючи доступність крізь отвори і прорізи люків, і внутрішні аспекти, такі як міцність приміщень, блокування, системи виявлення і запобігання пожежам (включаючи сигналізацію), аналогічно і для виявлення води або рідини, несправності систем живлення тощо.

Нині існує багато проблем, які необхідно виявляти:

зони, відкриті для фізичного проникнення чи для обходу контролю; наприклад, блокатори дверей (кодові замки клавішні і карткові);

неадекватні механізми чи невірне встановлювання технічних засобів, наприклад, відсутність чи недостатнє встановлення, чи невірний тип датчиків контролю. Чи досить детекторів диму/нагрівання для приміщень, чи вірна висота встановлювання? Чи є адекватна реакція на сигналізацію? Чи під'єднана пожежна сигналізація до пункту контролю? Чи є нові джерела небезпеки: можливо, хтось використовує приміщення для збереження легкозаймистих матеріалів? Чи використовують засоби резервного живлення і системи відновлення? Чи використовують кабелі відповідних типів і чи не проходять вони поблизу гострих країв? Щоб знайти прогалини в захисті для інших аспектів безпеки, для захисту персоналу та управління цим процесом, а також захисту програмного забезпечення можуть виявитися корисними такі питання:

1) для захисту персоналу: Чи отримані інструкції? Чи ліквідовані виявлені прогалини? Чи персонал дійсно усвідомлює ситуацію і добре обізнаний в захисті? Чи залежить ключова функція від однієї особи?;

2) для управління захистом: Як насправді розпоряджаються документами? Чи є сучасною і актуальною документація загального користування? Чи використовують аналіз ризику, перевіряння стану і ведення звітності інцидентів так, як їх треба здійснювати? Чи правильні плани продовження роботи, і чи дійсно вони сучасні?;

3) для захисту програмного забезпечення: Чи має місце дублювання на необхідному рівні? Наскільки ефективний вибір ідентифікатора/пароля користувача і процедури? Чи охоплюють контрольні точки реєстрацію помилок і положення трасування до правильного вибору і градації? Чи відповідають оцінені продукти вимогам? Чи необхідне дублювання для захисту комунікацій? Якщо є віддалений доступ, чи є необхідне устаткування і програмне забезпечення і чи використовують їх належним чином? Якщо вимагаються кодування або авторизація повідомлення, то наскільки ефективна система управління ключами і відповідними операціями?

У цілому перевіряння відповідності захисту – це досить складне завдання і вимагає практичного досвіду й поінформованості для успішного завершення. Ці дії є незалежними від внутрішнього огляду або контролювання.

Керування змінами

Системи інформаційних технологій і оточення, в якому вони діють, постійно змінюються. Ці зміни розглядаються як результат появи нових особливостей і служб чи виявлення нових загроз і вразливостей. Ці зміни також можуть

спричинити нові загрози і вразливості. Зміни системи інформаційних технологій можуть містити:

нові процедури;

нові особливості;

модифікації програм;

апаратні перевірки;

нові користувачі, що включають зовнішні групи чи анонімні групи;

додаткову роботу з мережами і з'єднаннями.

Коли відбуваються заплановані зміни в системі, важливо встановити порушення, як такі що викликають зміни в захисті системи. Якщо система має пункт керування її конфігурацією чи іншу організаційну структуру з керування технічними змінами системи, то повинен бути призначений системний фахівець та його представники на пункті з обов'язками робити висновки щодо того, чи викликає будь-яку зміну захисту порушення, а якщо так, то яким способом. Для змін, що спричинені придбанням нових апаратних засобів, програмного забезпечення чи служб, необхідне аналізування, щоб встановити нові вимоги захисту. З іншого боку, багато змін, зроблених у системі, незначні і не вимагають значного аналізування, що необхідне для великих змін, але все-таки певного аналізування потребують. Для обох типів змін потрібно виконати аналізування, що оцінює переваги і витрати. Для незначних змін це можна виконати неофіційно на зустрічах, але результати і рішення керівництва мають бути задокументовані.

Контролювання

Контролювання – вирішальна частина циклу захисту інформаційних технологій. Якщо його проводять коректно, то це дає адміністрації чітке уявлення про те:

що було досягнуто порівняно з поставленими цілями;

чи переконливими є досягнення, і які специфічні ініціативи впроваджено.

Всі зміни в активах, загрозах, вразливості засобів захисту потенційно можуть мати істотний вплив на ризики, і раннє виявлення змін дозволяє здійснити запобіжні заходи. Ведуться журнали з безпеки для фіксації подій. Ці журнали треба, як мінімум, періодично переглядати, і, якщо можливо, аналізувати за допомогою статистичних методів для раннього прогнозування тенденцій до змін і прогнозування повторів несприятливих подій. Використовування журналів тільки для аналізування подій, що відбулися, веде до втрати потенційних можливостей засобів захисту.

Контролювання повинне також охоплювати процедури для звітності контролеру безпеки інформаційних технологій і для керування на постійній

основі. Повинен бути підготовлений план щоденного контролювання, щоб забезпечити додатковими інструкціями і процедурами для гарантування поточного функціонування із захисту. Користувачі, операційний персонал і розробники системи повинні періодично консультуватися для гарантування, що всі проблеми безпеки враховано і план захисту інформаційних технологій залишається сучасним. Одна з причин, чому контролювання є важливою частиною супроводу безпеки інформаційних технологій, – це те, що воно дає змогу знайти впливаючи на захист зміни. Серед положень, що повинні бути перевірені, – матеріальні носії інформації і її значення, загрози та вразливості інформації і засобів захисту, що страхують інформацію. Активи контролюють для виявлення змін їхніх цінностей і відповідних змін цілей безпеки системи інформаційних технологій. Можливими причинами цих варіацій є зміни:

бізнесових цілей організації;

вимог до системи інформаційних технологій;

інформації, оброблюваної в системі інформаційних технологій;

устаткування інформаційних технологій.

Загрози та вразливість контролюють, щоб виявляти зміни їхньої важливості (наприклад, спричинені змінами оточення, інфраструктури чи технічних можливостей) та виявляти на ранньому етапі появу інших загроз чи вразливостей. Зміни загроз і вразливостей можуть спричинятися змінами активів.

Засоби захисту постійно контролюють, щоб перевіряти їхню продуктивність і ефективність. Потрібна гарантія, що вони є дієздатними і захищають системи інформаційних технологій відповідно до необхідного рівня захисту. Можливо, що зміни активів, загроз і вразливостей впливають на ефективність і відповідність засобів захисту. Крім того, коли впроваджують нові системи інформаційних технологій чи коли роблять зміни в наявних системах, необхідно гарантувати, що такі зміни не вплинуть на стан наявних засобів захисту і що нові системи уведені з відповідними засобами захисту.

Коли знайдені аномалії в захисті, необхідно розслідувати і повідомити обставини керівництву для можливого аналізу складу засобів захисту чи, у серйозних обставинах, переглянути політику безпеки системи інформаційних технологій і ініціювати дії з аналізування ризику.

Для забезпечення погодженості з методикою безпеки системи інформаційних технологій потрібно виділити відповідні ресурси для забезпечення відповідного рівня щоденного контролювання:

наявних засобів захисту;

уведених нових систем чи служб;

запланованих змін в наявних системах чи службах.

Щоб вірно зрозуміти природу складного випадку, необхідно взяти інформацію з різних журналів і звести її в єдиний звіт випадку. Ці зведені звіти випадків треба потім аналізувати. Зведення звіту випадків – складне завдання і його найважливіший аспект – визначання умов, які дадуть змогу різні записи в журналі поєднати з потрібним ступенем довіри.

Техніка менеджменту для керування щоденним моніторингом – це підготовка документації оперативних процедур захисту для подальшого використання. Ця документація описує всі дії щодо гарантування необхідного рівня захисту для всієї системи і служб; цього повинні безкомпромісно дотримуватися у всіх системах і службах в подальшому.

Повинні бути задокументовані процедури з модифікації наявної конфігурації захисту. Вони повинні містити відкориговані параметри захисту і всі зміни будь-якої інформації з керування захистом. Ці зміни повинні бути задокументовані і підтверджені процесом керування конфігурацією системи. Мають бути визначені процедури для виконання ручного супроводу, для гарантії, що захист не є під загрозою. Відповідальний розподіл процедур повинен бути описаний для кожної задіяної компоненти захисту.

Необхідно визначити умови і періодичність аналізу журналів безпеки. Повинно бути описано використання методів статистичного аналізування та їх застосування. Керівництво повинно дати інструкції як організувати аудит різних оперативних станів за порогом базового.

Обробляння інцидентів

Практично неможливо уникнути небажаних інцидентів у захисті. Кожний інцидент потрібно досліджувати настільки глибоко, наскільки вагомий збиток він спричинив. Регулювання інциденту дає змогу відповідно реагувати на випадкові або навмисні збої нормального режиму роботи системи інформаційних технологій. Отже, проект звітності і розслідування інцидентів повинні бути придатними для всієї організації і сервісних служб системи інформаційних технологій. Після цього потрібно об'єднати між організаційні плани звітності для глибшого уявлення про місця виявлення інцидентів безпеки інформаційних технологій і пов'язаних з ними загроз, їх впливу на активи інформаційних технологій та ділову активність.

Основними цілями розслідування інцидентів безпеки інформаційних технологій повинні бути виявлення компетентності і ефективності реагування на інцидент, а також формування висновків про інциденти з метою запобігання подібним несприятливим подіям. Підготовлений план дій із наперед

визначеними рішеннями дає змогу організації реагувати на прийнятних умовах для припинення подальшого пошкодження і, якщо можливо, продовжувати ділову активність із запасними засобами. План реагування на інциденти повинен включати вимоги хронологічного документування всіх подій і заходів; це повинно допомогти ідентифікувати джерела інцидентів. Це є передумовою для досягнення іншої мети – зменшення ризику в майбутньому через вдосконалення засобів захисту. Інший позитивний наслідок інцидентів – збільшення готовності інвестувати в засоби захисту.

Важливо також проаналізувати здійснення й документування інциденту, керуючись такими питаннями:

що сталося і коли саме?

чи діяв персонал згідно з планом?

чи вчасно необхідна інформація була в розпорядженні персоналу?

що персонал запропонував робити інакше наступного разу?

Відповіді на ці питання допоможуть зрозуміти інцидент. Також це допоможе знизити ризик шляхом збільшення релевантності проектів і методик захисту інформаційних технологій (наприклад, вдосконалення засобів захисту, зменшення уразливості й адаптування програми компетентності в захисті).

Щоб визначити ризики і визначити їх серйозність, треба старанно аналізувати ризики. Для підтримки аналізування ризиків і поліпшення результатів необхідна інформація про інциденти захисту. Потрібно зібрати цю інформацію й проаналізувати надійним способом, і зрозуміти отриману користь. Також важливо, щоб організація належним чином розробила план і організувала дієве аналізування інцидентів інформаційних технологій, і щоб отримана та оброблена інформація була доступна для підтримки аналізування ризику, керування та іншої діяльності, пов'язаної з захистом.

Для успішного виконання вимог дійсних і потенційних користувачів дієвого аналізування інцидентів потрібно створювати на підставі їхніх вимог. Перед виконанням будь-якої операції потрібно здійснювати ґрунтовний опис інциденту в програмі компетентності в захисті, який гарантує, що весь ймовірно задіяний персонал розуміє, що таке дієве аналізування інцидентів, пропонована нею користь і як можна використовувати отримані результати у:

поліпшенні аналізування ризику та оглядах керування;

допомозі в запобіганні інцидентам;

приведенні до необхідного рівня компетентності безпеки інформаційних технологій відповідних інструкцій;

забезпеченні "аварійною" інформацією комп'ютерних груп реакції на

надзвичайні обставини.

Відповідні цьому ключові аспекти, що повинні враховуватися в будь-якій дієвий аналіз інцидентів:

випереджуюча розробка планів обробляння небажаних інцидентів, коли вони відбуваються і викликані зовнішньою чи внутрішньою логічною чи фізичною атакою, або випадковою несправністю устаткування чи людською помилкою;

навчання персоналу, призначеного для розслідування випадків, наприклад, щоб сформувати групи реакції на надзвичайні обставини.

Реакції на надзвичайні обставини може бути більш-менш визначена як певна група осіб, що розслідують причини інцидентів інформаційних технологій, вивчають потенційні майбутні прояви чи виконують всі періодичні вивчення і досліджування попередніх подій. Результатом цієї роботи можуть бути відновлювальні заходи. Група реакції на надзвичайні обставини може бути внутрішньою чи зовнішньою щодо організації (наприклад контрактна).

Якщо є план заходів і підготовлений персонал і відбувається небажаний інцидент, то поспішних рішень можна уникнути і будуть збережені свідоцтва, які можна використовувати у відстежуванні та ідентифікуванні джерела інциденту, набагато швидше буде встановлений захист цінних активів, і витрати, пов'язані не тільки з інцидентом, але і з усуненням наслідків будуть скорочені. Надалі будь-який негативний розголос буде мінімізований.

Організації повинні готувати і планувати інциденти відповідно до дієвого аналізування інцидентів, що мають місце, зокрема:

готування – наперед задокументовані попереджувальні заходи, інструкції і процедури обробляння інцидентів (разом зі збереженням свідоцтв ведення журналів реєстрування подій) і контроль зв'язків з громадськістю, інструктивна документація і плани безперервності роботи;

повідомлення – процедури, засоби та обов'язки для звіту про інциденти і їхній вплив;

оцінювання – процедури та обов'язки з досліджування інцидентів і визначання їхньої серйозності;

відновлення – процедури та обов'язки з відновлення нормальної діяльності;

керування – процедури та обов'язки з таких питань: як діяти, щоб обмежити збитки від інциденту, подолати його та повідомити керівництво більш високого рівня;

оглядання – процедури та обов'язки для після інцидентних дій, разом з дослідженнями легального характеру та аналізом тенденцій.

Варто підкреслити, що хоч і є вигода від використання дієвого аналізування

інцидентів організаціями індивідуально, але організації можуть одержати більше користі від спільного використання деякої інформації про інциденти; це забезпечить ширшу базу щодо виявлення "тривог", швидкого визначання тенденцій та їхнього запобігання. Щоб полегшити це, треба використовувати структуру бази даних дієвого аналізування інцидентів, яка повинна бути досить гнучкою, щоб охопити весь діапазон вимог для всього (всіх секторів, типів загроз і уражень) і визначити вимоги сектора/загрози/ураження. Немає значення, чи то розділ чи організація входить до дієвого аналізування інцидентів, вони повинні використовувати подібну топологію, виміри і структуру для реєстрації інформації щодо інцидентів. Це дозволить порівнювати та аналізувати. Використання загальної структури – можливість отримувати всеохоплюючі результати і особливо більш ґрунтовну базу для швидкого розпізнавання "тривог". Маючи на увазі викладене вище, досягнення взаємодії між дієвим аналізування інцидентів та аналізуванням ризику і методами керування можна істотно поліпшити результати, а отже, збільшити користь від впровадження дієвого аналізування інцидентів.

Інформація щодо появи загроз значно вплине на якість оцінювання загроз і оцінювання ризику. Далі в процесі досліджування інцидентів, імовірно, буде зібрано нову і додаткову інформацію з урахуванням вразливостей і з вказівкою на способи її використання. Супровід дієвого аналізування інцидентів дає можливість користувачу визначити та оцінити вразливість і, отже, забезпечити цінними вихідними даними аналізування ризику. В її основу буде частково введена інформація з урахуванням загроз і, частково, результати розслідувань передумов інциденту, повідомлені комп'ютерними групами реакції на надзвичайні обставини. Наприклад, загроза логічного проникнення (присутність нападника і привабливість оброблюваної інформації) може бути пов'язана з вразливістю до логічного проникнення (недостатність чи відсутність відповідних логічних механізмів контролювання за доступом) і в такий спосіб створювати ризик. Тому використовування дієвого аналізування інцидентів для визначання та оцінювання вразливості використовуванням інформації про загрозу, що занесена до бази даних інцидентів, які вже були розслідувані, разом з інформацією з інших джерел, особливо дослідження реакції інформаційної системи на надзвичайні обставини може розкрити неідентифіковані до цього часу вразливості.

Треба відзначити, що функція дієвого аналізування інцидентів відповідає повідомленням тільки щодо інцидентів, що відбулися. Тому будь-яке дієве аналізування інцидентів не може безпосередньо забезпечувати інформацією про ті вразливості, що можуть існувати, але не були визначені як інциденти інформаційних технологій. Крім того, інформацію від дієвого аналізування

інцидентів треба із застереженням використовувати для статистичного аналізування та аналізування тенденцій, тому що вихідні дані можуть бути неповними чи помилково визначеними. Проте результати досліджень групи реакції на надзвичайні обставини може дати деякі уявлення щодо непередбачених вразливостей. У цілому, регулярні вихідні дані дієвого аналізування інцидентів для аналізування ризику та огляду керування можуть допомогти покращити якості оцінювання загроз, ризику і вразливостей.

Питання для самоконтролю

1. Які ви знаєте канали несанкціонованого доступу до інформації?

2. Які ознаки є основними при класифікації каналів несанкціонованого одержання інформації?

3. На скільки класів поділяються канали несанкціонованого одержання 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 сприяє порушенню конфіденційності інформації?За умови подолання чого вони можуть бути реалізовані?

9. Що сприяє порушенню цілісності інформації?За умови подолання чого вони можуть бути реалізовані?

10. Які причини є основними при порушенні цілісності інформації?

11. Які ви знаєте групи і класи причин порушення цілісності інформації? назвіть їх та наведіть кілька прикладів з життєвого досвіду.

12. Що сприяє порушенню доступності до інформації?За умови подолання чого вони можуть бути реалізовані?

13. Опишіть загальну схему визначення показників уразливості інформації.

14. Яким особливостями характеризуються виділені зони безпеки інформації?

15. Опишіть сутність та зміст зовнішньої неконтрольованої зони.

16. Опишіть сутність та зміст зовнішньої контрольованої зони.

17. Опишіть сутність та зміст зовнішньої зони приміщень ІС.

18. Опишіть сутність та зміст зовнішньої зони ресурсів.

19. Опишіть сутність та зміст зовнішньої зони даних.

20. Опишіть особливості проявів дестабілізуючих факторів.

21. *Назвіть головні шляхи доопрацювання засобів захисту інформації. Розкрийте їх сутність.*

Розділ 5
СОЦІОІНЖЕНЕРНІ МЕТОДИ РІШЕННЯ ПРОБЛЕМ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ: ТЕСТУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРОНИКНЕННЯ

Соціоінженерний підхід сформувався в рамках індустріальної соціології у 30-х рр. XX століття. Його найбільш характерними рисами є:

орієнтація на вивчення й зміну штучних соціальних систем, насамперед соціальних організацій;

застосування наукових методів і засобів у соціальному управлінні;

безпосереднє поєднання прикладної соціології з практикою соціального управління;

установка на використання соціальних ресурсів, людського потенціалу в організаціях;

створення постійних або тимчасових служб, що професійно займаються соціальною роботою.

Насамперед здійснюється орієнтовний зондаж досліджуваного соціального об'єкта й оцінюється реальна ситуація шляхом її порівняння з нормативною моделлю. Розходження між існуючим положенням справ і бажаним виступає основою виділення розв'язуваної соціальної проблеми. Варіант рішення являє собою ідею або гіпотезу, що повинна містити певні способи досягнення цілей соціального управління. При цьому складається вичерпний перелік заходів, що дозволять максимально зблизити або привести у відповідність реальну ситуацію й нормативну модель. Збір і аналіз інформації служать засобом уточнення й вибору гіпотетичних рішень, на основі яких виробляються й реалізуються практичні рекомендації, здійснюється прогноз можливих проблемних ситуацій у зв'язку з нововведеннями. Такий неодноразово повторюваний цикл рішення соціальних проблем становить основу рішення проблем соціотехнічної безпеки установи.

Методи соціоінженерної діяльності постійно вдосконалюються, видозмінюються й коректуються відповідно до виникаючих завдань і умов. У їхній основі лежать різні види прикладних, соціологічних досліджень, побудовані на знанні соціальної діагностики й консультування, а також соціального нормування, прогнозування, програмування й проектування. *Соціальна діагностика* – метод оцінки стану соціального об'єкта. Вплив на організацію тут ґрунтується на саморефлексії, у результаті якої показ дійсного стану породжує потреба в удосконалюванні роботи («ефект дзеркала»). У ході

соціальної діагностики можуть вирішуватися наступні завдання:

виявлення пріоритетності окремих соціальних проблем;

аналіз і оцінка окремих показників соціального розвитку;

аналіз і оцінка стану соціальної організації в цілому;

оцінка результатів соціального розвитку за певний період;

оцінка ефективності проведених заходів і ін.

Соціальне планування – метод наукового визначення цілей організації й засобів їхньої реалізації, при якому загальні цілі конкретизуються у вигляді системи приватних цілей і виражаються сукупністю соціальних показників, якщо вони не задаються вищими інстанціями. Найчастіше ведеться шляхом екстраполяції існуючих тенденцій. *Соціальне прогнозування.* На відміну від плану, що носить директивний характер і передбачає однозначне рішення, прогноз має імовірнісний характер і містить альтернативи. *Соціальне нормування* – метод досліджень і розробок, за допомогою якого вирішуються проблеми побудови й використання нормативів, що виражають типові вимоги до функціонування соціальних організацій. *Соціальне програмування* – різновид соціального планування, при якій детально визначаються етапи рішення досить великих проблем, плануються засоби, заходи, терміни та очікувані результати. *Соціальне проектування* складається в науково обґрунтованому визначенні основних параметрів майбутньої соціальної організації з їхньою прив'язкою до конкретних умов її функціонування. *Соціальне консультування* – метод удосконалювання практики соціального керування й експертної допомоги керівникам у рішенні вартих завдань. Консультування здійснюють професійні консультанти, консультаційні організації, науковці, фахівці.

Рішення проблем соціотехнічної безпеки припускає при цьому чітку фіксацію способів і засобів організації соціальних процесів, дій органів управління й виконавців, здійснюваних у певній послідовності. Це дозволяє об'єднати дії керівників і виконавців у єдину систему, чітко визначивши границі дій кожного, знизити витрати на підготовку й проведення окремих заходів, накопичувати досвід рішення соціальних проблем. Одним з основних способів визначення рівня соціотехнічної безпеки підприємства є оцінювання ступеня готовності його ІКС до функціонування в умовах соціотехнічних атак шляхом проведення так званих «тестів на проникнення» або інакше проведення тестування системи захисту ІКС.

5.1 Тестування системи захисту інформації на проникнення

Тестування на проникнення (тести на подолання захисту, penetration testing, pentest, пентест) – доволі популярна в усьому світі послуга, що дозволяє [134]:

виявляти недоліки в області інформаційної безпеки (ІБ) з погляду сторонньої людини, які не були враховані при розробці політики безпеки;

розкривати внутрішні і зовнішні спроби проникнення до інформаційної системи (ІС) й запобігати їх.

Суть тестування на проникнення полягає в реалізації санкціонованої спроби обійти існуючий комплекс засобів захисту ІС. В ході його проведення аудитор відіграє роль зловмисника, мотивованого на порушення ІБ мережі замовника. Як правило, інтенсивній перевірці піддаються технічні засоби захисту корпоративної мережі, але залежно від поставлених умов, можуть оцінюватися й інші, наприклад, соціотехнічні аспекти безпеки (рівень поінформованості користувачів тощо).

Тестування на проникнення повинно допомогти користувачеві знайти відповідь на такі основні питання: по-перше, чи всі пункти політики безпеки досягають своїх цілей і використовуються так, як це було задумано й, по-друге, чи існує що-небудь не прописане у політиці безпеки, що може бути використане зловмисником для досягнення запланованих ним цілей. Воно може проводитися як у складі аудита на відповідність стандартам, так і у вигляді самостійної роботи. Так, наприклад, при аудиті 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.д. У вигляді самостійної роботи тести можуть проводитися із двома основними цілями:

1) обґрунтування необхідності проведення робіт з підвищення захищеності;

2) одержання незалежної оцінки рівня безпеки інформаційної системи.

У першому випадку замовником, як правило, є далекоглядні керівники IT підрозділів або підрозділів ІБ, яким необхідно продемонструвати вищому керівництву недоліки існуючої системи управління інформаційної безпеки (СУІБ). Оскільки, у порівнянні з іншими роботами в області ІБ тестування на проникнення є досить недорогим видом послуг, найчастіше можна провести його за рахунок бюджету підрозділу. У другому випадку роботи проводяться або після впровадження комплексу засобів захисту (КЗЗ), або перед переведенням якої-небудь системи в промислову експлуатацію. У цьому випадку результати тестування дозволяють реально оцінити залишкові ризики, а можливо й виявити приховані недоліки в системі. Типовими прикладами подібних робіт є тести із використанням (Додаток Д):

1) методів соцінженерії для виявлення рівня поінформованості користувачів;

2) технічних засобів шляхом "злому", наприклад, нового WEB-Інтерфейсу.

При плануванні тестування на проникнення необхідно визначити межі й режим проведення тесту. Роботи можуть проводитися з повідомленням персоналу (системних і мережних адміністраторів) або без нього. Якщо користувачі і адміністратори не знають про "злом", що готується – керівництво одержить можливість оцінити ефективність використовуваних механізмів виявлення й розслідування комп'ютерних інцидентів та підвищення поінформованості в області ІБ. З іншого боку, "прихований" тест підвищує ймовірність виникнення відмови в результаті помилки експерта або не зовсім коректного настроювання серверів і мережного встаткування. Тому часто залежно від вибору мережі, з якої здійснюється проникнення в систему тести класифікуються на:

зовнішні – моделюються дії зловмисника, що здійснює проникнення в інформаційну систему клієнта з мережі Інтернет;

внутрішні – моделюється поводження інсайдера (зловмисника, що якимось чином одержав доступ до внутрішньої мережі компанії й намагається через неї проникнути до інформаційної системи).

При цьому аудиторами використовуються методи так званих «чорного» і «білого» ящиків. Метою методу «Чорного ящика» (Black box test) є оцінювання захищеності інформаційних ресурсів (IP) організації, які можна одержати з мережі Інтернет. Використання цього методу характерно при проведенні зовнішнього тесту на проникнення. У цьому випадку моделюються дії зловмисника, що володіє тільки загальнодоступними відомостями про компанію (доменні імена, зовнішні IP-адреси тощо). Метою методу «Білого ящика» (White box test) є оцінювання захищеності IP організації, доступ до яких можна одержати із внутрішньої мережі. Метод припускає моделювання дій інсайдера, що заволодів певними відкритими або закритими інформаційними ресурсами такими як, наприклад, структура мережі компанії, результати щоквартального сканування уразливостей, результати попередніх тестів на проникнення тощо.

Найбільш близьким до реальних дій зловмисників є так званий ***комплексний тест на проникнення*** [136–139]. Використовуючи різні технічні й соціоінженерні методи (табл. 5.1), аудитори в ході його проведення намагатимуться обійти існуючі захисні механізми з метою виконання поставлених Замовником завдань (підвищення привілеїв, одержання доступу до конфіденційної інформації, модифікація даних із СУБД тощо).

Таблиця 5.1

Алгоритм дій при використанні технічних і соціоінженерних методів в ході проведення комплексного тесту на проникнення

Технічні методи	Соціоінженерні методи
1) Одержання попередньої інформації про мережу Замовника. Використовуються ті ж джерела інформації, які доступні зловмисникам (Інтернет, новини, конференції). 2) Складання карти мережі, визначення типів пристроїв, ОС, додатків по реакції на зовнішній вплив. 3) Ідентифікація уразливостей мережних служб і додатків. 4) Аналіз WEB-додатків Замовника. За допомогою автоматизованих утиліт і ручних методів детектується: впровадження операторів SQL (SQL Injection); міжсайтове виконання сценаріїв (Cross-Site Scripting); підміна вмісту (Content Spoofing); виконання команд ОС (OS Commanding); виконання уразливостей, пов'язаних з некоректним настроюванням механізмів аутентифікації й авторизації тощо. 5) Експлуатація уразливостей. Методи та інструментарій вибираються індивідуально для кожного типу уразливості. Можуть бути використані як загальнодоступні утиліти, так і інструментарій власної розробки. 7) За узгодженням із Замовником можуть проводитися базові роботи з контролю захищеності бездротових мереж. 8) За узгодженням із Замовником може бути проведена перевірка стійкості зовнішнього периметра й відкритих ресурсів на атаки типу відмови в обслуговуванні. При цьому оцінюється ступінь стійкості мережних елементів і можливий збиток при проведенні найбільш імовірних сценаріїв таких атак. 9) Перевірка стійкості мережі до атак на канальному рівні. Проводиться моделювання атак на протоколи канального рівня STP, VTP, CDP, ARP. 10) Аналіз мережного трафіка. У випадку проведення робіт у мережі Замовника або при одержанні такої можливості в ході експлуатації уразливостей проводиться аналіз мережного трафіка з метою одержання, наприклад, паролів користувачів, конфіденційних документів тощо. 11) Перевірка стійкості маршрутизації. Проводиться моделювання маршрутів і проведення атаки типу відмови в обслуговуванні проти використовуваних протоколів маршрутизації. 12) Перевірка можливості одержання зловмисником несанкціонованого доступу до конфіденційної інформації або інформації обмеженого доступу Замовника. Проводиться шляхом перевірки прав доступу до різних IP Замовника із привілеями, отриманими на різних етапах тестування. 13) Отримана в ході аналізу уразливостей і спроб їхньої експлуатації інформація документується й аналізується для вироблення рекомендацій з поліпшення захищеності мережі.	1) Із Замовником узгоджуються методи соціальної інженерії, які будуть використані при проведенні тесту. Серед них можуть бути такі, як: - розсилання поштових/ІМ повідомлень від імені анонімних користувачів і співробітників Замовника, що містять посилання на Web-ресурси з виконуваним кодом, що містять виконуваний код у тілі листа, що містять прохання змінити паролі, переслати паролі або свою персональну інформацію та ін.; - вибіркова перевірка виконання політики "чистого стола" (стікери з паролями; незаблоковані під час відсутності користувача консолі; наявність конфіденційних документів в офісі, доступних відвідувачам; залишені без догляду стільникові телефони й КПК та ін.); - дзвінки користувачам від імені ІТ персоналу і персоналу служби ІБ із проханнями одержання/зміни пароля, пересилання конфіденційних документів та ін. 2) Вибір цільових груп користувачів і визначення методів тестування для кожної із груп. 3) Проведення тесту: розсилання поштових повідомлень, дзвінки користувачам, виїзд в офіс Замовника для проведення дослідження. 4) Використання отриманих у результаті попередніх етапів привілеїв для одержання несанкціонованого доступу до ресурсів Замовника (див. Технічні методи).
Аналіз і консолідація результатів різних тестів.	

Всі спроби проникнення повинні контролюватися обома сторонами – як зломщиком, так і "клієнтом". Це допоможе протестувати систему набагато ефективніше. При цьому особа, яка проводить тести, повинна відповідати таким вимогам:

мати гарні технічні знання;

бути дружелюбною й легко розташовувати до себе;

викликати симпатію у керівництва та співробітників.

Окрім цього вона повинна мати таке ж положення, як і в потенційного зловмисника: у її розпорядженні повинні бути час, терпіння й максимальна кількість технічних засобів, які можуть бути використані зломщиком.

Залежно від поточних потреб і завдань клієнта можуть бути запропоновані три різних рівні тестування на проникнення (таблиця 5.2), які відрізняються глибиною і складністю виконуваних перевірок.

Таблиця 5.2

Рівні тестування на проникнення

Рівень 1	Рівень 2	Рівень 3
Автоматизована перевірка рівня захищеності інформаційних ресурсів проти атак з боку шкідливого коду (хробаків) і зловмисників, які мають невисоку кваліфікацію (напр. початківців хакерів). Наявність уразливостей, виявлених на цьому рівні тестування, свідчитиме про високу ймовірність реалізації загроз відносно IP незалежно від його важливості й типу оброблюваної інформації.	Автоматизована перевірка захищеності IP проти цілеспрямованих атак зловмисників, які мають високу кваліфікацію і мотивацію. Наявність уразливостей, виявлених на даному рівні тестування, свідчитиме про наявність потенційних ризиків відносно IC та IP , що обробляють конфіденційну інформацію або надають важливі сервіси, які можуть бути використані зловмисниками в корисливих цілях.	Автоматизована перевірка захищеності IP проти цілеспрямованих атак з боку внутрішніх або добре підготовлених зовнішніх зловмисників, що володіють додатковими інсайдерськими даними про тестовану систему або додаток. До таких даних може бути віднесена інформація про конфігурацію системи, облікові записи користувачів і адміністраторів, вихідний код додатків, внутрішні регламенти, процедури тощо.

Блок-схема алгоритму цього процесу наведена на рис. 5.1.

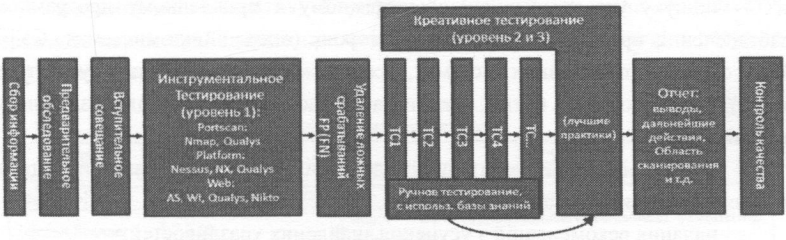


Рис. 5.1. Блок-схема алгоритму реалізації тесту на проникнення

Тестування 1-го рівня виконується з використанням спеціальних програмних засобів (сканерів уразливостей, типових наборів експлойтів і т.п.). Тестування 2-го й 3-го рівнів виконується вручну й дозволяє виявити уразливості, які не можуть бути знайдені в ході тестування 1-го рівня. На цьому етапі можуть бути виявлені, у тому числі, 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 й порівнює їх з

результатами тестування 1-го рівня. Також має бути проведений аналіз пропущених уразливостей (FalseNegatives, FN) – тобто уразливостей, які помилково не були знайдені. Після їх виявлення вибірково, за домовленістю із Клієнтом, мають бути проведені заходи з їх експлуатації (для того, щоб продемонструвати клієнтові можливі наслідки). Окремо повинно бути обговорено процедуру виконання атак, які можуть істотно вплинути на функціонування систем і процесів Замовника, наприклад, DoS атак.

Результатом роботи має бути звіт, що містить:

методику проведення тесту;

висновки для керівництва, що містять загальну оцінку рівня захищеності;

опис виявлених недоліків СУІБ;

опис ходу тестування з інформацією про усі виявлені уразливості та результати їхньої експлуатації;

рекомендації з усунення виявлених уразливостей.

Логічним продовженням тесту на проникнення можуть бути роботи з побудови комплексної системи управління рівнем захищеності, проведення моніторингу захищеності периметра корпоративної мережі, розробки програми підвищення поінформованості в області ІБ та впровадження системи управління ІБ.

Комплексна система управління рівнем захищеності повинна вирішувати завдання з:

пошуку уразливих місць у системному й прикладному програмному забезпеченні, програмно-апаратних пристроях (операційних системах, СУБД, WEB серверах, прикладних системах, міжмережевих екранах, маршрутизаторах тощо), які можуть бути використані зловмисниками для здійснення несанкціонованої діяльності;

оцінювання рівня критичності ідентифікованих уразливостей, а також можливості їх експлуатації;

надання рекомендацій з усунення знайдених уразливостей;

формування трендів, що показують зміни в стані захищеності протягом часу й дозволяють персоналу, відповідальному за забезпечення ІБ Замовника, вживати превентивні дії.

Побудова такої системи дозволить:

підвищити рівень захищеності інформаційних систем компанії;

знизити кількість інцидентів порушення інформаційної безпеки;

підвищити ефективність діяльності служби ІБ і її взаємодії зі службою ІТ;

одержати об'єктивну картину рівня захищеності як у рамках окремих підрозділів, так і організації в цілому.

У ході ***моніторингу захищеності периметра корпоративної мережі*** мають бути реалізовані заходи щодо:

детального дослідження існуючого периметра корпоративної мережі та організації його захисту (формується звіт по виявлених уразливих і проблемних областях і рекомендації з їхнього усунення. У процесі усунення уразливостей проводиться консультування фахівців Замовника);

формування графіку проведення моніторингу та політики для системи управління рівнем захищеності, основою якої може бути, наприклад, один із провідних сканерів уразливостей наведених у табл. 5.3 [135];

визначення контактних осіб з боку Замовника, яким будуть надсилатися звіти (визначаються особи, з якими необхідно підтримувати оперативний зв'язок при виявленні висококритичних уразливостей);

фіксації стану периметра мережі (за узгодженням із Замовником);

проведення щоденного моніторингу інформації про уразливості мережних служб Замовника доступних з мережі Інтернет;

періодичного сканування мережного периметра відповідно до встановленого графіку (при виявленні змін мережного периметра – нових вузлів, нових мережних служб, проводиться аналіз цих змін з погляду безпеки);

проведення консультацій фахівців Замовника на предмет серйозності виявлених уразливостей і способів їхнього усунення;

внесення змін в політику й графік моніторингу при змінах в архітектурі мережного периметра, а також при зміні функціональних призначень ресурсів і конфігурації засобів захисту.

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

Результати порівняльного аналізу мережних сканерів наведені у таблиці 5.4.

Лідируючі позиції за всіма критеріями даного порівняння займає сканер MaxPatrol. Це пояснюються насамперед якісною ідентифікацією цим сканером сервісів і додатків. Друга причина успіху обумовлюється повнотою бази та її адекватністю поставленому завданню й взагалі "сьогоднішньому дню". Третя

причина – якісний аналіз версій додатків з урахуванням операційних систем, дистрибутивів і різних "відгалужень". Нарешті, можна ще додати, що 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 моментів був навіть точніше сканера MaxPatrol. Головна причина відставання Nessus – це пропуски уразливостей, але не через відсутність перевірки в базі, як у більшості інших сканерів, а в силу особливостей реалізації. По-перше (і цим обумовлена значна частина пропусків), у сканері Nessus намітилася тенденція розвитку убік "локальних" або системних перевірок, що припускають підключення з обліковим записом. По-друге, у сканері Nessus враховано менше (у порівнянні з MaxPatrol) джерел інформації про уразливості. Це чимсь схоже на сканер SSS, заснований більшою мірою на базі SecurityFocus. Результати інших сканерів з таблиці 4.4 істотно нижче [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
З них викликані необхідністю аутентифікації	0	6	16	36	0	0
З інших причин	7	1	10	56	42	3

Основною метою ***розробки програми поінформованості*** є формування механізму повідомлення вимог ІБ до всіх категорій співробітників компанії й контролю за поінформованістю співробітників. Всі співробітники повинні розуміти свої обов'язки й відповідальність за забезпечення ІБ. У загальному випадку порядок проведення робіт наступний:

визначення областей ІБ, у яких необхідно підвищити поінформованість співробітників;

збір і аналіз діючих у компанії організаційних документів по ІБ, інформація з яких повинна бути доведена до співробітників;

розробка вимог ІБ у тих областях, по яких у Замовника відсутні нормативні документи;

формування програми поінформованості.

Результатом роботи буде звіт "Програма поінформованості співробітників з питань ІБ", що містить: перелік вимог по ІБ, категорії співробітників, для яких призначена програма, порядок реалізації програми й способи доведення й контролю виконання вимог; курси по інформаційній безпеці у форматі Microsoft PowerPoint по різних областях ІБ, контрольний список питань для кожного курсу для контролю засвоєння матеріалу. Можуть створюватися також маркетингові матеріали: листівки, постери, флешроліки, відеоролики тощо.

У ході ***впровадження системи управління ІБ (СУІБ)*** необхідно: визначити відповідальних за забезпечення ІБ і регламентувати взаємодію між ними; формалізувати процеси управління системою захисту; визначити корпоративні норми й правила, яких повинні дотримуватись усі співробітники компанії.

Від цілого ряду загроз ІБ неможливо або вкрай складно забезпечити захист тільки технічними засобами. У першу чергу це стосується внутрішніх загроз, що виходять від співробітників компанії, оскільки близько 80% збитку наносять інциденти, викликані саме ними. У таких ситуаціях, на перший план виходять організаційні заходи. Організаційне забезпечення ІБ повинне являти собою взаємозалежну структуру документів, об'єднаних єдиними принципами, починаючи з концептуальних і закінчуючи детальними документами, орієнтованими на ту або іншу технологію або область діяльності, а саме: концепції ІБ, політики ІБ, інструкцій і регламентів по ІБ та ін. При цьому, наприклад, в «Концепції інформаційної безпеки» повинні бути визначені мета, завдання та принципи забезпечення ІБ, описані об'єкти захисту із вказівкою критичних ресурсів і бізнес-процесів, побудовані моделі загроз і потенційного зловмисника, сформована цільова функціональна архітектура системи забезпечення ІБ й визначені зони відповідальності підрозділів компанії за забезпечення ІБ.

У документі, що визначає загальну політику безпеки, повинні бути включені:

вимоги по аутентифікації;

вимоги по контролю й розмежуванню доступу;

правила надання доступу до ресурсів;

вимоги до обробки інформації, що становить комерційну таємницю й персональних даних;

вимоги по роботі із засобами вилученого доступу, мобільними засобами доступу, електронною поштою, Інтернет, засобами криптографічного захисту;

вимоги по антивірусному захисту, резервному копіюванню та ін.

На відміну від концепції і політик, ***інструкції з ІБ*** зв'язані безпосередньо з конкретними ролями, а ***регламенти по ІБ*** – із процесами. Інструкції розробляються для певних категорій персоналу Замовника (ролей). Вони повинні

містити опис обов'язків, повноважень і відповідальності, які покладають на ту або іншу роль, опис того, як дана роль здійснює взаємодію з іншими ролями. Інструкції можуть бути розроблені, наприклад, для адміністраторів ІБ, аудиторів ІБ, аналітиків ІБ та ін. Окремо, можуть розроблятися розділи по ІБ в інструкції для корпоративних користувачів і співробітників ІТ служби. Регламенти призначені для того, щоб формалізувати процеси, пов'язані із забезпеченням ІБ і визначити ролі, відповідальні за коректну організацію того або іншого процесу. Регламенти можуть бути розроблені для:

процесів резервного копіювання й відновлення;

антивірусного захисту;

випуску, експлуатації й відкликання криптографічних ключів;

управління обліковими записами користувачів;

обробки інцидентів ІБ;

обробки позаштатних/надзвичайних ситуацій та ін.

Таким чином тестування на проникнення, що імітує дії зломщика та моделює зловмисника виходячи з поставлених цілей й, бо того ж виконується досвідченим фахівцем – практично завжди адекватне і результативні. Саме в такому ключі це найбільш ефективний спосіб виявити реальні проблеми інформаційної безпеки в компанії й привернути до них увагу керівництва. Адже про якість захисту набагато краще свідчить демонстрація успішного доступу до інформації, що вважається добре захищеною, або демонстрація повного контролю над особистими комп'ютерами відповідальних співробітників, чим товсті звіти сканерів уразливостей.

5.2 Постановка задачі експертного оцінювання

В ході проведення тестування на проникнення доволі часто постають завдання щодо оцінювання параметрів інформаційно-комунікаційної системи на кожному із його рівнів. При цьому деякі з параметрів можуть бути або безпосередньо виміряні, або ж вирахувані як за відомими аналітичними залежностями, так й шляхом застосування неформальних методів оцінювання, заснованих на оцінках фахівців у відповідній сфері. З останніх найбільш відомими і найбільш застосовуваними нині є методи експертного оцінювання.

Під експертним оцінюванням нині розуміють комплекс взаємозалежних заходів, що визначають мету роботи, умови та способи її організації і проведення, а також права та обов'язки осіб, що залучаються [140]. Воно 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) й здійснюється за певним набором критеріїв, що отримали назву оціночних факторів. Останні у свою чергу поділяються на основні і допоміжні й можуть носити як детермінований (визначаються на підставі суворих детермінованих залежностей), так стохастичний (описуються випадковими величинами з відомим законом розподілу) і невизначений (для кожного з них може бути відома лише область можливих значень) характер. Виходячи з такого *будь-яка задача експертного оцінювання може бути сформульована в такий спосіб*: при заданих значеннях детермінованих $A_1,...,A_i,...,A_p$, невизначених $B_1,...,B_i,...,B_n$ і стохастичних $X_1,...,X_i,...,X_n$ факторів, знайти оптимальне значення $Y_1,...,Y_i,...,Y_m$ з області $Q_{Y_1},...,Q_{Y_i},...,Q_{Y_m}$, тобто *розв'язати певну конфліктну ситуацію, через вихід на нове цілісне бачення об'єкта (процесу) з ширшим колом інтересів* (рис. 5.2).

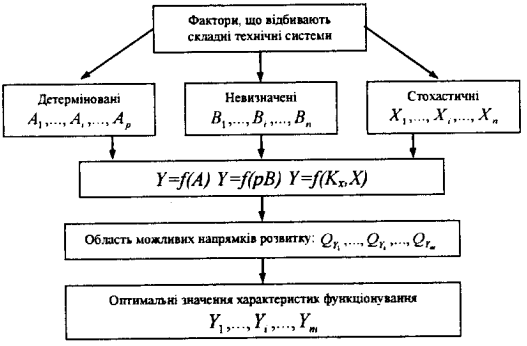


Рис. 5.2. Структурнр-логічна схема проведення експертного оцінювання

Головними етапами реалізації цієї задачі є:

формулювання мети і завдань оцінювання;

формування рішення на організацію і проведення оцінювання та добір складу групи управління;

добір експертної групи та формування опитувальних анкет;

вибір методу одержання експертної інформації та способу її опрацювання;

аналіз матеріалів експертного оцінювання;

інтерпретація отриманих результатів і підготовка висновку для ОПР;

упорядкування звіту.

Етап формулювання мети і завдань експертного оцінювання є основним. Багато в чому він визначається суттю проблеми, що розглядається. Від нього

залежить також надійність і прагматична цінність очікуваного результату. Ступінь реалізації етапу здебільшого обумовлюється:

повнотою наявної вхідної інформації та її надійністю;

термінами і формою подання замовнику отриманих результатів;

можливістю залучення фахівців з інших галузей знань тощо.

Завдання на організацію і проведення експертного оцінювання на другому етапі цього процесу ставить та оформлює у виді рішення Замовник. Цим же рішенням визначається керівник експертизи який, у свою чергу, формує експертну групу управління. На *групу управління* в процесі експертного оцінювання покладається не тільки вся організаційно-планова робота з забезпечення сприятливих умов для ефективної творчої діяльності експертів, але й аналітична робота з добору експертної групи, визначення методів одержання і опрацювання інформації, упорядкування опитувальних анкет, змістовної інтерпретації одержуваних результатів. Для рішення цих задач в групу управління доцільно включити висококваліфікованих комунікабельних фахівців як в області розглядуваної проблеми, так і в інших областях знань – математиці, психології, соціології тощо.

Добір експертної групи і визначення її оптимального кількісного складу є чи не найголовнішим практичним завданням групи управління [141]. При цьому характеристики її членів визначаються на основі індивідуальних характеристик експертів, а саме їх компетентності, креативності, конформізму, відношення до експертизи, конструктивності мислення, колективізму, самокритичності тощо.

При *виборі методу одержання експертної інформації і способу її опрацювання* групою управління розробляється докладний сценарій проведення збору і аналізу експертних думок (оцінок), включаючи як конкретний вид експертної інформації (слова, умовні градації, числа, ранжировки, розбивки або інші види об'єктів нечислової природи) так і конкретні методи аналізу цієї інформації (обчислення медіани Кемені, статистичний аналіз люсіанів або парних порівнянь та інші методи статистики об'єктів нечислової природи й інших розділів прикладної статистики).

Опрацювання та якісний аналіз експертної інформації є заключним етапом експертного оцінювання. Він полягає у:

проведенні оцінювання ступеня погодженості думок експертів з урахуванням догм погодженості і одномірності;

виділенні груп експертів з близькою думкою (у випадку наявності істотної розбіжності в їхніх відповідях);

виявленні розкиду думок, впливу характеристик експертів на зміст їхніх відповідей;

ранжируванні відповідей в однорідних групах та формуванні об'єднаних відповідей.

При цьому *догма погодженості* передбачає, що рішення може бути прийнято лише на основі погоджених думок експертів. Тому з експертної групи виключають тих, чия думка відрізняється від думки більшості, а саме відсіваються як некваліфіковані особи, що потрапили до складу експертної комісії з непорозуміння або з міркувань, що не мають відносини до їхнього професійного рівня, так і найбільш оригінальні мислителі, які проникнули в проблему набагато глибше, чим більшість. Перевірка погодженості здійснюється на основі коефіцієнтів рангової кореляції Кендалла або Спірмена, які одержали назву коефіцієнтів конкордації. При цьому позитивний результат перевірки погодженості означає ні більше, ні менше, як відхилення статистичної гіпотези про незалежність і рівномірну розподіленість думок експертів на множині всіх ранжировок. *Догма одномірності* відіграє роль у випадку, коли надто важливою є конкретна (вузька) постановка задачі перед експертами. Найчастіше ж така постановка відсутня й "ігри" з розробки узагальненого показника якості, наприклад, у вигляді лінійної функції від перерахованих змінних, не можуть надати об'єктивних висновків. Альтернативою єдиному узагальненому показнику є математичний апарат типу багатокритеріальної оптимізації – множини Парето й т.д. [142].

Етап *інтерпретації отриманих результатів* необхідний для організації зворотного зв'язку у процесі експертного оцінювання. Зворотний зв'язок з експертами група управління може здійснювати або за методом Дельфи, або за іншими методами (методом нарад тощо) з обговоренням результатів анонімних опитувань.

4.2.1 Процедура формування експертної групи

Добір кандидатів до складу експертної групи (колективу) суттєво залежить від характеру і змісту досліджуваної проблеми й може проводитись або шляхом самооцінки кандидатів в експерти, або за результатами їх минулої діяльності, або з урахуванням їх компетентності, або ж за результатами оцінювання кожного кандидата групою. Останній метод є найбільш ефективним. Основним способом його проведення є соціометричне опитування (рис. 5.3). Воно полягає у проведенні низки ітерацій з формування як попереднього, так і остаточного складу експертної

групи й завершується за умови, якщо список експертів перестає поповнюватися новими прізвищами. Процедура добору може бути перервана і раніше, коли буде зафіксовано біля 95% повторень. Як показує практика проведення експертиз, помилка в цьому випадку несуттєва для подальших оцінок.

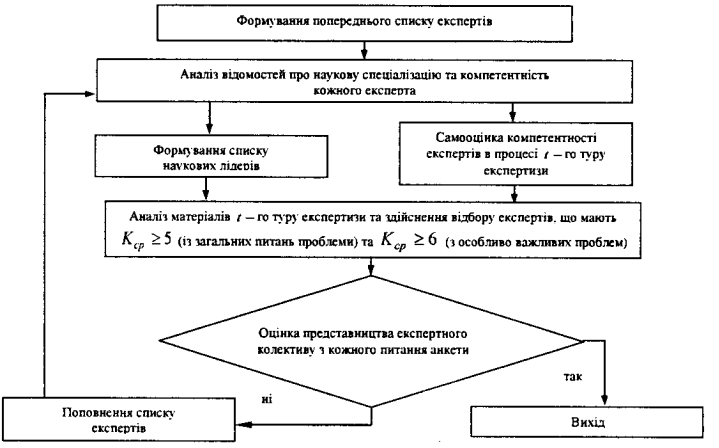


Рис. 5.3. Алгоритм процесу формування експертного колективу

Задача формування експертної групи шляхом соціометричного опитування може бути сформульована таким чином [143–146]. Припустимо, що $EXP = (\exp_1, \ldots, \exp_n)$ – множина можливих кандидатів до експертної групи, H – кількість учасників експертної групи, k_i – ваговий коефіцієнт або інакше степінь компетентності i-го кандидата, p_i – ознака щодо включення ($p_i = 1$), або не включення ($p_i = 0$) i-го кандидата до експертної групи, c_i – вартість послуг i-го кандидата, а C – загальна вартість проведення експертизи. Необхідно за обмежень $\sum_{i=1}^{H} c_i \cdot p_i \leq C$ та $20 \geq H \geq 10$, тобто коли кількість експертів у групі має бути такою, щоб за кожним запитанням анкети було отримано не менш 15–20 оцінок, а кількість експертів з мінімальною компетентністю не повинна перевищувати 25% від загальної чисельності колективу, сформувати експертну групу, яка матиме максимальну компетентність:

$$\sum_{i=1}^{H} k_i \cdot p_i \to \max, \tag{5.1}$$

Така постановка задачі правомірна лише за умови, якщо кандидати до експертної групи за компетентністю якісно однорідні, тобто:

$$W_{zp} = \left(1 - \sigma_{zp}\right) / K_{zp}^{cp} \geq 0.8, \text{ (висока однорідність)} \qquad (5.2)$$

де σ_{zp} – точність оцінювання експертною групою; K_{zp}^{cp} – середнє значення коефіцієнта компетентності H членів експертної групи.

Якщо склад експертної групи за компетентністю неоднорідний, виникає, як правило, принципова помилка, яка для визначення ступеня впливу компетентності кожного окремого експерта на результат експертизи потребує застосування дисперсії σ^2 або середньоквадратового відхилення σ. При цьому чим менше дисперсія (відхилення), тим менше помилка і тим вище точність оцінювання експерта.

Припустимо, що $\sigma_1, \sigma_2, ..., \sigma_N$ – показники точності оцінювання експертів (середні оцінки), причому для кожного наступного експерта вони зменшуються рівномірно (тобто рівномірно у l разів збільшується відхилення). Тоді показник точності групового оцінювання може бути обчислений з виразу:

$$\sigma_{zp} = \frac{1}{H}\sqrt{\sum_{i=1}^{H}\sigma_i^2}. \qquad (5.3)$$

Зважаючи, що всі експерти мають різну компетентність, упорядкуємо їх за цією ознакою $\sigma_1 < \sigma_2 < ... < \sigma_H$ та, як результат, отримаємо:

$\sigma_1;\ \ \sigma_2 = l \cdot \sigma_1;\ \ \sigma_3 = l \cdot \sigma_2;\ \ ....;\ \ \sigma_H = l \cdot \sigma_{H-1}$ або

$\sigma_1;\ \ \sigma_2 = l \cdot \sigma_1;\ \ \sigma_3 = l^2 \cdot \sigma_1;\ \ ....;\ \ \sigma_H = l^{H-1} \cdot \sigma_1$.

Відповідно до формули (3.3)

$$\sigma_{1-N} = \frac{1}{H}\sqrt{\sum_{i=1}^{H}\sigma_i^2} = \frac{1}{H}\sqrt{\sum_{i=1}^{H}\left(l^{i-1}\sigma_1\right)^2} = \frac{1}{H}\sqrt{\sum_{i=1}^{H}\left(l^{i-1}\right)^2\sigma_i^2} = \frac{\sigma_1}{H}\sqrt{\sum_{i=1}^{H}\left(l^2\right)^{i-1}}. \qquad (5.4)$$

Розглянемо, як поводиться графік залежності σ_{1-H} від H при різних значеннях l. Збільшення кількості експертів, починаючи з деякого моменту (рис. 5.4), призводить до росту помилки експертизи.

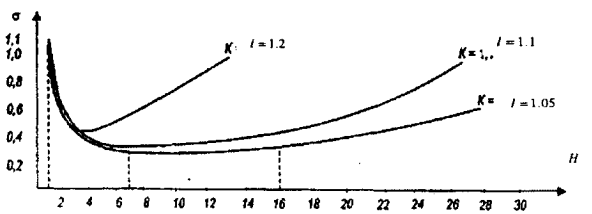


Рис. 5.4. Залежність середньої похибки σ від кількості членів експертної групи H.

Як видно з графіків, найвища точність оцінювання досягається за умови присутності у експертній групі лише одного кандидата. Якщо таких у групі більше одного 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 – $m_в = 16$). При подальшому збільшенні кількості членів експертної групи помилка експертизи буде збільшуватися. Якщо точність оцінок кожного наступного члена експертної групи відрізняється від попереднього на 10% ($l = 1.1$), то мінімум досягається при 7 експертах (нижня межа – $m_н = 7$).

Таким чином можна констатувати, що з урахуванням компетентності експертів, в експертну групу доцільно включати не більш 10–15 найбільш компетентних серед них. Разом з цим слід мати на увазі, що відповідно до масштабу експертного оцінювання кількість експертних груп, які притягаються до роботи, може коливатися від 1–2, наприклад, при прогнозуванні конкретних науково-технічних проблем до декількох десятків – при прогнозуванні комплексних галузевих проблем.

5.2.2 Методи оцінювання компетентності представників експертної групи

Компетентність експерта є ступенем його кваліфікації у певній галузі знань. Вона визначається за допомогою аналізу його професійної підготовки (посада, вчене звання, ступінь), професійної діяльності та широти кругозору щодо перспектив розвитку досліджуваної проблеми. Компетентність експерта повинна поширюватися як на об'єкт оцінювання якості (професійна компетентність), так і на методологію оцінювання (кваліметрична компетентність). Професійна компетентність припускає знання історії досліджуваної проблеми. Кваліметрична компетентність забезпечує чітке розуміння експертом методів оцінки, уміння користуватися різними типами оцінюючих шкал, розрізняючи при цьому досить велику кількість їх градацій.

Нині при оцінюванні професійної компетентності експерта користуються, як правило, методами самооцінки [146], взаємної оцінки [147] та контрольних експертиз [148]. *У першому випадку індивідуальну компетентність експерта оцінюють* коефіцієнтом $k(0 \le k \le 1)$, який експерт визначає на основі власних суджень про ступінь своєї інформованості з проблеми, що розглядається ($k_н$), а також ступінь аргументації власних думок ($k_а$) [141]:

$$k = 0.5(k_н + k_а). \qquad (5.5)$$

Коефіцієнт інформованості одержують на основі самооцінки експерта за десятибальною шкалою, як

$$k_u = 0.1 \cdot X_{інф}, \tag{5.6}$$

де $X_{інф}$ – бал, виставлений експертом.

При цьому на підставі аналізу літератури [144–149] для оцінювання ступеню інформативності експертів можна рекомендувати наступну 10-бальну шкалу:

$X_{інф} = 0$ – не знає даної проблеми (питання);

$0 < X_{інф} \le 2$ – слабко знає проблему, цікавиться нею не систематично;

$2 < X_{інф} \le 4$ – задовільно знає проблему, займається нею несистематично;

$4 < X_{інф} \le 6$ – добре знає проблему по попередньому досвіду роботи; зараз, можливо, не працює в даній галузі, але систематично нею цікавиться;

$6 < X_{інф} \le 8$ – добре знає проблему, постійно працює над нею і має опубліковані праці в даній галузі;

$8 < X_{інф} < 10$ – відмінно знає проблему, має в її рішенні загальновизнані результати і є одним з вітчизняних лідерів (авторитетом) у її розробці;

$X_{інф} = 10$ – міжнародний авторитет у певній галузі.

Значення коефіцієнта k_a визначають як функцію, що залежить від коефіцієнта довіри $k_o = k' \cdot k''$ та коефіцієнта відповідності $k_в$:

$$k_a = F(k_o, k_в), \tag{5.7}$$

У певному випадку функція F може являти собою середньоарифметичне величин $k_в$ і $k_в$. При цьому значення коефіцієнтів k', k'' приймаються рівними 1 або 0,5 і можуть бути визначені з таблиці 5.5, а значення коефіцієнта відповідності $k_в$ – з таблиці 5.6.

Таблиця 5.5

Числові значення складових k', k'' коефіцієнта довіри

	Рівень спеціалізації експерта	
Рівень обговорення проблеми	$k' = 1$	$k' = 0{,}5$
	$k' = 0{,}5$	$k' = 1$

Галузь безпосередньої роботи $k' = 1$

Суміжна галузь $k' = 0{,}5$

Таблиця 5.6

Еталонні значення оцінки коефіцієнта відповідності

Джерела аргументації	Ступінь впливу джерела на Вашу думку		
	В (висока)	С (середня)	Н (низька)
Проведений Вами теоретичний аналіз	0,3	0,2	0,1
Ваш виробничий досвід	0,5	0,4	0,2
Узагальнення робіт вітчизняних авторів	0,05	0,05	0,05
Узагальнення робіт закордонних авторів	0,05	0,05	0,05
Ваше особисте знайомство зі станом справ за кордоном	0,05	0,05	0,05
Ваша інтуїція	0,05	0,05	0,05
	max 1	max 0.8	max 0.5

Оцінюючи певне джерело за градаціями В, С та Н та користуючись еталонними значеннями таблиці 5.6 експерт у пустих клітинках такої таблиці проставляє власні значення. Їх підсумовування за кожним стовпчиком надасть, як результат, значення коефіцієнта k_a. При цьому саме інтервальний характер пропонованих шкал дозволить помітно підвищити їх розрізнювальну здатність та надасть достатню значеннєву визначеність не тільки при доборі експертів, але і при аналізі компетентності експертної групи (колективу) в цілому.

Другий метод полягає в обчисленні індивідуальних коефіцієнтів компетентності на основі матриць, що складені експертами за результатами взаємного оцінювання. Він використовується за умови, якщо кандидати знають один одного за спільною діяльністю й полягає в оцінюванні кожним з них обсягу та якості знань інших кандидатів з питань анкети. При складанні анкет за цим методом необхідно заздалегідь виявляти можливі цілі експертів, що суперечать меті експертизи, тобто виключати ті причини, що можуть спонукати експерта свідомо спотворювати оцінки знань інших кандидатів. Однією з ефективних модифікацій методу взаємного оцінювання є процедура, що ґрунтується на такій послідовності кроків.

Крок 1. Члени групи управління висловлюють власну думку щодо залучення кандидатів у групу експертів. Названі особи роблять, у свою чергу, те ж саме. За декілька турів такого опитування складається задовільний за повнотою список кандидатів.

Крок 2. За результатами опитування формується матриця суміжності $Z = \|z_{ij}\|, \quad i = \overline{1,n}, \quad j = \overline{1,n}$, елементами якої є одиниці або нулі залежно від того, чи висловився кандидат з номером i на користь залучення в групу кандидата з номером j або ні відповідно (i – номер рядка матриці суміжності, j – номер стовпця).

Крок 3. За матрицею суміжності $Z = \|z_{ij}\|, \quad i = \overline{1,n}, \quad j = \overline{1,n}$ обчислюються

коефіцієнти компетентності кандидатів γ_i. Сутність алгоритму знаходження значень γ_i полягає в тому, що на першій ітерації $(t=1)$ група управління підраховує відношення суми голосів, поданих за кандидата з номером γ, до загальної кількості всіх голосів (сума одиниць у матриці суміжності). На наступних ітераціях $(t>1)$ голоси зважуються коефіцієнтами компетентності кандидатів у $\gamma_i^{(t-1)}$, обчисленими на попередній ітерації. Для цього:

1) задається критерій зупинки і необхідна точність ε обчислення $\gamma_i = \overline{1,n}$. Значення аргументу ε вибирають на один-два порядки менше розміру $\frac{1}{n}$. Іноді як критерій зупинки використовують умову $t = t_{mp}$. При цьому t_{mp} вибирають в діапазоні 3–5, що обумовлено швидкою збіжністю процесу;

2) покладається, що $t=0$ і усі $\gamma_i^{(t)} = \frac{1}{n}$, $i = \overline{1,n}$;

3) покладається $t = t+1$ та обчислюється: $\gamma_j^{(t)} = \frac{\sum_{i=1}^{n} x_{ij}\gamma_i^{(t-1)}}{\sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij}\gamma_i^{(t-1)}}, j = 1...n;$ (5.8)

4) перевіряється умова $\left|\gamma_i^{(t)} - \gamma_i^{(t-1)}\right| \le \varepsilon, i = \overline{1,n}$. Якщо вона виконується, то здійснюється перехід до п. 5, інакше – до п. 3;

5) обчислення припиняється. Отримані $\gamma_i^{(t)}$ приймають за коефіцієнти компетентності γ_i.

Викладена процедура дозволяє не тільки оцінити компетентність уже відібраних кандидатів, але й одночасно виявити можливо повну множину фахівців із розглянутої проблеми та сформувати їх список.

Третій метод оцінювання індивідуальної компетентності кандидатів полягає у перевірці достовірності (надійності) суджень кожного з них у ході проведення контрольних експертиз. Контрольна експертиза передбачає опитування експертів за питаннями, яким можна присвоїти позитивний числовий еквівалент w_i, $i = \overline{1,N}$ в межах заданої шкали такий, що:

$$0 \le w_i \le 1, \sum_{i=1}^{N} w_i = 1,$$

де N – загальна кількість поставлених запитань;

w_i – коефіцієнти відносної важливості (характеризують у скільки разів запитання важливіші одне за інше).

Керівникам опитування можуть бути заздалегідь відомі достовірні відповіді на

такі запитання, які при цьому повинні бути абсолютно невідомими учасникам опитування. За таких умов коефіцієнт достовірності суджень кожного експерта визначається як відношення кількості запитань, на які експерт дав правильні відповіді, до їх загальної кількості:

$$\gamma_i^{[Д]} = \frac{N_{П_i}}{N}, i = \overline{1,n} \tag{5.9}$$

де $N_{П_i}$ – кількість правильних відповідей i-го експерта.

Якщо достовірні відповіді на поставлені запитання невідомі, для оцінювання компетентності експертів може бути використаний підхід, заснований на опрацюванні нормованих бальних оцінок. Він припускає, що спочатку всі експерти мають рівну компетентність. Як вагові коефіцієнти за таких обставин використовують значення середньозважених оцінок усіх запитань, які нормуються їхньою сумою і використовуються як уточнені значення коефіцієнтів компетентності. Результатом такої операції є те, що для експерта, оцінки котрого ближче до середньозважених, коефіцієнт його компетентності збільшується. Така процедура в ході контрольних експертиз може повторюватися неодноразово.

Наступним кроком є математична обробка оцінок індивідуальної компетентності експертів, результатом якої є остаточне уточнення складу експертної групи для забезпечення мінімального розкиду компетентності. Експерт, що одержав максимальний коефіцієнт компетентності, визначається як *Головний Експерт*. Він виступає далі як *Особа, яка уповноважена приймати рішення (ОПР)* й саме на яку покладається вибір раціонального рішення серед 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, які можуть бути виражені таблично або у балах відносної важливості j-го параметра i-м експертом (c_{ij}) за будь-якою шкалою, або у виді рангових оцінок (r_{ij}).

У першому випадку частіш за все використовуються 100-бальні або 10-бальні шкали, де максимально можливому ступеню важливості відповідає оцінка у 100 або у 10 балів відповідно. 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 m експертів, що прийняли участь в оцінюванні, за кожним j-м параметром з n можливих, найчастіше використовуються:

по-перше, середнє арифметичне значення оцінок за j-м параметром:

$$\overline{C_j} = \frac{1}{m_j} \cdot \sum_{i=1}^{m_j} C_{ij}, \quad (j = \overline{1,n}), \tag{5.10}$$

яке може змінюватись в інтервалі:

$0 \le \overline{C_j} \le 100$, якщо прийнята 100-бальна шкала оцінок;

$0 \le \overline{C_j} \le 10$, якщо прийнята 10-бальна шкала оцінок;

по-друге, сума рангів оцінок, отриманих j-м параметром:

$$R_j = \sum_{i=1}^{m_j} r_{ij}, \ (j = \overline{1,n}). \tag{5.11}$$

Значення R_j визначається для кожного з параметрів і змінюється в інтервалі від 1 (одиниці) до n. При цьому, як правило, найбільш важливому параметру (має максимальний бал) приписується порядковий номер, що дорівнює одиниці, а найменш важливому – номер n. Чим менше значення R_j, тим значимішим (більш важливим) є досліджуваний параметр;

по-третє, частота максимальних оцінок в балах або присудження експертами першого рангового місця j-му параметру:

$$K_j = m_j^{'} / m_j, \tag{5.12}$$

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,

являють 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.д., а також провести тестування системи безпеки, на проникнення результати якого у свою чергу й повинні забезпечити компанії захист від стороннього кібернетичного впливу. При цьому доцільно:

не покладатися на систему внутрішньої ідентифікації;

реалізувати систему перевірки за допомогою зустрічного дзвінка, коли повідомляєте захищену інформацію;

реалізувати програму навчання користувачів в області безпеки;

призначити відповідальних за технічну підтримку;

створити систему оповіщення про загрози та ін.

Основні кроки посилення соціотехнічної безпеки можуть полягати в залученні уваги співробітників компанії до питань безпеки, усвідомленні ними всієї серйозності проблеми формування політики безпеки організації, а також вивченні й впровадженні необхідних методів і дій для підвищення захисту інформаційного забезпечення.

5.3 Одержання вихідної інформації евристичного походження. Основні переваги та недоліки індивідуальних і колективних методів

Методи одержання експертної інформації поділяються на **методи індивідуального** і **колективного** експертного оцінювання. Загальний алгоритм опрацювання інформації евристичного походження наведений на рис.5.5. У групі методів **індивідуального експертного оцінювання** найбільшого практичного застосування отримали морфологічний метод (метод морфологічного аналізу), метод сценаріїв підгрунтям для якого є методи згортання і розгортання проблем, а також методи інтерв'ю та аналітичних доповідних записок [149, 150]. *Морфологічний метод*, уперше запропонований Ф. Цвіккі, дозволяє вирішувати великомасштабні проблеми на кшталт конструкторських задач загального плану. Достатньо ефективним він є при проектуванні об'єктів і пошуку системних рішень. Метод заснований на комбінаториці – систематичному дослідженні всіх теоретично можливих варіантів рішення, що випливають із закономірностей побудови об'єкту, який аналізується. Його робочі процедури зводяться до:

точного 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 вирішення певної проблеми;

побудови морфологічної "множини" або інакше морфологічної двомірної або тривимірної матриці виду:

$$\begin{matrix} p_1^1 & p_1^2 & \dots & p_1^{k_1} \\ p_2^1 & p_2^2 & \dots & p_2^{k_2} \\ \dots & \dots & \dots & \\ p_n^1 & p_n^2 & \dots & p_n^{k_n} \end{matrix}; \qquad (5.13)$$

аналізу отриманих варіантів рішень та вибору відносно кращого серед них на підставі індивідуальних оціночних критеріїв.

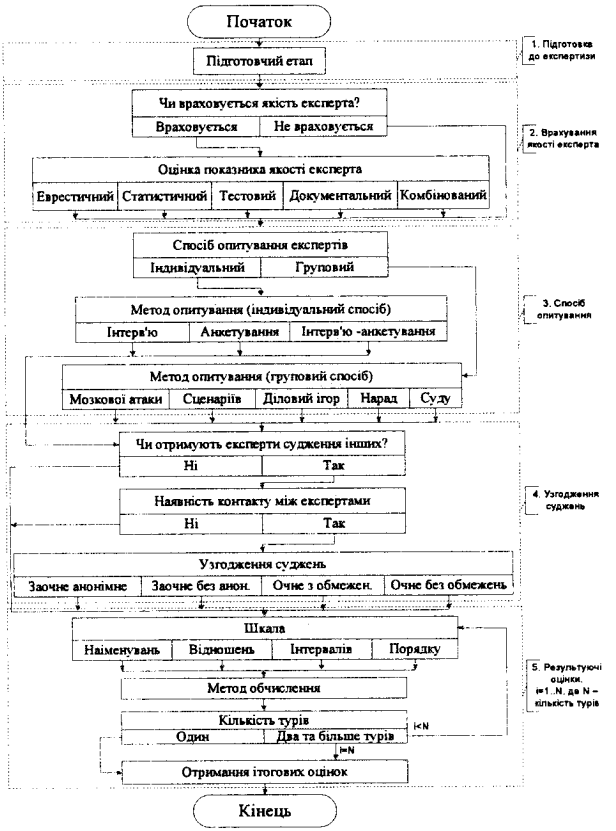


Рис. 5.5. Алгоритм опрацювання інформації евристичного походження

Недоліками методу є відносна трудомісткість (необхідність перегляду варіантів) та відсутність надійного методу оцінювання ефективності застосування того чи іншого варіанту.

Метод сценаріїв є напіваналітичним методом, який застосовується для створення штучних ситуацій (сценаріїв) у тому випадку, коли реальні факти відсутні, наприклад, при визначенні цілі і виходів операції, в ході вибору показників і критеріїв ефективності тощо. При цьому під сценарієм розуміють логічний і правдоподібний опис подій з встановленням орієнтованого часу щодо їх здійснення і зв'язків, в результаті яких ці події можуть відбутися. Він складається з метою уточнення умов, за яких буде вирішуватися проблема і разом з тим стимулює та дисциплінує мислення експерта (групи експертів), заставляє його (їх) враховувати деталі і динаміку, висвітлювати взаємозв'язок багатьох факторів, наглядно у спрощеному виді представляти складну багатоваріантну дійсність. Особлива увага при розробці сценаріїв приділяється "критичним" точкам, після яких події можуть розвиватися в різних напрямках.

Метод сценаріїв, як правило, базується на аналізі результатів, що отримані за допомогою методів *"розгортання" ("згортання")* проблем. Ідея першого з них – методу *"розгортання" проблем*, полягає у послідовному поділі проблем певного рівня на підпроблеми, що складають елементи наступного рівня. В результаті цього формується "розгортка" підпроблем. При цьому досить важливо, щоб дотримувався причинно-наслідковий зв'язок, тобто проблеми нижчих рівнів обумовлювалися проблемами верхніх рівнів. Це досягається багатоетапним цілеспрямованим експертним опитуванням аж до повного узгодження суджень усіх експертів. Ідея другого з них – методу *"згортання" проблем*, полягає в послідовному зведенні проблем нижчих рівнів до проблем більш високих рівнів. В результаті застосування методу формується проблема, вирішення якої необхідно в майбутньому. За результатами методів *"розгортання" ("згортання")* проблем, які передбачають залучення груп експертів і носять ітеративний характер, обирається один опорний сценарій або їх мінімально можлива кількість.

Методи інтерв'ю та *аналітичних доповідних записок* використовують у задачах формування вихідної множини стратегій, задачах аналізу невизначеностей. При цьому перший з них полягає в опитуванні експерта за заздалегідь сформульованими питаннями, на які експерт дає відповіді експромтом, а другий припускає тривалу і ретельну самостійну роботу експерта над аналізом тенденцій розвитку, оцінкою поточного стану і шляхів розвитку об'єкта дослідження.

Основні переваги методів індивідуального експертного оцінювання полягають

в їх оперативності, можливості повною мірою використовувати індивідуальні здібності експерта, відсутності тиску авторитетів, низьких витрат на експертизу. Головним недоліком цих методів є високий ступінь суб'єктивності одержуваних оцінок через обмеженість знань одного фахівця.

У групі методів **колективного експертного оцінювання** найбільшого практичного застосування отримали метод мозкової атаки, метод Дельфи, метод аналізу ієрархій, метод анкетування та метод колективної генерації ідей [151]. Головними кроками їх реалізації є (рис. 5.6):

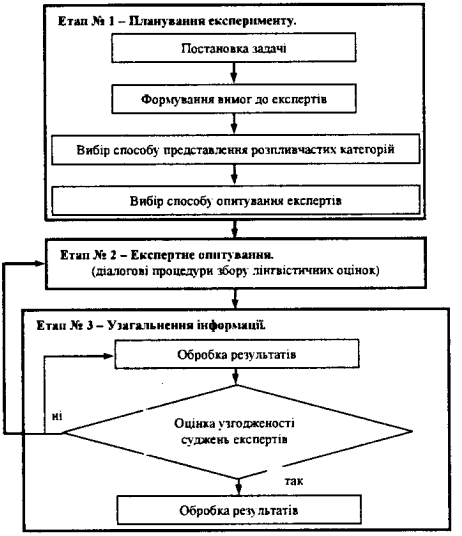


Рис. 5.6 Загальна схема збору та колективної обробки експертної інформації

1) надання організаторами експертизи кожному експертові інформації з проблеми у виді сформульованої мети опитування та анкети, що включає сукупність оцінюваних факторів або подій;

2) вирішення кожним експертом сформульованого завдання незалежно від інших членів експертної групи;

3) проведення організаторами експертизи статистичної обробки анкет, виявленні та узагальнюють аргументів, що відповідають різним судженням;

4) формування організаторами експертизи колективного рішення та ознайомлення з ним членів експертної групи;

5) пояснення членами експертної групи причин незгоди з колективним рішенням та перегляд за згодою власної точки зору.

6) проведення починаючи з 2-го кроку з метою звуження діапазону оцінок експертів 2-го туру експертизи і т.д.

При цьому процедура експертного оцінювання (цикл експертизи) може повторюватися декілька разів (до 3–4), до встановлення певної стабільності у судженнях кожного експерта.

Метод мозкової атаки (Breinstorming) або "мозкового штурму" (винайдений у 1939 р. Осборном, м. Буффало, США) – є одним із методів колективного генерування ідей (пропозицій, гіпотез тощо), заснованим на припущенні, що серед їх розмаїття є хоча б декілька таких, які, принаймні, заслуговують уваги. Метод широко застосовується як у теорії та практиці управління, так і у процесах одержання та використання соціологічної інформації, тобто у ситуаціях коли необхідно: одержати уявлення про напрямки формування (розвитку) певної проблеми; одержати набір варіантів можливих рішень щодо реалізації цих напрямків; виявити коло факторів, доцільних з точки зору вибору раціонального варіанту рішення певного напрямку.

Головними етапами методу є [152]:

1) формування групи управління (з 2–4 членів) та експертної групи (з 10–15 членів);

2) складання групою управління проблемної записки де визначені: мета дослідження та перелік обмежень, пропонованих до варіантів можливих рішень проблеми; масштаб і точність вимірів та оцінок; організаційне, фінансове й матеріально-технічне забезпечення тощо. Вручення проблемної записки особисто кожному члену експертної групи або оголошення її змісту Головним експертом (ОПР) перед усіма членами експертної групи;

3) генерація кожним експертом власних ідей (гіпотез тощо) за певною проблемою. Критика попередніх висловлювань при цьому не допускається, але вітається комбінування та подальший розвиток ідей. Результатом етапу може стати формування списку варіантів можливих рішень проблеми;

4) систематизація (класифікація і групування) групою управління всіх висловлених ідей (пропозицій, гіпотез тощо);

5) аналіз і оцінювання експертною групою усіх висловлених ідей (пропозицій, гіпотез тощо) на практичну реалізованість;

6) систематизація групою управління всіх висловлених зауважень та формування нею списку раціональних ідей (пропозицій, гіпотез тощо).

Основні правила, яких мають дотримуватись члени експертної групи в ході "мозкової атаки" полягають у:

недопущенні озвучення учасниками наради явно помилкових ідей;

недопущенні призупинення на нараді обговорення жодної з ідей, висловлених експертами;

підтримці в ході наради ідей будь-якого роду, навіть якщо їх доречність або реалізованість здаються сумнівними;

наданні однакової підтримки усім учасникам наради, не зважаючи на їх службове становище, вчене звання та досвід роботи.

Не зважаючи на явні переваги методу "мозкової атаки" порівняно з іншими методами колективного експертного оцінювання, йому притаманні й деякі слабкі сторони. Так, наприклад, на судження більшості експертів можуть вплинути висловлювання найбільш авторитетних або активних фахівців, що значною мірою обезцінює заходи, які проводяться. З іншого боку, інколи віддзеркалюється психологічна риса: експерт не намагається виділитися з середи більшості або, висловивши свою точку зору, не намагається її відстояти.

Метод Дельфи (the Delphi method) – метод групового експертного опитування із збереженням анонімності суджень його учасників. Його сутність полягає в тому, що прогнозні оцінки на майбутнє визначаються на підставі висновків учасників опитування, яким доручається аргументоване обґрунтування власної точки зору про стан і розвиток певної проблеми або проблемної ситуації [153]. Метод ґрунтується на припущенні, що визначення майбутнього буде більш точним, якщо в процесі експертного опитування братимуть участь від 20 до 60 осіб ($20 \le X \le 60$), а не одна людина. При цьому узагальнена оцінка експертів повинна мати найменшу дисперсію, а медіанне значення індивідуальних оцінок має наближуватися до фактичного значення прогнозованого показника. Процедура експертного опитування за методом Дельфи зводиться до проведення комплексу операцій, які формують групову думку за окремими предметами обговорення. Для цього групі експертів на підставі переліку показників за темою дослідження [141, 153] пропонують скласти анонімний прогноз у певній галузі знань на близьку і більш віддалену перспективу. Обробка думок членів експертної групи здійснюється з використанням прийомів математичної статистики та евристичних методів (табл. 5.7) [154]. Узгодження їх індивідуальних оцінок забезпечується за рахунок послідовного анонімного ознайомлення кожного експерта з оцінками інших. Зворотній зв'язок, що регламентується у цьому випадку аналітиками, дозволяє виявити переважні судження фахівців та зблизити їхні точки зору на проблему. Він встановлюється у виді повідомлення про середньостатистичний результат обробленої інформації по всій групі експертів на попередніх етапах опитування. З урахуванням цієї інформації кожен експерт корегує власний

прогноз, кінцевим результатом якого знову вважається середній показник, що повідомляється експертам, і весь процес повторюється.

У своєму первісному виді метод Дельфи мав ряд недоліків, обумовлених головним чином організацією опитування (змістом анкети) і суб'єктивними основами самого методу, що відбивають великий вплив поглядів авторів запитань і якості підбора експертів. Головними з них слід вважати:

зниження ваги значення, що додається подіям більш віддаленого майбутнього;

прагнення до пророкувань інтуїтивного характеру і спрощення змісту прогнозу тощо.

Таблиця 5.7

Статистичні й евристичні показники математичної статистики

Вид показника	Формула	Позначення
Статистичні	$\overline{\varphi(i)} = \frac{\sum_{j=1}^{m} \varphi(i)_j}{m}$	$\overline{\varphi(i)}$ - середнє арифметичне значення вагомості i-го показника; $\varphi(i)_j$ - вагомість, зазначена j-м експертом по i-му показнику; m - число експертів
	$\bar{\sigma} = \sqrt{\frac{\sum_{j=1}^{m} [\varphi(i)_j - \overline{\varphi(i)}]^2}{m}}$	$\bar{\sigma}$ - середньо-квадратове відхилення для i-го показника;
	$V = \frac{\bar{\sigma}}{\overline{\varphi(i)}} \cdot 100$	V - коефіцієнт варіації (коефіцієнт мінливості думок експертів) по i-му показнику
Евристичні	$s = \sum_{i=1}^{n} \rho_i$	ρ_i - ранг оцінки вагомості i-го показника (ціле або дробове число);
	$\bar{s} = \frac{s}{n}$	$\bar{s}$ - середнє арифметичне значення суми рангів по всім n показникам
	$d_i = s - \bar{s}$	d_i - відхилення суми рангів від середнього арифметичного значення
	$T_i = \sum_{l=1}^{L} (t_l^3 - t_l)$	T_i - показник зв'язаності рангів; L - кількість груп зв'язаних рангів; t_l - кількість зв'язаних рангів в l - й групі;
	$W = \frac{12 \cdot \sum_{i=1}^{n} d_i^2}{m^2 \cdot (n^3 - n) - m \cdot \sum_{i=1}^{n} T_i}$	W - коефіцієнт конкордації. Основний показник, що характеризує погодженість думок експертів по усіх n показниках
	$\chi_R^2 = \frac{12 \cdot \sum_{i=1}^{n} d_i^2}{m \cdot n \cdot (n+1) - \frac{1}{n-1} \cdot \sum_{i=1}^{n} T_i}$	Фактичне значення критеріальної статистики χ_R^2, яка розподілена по χ^2 при $\vartheta = n - 1$

З метою усунення цих недоліків та знаходження нових галузей застосування в існуючий методичний апарат методу Дельфи останнім часом були впроваджені нові підходи до формування експертних груп, а також

сучасні методи оцінювання міркувань експертів із застосуванням багатомірних шкал і моделювання. Це дозволило підвищити надійність методу, яка вважається відносно високою при прогнозуванні на період як від 1 до 3 років, так і на більш віддалений період часу, а також застосовувати його для:

1) визначення переліку подій, які є найбільш важливими;

2) визначення переліку припущень щодо часу, коли ці події можуть відбутися;

3) визначення переліку припущень про можливості виникнення подій у певний час;

4) визначення переліку припущень про наслідки певних подій у разі їх виникнення;

5) оцінювання бажаності наслідків певних подій у разі їх виникнення;

6) обґрунтування причин існування вкрай протилежних думок на будь-якому етапі процесу прийняття рішення;

7) опису та оцінювання альтернативних подій, які могли б збільшити (зменшити) можливість виникнення бажаних (небажаних) серед них тощо.

Метод аналізу ієрархій (MAI) [141, 143] є системною процедурою для ієрархічного представлення 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 знаходження альтернативних рішень (рис. 5.7). Його основне призначення – підтримка прийняття рішень за допомогою ієрархічної декомпозиції проблеми, що розглядається, на більш прості складові частини та подальше рейтингування обраних альтернатив на основі їх попарного порівняння.

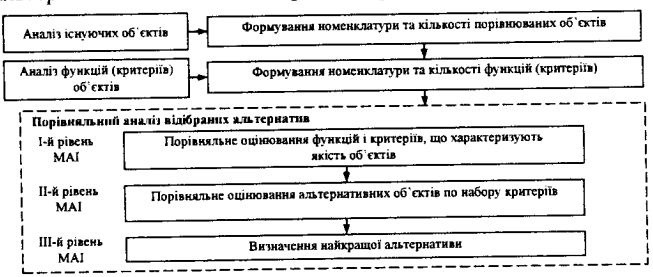


Рис. 5.7. Схема проведення досліджень

В результаті декомпозиції проблеми виділяють мету, наприклад, придбання найкращого програмного засобу (ПЗ) серед сукупності подібних засобів однакового функціонального призначення. Вона відповідає першому рівню ієрархії. Наступний рівень – основні функції, що мають бути реалізовані

цим ПЗ. Після поділу функцій другого рівня може бути сформований третій рівень – це сукупність критеріїв (підфункцій) другого рівня і так далі. Останній рівень створюють альтернативи, тобто варіанти ПЗ, що реалізують вказані дослідником функції та підфункції.

Для оцінювання альтернатив та визначення серед них найважливішої (найбільш раціональної для вирішення конкретного завдання) застосовують метод попарних порівнянь оцінок функцій і критеріїв з точки зору їхнього впливу на ціль та обраних альтернатив між собою за кожним критерієм окремо. При цьому на кожному рівні ієрархії застосовуються власні принципи, а саме:

на першому – принцип ідентичності та декомпозиції;

на другому – принцип дискримінації та порівняльного аналізу;

на третьому – принцип синтезування (табл. 5.8).

Таблиця 5.8

Зміст принципів та етапів МАІ

Рівень ієрархії	Застосовуваний на етапі принцип МАІ	Проведені на етапі операції
1	Принцип ідентичності та декомпозиції	1. Складання і попереднє обґрунтування переліку й числа оціночних показників. 2. Підготовка таблиці вихідних даних (в кількісному або якісному вираженні) для всіх варіантів зразка СТС. 3. Структурування проблеми та її декомпозиція в ієрархію (мережу).
2	Принцип дискримінації та порівняльного аналізу	1. Оцінка кожного варіанту (альтернативи) за обраними критеріями (показниками) і формування матриць попарних порівнянь для рівнів 2 й 3 ієрархії. 2. Проведення експертизи й заповнення попарних порівнянь. Порівняння відбувається у відповідності з вербальною шкалою, враховуючи вплив порівнюваних зразків СТС на загальну для них характеристику. Для визначення альтернативи можуть бути використані судження як одного експерта, так і колективні погляди групи експертів. Емпіричним шляхом встановлено, що найбільш оптимальною в кількісному відношенні є група експертів з 10-15 чоловік. 3. Виявлення найважливішого варіанту (альтернативи)
3	Принцип синтезування	1. Визначення локальних пріоритетів. 2. Оцінка погодженості матриць попарних порівнянь. 3. Визначення глобальних (складових) пріоритетів. 4. Порівняння глобальних пріоритетів СТС й вибір однієї з них для подальшої розробки

Першим етапом використання методу є здійснення експертами парних порівнянь оцінюваних критеріїв. Для цього кожен експерт, користуючись спеціальною вербально-числовою шкалою (табл. 5.9), основна мета застосування якої полягає в тому, щоб забезпечити об'єктивність оцінок, полегшити задачу залучених до експертизи фахівців і забезпечити єдине тлумачення оцінок різними експертами, заповнює матрицю виду:

$$A_l = \left\| \begin{matrix} a_{11}^{(l)}, a_{12}^{(l)}, \cdots, a_{1m}^{(l)} \\ a_{21}^{(l)}, a_{22}^{(l)}, \cdots, a_{2m}^{(l)} \\ \cdots\cdots\cdots \\ a_{11}^{(l)}, a_{12}^{(l)}, \cdots, a_{mm}^{(l)} \end{matrix} \right\|, \; l = \overline{1, n}, \qquad (5.14)$$

де n – кількість експертів; $a_{jk}^{(l)}$ – результат порівняння l-м експертом j-го показника з k-м, $j=\overline{1,m}$, $k=\overline{1,m}$.

Таблиця 5.9

Оціночна шкала відносної важливості (ваг)

Інтенсивність відносної важливості v_{jk}	Визначення	Пояснення
1	Рівна важливість	Рівний внесок двох видів діяльності в обрану мету
3	Помірна перевага одного над іншим	Досвід і судження (експертний аналіз) дають легку 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 дається 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
Зворотні розміри цих чисел	Якщо при порівнянні одного виду діяльності з іншим отримано, наприклад, 3, то результат зворотного порівняння - 1/3.	

Попарне порівняння об'єктів повинне бути виконане за умови – якщо важливість одного об'єкта в порівнянні з іншим дорівнює k (де $k=\overline{1,9}$), то важливість другого об'єкта в порівнянні з першим дорівнює $1/k$ (тобто, має виконуватись властивість зворотної симетричності). При цьому елементи матриць парних порівнянь a_{jk} розглядаються як оцінки відносин w_j і w_k, тобто $a_{jk}=w_j/w_k$, де $w=\{w_1,w_2,...,w_m\}$ – вектор дійсних шуканих коефіцієнтів відносної важливості (ВВ) показників, оцінка коефіцієнтів яких зводиться до розрахунку за формулою: $w_i=1/a_{ki}$, де $i=\overline{1,m}$.

Наступним кроком в обчисленнях є нормалізація отриманої таким чином колонки чисел шляхом ділення кожного з них на їх загальну суму:

$$c_i=a_i\Big/\sum_{i=1}^{m}a_i, \tag{5.15}$$

де c_i – нормалізована компонента власного вектора сформованої матриці по рядку i.

Оскільки на першому рівні ієрархії завжди знаходиться один елемент (фокус проблеми), що передбачено методичними положеннями MAI, то матриця попарних порівнянь для елементів другого рівня теж буде одна. Як наслідок, її нормований власний вектор $C(c_1,c_2,...,c_m)$ і буде вектором пріоритетів другого рівня ієрархії.

Для визначення пріоритетів окремих компонент інших рівнів ієрархічної структури досліджуваного процесу (починаючи з третього і до останнього) кількість матриць попарних порівнянь завжди відмінна від одиниці. У випадку повної ієрархії їх число зумовлюється кількістю структурних елементів вищого рівня, а при неповній ієрархії – кількістю причинно-наслідкових зв'язків між сусідніми рівнями. Тому з'являється необхідність зважування нормалізованих векторів, отриманих з матриць попарних порівнянь для елементів нижчого рівня, на пріоритети елементів вищого рівня. Це досягається шляхом перемноження справа матриці нормалізованих векторів, розрахованих для кожного причинно-наслідкового зв'язка між елементами сусідніх рівнів, на вектор пріоритетів елементів вищого рівня. У матричному вигляді розрахунки здійснюються за формулою:

$$B^{r+1} = C^{r+1} \times B^{r}, \tag{5.16}$$

де B^{r+1}, B^{r} – вектор пріоритетів елементів ієрархії на рівнях $r+1$ та r; C^{r+1} – матриця нормалізованих векторів елементів $r+1$ рівня ієрархії [141, 143].

Оскільки при низькій погодженості матриці зменшується об'єктивність прийнятого рішення вибору раціонального варіанта з заданої множини альтернатив, необхідно провести аналіз її погодженості, тобто

$$b_{ji} \cdot b_{ik} = b_{jk}. \tag{5.17}$$

Для того, щоб підрахувати індекс погодженості необхідно спочатку підсумувати кожен стовпець порівнянь, потім суму першого стовпця збільшити на значення першої компоненти нормалізованого вектора пріоритетів, суму другого стовпця на другий компонент і т.д. Потім отримані числа додати з урахуванням власного числа матриці B – $\lambda_{\max}$. У тому випадку, коли судження експертів цілком погоджені, має виконуватися рівність $B \cdot w = m \cdot w$. Якщо властивість погодженості елементів матриці не дотримується і має місце непослідовність у відповідях експертів, то справедлива рівність: $B \cdot w = \lambda_{\max} \cdot w$, і задача оцінки 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 у методі Сааті розглядається величина C.I. (*consistency index*), що отримала назву індексу погодженості – $k_{узгодж}$:

$$C.I. = k_{узгодж} = (\lambda_{\max} - m)/(m-1). \tag{5.18}$$

Матрицю парних порівнянь, отриманих від експерта, можна використовувати

для подальших розрахунків без уточнення, якщо $k_{відп} = k_{узгодж} / k_{вип} < 0.1$, де $k_{вип}$ – випадковий індекс (random index), $k_{відп}$ – відношення відповідності (*consistency ratio*). Якщо $k_{узгодж}$ розділити на число, що відповідає випадковій погодженості матриці B того ж порядку, одержимо відношення погодженості (ВП), що не повинне перевищувати значення 0.1. У деяких випадках воно може досягати 0.2, але не більше.

Незважаючи на те, що МАІ не має суворого наукового обґрунтування він знайшов широке практичне застосування через свою простоту й наочність. Так, наприклад, застосування МАІ в якості методологічної основи в методиках порівняльної воєнно-економічної оцінки озброєння дає можливість:

по-перше, виключити застосування апарату регресійного аналізу;

по-друге, більш об'єктивно враховувати якісні характеристики в корисності системи;

по-третє, завдяки ієрархічному представленню структури розв'язуваної задачі (проблеми) чітко виражати судження експертів;

по-четверте, уникнути необхідності пошуку функціональних залежностей корисності (важливості) альтернативи від її часткових критеріїв;

по-п'яте, завдяки використанню парних порівнянь часткових критеріїв у шкалі відносин виключити необхідність нормування метричних критеріїв і зменшити погрішність при перекладі якісних характеристик у числові (тому що експерту значно простіше провести порівняння двох неметричних критеріїв, чим привласнити їм числові значення).

Тим не менш в ході детального дослідження МАІ виявлені такі істотні недоліки, як:

неузгодженість, пов'язана із труднощами оцінки відносин складних елементів (1-й вид неузгодженості);

неузгодженість, пов'язана із запропонованою дискретною шкалою для оцінки елементів (2-й вид неузгодженості);

різке збільшення кількості оцінок зі збільшенням набору елементів, тобто коли набір обраних для порівняння елементів більше 9;

перерахування відносин значимості елементів у їхню важливість здійснюється наближеним методом;

відсутність формального механізму синтезу колективного судження, у результаті чого воно виробляється безпосередньо в експертній групі шляхом проведення "круглого столу" (проведенням дебатів і досягненням консенсусу).

Метод анкетування є одним з найбільш перспективних методів щодо

вирішення проблем з соціальним, політичним та воєнним змістом [141, 143, 152, 153]. Його можна застосовувати для безпосереднього використання суджень та інтуїції експертів у деякій формалізованій структурі. При цьому експерти, що входять до складу різних організацій, об'єднуються в декілька груп, що дозволяє спростити адміністративне управління їх роботою. У кожній групі призначається виконавець. Він несе відповідальність за організацію роботи своєї групи, основним способом збору інформації якої є опитувальний лист – *анкета*, що містить логічно ув'язану систему питань за проблемою, яка цікавить.

В анкетах варто передбачити стандартний перелік питань або подій, на які експерти повинні дати свої відповіді. Питання в анкетах необхідно формулювати таким чином, щоб поряд з якісною можна було дати кількісну характеристику відповідям експертів. Крім цільових запитань анкета повинна містити інформацію про правила її заповнення та передбачати можливість уточнення питань і відповідей. До того ж щоб експертні висновки забезпечували об'єктивність інформації, при складанні анкет необхідно також передбачити й включення ряду показників компетентності експертів у відношенні кожної із зроблених ними оцінок.

Опитування експертів здійснюється анонімно у декілька етапів. Під етапом розуміється сукупність операцій із збору та обробки експертних висновків (думок і оцінок), що закінчується одержанням остаточного результату з певної частини проведеного експерименту. Кожен етап проводиться в декілька турів (тур – це цикл робіт з експертами, що включає 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 одержанні остаточного результату по оцінюваному питанню.

На першому етапі проводять опитування по анкетах з питаннями відкритого типу. В подальшому опитування, як правило, проводять по анкетах з питаннями закритого типу. При цьому в анкеті не повинно міститися запитань, що допускають подвійне тлумачення. Сама побудова запитань повинна бути такою, щоб експерт послідовно розкривав суть проблеми, щоразу спираючись на інформацію, яка міститься у попередніх питаннях. Це означає, що відповіді на перші в загальній ієрархії питання повинні базуватися на самій надійній і доступній для експерта інформації та носити по можливості якісний характер. Експерт повинний зазначити, наприклад, розходження альтернатив по перевазі. Подальші запитання анкети повинні складатися так, щоб для відповіді на них була потрібна більш досконала інформація, наприклад, у формі діапазонів значень чинників, що

цікавлять дослідника. Останніми питаннями анкети мають бути такі, для відповіді на які потрібна інформація у вигляді крапкової оцінки (числа). Якщо, наприклад, мета експертизи полягає у виявленні відносного внеску кожного з чинників в досягнення цілі операції, то останнім в анкеті повинне бути питання: "Який на Вашу думку внесок кожного чинника в підвищення ефективності? Оцініть внесок кожного чинника в десятибальній шкалі". Якщо експерту відразу задати останнє питання, то відповідь на нього викликає значні труднощі або він взагалі відмовиться відповідати. Організація анкети за принципом логічного ув'язування й ускладнення запитань дозволяє експерту самому глибше розібратися в проблемі і видати обґрунтовану, позбавлену від протиріч інформацію.

Залежно від мети тура й змісту поставлених в анкеті питань відповіді експертів можуть будуватися на *логічному* (передбачає, що експерт на основі логічних міркувань, синтезуючи наявні в його розпорядженні матеріали, визначає відповідь на поставлене питання), *якісному* (передбачає, що експерт, виділяючи найбільш важливі ознаки й досліджуючи вже існуючу їх градацію, будує узагальнену відповідь на основі декількох ознак), *комплексному* (є синтезом двох попередніх підходів і полягає в тім, що крім якісної одночасно виробляється й логічна градація) або *каталізаційному* (передбачає наявність вихідної інформації, яку експерт повинен оцінити й доповнити) підходах.

Обробка експертних даних при застосуванні методу анкетування залежно від складності або ступеня невизначеності проблеми, її конкретних аспектів та динаміки здійснюється різними математичними методами або їх сполученнями. Це, як результат, дає можливість отримати узагальнену думку (оцінку) та визначити ступінь узгодженості експертних висновків. Таким чином, метод анкетування, як впорядкований та систематизований процес виявлення у визначеній послідовності суджень спеціалістів раціонального, відкриває реальні можливості для поглибленого вивчення тих проблем, які не можуть бути вирішені іншими методами.

Окрім перелічених вище методів для одержання колективної експертної оцінки доволі часто застосовують методи компенсації, комісій та зваженої суми оцінок критеріїв, методи індивідуальної і безпосередньої оцінки, 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 підбору складу відповідної комісії та рівня організації її роботи. Основний недолік – прагнення кожного експерта до компромісу. *Метод зваженої суми оцінок критеріїв* припускає, 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, отримані показники підсумовуються – 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 потім, за допомогою якого-небудь прийому ці оцінки поєднуються в одну узагальнену (погоджену). Зважаючи на те, що висновки, до яких часто приходять фахівці, часто залежать від їхнього наукового і особистого інтересів, необхідності підтримки репутації, від сформованих поглядів і переконань, бажано щоб усі вихідні дані, на базі яких робляться оцінки, були обґрунтовані і доступні для перевірки і критики.

Метод безпосередньої оцінки використовується в тих випадках, коли існує чітка різниця між альтернативами, що розглядаються та (або) вони піддаються безпосередньому вимірюванню, так як мають однакову природу. Суть методу полягає у тому, що експерт повинен кожну складну систему, яка розглядається, поставити на відповідне їй місце відповідно ступеня наявності тієї чи іншої властивості, або відповідно із запропонованим цим же експертом коефіцієнтом значимості. В такому випадку більше значення комплексної оцінки відповідає кращій системі.

Метод розміщення (judgmental bootstrapping) часто використовується при створенні комп'ютерних експертних програм. Він застосовується у випадку, коли залучаються експерти з різним рівнем компетентності або знаннями тільки про окремі аспекти проблеми й прогнози яких неможливо прямо порівнювати один з одним. Якщо при експертному оцінюванні за звичай прийнято вважати, що думки всіх фахівців однаково вагомі, то метод розміщення виходить з того, що до одних експертів варто прислухатися більш уважно, ніж до інших. Фахівці ранжируються залежно від оцінного рівня їхньої компетентності (хоча б з суб'єктивної точки зору аналітика) та обсягу інформації про певну проблему, яким вони володіють. Після цього за досить складною схемою відбувається "зважування" і визначення кінцевого прогнозу, найбільший вплив на який має думка самих авторитетних експертів.

Описані методи експертного оцінювання базуються на відповідних процедурах опитування, що розрізняються за формою спілкування з експертом і способом постановки йому запитань. До таких процедур належать очні та заочні, відкриті і закриті опитування. При виборі конкретної процедури опитування слід враховувати як реальні обмеження проведення експертизи, так достоїнства і недоліки цих процедур.

Очні опитування мають переваги перед заочними за інформативністю. Вони дозволяють виключити можливе неправильне тлумачення експертом питань анкети або ж оперативно конкретизувати поставлені запитання шляхом нових формулювань і уточнень. Разом з тим з урахуванням витрат на одержання інформації та можливістю виключення психологічного тиску на експерта з боку ОПР (який може спотворити одержувану інформацію) більш кращим вважається *метод заочного опитування*. Але і йому властиві певні недоліки пов'язані з тим, що в ході заочного опитування експерт взагалі може не дати відповіді на деякі питання анкети через їхнє нерозуміння.

Важливу роль у процедурах експертного опитування відіграє, як правило, спосіб постановки запитань. Якщо ОПР бажає одержати конкретну відповідь з проблеми, яка цікавить, і разом з тим невпевнений у бажанні експерта надати повну інформацію – використовують, як правило, *процедуру закритого опитування*. Вона передбачає постановку перед експертом таких запитань, у формулюванні яких свідомо міститься перелік альтернативних відповідей. При цьому якщо питання передбачає відповідь у формі тільки "так" або "ні", то таке питання називається чисто закритим. Якщо потрібно зазначити один з більш, ніж двох запропонованих варіантів відповіді, то таке питання називається відкритим. *Процедуру відкритого опитування* застосовують, як правило, в ситуаціях, що вимагають нетривіального рішення (за своїм цільовим призначенням ця процедура подібна з методом колективної генерації ідей), а саме у задачах формування вихідної множини стратегій, вибору показників і критеріїв ефективності, прогнозування поведінки інших суб'єктів операції та в інших випадках, що вимагають виявлення за допомогою експертів неясних елементів проблемної ситуації. Процедура дає повну свободу відповідей експерта з розглянутої проблеми. Її недоліки обумовлюються тим, що обов'язковим є застосування неформальних методів опрацювання отриманої інформації у виді довільної інтерпретації питань і відповідей, а також високої кваліфікації експертів.

Враховуючи викладене можна стверджувати, що *достоїнством всіх індивідуальних і групових методів експертного оцінювання* є відносна простота і зручність застосування для прогнозування практично будь-яких ситуацій (наприклад, на ранніх етапах розробки або модернізації СТС), у тому числі в умовах неповної, невизначеної або неточної початкової інформації. Їх важливою особливістю є можливість:

встановлення ступеню складності і актуальності ситуацій (проблем);

визначення основних цілей ситуацій (проблем) та критеріїв оцінювання

їх ефективності;

виявлення найбільш важливих факторів, що впливають на досягнення поставлених цілей та взаємозв'язки між ними;

оцінювання ступеня відповідності ситуацій (проблем) світовому науково-технічному рівню;

ранжирування ситуацій (проблем) шляхом багатокритеріального кількісного оцінювання для вибору найкращої альтернативи тощо.

До основних недоліків таких методів слід віднести суб'єктивізм думок експертів і обмеженість їхніх суджень.

5.4 Опрацювання інформації евристичного походження

Одним з принципових питань, що виникають при використанні суджень експертів, є питання про степінь збереження об'єктивності дослідження. На практиці це може бути забезпечено за рахунок високої компетентності членів експертної групи, а також аргументованості їх суджень. Зважаючи, що останні за оцінюваними експертами питаннями, як правило, розходяться виникає завдання щодо їх систематизації та формалізації. Для цього останнім часом застосовують методи парних порівнянь, ранжирування і шкальних оцінок, методи теорії корисності та теорії проспектів, методи ELECTRE та інші.

Метод парних порівнянь призначений для визначення порядку розташування n певних факторів (об'єктів) з погляду їхньої важливості (переваги) шляхом їх попарного порівняння один з одним [155]. Тобто, розглядаючи всі можливі пари факторів (об'єктів), експерт у кожній з них встановлює ту причину, що на його думку найсильніше впливає на наслідок. Виникає логічне запитання, як отримати оцінку всієї сукупності об'єктів на основі результатів парного порівняння, виконаного групою експертів.

Припустимо, що кожен з m експертів, оцінюючи вплив на результат всіх пар факторів (об'єктів), встановлює таку числову оцінку:

$$r_{ij}^{h} = \begin{cases} 1, & \text{якщо об'єкт } O_i \text{ має більше значення, ніж } O_j \\ 0.5, & \text{якщо об'єкти } O_i \text{ та } O_j \text{ рівноправні} \\ 0, & \text{якщо об'єкт } O_i \text{ має менше значення, ніж } O_j \end{cases},$$

де $h = \overline{1,m}$ – номер експерта; $i = \overline{1,n}$ та $j = \overline{1,n}$ – номера об'єктів, досліджуваних при експертизі.

При цьому, якщо:

m_i експертів з їх загальної кількості віддали перевагу O_i;

m_j експертів висловились на користь O_j;

m_p експертів вважає порівнювані фактори (об'єкти) рівноправними, – то оцінка МОЧ дискретної випадкової величини r_{ij} дорівнюватиме:

$$x_{ij} = M[r_{ij}] = 1 \cdot \frac{m_i}{m} + 0.5 \cdot \frac{m_p}{m} + 0 \cdot \frac{m_j}{m}, h = \overline{1,m}. \quad (5.19)$$

Враховуючи, що загальна кількість експертів $m = m_i + m_p + m_j$, а $m_p = m - (m_i + m_j)$ з виразу (1), отримаємо:

$$x_{ij} = \frac{m_i}{m} + 0.5 \cdot \frac{(m - m_i - m_j)}{m} = \frac{1}{2} + \frac{m_i - m_j}{2 \cdot m}, \text{ де } x_{ij} + x_{ji} = 1. \quad (5.20)$$

Таким чином, сукупність величин x_{ij} утворить, як результат, матрицю МОЧ оцінок всіх парних порівнянь факторів (об'єктів) розмірності $n \times n$ (табл. 5.10), що дозволить визначити коефіцієнти їх відносної важливості, тобто сформувати вектор $k = [k_1, k_2, ..., k_n]^T$. Одним із способів визначення значень елементів вектора k є ітераційний алгоритм виду:

а) початкова умова: $t = 0$, $k^0 = \underbrace{[1,1,...,1]^T}_{n}$;

б) рекурентні співвідношення: $k^t = \frac{1}{\lambda^t} \times X \times k^{t-1}$, $\lambda^t = [1,1,...,1] \times X \times k^{t-1}$, $t = \overline{1,n}$, де X – матриця МОЧ оцінок пар об'єктів, k^t – вектор коефіцієнтів відносної важливості об'єктів порядку t. $\sum_{i=1}^{n} k_i^t = 1$ – умова нормування;

в) ознака закінчення алгоритму $\|k^t - k^{t-1}\| < E$.

Таблиця 5.10

Результати попарних порівнянь різних факторів

	O_1	....	O_j	....	O_n
O_1					
....					
O_i		$x_{ij} = M[r_{ij}]$			
....					
O_n					

$\Rightarrow$

k
k_1
....
k_i
....
k_n

Якщо матриця X невід'ємна і нерозкладна (тобто шляхом перестановки рядків і стовпців її не можна привести до трикутного вигляду), то при збільшенні порядку $t \to \infty$ величина λ^t сходиться до її максимального власного

числа, тобто $k = \lim_{t\to\infty} k^t$, $\sum_{i=1}^{n} k_i = 1$. Це твердження випливає з теореми Перрона-Фробеніуса й доводить збіжність наведеного вище алгоритму.

ПРИКЛАД 5.1 [143].

Припустимо, що в результаті опитування трьох ($m=3$) експертів про ступінь впливу на результат трьох ($n=3$) різних факторів (об'єктів) отримані 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

Для одержання групової оцінки ступеня впливу кожного з об'єктів на результат, побудуємо матрицю математичних очікувань оцінок кожної з пар об'єктів, що для розглянутого приклада буде мати вигляд:

	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 отримані з наступних виразів:

$$x_{11} = \frac{1}{2} + \frac{0-0}{2\times 3} = \frac{1}{2},\quad x_{12} = \frac{1}{2} + \frac{2-0}{2\times 3} = \frac{5}{6},$$

$$x_{13} = \frac{1}{2} + \frac{1-0}{2\times 3} = \frac{4}{6}$$

$$x_{21} = 1 - x_{12} = \frac{1}{6},\quad x_{23} = \frac{1}{2} + \frac{0-2}{2\times 3} = \frac{1}{2},\quad x_{31} = 1 - x_{13} = \frac{2}{6},\quad x_{32} = 1 - x_{23} = \frac{5}{6}.$$

$x_{11} = x_{22} = x_{33} = \frac{1}{2}$

Для наочності, кожний із кроків формування вектора відносної важливості об'єктів представимо у вигляді:

Крок 0: $k^0 = [1 \quad 1 \quad 1]^T$.

Крок 1:

$$Y^1 = X \times k^0 = \frac{1}{6} \times \begin{bmatrix} 3 & 5 & 4 \\ 1 & 3 & 1 \\ 2 & 5 & 3 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{6} \times \begin{bmatrix} 3+5+4 \\ 1+3+1 \\ 2+5+3 \end{bmatrix} = \frac{1}{6} \times \begin{bmatrix} 12 \\ 5 \\ 10 \end{bmatrix},$$

$$\lambda^1 = [1 \quad 1 \quad 1] \times Y^1 = [1 \quad 1 \quad 1] \times \frac{1}{6} \times \begin{bmatrix} 12 \\ 5 \\ 10 \end{bmatrix} = \frac{1}{6} \times 27 = \frac{27}{6},$$

$$k^1 = \frac{1}{\lambda^1} \times Y^1 = \frac{6}{27} \times \frac{1}{6} \times \begin{bmatrix} 12 \\ 5 \\ 10 \end{bmatrix} = \frac{1}{27} \times \begin{bmatrix} 12 \\ 5 \\ 10 \end{bmatrix} = \begin{bmatrix} 0.444 \\ 0.185 \\ 0.370 \end{bmatrix}.$$

Крок 2:

$$Y^2 = X \times k^1 = \frac{1}{6} \times \begin{bmatrix} 3 & 5 & 4 \\ 1 & 3 & 1 \\ 2 & 5 & 3 \end{bmatrix} \times \frac{1}{27} \times \begin{bmatrix} 12 \\ 5 \\ 10 \end{bmatrix} = \frac{1}{6 \times 27} \times \begin{bmatrix} 36+25+40 \\ 12+15+10 \\ 24+25+30 \end{bmatrix} = \frac{1}{6 \times 27} \times \begin{bmatrix} 101 \\ 37 \\ 79 \end{bmatrix},$$

$$\lambda^2 = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \times Y^2 = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \times \frac{1}{6 \times 27} \times \begin{bmatrix} 101 \\ 37 \\ 79 \end{bmatrix} = \frac{217}{6 \times 27},$$

$$k^2 = \frac{1}{\lambda^2} \times Y^2 = \frac{6 \times 27}{217} \times \frac{1}{6 \times 27} \times \begin{bmatrix} 101 \\ 37 \\ 79 \end{bmatrix} = \frac{1}{27} \times \begin{bmatrix} 101 \\ 37 \\ 79 \end{bmatrix} = \begin{bmatrix} 0.465 \\ 0.171 \\ 0.364 \end{bmatrix}.$$

$$\max\left(|0.465 - 0.444|,\ |0.171 - 0.185|,\ |0.364 - 0.370|\right) = 0.021 > 0.001.$$

Крок 3: Продовжуючи ітераційний процес доти, поки норма оцінки не буде менше заданої ($\max_i\left(|k_i^l - k_i^{l-1}|\right) < 0.001$) отримаємо, що за групову оцінку ступеня впливу на результат може бути прийнятий вектор коефіцієнтів відносної важливості об'єктів виду: $k = k^4 = [0.468 \quad 0.169 \quad 0.363]^T$.

Метод ранжирування застосовують, як правило, у випадку коли необхідно впорядкувати у часі або просторі певні фактори (об'єкти), які визначають кінцеві результати, але не піддаються безпосередньому виміру [152, 156]. Для цього експерт повинен розташувати їх у порядку, що представляється йому найбільш раціональним (порядку зростання або убування) і приписати кожному з факторів (об'єктів) числа натурального ряду – порядкові номери або інакше ранги. Порядковий номер, що дорівнює 1 одержує найкращий фактор (об'єкт), а найменш важливий серед усіх можливих отримує порядковий номер – n. Якщо серед параметрів $x_1, x_2, \ldots, x_n$ відсутні групи факторів (об'єктів), рівнозначних з погляду їхньої важливості, то порядковий номер (ранг) такого фактора (об'єкта) у ранжируваній послідовності матиме, наприклад, такий вид $x_3^{(1)}, x_6^{(2)}, x_1^{(3)}, \ldots, x_k^{(n)}$. Для кожної групи рівнозначних факторів (об'єктів) їх ранги є однаковими і якнайчастіше дробовими. Вони знаходяться як середнє арифметичне відповідної вибірки порядкових номерів факторів (об'єктів), що входять до певної групи. Припустимо, що фактори (об'єкти) x_2, x_7, x_1, x_5 є рівнозначними й мають порядкові номери з 1 по 4. Ранг кожного з факторів x_2, x_7, x_1, x_5 у цьому випадку дорівнює $\frac{1+2+3+4}{4} = 2\frac{1}{2}$. Якщо ранжирування проводиться декількома (m) експертами, то для кожного фактора (об'єкта) спочатку підраховують суму рангів, отриману від усіх експертів, а потім, виходячи з отриманого результату встановлюють його результуючий ранг. Найвищий (перший ранг) привласнюють

при цьому фактору (об'єкту), який одержав найменшу суму рангів й, навпаки, фактору (об'єкту), який одержав найбільшу суму рангів – найнижчий ранг. Інші фактори (об'єкти) впорядковують відповідно із значенням суми рангів щодо фактора (об'єкта), якому привласнюється перший ранг.

На підставі здобутих даних формується матриця рангів $\|x_{ij}\|$ розмірності $n \times m$, де n – кількість факторів (об'єктів), m – кількість експертів ($i = \overline{1,n}$, $j = \overline{1,m}$). Отримані дані зводяться в таблицю такого виду.

Ознаки	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} відбивають порядок віддання переваги i-му фактору (об'єкту) j-м експертом перед іншими факторами (об'єктами). При цьому сума рангів для i-го фактора (об'єкта) з урахуванням компетентності експертів може бути обчислена за формулою:

$$x_i = \sum_{j=1}^{m} (p_j \cdot x_{ij}), \tag{5.21}$$

де p_j – показник компетентності експертів: $0 \le p_j \le 1$, $j = \overline{1,m}$.

Отримані значення дозволяють впорядкувати фактори (об'єкти) за ланцюжком нерівностей: $x_r < x_t < \ldots < x_q$, де $x_r = \min_i (x_i)$, $x_t = \min_{i,i \ne r} (x_i)$, $x_q = \max_{i,j \ne r,j \ne l} (x_i)$.

Наступним кроком визначається середній ранг, тобто середнє статистичне значення i-го фактора (об'єкта) за формулою:

$$S_i = \left(\sum_{j=1}^{m} x_{ij} \right) \Big/ m, \tag{5.22}$$

де j – номер експерта ($j = \overline{1,m}$), i – номер ознаки ($i = \overline{1,n}$).

Слід зазначити, що побудова таких ранжировок є коректною процедурою лише в тому випадку, якщо ранги призначаються як місця об'єктів у вигляді натуральних чисел $1,2,\ldots,n$. Однак ранги об'єктів визначають тільки порядок розташування об'єктів за показниками порівняння. Як числа вони не дають можливість зробити висновок про те, на скільки або у скільки разів один об'єкт є переважнішим за інший.

Разом з тим для використання знань, отриманих від експертів, необхідно не тільки впорядкування або ранжирування факторів (об'єктів) за ступенем

їхнього впливу на кінцевий результат, але й визначення кількісної оцінки ступеня такого впливу. Найпростішим методом для реалізації цієї задачі є алгоритм, заснований на комплексному підході, що передбачає перехід від матриці ранжировок до матриці парних порівнянь. Для цього усіма експертами на основі матриці $\|x_{ij}\|$ будуються m матриць парних порівнянь $X_j (j = 1,2,...,m)$, елементи яких визначаються з умови:

$$X_j = \|x_{ir}^j\| = \begin{cases} 1, якщо \quad O_i^j > O_r^j \quad тобто \quad x_{ij} < x_{rj} \\ 0.5, якщо \quad O_i^j \approx O_r^j \quad тобто \quad x_{ij} = x_{rj} \\ 0, якщо \quad O_i^j < O_r^j \quad тобто \quad x_{ij} > x_{rj} \end{cases}, \tag{5.23}$$

де m – кількість експертів; j – номер експерта;

i та r – номери порівнюваних факторів (об'єктів).

До отриманих m матриць застосовується метод обробки парних порівнянь, ітераційна процедура якого дозволяє одержати коефіцієнти відносної важливості об'єктів за ступенем їхнього впливу на результат.

ПРИКЛАД 5.2 [143].

Нехай три експерти ($m = 3$) провели ранжировку трьох об'єктів ($n = 3$) за ступенем їх впливу на певний результат. Матриця рангів подана таблично.

Об'єкт O_i	Експерт 1	Експерт 2	Експерт 3
O_1	1	1	2
O_2	2	3	1
O_3	3	2	3

Матриці парних порівнянь для першого, другого і третього експертів, отримані на основі цієї таблиці, мають вид:

$$X_1 = \|x_{rj}^1\| = \begin{Vmatrix} 0.5 & 1 & 1 \\ 0 & 0.5 & 1 \\ 0 & 0 & 0.5 \end{Vmatrix}, \; X_2 = \|x_{rj}^2\| = \begin{Vmatrix} 0.5 & 1 & 1 \\ 0 & 0.5 & 0 \\ 0 & 1 & 0.5 \end{Vmatrix}, \; X_3 = \|x_{rj}^3\| = \begin{Vmatrix} 0.5 & 0 & 1 \\ 1 & 0.5 & 1 \\ 0 & 0 & 0.5 \end{Vmatrix}.$$

Використовуючи метод обробки парних порівнянь отримаємо послідовність векторів коефіцієнтів відносної важливості об'єктів:

Крок	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 з заданою точністю ($E = 0.001$) є збіжною на четвертому кроці до значень: $K = [0.500 \quad 0.349 \quad 0.151]^T$, що дозволяє кількісно

оцінити ступінь впливу кожного об'єкта на результат, отриманий на основі вихідного ранжирування експертів.

Одним із різновидів методу ранжування є ***метод ідеальної точки***, що був запропонований К.Юнгом та С.Вангом [150]. Метод базується на тому, що кращі рішення мають найменші відстані від від'ємно-ідеального рішення. При цьому передбачається, що кожний критерій має монотонно убутну або збільшувану корисність. Тоді додатньо-ідеальне рішення формується з кращих значень критеріїв за всіма альтернативними варіантами, а від'ємно-ідеальне – з гірших.

Алгоритм методу полягає у виконанні таких кроків.

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 додатньо-ідеального (A^+) та від'ємно-ідеального (A^-) рішення, які описуються відповідно таким чином:

$$A^+=\left\{\max_i V_{ik} | i\in[1,n], k\in[1,q]\right\}=\left\{V_1^+ ... V_k^+ ... V_q^+\right\}, \tag{5.24}$$

$$A^-=\left\{\min_i V_{ik} | i\in[1,n], k\in[1,q]\right\}=\left\{V_1^- ... V_k^- ... V_q^-\right\}. \tag{5.25}$$

Крок 3. Обчислення відстані від поточної альтернативи до додатньо-ідеальної та від'ємно-ідеальної точок за 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 додатньо-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. Ранжирування альтернативних варіантів у напрямку убування. Якщо $L_i^+ > L_j^+$, то $a_i > a_j$.

Враховуючи викладене можна констатувати, що точність і надійність процедури ранжирування значною мірою залежать від кількості об'єктів (n). У принципі, чим таких об'єктів менше ($n<10$), тим вище їх "розрізнення" з

погляду експерта, і, отже, тим надійніше можна встановити ранг об'єкта.

Французькою школою теорії прийняття рішень, очолюваною Б. Руа [157, 158], свого часу був запропонований конструктивний підхід до формування рішень, у рамках якого методи, моделі і концепції почали розглядатися як допоміжні засоби практичного аналізу ситуації. Вони дозволяли дослідникові не тільки усвідомити мету прийняття рішення, а й краще зрозуміти переваги ОПР. Невдовзі такий підхід отримав узагальнену назву – ***метод ELECTRE***.

Метод ELECTRE полягає в тому, що навіть за умови математичного домінування однієї альтернативи над іншою, ОПР може розглядати альтернативу a_i майже стовідсотково кращою за альтернативу a_j. Його головними кроками є:

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 отриманої матриці за правилами:

$$C_{ik}^r = \frac{C_{ik} - C_k^{\min}}{C_k^{\max} - C_k^{\min}}$$ для критерію ефективності (чим більше, тим краще);

$$C_{ik}^r = \frac{C_k^{\max} - C_{ik}}{C_k^{\max} - C_k^{\min}}$$ для критерію вартості (чим менше, тим краще);

де $C_k^{\max}$ та $C_k^{\min}$ – 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 включає всі критерії за якими a_i є переважнішою за a_j: $F_{ij} = \{k | V_{ik} > V_{jk}\}$ і навпаки масив неузгодженості включає всі інші критерії – $G_{ij} = \{k | V_{ik} < V_{jk}\}$;

4) розрахунок індексів узгодженості і неузгодженості.

Індекс узгодженості визначається як сума ваг критеріїв, що входять в масив узгодженості: $f_{ij} = \sum_{k \in F_{ij}} W_k$. Індекс неузгодженості відбиває ступінь того, наскільки альтернатива a_i є гіршою за a_j й визначається таким чином:

$$g_{ij} = \max_{k \in G_{ij}} |V_{ik} - V_{jk}| \Big/ \max_{k \in [1,q]} |V_{ik} - V_{jk}|. \qquad (5.28)$$

Очевидно, що $f_{ij} \in [0,1]$ та $g_{ij} \in [0,1]$. Більше значення f_{ij} а означає, що a_i є переважнішою за a_j. Більше значення g_{ij} означає, що за критерієм неузгодженості

навпаки альтернатива a_j є переважнішою за a_i;

5) визначення індексів домінування (порогів) узгодженості і неузгодженості. На цьому етапі ОПР задає значення порогу узгодженості P та порогу неузгодженості Q:

$$\text{якщо } f_{ij} > P \text{ та } g_{ij} < Q, \text{ то } a_i > a_j. \tag{5.29}$$

Недоліком методу ELECTRE є те, що він є допоміжним засобом, а не способом вироблення кращого рішення як при аксіоматичному підході й не дозволяє інтелектуалізувати процес прийняття рішення, тому, що вироблення остаточного рішення завжди залишається за керівником (ОПР).

Метод шкальних оцінок дозволяє одержати кількісну оцінку ступеня важливості кожного з факторів, що належать певній сукупності [159, 160] відносно шкали їх певних базових (еталонних) згачень. У цьому випадку оцінки відносної важливості кожного фактора виражаються 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 табл. 5.11, де C_{ji} – відносна важливість параметра x_i з погляду j-го експерта, що виражається або відповідним балом, або значенням рангу.

Таблиця 5.11

Результати опитування експертів по методу шкальних оцінок різних факторів

Експерт	Фактор (параметр)					
	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}

Середнєарифметичне оцінок C_i кожного з факторів визначається з виразу $C_i = \frac{1}{m_i} \cdot \sum_{j=1}^{m_i} C_{ji}$, де m_i – кількість експертів, що оцінювали важливість фактора x_i.

Величини C_{ji} й відповідно C_i можуть виражатися кількісно як у балах, так і у рангах. В першому випадку величина C_i має назву середнього бала (середньої величини) фактора x_i, у другому – середнього рангу. Якщо ранжирування факторів проводити за методом попарних порівнянь, то дані

таблиць від m експертів зводяться в одну загальну таблицю, сумарну матрицю порівнянь. У кожній чарунці ij цієї таблиці стоїть певне число γ_{ij}, що аргументує перевагу i-го фактора над j-м, отриманому від усіх m експертів. За повної згоди експертів C_n^2 чарунок загальної таблиці буде містити число $\gamma = m$, а інші чарунки – 0. При мінімальній кількості згод кожна чарунка міститиме число $\gamma = \frac{1}{2} \cdot m$, якщо m парне і $\gamma = \frac{1}{2} \cdot (m+1)$, якщо m непарне.

Підсумовування чисел γ_{ij} по рядках з наступним діленням отриманого результату на m дає середню ранжировку факторів $x_1, x_2, ..., x_n$, що, у свою чергу, служить показником узагальненої думки про важливість факторів (чим менше сума по рядку j, тим більш важливу роль відіграє фактор i. Відносно сум по стовпцях має місце зворотна картина).

Оскільки показник узагальненої думки C_i й еталонне значення по своїй суті представляють одне й те саме та відрізняються лише своїм призначенням, надалі для простоти міркувань будемо говорити про центр групування шкальних оцінок, вважаючи, що це поняття включає два попередніх. Методика пошуку центра групування експертних даних на шкалі оцінок для будь-якого закону розподілу використовує або середньостатистичне значення оцінок, або середньозважене. Такий підхід (особливо використання середньозваженого значення) дозволяє в достатньому ступені наближення об'єктивно визначати центр групування. Однак при великому діапазоні значень шкали урахування всіх значень без винятку в деяких випадках, як це буде показано нижче, може дати відчутне зрушення центра групування.

Позначимо центр групування оцінок при заданому розподілі експертів по значеннях, що надаються ними через C. Значення C залежить від наступних величин:

$$C = F(k, h, W_h), \tag{5.30}$$

де k - кількість експертів у групі; h - крок пошуку області групування; W_h - діапазон значень оцінок, якому відповідає кількість експертів не менш θ_k, при найменшому кроці ($0 < \theta_k < 1$).

Нехай є шкала зі значеннями i, де $i = 0,1,2,...,n$. Тоді m_i – є кількість експертів, що дали i-е значення. Якщо в групі k експертів, то $\sum_{i=1}^{n} m_i = k$.

Припустимо, що має місце такий розподіл (рис. 4.8).

На першому кроці пошуку центра групування $h = 1$ визначаються ті пари значень, які задовольняють наступному співвідношенню: $\sum_{i \in W_h}^{n} m_i \geq \theta_k$ (5.31)

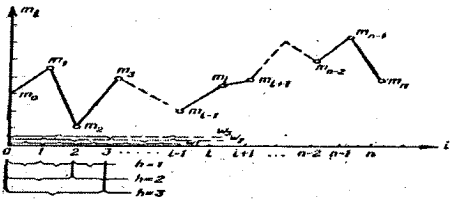


Рис. 4.8. Розподіл оцінок висловлювань експертів

При цьому можливі три випадки:

1) жодна пара значень на даному кроці пошуку не задовольняє співвідношенню (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 при даному кроці пошуку, що задовольняє співвідношенню (5.31). У цьому випадку область групування знайдена й центр групування визначається як середньозважене всіх значень, що належать даній області:

$$C = \sum_{i \in W_h}^{n} i \cdot m_i \Big/ \sum_{i \in W_h}^{n} m_i ; \qquad (5.32)$$

3) існує кілька областей, що задовольняють співвідношенню (5.32). Тоді область групування визначається в такий спосіб: ліва границя являє собою найменше значення для всіх значень знайдених областей, а права границя - відповідно їхнє найбільше значення. Область групування визначається як середньозважене всіх значень, що належать області групування:

$$C = \sum_{i \in G}^{n} i \cdot m_i \Big/ \sum_{i \in G}^{n} m_i , \qquad (5.33)$$

де G - множина всіх значень шкали, що належать області групування.

ПРИКЛАД 5.3 [143].

Дана шкала від 0 до 10 і відповідне кожному значенню шкали число експертів m_i.

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% порівняння на практиці найпоширеніше. Загальна кількість експертів $m = 100$. Поклавши $h = 1$, підрахуємо кількість експертів, що доводиться на кожну область.

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

За даними останньої таблиці жодна область при заданому кроці не задовольняє співвідношенню (5.31). Тому крок пошуку збільшується й здійснюється підрахунок розширених областей, результати чого подані у таблиці, що наведена нижче.

W_2	0-2	1-3	-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 видно з наведених даних, і на цьому кроці немає жодної області, що задовольняє співвідношенню (5.32). Тому крок пошуку знову збільшується й процедура повторюється.

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 випадку існує рівно одна область, що задовольняє співвідношенню (5.33), – область 1–4. Вона і є областю групування. Використовуючи співвідношення (5.33), знаходимо значення центра групування

$$C_1 = \sum_{i\in G}^{n} i\cdot m_i \Big/ \sum_{i\in G}^{n} m_i = \frac{1\cdot 17+2\cdot 9+3\cdot 1+4\cdot 31}{17+9+1+31} = \frac{162}{58} \approx 3.$$

Якщо ж брати як центр групування середньозважене значення всієї шкали, то одержимо

$$C_1 = \sum_{i\in G}^{n} i\cdot m_i \Big/ \sum_{i\in G}^{n} m_i == \frac{475}{100} \approx 5.$$

Як видно з наведеного приклада, підрахунок через область групування дав корекцію порядку 40% у порівнянні з середньозваженим значенням.

Враховуючи викладене можна стверджувати, що застосування методів парних порівнянь, ранжирування і шкальних оцінок, методів теорії корисності та теорії проспектів, а також методів ELECTRE значно полегшує математичну обробку інформації евристичного походження та їх інтерпретацію. 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 квартилей).

5.5 Оцінювання ступеня погодженості суджень групи експертів та їх статистичної достовірності

Якісний аналіз експертної інформації є заключним етапом експертного оцінювання. Він полягає у [143, 161, 162]:

проведенні оцінювання ступеня погодженості думок експертів;

виділенні груп експертів з близькою думкою (у випадку наявності істотної розбіжності в їхніх відповідях);

виявленні розкиду думок, впливу характеристик експертів на зміст їхніх відповідей;

ранжируванні відповідей в однорідних групах та формуванні об'єднаних відповідей.

Як показники ступеня погодженості суджень експертів частіш за все використовуються коефіцієнт варіації [163], коефіцієнт парної рангової кореляції та коефіцієнт конкордації.

Коефіцієнт варіації (v_j) характеризує відносну ступінь варіїрування параметрів і обчислюється за формулою:

$$v_j = \frac{S_j}{\overline{C_j}} \cdot 100\%, \tag{5.34}$$

де $S_j = \sqrt{D_j}$ – стандартне (середньоквадратове) відхилення оцінок, отриманих j-м параметром [141];

$D_j = \frac{1}{m_j - 1} \cdot \sum_{i=1}^{m_j} \left(C_{ij} - \overline{C_j}\right)^2$ – дисперсія оцінок.

Чим менше v_j, тим вище ступінь погодженості групи експертів про відносну важливість j-го параметра (фактора). Наближено значення похибки коефіцієнта варіації може бути обчислене за формулою:

$$S_{v_j} = \frac{v_j}{\sqrt{2 \cdot m_j}} \cdot \sqrt{1 - 2 \cdot \left(\frac{v_j}{100}\right)^2}. \tag{5.35}$$

З певним наближенням можна вважати, що у генеральній сукупності коефіцієнт варіації для j-го параметра знаходиться в межах $v_j \pm 3 \cdot S_{v_j}$.

Коефіцієнт парної рангової кореляції ($\rho_{\alpha\beta}$) – характеризує окремих експертів, міркування яких у цілому погоджуються, або, напроти, експертів, які мають

різке розходження в судженнях про важливість факторів. Він приймає значення в інтервалі $(-1 \le \rho_{\alpha\beta} \le +1)$ і може бути обчислений за формулою:

$$\rho_{\alpha\beta} = 1 - \frac{\sum_{j=1}^{p} \psi_j^2}{\frac{1}{6} \cdot (p^3 - p) - \frac{1}{12} \cdot (T_\alpha - T_\beta)}, \tag{5.36}$$

де ψ_j^2 – абсолютне значення різниці рангів R_{α_j} і R_{β_j} оцінок j-го параметра (фактора), призначених експертами α та β:

$$\psi_j = \left| R_{\alpha_j} - R_{\beta_j} \right|, \tag{5.37}$$

T_α, T_β – показники зв'язних рангів у ранжировках експертів α і β;

p – загальна кількість груп ранжировок.

При цьому значення $\rho_{\alpha\beta}$ знаходяться в інтервалі $-1 \le G \le +1$ й можуть відповідати таким випадкам:

$$\rho_{\alpha\beta} = \begin{cases} 0, & \text{означає, що показники незалежні (відсутність зв'язку між судженнями експертів)} \\ +1, & \text{означає, що ранжирування за показниками співпадає (погодженість думок)} \\ -1, & \text{означає, що ранжирування за показниками цілком протилежне} \end{cases}.$$

Коефіцієнт рангової кореляції для сумарної ранжировки був запропонований у 1940 році М. Кендаллом та Б. Смітом [164] і отримав назву *коефіцієнта конкордації* (W). Він характеризує ступінь погодженості суджень групи експертів у цілому за сукупністю параметрів (об'єктів, факторів, показників, заходів, напрямків дослідження тощо) та обчислюється за таким алгоритмом.

На першому кроці [165–167] визначається середнє арифметичне сум рангів оцінок, отриманих усіма параметрами:

$$\overline{R} = \frac{1}{n} \cdot \sum_{j=1}^{n} R_j \tag{5.38}$$

де R_j - сума рангів оцінок, отриманих j-м параметром.

На другому кроці розраховується відхилення d_j сум рангів оцінок, отриманих j-м параметром, від середнього арифметичного сум рангів оцінок, отриманих усіма параметрами:

$$d_j = R_j - \overline{R}. \tag{5.39}$$

На третьому кроці обчислюється сума квадратів цих відхилень:

$$S = \sum_{j=1}^{n} d_j^2 . \qquad (5.40)$$

На четвертому кроці визначається показник T_i зв'язаних (рівних) рангів оцінок, призначених i-м експертом. Якщо всі n рангів, отриманих i-м експертом, є різними, 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 щодо відносної важливості 9 параметрів подані таблично.

Показники	Параметри: $j = 1..9$								
	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

В 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

$$T = \sum_{l=1}^{6} \left(t_l^3 - t_l\right) = \left(2^3 - 2\right) + \left(3^3 - 3\right) = 30 . \qquad (5.41)$$

На п'ятому кроці визначається коефіцієнт конкордації W [141]:

$$W = \frac{S}{Sm} = \frac{12 \cdot \Delta S^2}{m^2 \cdot \left(p^3 - p\right)}, \qquad (5.42)$$

де $\Delta S^2 = m^2 \cdot \sum_{i=1}^{n} \left(C_i - \frac{1}{2} \cdot (p+1)\right)^2$ – міра ступеня узгодженості думок експертів (сума квадратів відхилень фактичних значень рангів від їх ідеальних значень).

При цьому значення коефіцієнта конкордації може змінюватися в інтервалі $0 \le W \le +1$:

$$W = \begin{cases} 0, & \text{означає, що міркування експертів не співпадають} \\ +1, & \text{означає, що міркування експертів повністю співпадають} \end{cases}.$$

Якщо у ранжировці є ранги, що співпадають [164–167], то коефіцієнт конкордації обчислюється за формулою:

$$W = \frac{12 \cdot S}{z^2 \cdot \left(p^3 - p\right) - z \cdot \sum_{i=1}^{z} T_i}, \quad S = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} r_{ij} - \bar{r}^2 \right), \quad \bar{r} = \frac{1}{n} \cdot \sum_{i=1}^{n} r_i , \quad r_i = \sum_{j=1}^{m} r_{ij} , \qquad (5.43)$$

де z – кількість груп ранжировок зв'язаних (рівних) рангів; T_i – кількість зв'язаних рангів у i-й ранжировці; t_{l_i} – кількість зв'язаних (рівних) рангів у l-й групі i-ї ранжировки; L – кількість груп зв'язаних (рівних) рангів у i-й ранжировці;

r_{ji} – матриця результатів ранжирування i-ї альтернативи j-м експертом.

У таблиці, що приведена нижче, подано приклад груп зв'язаних (рівних) рангів. У цьому випадку для трьох груп зв'язаних (рівних) рангів $(L=3)$, для яких $t_1=2$, $t_2=3$, $t_3=2$:

$$T_i=\left(2^3-2+3^2-3+2^3-2\right)=36.$$

Оцінка j-м експертом	Фактор (параметр)								
	a	b	c	d	e	f	g	h	k
Ранги	5	1,5	3	7,5	1,5	7,5	5	9	5

На шостому кроці проводять оцінку статистичної достовірності коефіцієнта конкордації W шляхом перевірки нульової гіпотези $H_0: W=0$. При цьому методика перевірки залежить від значень m та n. При невеликих m і $n\le 7$ для перевірки нульової гіпотези при рівні значимості $q=0.05$ можна скористатися табличними значеннями S_{kp}, що подані нижче.

Кількість експертів $\left(\overline{j=1,m}\right)$	Кількість параметрів $\left(\overline{j=1,n}\right)$				
	3	4	5	6	7
3	---	---	64.6	103.9	157.3
4	---	49.5	88.4	143.3	2170
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, за звичай, використовують критеріальну статистику χ^2_R, яка розподілена по χ^2 при $\vartheta=n-1$

$$\chi^2_R=\frac{12\cdot S}{m\cdot n\cdot(n+1)}. \tag{5.44}$$

Якщо кількість зв'язків велика або їх довжина є значною, то

$$\chi^2_R=\frac{12\cdot S}{m\cdot n\cdot(n+1)-\frac{1}{n-1}\cdot\sum_{j=1}^{m}T_i}. \tag{5.45}$$

Правила прийняття статистичного рішення:

H_0 приймається при $\chi^2_R<\chi^2_{q,\vartheta}$;

H_0 відхиляється при $\chi^2_R\ge\chi^2_{q,\vartheta}$, де $\chi^2_{q,\vartheta}$ критичне значення при $\vartheta=n-1$ та заданому рівні значимості q, яке подане таблично:

Нульову гіпотезу можна знайти й іншим чином, а саме: за таблицею, що подана вище знаходять значення $q_{табл}$ для емпіричного χ^2_R при $\vartheta=n-1$. Потім

порівнюють $q_{табл}$ із заданим $q = 10\%$. Якщо $q_{табл} < 10\%$, то має місце невипадкова узгодженість суджень групи експертів.

Число ступенів свободи	Рівні значимості		Число ступенів свободи	Рівні значимості	
	$q = 0.2$	$q = 0.1$		$q = 0.2$	$q = 0.1$
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

Незалежно від використовуваних коефіцієнтів у результаті розрахунків отримують квадратну матрицю мір близькості експертів за характером відповідей. При цьому її можна розбити на однорідні групи одним з алгоритмів таксономії (багатомірної класифікації). Результати таксономії з визначеною щільністю зводяться до однієї з ситуацій, коли:

по-перше, відповіді більшості експертів утворять компактну групу, склад якої стабільний при різних розбивках;

по-друге, в процесі розбивки виділяється декілька стабільних, чітко розмежованих груп;

по-третє, відповіді експертів рівномірно розташовані в просторі ознак (альтернатив), але на різних етапах розбивки утворюють нестабільні групи.

У першому випадку існує достатня погодженість думок більшості експертів. В другому можливе висування гіпотези про неоднорідність колективу експертів, яка припускає виявлення набору об'єктивних характеристик експертів, що викликають цю неоднорідність та формування упорядкованої послідовності ознак для кожної виділеної групи експертів. Третій випадок є результатом або невдалої побудови анкети опитування з погляду набору альтернатив і кількості градацій шкали, або сильно вираженої неоднорідності та некомпетентності експертної групи. Можливий вплив і обох причин одночасно. Тоді переходять до більш детального дослідження відповідей за окремими альтернативами, і якщо ступінь варіації по окремих з

них різко відрізняється, то можливі два рішення: або переробити анкету опитування, або ранжирувати тільки ті альтернативи, по яких існує досить висока погодженість експертів.

ПРИКЛАД 5.3 [143] – *оцінювання відносної важливості п'яти параметрів.*

Ґрунтуючись на результатах колективної експертизи, вирішити статистичну задачу по оцінці відносної важливості п'яти параметрів. Первинна інформація наведена у таблиці, що подана нижче.

$$\overline{R_j} = \frac{1}{5}\sum_{j=1}^{5} R_j = \frac{150}{5} = 30.$$

Для визначення коефіцієнта конкордації W необхідно: за формулою (5.39) знайти d_j; за формулою (5.40) знайти S; за формулою (5.41) знайти T_i.

Експерти $(i=\overline{1,10})$	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	
Загал. ранг	2		5		1		4		3	

Значення d_j та d_j^2 подані у 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:

$$T_1 = 0;\ T_2 = (2^3 - 2) = 6;\ T_3 = (3^3 - 3) = 24;\ T_4 = (2^3 - 2) = 6;\ T_5 = (2^3 - 2) = 6;$$

$$T_6 = 0;\ T_7 = 0;\ T_8 = 0;\ T_9 = (2^3 - 2) = 6;\ T_{10} = 0;\quad \sum_{i=1}^{10} T_i = 48.$$

Коефіцієнт конкордації W обчислимо за формулою (5.42):

$$W = \frac{12 \cdot 551.5}{10^2 \cdot (5^2 - 5) - 10 \cdot 48} = \frac{6606}{11520} = 0.55.$$

Так як $n<7$, то оцінку значимості емпіричного коефіцієнта проведемо для критичних значень S (для коефіцієнта W). При рівні значимості $q=0.05$, $n=5$ та $m=10$, $S_{kp}=231.2$. Емпіричне значення $S=551.5$. Так як $S>S_{kp}$, то нульова гіпотеза $H_0: W=0$ відхиляється та із заданим рівнем значимості q приймається суттєвість значення $W=0.55$. Тобто узгодженість суджень експертів при оцінюванні відносної важливості параметрів є суттєвою.

ПРИКЛАД 5.4 [143] – *оцінювання відносної важливості восьми параметрів.*

Ґрунтуючись на результатах колективної експертизи, вирішити статистичну задачу по оцінюванню відносної важливості восьми параметрів.

Результати опитування п'яти експертів наведені у таблиці, що подана нижче. Показники зв'язаних рангів для кожного i-го експерта мають при цьому такі значення:

$$T_1=(2^3-2)=6;\ T_2=(2^3-2)+(2^3-2)=12;\ T_3=(2^3-2)=6;$$
$$T_4=(2^3-2)+(3^3-3)=30;\ T_5=(2^3-2)+(2^3-2)=12.$$

Експерти $(i=\overline{1,5})$	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	
Загал. ранг	2		4		1				3		7		8		6	
d_j	-13		-0.5		-15.5		2		-2.5		11		14		4.5	

Середнє значення рангів: $\overline{R_j}=\frac{1}{8}\cdot\sum_{j=1}^{8}R_j=\frac{180}{5}=22.5$. Сума квадратів d_j: $S=\sum_{j=1}^{8}d_j^2=757$. Коефіцієнт конкордації W обчислимо за формулою (5.43):

$W=\frac{12\cdot 757}{5^2\cdot(8^2-8)-5\cdot 66}=\frac{9084}{12300}=0.7$. Для оцінки емпіричного коефіцієнта $W=0.7$ висловимо нульову гіпотезу про відсутність погодженості суджень експертів $H_0: W=0$. Так як $n>7$, 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 $\chi_{q,\vartheta}^2$. При $q=0.1$ та $\vartheta=n-1=8-1=7$, $\chi_{10\%,7}^2=12$. Так як $\chi_R^2\geq\chi_{q,\vartheta}^2$, H_0 відхиляється й приймається гіпотеза H_1, яка свідчить про наявність погодженості думок експертів. Схема

алгоритму рішення статистичної задачі з оцінки відносної важливості параметрів за результатами колективної експертизи наведена на рис. 5.9.

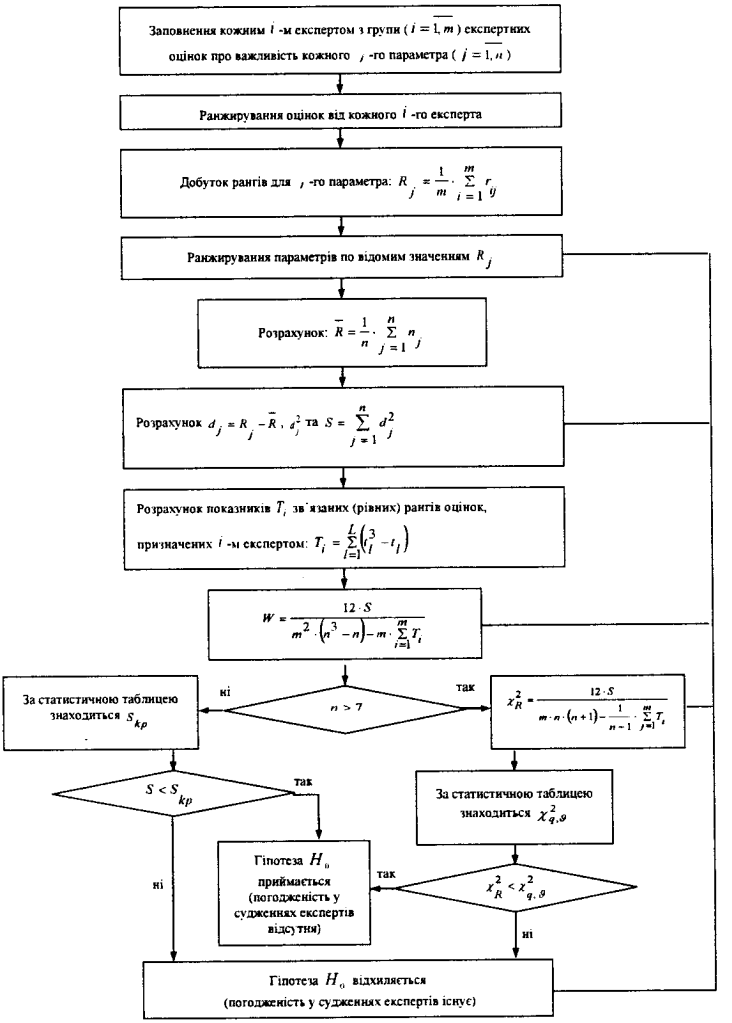


Рис. 5.9. Схема алгоритму рішення статистичної задачі з оцінки відносної важливості параметрів (при знаків, об'єктів, факторів, заходів тощо) за результатами колективної експертизи

Враховуючи викладене можна стверджувати, що застосування коефіцієнтів

варіації, парної рангової кореляції та конкордації сприятиме визначенню ступеня погодженості суджень експертів.

Приклад застосування соціоінженерних методів рішення проблем інформаційної кібербезпеки подано у Додатку Е.

Питання для самоконтролю

1. Назвіть характерні риси соціоінженерного підходу. Дайте визначення методам соціоінженерної діяльності: соціальній діагностиці, соціальному плануванню та прогнозуванню та іншим.

2. Що являє собою процедура тестування системи захисту на проникнення? У чому його сутність? Як класифікують тести на проникнення?

3. В чому полягає комплексний тест на проникнення? Дотримання яких технічних і соціоінженерних він вимагає?

4. На яких рівнях має проводитись тестування на проникнення? Розкрийте їх сутність

5. Що є логічним продовженням тесту на проникнення? Які завдання має вирішувати комплексна система управління рівнем захищеності?

6. Які заходи підлягають реалізації в процесі моніторингу захищеності периметра корпоративної мережі?

7. Що є метою розробки програми поінформованості? Які роботи мають бути виконані в процесі її реалізації?

8. Чим супроводжується впровадження системи управління ІБ?

9. Що слід розуміти під проведенням експертного оцінювання? Сформулюйте задачу експертного оцінювання та головні етапи її реалізації.

10. Розкрийте сутність головних етапів експертного оцінювання.

11. Розкрийте сутність формування експертної групи.

12. Назвіть відомі Вам методи оцінювання індивідуальної компетентності представників експертної групи. Стисло розкрийте їх сутність.

13. Які методи одержання експертної інформації евристичного походження Вам відомі? 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 Дельфи: 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. Які методи опрацювання інформації евристичного походження Вам відомі?

21. Метод парних порівнянь: призначення, приклади застосування.

22. Метод ранжирування: 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 проведення аналізу експертної інформації? Які показники ступеня погодженості суджень експертів Ви знаєте?

27. Розкрийте сутність коефіцієнтів варіації та парної рангової кореляції.

28. Розкрийте сутність коефіцієнта конкордації. Наведіть приклади його застосування.

ПІСЛЯМОВА

За результатами викладеними в підручнику можна зробити однозначний висновок – забезпечення інформаційної і кібербезпеки (ІКБ) складний, неперервний і багатогранний процес, реалізація якого обумовлюється соціумумом й залежить від кожної конкретної особистості в ньому. Він ґрунтується на необхідності формування виваженої державної політики у цій сфері та потребує значних зусиль усіх гілок влади, вітчизняної науки, керівників усіх рівнів. Водночас це не повинно гальмувати процеси формування національного інформаційного і кіберпросторів, які відповідали б інформаційно-інтелектуальному потенціалові держави та не перешкоджали входженню України до світового інформаційного суспільства як суб'єкта рівноправних міжнародних відносин. Зважаючи на це, стратегічним завданням державної політики щодо інформаційної і кібербезпеки має стати формування комплексної системи на основі науково обґрунтованих політичних, соціальних, економічних критеріїв та світового досвіду правового регулювання та організації забезпечення її функціонування.

В умовах стрімкого зростання рівня та значного розширення спектра стороннього кібернетичного впливу відсутність налагодженої і цілісної системи інформаційної і кібербезпеки може становити серйозну небезпеку міжнародній безпеці й призвести до втрати політичної незалежності будь-якою державою світу, у тому числі і Україною. Зважаючи на таке одним з найбільш ефективних засобів профілактики, протидії та боротьби з найрізноманітнішими кібернетичними втручаннями і загрозами, поступово перетворюючись з діяльності щодо своєчасного викриття ознак підготовки імовірного конкурента до нападу в діяльність, орієнтовану на досягнення та/або утримання над ним певної інформаційної переваги невдовзі стане саме розвідка ІТ систем. При цьому завдяки раціональному поєднанню чотирьох основних процедур – пошуку, збору, обробки та подання інформації в інтересах певних сил, найбільш дієвим і, можливо, найбільш потужним способом ведення розвідувальної діяльності у відкритих і відносно відкритих електронних джерелах на найближчу перспективу залишатиметься саме кіберрозвідка.

Зважаючи на простоту реалізації, відносну складність виявлення, незначні фінансові вкладення та мінімальний ризик провалу найбільш результативним методом кіберрозвідки, організованим з метою забезпечення доступу до будь-яких найзахищеніших ІР на відміну від SQL-ін'єкцій, застосування експлойтів, вірусів, переповнення буфера, DoS і DDoS-атак, бекдорів, руткітів та інших

методів проникнення й виведення систем з ладу і надалі вважатиметься метод соціальної інженерії (СІ). Застосовуючи його сумісно з деперсонофікованими центрами Internet-доступу, портативною ЕОТ, сертифікованими БД (БЗ) пошукових матеріалів і джерел інформації тощо, неавторизовані користувачі та підрозділи спеціального призначення матимуть можливість:

викривати ознаки підготовки протиборчих сторін до збройного нападу, визначати порядок їх ходів та очікувані виграші;

відстежувати всі етапи проходження інформації, що циркулює в ІТС;

уникати ускладнень у ході пошуку та оброблення інформації, а також її накопичення та зберігання тощо.

Враховуючи, що всі методи й техніки неавторизованих користувачів засновані насамперед на використанні слабостей людського фактора можно стверджувати, що типових засобів протидії атакам методом СІ нині, на жаль, не існує. Разом з тим наявність добре розробленої політики безпеки, застосування технологій, що взаємодоповнюють системи розпізнавання атак (IDS) та надають можливість відстежувати всі пакети, які проходять через мережевий інтерфейс, вивчення слабких місць прикладного ПЗ на підставі даних корпорацій CERT та Bugtrad (http://www.cert.com та http://www.securityfocus.com відповідно), а також дослідження спеціальних аналітичних додатків із застосуванням log-файлів операційних систем та мережевих log-файлів тощо дасть можливість співробітникам правильно реагувати на спроби змусити або переконати їх надати доступ до корпоративних ресурсів або розголосити інформацію, пов'язану із системою безпеки та максимально зменшити можливі наслідки від такого впливу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.: НАУ, 2013. – 432 с.
2. Гнатюк С.О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. // Безпека інформації. – 2013. – Том 19, № 2 (2013) – 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. – Том 19, №1. – 2013. – С. 40-45.
7. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Збірник наукових праць Військового інституту КНУ ім. Тараса Шевченка. – К. : ВІКНУ, 2011. – Вип. 30. – С. 159-165.
8. Словник термінів з кібербезпеки / За загальною редакцією Копана О.В., Скулиша Є.Д. – К. : ВБ «Аванпост-Прим». – 2012. – 214 с.
9. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства // Сучасна спеціальна техніка. – 2011. – № 3 (26). – 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'язка 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/main.cgi. – 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]. – 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. https://www.sugarsync.com/pf/D6870693_7400982_60553
28. Семенов Ю.А. Обзор по материалам ведущих фирм, работающих в сфере сетевой безопасности. [Електронний ресурс]. – 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. пр. : Вип. 4 (28). – К. : НАУ, 2009. – 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 / С.Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика) [Електронний ресурс]. – 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?», Proceedings of the 20th National Information Systems Security Conference, 1997, pp. 285-289.
39. Довгань О.Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хланъ // Інформаційна безпека людини, суспільства, держави – №3 (7), 2011. – 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 [Електронный ресурс] / Ukrainian Scientific Journal of Information Security, 2013, vol. 19, issue 2 128 Ю. Травников. – Режим доступа: 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 – №1 (3), 2010. – С. 26-30.
43. Малышенко Д.Г. Противодействие компьютерному терроризму – важнейшая задача современного общества и государства / Д.Г. Малышенко // ВНИИ МВД России, «Вестник РАЕН». – № 4 – Т. 3. – 2004.

44. Старостина Е. Терроризм и кибертерроризм – новая угроза международной безопасности [Электронный ресурс]. – Режим доступа : http://www.crime–research.ru/articles /starostina
45. Kerr K. Putting cyberterrorism into context [Electronic resource]. – URL : 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. : КИТ, 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. // Сборник научных трудов международной конференции "Информационные технологии и безопасность". Выпуск 3. – Киев: 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. [Електронний ресурс] / В.А. Мазуров. – 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 международной научно-практической конференции.. – Донецк.: ДЮИ ЛГУВД, 2007. – 352 с.
52. Евгений Касперский. Киберпреступность как бизнес. / Е. Касперский. [Електронний ресурс]. – Режим доступу: http://www.crime-research.ru/analytics/cybercrimes20101/2.
53. Бурячок В.Л., Шарий О.В. Кіберзлочинність і кібертероризм – загрози національній безпеці та інтересам України // 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., Бурячок В.Л. До питання захисту інформаційно-телекомунікаційної сфери від стороннього кібернетичного впливу // Наука і оборона. – 2010. – № 4. – С. 35–40.
56. Бурячок В.Л., Гулак Г.М., Хорошко В.О. Завдання, форми та способи ведення воєн у кібернетичному просторі // 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 // Захист інформації. – 2011. – № 3(52). – С. 19–27.
59. Бурячок В.Л., Гулак Г.М., Хорошко В.О. До питання організації та проведення розвідки у кібернетичному просторі // Наука і оборона. – 2011. – № 2. – С. 19–23.
60. Бурячок В.Л., Корченко О.Г., Бурячок Л.В. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем // 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., Бурячок Л.В., Костюк Т.Я. Обґрунтування вибору раціональної системи електронного документообігу для державних структур спеціального призначення // Вісник воєнної розвідки. – № 24. – 2011. – С. 67–74
64. Е.А.Гвильдис. Человеческий фактор в проблеме обеспечения информационной безопасности компании. Сборник научных трудов «Защита информации». – К.: НАУ, 2007. – С. 166–171
65. Www.kommersant.ru. Материалы семинара "Современные технологии управления".
66. А. Маслоу. Маслоу о менеджменте. Изд. Питер, Санкт-Питербург-2003, -416с.
67. Www.bezpeka.desant.com.ua. Е.И. Гаврюшин. Человеческий фактор в обеспечении безопасности конфиденциальной информации.
68. Андрей Мирошниченко. Зарплата и пустота. Банковское обозрение, №10(88), 2006.
69. Бондаренко Е. Социальные сети как инструмент развития: виды и возможности- http://www.trainings.ru/library/articles/?id=10067
70. Все социальные сети развиваются по графику - http://www.soobshestva.ru/news/?p=233
71. Гуц А.К. и др. 1. Социальные системы. Формализация и компьютерное моделирование. Уч. пос. – Омск. Омск. Гос. Ун-т, 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 – http://www.soobshestva.ru/news/?p=243
74. Эйдман И.В. Свободный человек в мире социальных сетей. Каким будет новое глобальное интернет-общество - http://www.vremya.ru/2008/22/4/197454.html
75. International Network for Social Network Analysis - http://www.insna.org/
76. Каталог русских web 2.0 сайтов, социальных сетей и сервисов - Catalogr.ru
77. Максим Кутик. Две трети украинских компаний видят в социальных сетях угрозу IT-безопасности. 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.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «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.-корр. РАН Д.А.Новикова. – М.: Изд-во физ.-мат.литер., 2010. – 228 с.
80. Офіційний сайт Trenfrr http://www.trendrr.com/ 16.12.2009
81. Офіційний сайт Trackur http://www.trackur.com/ 16.12.2009
82. Офіційний сайт SentimentMetrics http://www.sentimentmetrics.com/ 16.12.2009
83. Цвиркун А. Д. Основы синтеза структуры сложных систем. – М.: Наука, 1982. – 200 с.
84. Краснощеков П.С., Петров А.А., Федоров В.В. Информатика и проектирование. – М.: Знание, 1986. – 48 с. (сер. "Математика, кибернетика" № 10).
85. Советов Б.Я., Яковлев С.А. Моделирование систем. – М.: Высш. шк., 1985. – 217 с.
86. Бусленко Н.П. Моделирование сложных систем. – М.: Наука, 1978. – 399 с.
87. Дружинин В.В., Контуров Д.С. Проблемы системологии. – М.: Сов. радио, 1976. – 296 с.
88. Клиланд Д., Кинг В. Системный анализ и целевое управление. Пер. с англ. – М.: Сов. радио, 1974. – 280 с. с ил.
89. Радвик Б. Военное планирование и анализ систем. – М.: Воениздат, 1972. – 478 с.
90. Моисеев Н.Н. Математические задачи системного анализа. Изд. 2. – М.: Наука, 2012. – 488 с.
91. Громов Ю.Ю., Земской Н.А., Лагутин А.В., Иванова О.Г., Тютюнник В.М. Системный анализ в информационных технологиях: Учеб. пособие. – Тамбов: Изд-во Тамб. гос.техн. ун-та, 2004. – 176 с.

92. Романов А.И. Основы теории телекоммуникационных сетей: учебное пособие для вузов. / А.И. Романов. – К.: ВІТІ НТУУ "КПІ", 2002. – 157 с.
93. Пятибратов А.П. Вычислительные машины, сети и телекоммуникационные системы: Учебно-методический 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. НУ "Львівська політехніка", 2004. – 220 с.
98. Козиол Дж. Искусство взлома и защиты систем. / Дж. Козиол, Д. Личфилд, Д. Эйтэл, К. Энли и др. // .– СПб: Питер, 2006. – 416 с: ил.
99. М. Кузнецов. Социальная инженерия и социальные хакеры. / М. Кузнецов, И. Симдянов. // – Петербург: БХВ-Петербург, 2007. – 368 с.
100. Мошенничество с помощью фарминга: перенаправление на фальшивые сайты http://www.microsoft.com/rus/athome/security/privacy/pharming.mspx
101. В. Бычек. Социальная инженерия в интеллектуальной битве "добра" и "зла". / В. Бычек, Е. Єршова // [Електронний ресурс]. – 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. Крис Касперски. Секретное оружие социальной инженерии. [Електронний ресурс]. – 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:
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" http://www.iz-news.ru/news/317/
109. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320с.
110. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб: БХВ- Петербург, 2003. – 752 с.
111. Чириль Дж. Защита от хакеров (+CO). – СПб.: Питер, 2002. – 480с.
112. Мак-Клар Стюард, Спенбреб Джоел, Курц Джордж. Секреты хакеров. Безопасность сетей - готовые решения. – 4-е изд.: Пер. с англ. – М.: Изд. дом «Вильямс», 2004. – 656 с.
113. Коул Ерик. Руководство по защите от хакеров: Пер. с англ. – М.: Изд. дом «Вильямс». 2002. – 640с.
114. Бабок В. П., Корченко О. Г. Інформаційна безпека та сучасні мережеві технології. Англ.-укр. рос. слов, термінів. – К.: НАУ, 2003. – 670 с
115. Kevin U. Mitnik, William L. Simon, Steve Wozniak,. The Art Of Deception: Wiley, 2002. – 304 с.
116. Корченко А. Г. Несанкционированный доступ к компьютерным системам и методы защиты: Учеб. пособие. – К.: КМУГА, 1998. – 116 с.
117. Robert B. Cialdini. The Science of Persuasion II Scientific American Magazine. – 2001, №2. – P.76-81.
118. И. Н. Кузнецов Информация: сбор, защита, анализ. Учебник по информационно-аналитической работе. – М.: ООО Изд. Яуза, 2001. – 100с.
119. О.Г. Корченко О.Г.Паціра Є.В., Пуха Д.А. Класифікація методів соціального інжинірингу / Корченко О.Г., Паціра Є.В., Пуха Д.А. // Захист інформації. – К.: НАУ. – 2017. – №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 [Электронный ресурс] : <http://www.docflow.ru/news/analytics/detail.php?ID=1526> (15.04.2011).

125. Лукацкий А. В. Инженеры человеческих душ [Электронный ресурс]: < http://citforum.ru/internet/securities/soc_eng.shtml> (29.11.12).
126. How to Protect Insiders from Social Engineering Threats http://www.microsoft.com/downloads/details.aspx?FamilyID=05033e55-aa96-4d49-8f57-c47664107938&DisplayLang=en
127. Краткое описание атак с использованием социальной инженерии. 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 «Лаборатории Касперского» http://www.securelist.com/ru/
133. Защита пользователей от социальной инженерии. http://stud-baza.ru/sotsialnaya-injeneriya-vidyi-printsipyi-zaschita-doklad-kompyuternyie-seti
134. Тесты на проникновение. http://www.ptsecurity.ru/services/pen/
135. Лепихин Владимир Борисович. Сравнительный анализ сканеров безопасности. Часть 1: тест на проникновение (краткое резюме). http://www.itshop.ru/Sravnitelnyy-analiz-skanerov-bezopasnosti-Chast-1-test-na-proniknovenie-kratkoe-rezyume/l9i22670
136. Андрей Соколов. Тестирование на проникновение: инструментальный анализ уязвимостей или имитация действий злоумышленника? http://www.nobunkum.ru/ru/pentest
137. А. Дорофеев. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? http://www.npo-echelon.ru/doc/inside-dorofeev.pdf
138. Андрей Соколов. Тесты на проникновение повысят интерес топ-менеджмента к ИБ. http://www.cnews.ru/reviews/free/security2009/articles/pentest.shtml
139. Виктор Сердюк. Тест на проникновение как эффективный инструмент для оценки реальной защищенности банка от внешних угроз. http://www.abajour.ru/files/Serduk_04-2010.pdf
140. Райхман Э.П., Азгальдов Г.Г. Экспертные методы в оценке качества товаров. – М.: Экономика, 1974. – 151 с.
141. Саати Т., Кернс К. Аналитическое планирование. Организация систем. //Пер с англ. Под ред. И.А.Ушакова. – М.: Радио и связь, 1991. – 224с.

142. Комаринський Я., Яремчук І. Фінансово– інвестиційний аналіз. Навч. посібник. – К. Українська енциклопедія. – 1996. – 298 с.
143. Бурячок В.Л. Технологія прийняття рішень у складних соціотехнічних системах: Монографія. / В.Л. Бурячок, В.О. Хорошко. / Під заг. ред. докт. техн. наук, проф.В.О. Хорошка. – К.:ДУІКТ, 2012. – 344 с.
144. Добров. Г.И., Ершов Ю.А., Левин Е.И., Смирнов Л.П. Экспертные оценки в научно-техническом прогнозировании / Под общ. ред. В.С.Михалевича. – К.: Наукова думка, 1974. – 160 с.
145. Бешелев С.Д., Гурвич Ф.Г. Математико-статистические методы экспертных оценок. – М.: Статистика, 1980. – 263 с.
146. Д. Элти, М. Кумбс. Экспертные системы: концепции и примеры. – М.: Финансы и статистика, 1987. – 191 с.
147. Херес-Рот Ф., Уотерман Д., Ленан Д. Построение экспертных систем: Пер. с англ. /Под ред. Ф.Хейес-Рота. – М.: Мир, 1987. – 441 с.
148. Евланов Л.С., Кутузова В.А. Экспертные оценки в управлении. – М.: Экономика, 1978. – 133 с.
149. Самохвалов Ю.Я. Экспертное оценивание. Методический аспект. / Ю.Я. Самохвалов, Е.М. Науменко. – К.: ДУІКТ, 2007. – 263 с.
150. Литвак Б.Г. Экспертная информация. Методы получения и анализа. – М.: Радио и связь, 1982. – 184 с.
151. Китаев Н.Н. Групповые экспертные оценки. – 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. А. П. Частиков, Д. Л. Белов, Т. А. Гаврилова. Разработка экспертных систем. Среда CLIPS. – М.: BHV, 2003. – 608 с.
154. Уотермен Д. Руководство по экспертным системам. // Пер. с англ. под ред. В. Л. Стефанюка. – М.: Мир, 1989. – 388 с.
155. Дэвид Г. Метод парных сравнений. //Пер. с англ. Н. Космарской и Д. Шмерлинга. – М.: Статистика, 1978. – 144 с.
156. Раушенбах Г.В., Филиппов О.В. Экспертные оценки в медицине. Научный обзор. – М.: ВНИИММТИ Минздрава СССР, 1983. – 80 с.
157. Руа Б. Классификация и выбор при наличии нескольких критериев. //Вопросы анализа и принятия решений. – М.: Мир, 1976. – С. 80–107.
158. Гафт М.Г. Принятие решений при многих критериях. – М.: Знание, 1979. – 64 с.
159. Герасимов Б.М., Тарасов В.О., Токарев І.В. Людино–машинні системи прийняття рішень з елементами штучного інтелекту. – К.: Наукова думка, 1993. – 184 с.

160. Гмошинский В.Г., Флиорент Г.И. Теоретические основы инженерного прогнозирования. – 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. / Сборник трудов. – Вып.14. – М.: ВНИИСИ, 1986. – 124 с.
163. Бурячок В.Л., Мітрахович М.М., Луханін М.І. Методичні аспекти експертного аналізу зразків техніки у прогнозуванні їх використання та розвитку / М.М. Мітрахович, В.Л. Бурячок, М.І. Луханін. – К.: Наука і оборона, 2002. Вип №4. – С. 36–41.
164. Кендал М. Ранговые корреляции. // Пер с англ. под. ред. Е.М.Четыркина и Р.М.Энтона. – М.: Статистика, 1975. – 213с.
165. Кенуй М.Г. Быстрые статистические вычисления // Пер с англ. – М.: статистика, 1979. – 69 с.
166. Осипов В.П., Осипов Н.В., Рубцов В.С., Радковец Ю.И. Справочник по методам решения статистических задач. – К.: КВИРТУ ПВО, 1989. – 132 с.
167. Нечаев А.Н., Осипов В.П., Осипов Н.В., Рубцов В.С., Ручки В.А., Ермаков И.Г., Радковец Ю.И., Марков К.В. Оперативно-информационная подготовка: Комплекс программ решения статистических задач по результатам качественных измерений. Методические рекомендации // Под ред. докт. ф-м 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 кибер– учения. [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. докт. техн. наук, проф. В.О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.

180. Бурячок В.Л. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно-телекомунікаційних систем // 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. / В.С. Василенко, О.С. Бордюк, С.М. Полянський. [Електронний ресурс]. – 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 for the 44th Presidency, December 2008, at 11.
185. В.Иванов. 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. Н.Димлевич. Информационные войны в киберпространстве – США. [Електронний ресурс]. – Режим доступу: http://www.otechestvo.org.ua/main/201011/1520.htm, 15.11.10
187. William J. Lynn III W. Defending a New Domain: The Pentagon's Cyberstrategy.// 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. Николай Димлевич. 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 кибертерроризму в современных условиях. / В.А. Голубев. [Електронний ресурс]. – 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]. – Режим доступу: http://www.crime-research.ru/news/2004.10.21/1547
194. Николай Димлевич. Об использовании информационного оружия в киберпространстве. [Електронний ресурс]. – 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

Враховуючи низку об'єктивних та суб'єктивних факторів можливо зі стовідсотковою впевненістю стверджувати, що на сьогодні найбільш досконала система кіберзахисту **критично важливої інфраструктури** (частини інформаційної та/або кіберінфраструктури, ураження або знищення яких може привести до втрати інформаційним і кіберпросторами працездатності й поставити під загрозу суспільну і державну безпеку в цілому) функціонує у США. Національна політика країни у цій сфері формується Агентством національної безпеки (АНБ), а найважливіші стратегічні питання вирішуються, як правило, на рівні Ради національної та внутрішньої безпеки країни. Відповідні рішення оформляються у вигляді директив Президента. При цьому **під предметом кібернетичного захисту АНБ**, виходячи з визначення, перш за все **розуміє забезпечення конфіденційності, цілісності та доступності інформації, що циркулює в інформаційно-телекомунікаційних системах**.

Вперше питанням кіберзахисту приділив увагу Президент США Б.Клінтон. У липні 1996 року він зокрема оголосив про формування Президентської комісії із захисту критичних інфраструктур (*PCCIP*). У заключному звіті, виданому в жовтні 1997 року, комісія повідомила, що на сьогодні "... загрози критичним інфраструктурам реальні. ...Через взаємозв'язок і взаємозалежність вони можуть бути уразливі для 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 декількох хвилин або й навіть секунд без можливості ідентифікувати нападаючого або встановити його місце розташування ...". Рекомендації *PCCIP* призвели до видання Директиви Президента № 63 (*PDD-63*, червень 1998 року), якою були створені: Національний центр захисту інфраструктур (*NIPC*), Офіс безпеки критичних інфраструктур (*CIAO*), Національна рада захисту інфраструктур (*NIAC*) та приватні Центри розподілу і оцінки інформації (*ISACs*). В подальшому, а саме 24 вересня 1999 року, з метою просування по шляху вдосконалювання прийомів і методів роботи з доказами комп'ютерних злочинів, у США була відкрита Комп'ютерна

судова лабораторія Міністерства оборони (*Defense Computer Forensics Laboratory, DCFL*). Її робота була спрямована перш за все на обробку комп'ютерних доказів злочинів і шахрайств, а також проведення контр-розвідувальних заходів для всіх організацій, що здійснюють протикримінальні та контр-розвідувальні дослідження. При цьому в якості Виконавчого агентства для *DCFL* було визначене управління спеціальних досліджень ВПС США. На сьогодні в позитивний баланс лабораторії можна віднести вдалий захист і подальше розслідування наслідків атак на національні мережі США, відомих як: "Сонячний схід" ("*Solar Sunrise*"), "Цифровий демон" ("*Digital Demon*") та "Місячний лабіринт" ("*Moonlight Maze*").

У січні 2001 року Радою національної та внутрішньої безпеки США був прийнятий "Національний план захисту інформаційних систем". Окрім цього 13 вересня 2001 року Сенат США не тільки схвалив законопроект "*Combating Terrorism Act of 2001*", що дозволив застосування Федеральним бюро розслідувань військової системи тотального спостереження *Carnivore* (також відома, як *DCS1000*), але й збільшив асигнування на її розвиток.

У 2002 році Пентагон надав одному з найбільших науково-дослідних установ США (університету "*Carnegie Mellon*") 35,5 мільйона доларів на проведення досліджень в галузі боротьби з кібертероризмом. П'ятирічний грант передбачав розвиток ідентифікаційних технологій, покликаних відгородити користувачів *Internet* від несанкціонованого доступу до їхніх конфіденційних даних. Протягом 2003–2006 років США в галузі безпеки було прийнято чотири національних стратегії (рис. А.1), що фактично визначили розвиток ситуації у світі на початку XXI століття.

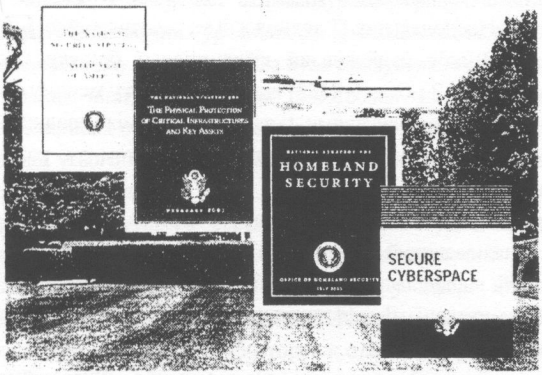


Рис. А.1. Чотири національних стратегії США, прийнятих у 2002 – 2003 роках: "Стратегія Національної безпеки", "Національна стратегія з фізичного захисту критичної інфраструктури і об'єктів національного статку", "Стратегія внутрішньої безпеки" та "Національна стратегія захисту кіберпростору"

У відповідності з ними були намічені такі основополагаючі принципи:

кіберпростір мав бути визнаним таким же простором війни, як море, суша і повітря;

кібероборона має вийти за рамки воєнних кібервідділів і розповсюдитись на комерційні мережі, згідно задачам забезпечення національної безпеки;

кібероборона має вестись разом з міжнародними союзниками для ефективного попередження загрози тощо.

При цьому в "Національній стратегії з фізичного захисту критичної інфраструктури і об'єктів національного статку" (2003) сформульовані цілі і принципи забезпечення національної інфраструктури США, а також визначені умови об'єднання зусиль різних державних і комерційних структур з підвищення ступеня їх захищеності. "Національна стратегія захисту кіберпростору" (2003) охоплює область забезпечення захисту технічних і програмних засобів, об'єднаних у комп'ютерні мережі, а також систем вирішення задач управління та інформаційного забезпечення на різних рівнях державних, суспільних і приватних структур, у тому числі в різних сферах національної економіки. Головна мета цієї стратегії – попередження кібератак проти об'єктів критичної інфраструктури, зменшення їх ефективності, а також максимальне скорочення періоду ліквідації наслідків нападів на комп'ютерні мережі. "Національна військова стратегія з проведення кібероперацій" (2006) визначає основні напрями і сфери дій кіберспільноти США у кіберпросторі. З метою кращого 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) був сформований Відділ національної кібернетичної безпеки (*National Cyber Security Division, NCSD*). З моменту [183] відкриття відділ у тісному співробітництві з урядом, промисловістю, науковими установами та міжнародним товариством зробив кібернетичну безпеку національним пріоритетом та розробив основні принципи її створення, що ґрунтуються на:

1) подальшому розвитку кіберпростору (особлива увага при цьому має бути приділена вдосконалюванню й розширенню широкополосних мереж);

2) розподілі відповідальності за кібербезпеку, налагодженні більш тісної взаємодії в цьому питанні між федеральними відомствами, місцевою владою й приватним бізнесом;

3) заохоченні та фінансуванні впровадження інноваційних розробок, зокрема продовженні вдосконалення створюваних у Міністерстві внутрішньої безпеки програмних продуктів під умовною назвою *Einstein-2* та *Einstein-3*,

призначених для ідентифікації, реєстрації, блокування й знищення шкідливих кодів у точках мережного доступу;

4) координованості та ефективності розподілу інформації тощо.

При цьому, наприклад, у рамках проекту *Einstein-2* Міністерство внутрішньої безпеки впроваджує сигнатурні сенсори, здатні у реальному масштабі часу контролювати вхідний *Internet* трафік американського уряду на предмет виявлення спроб несанкціонованого доступу до нього й пошуку зловмисного контента. Проект *Einstein-3* фактично можна вважати системою динамічної оборони, що запобігає вторгненню й знижує уразливість відомчого кіберпростору. Його метою є посилення ключових функцій захисту відомчих інформаційних систем, а саме – ідентифікації і аналізу зловмисного мережного трафіку, підвищення рівня поінформованості про складну ситуацію й автоматичне реагування на кіберзагрози до виникнення значимого результату. Фактично проект покликаний підтримувати вдосконалений інформаційний обмін з усіма федеральними відомствами, даючи можливість автоматичного оповіщення про виявлені спроби вторгненнях у мережі. При цьому обмін інформацією про кібератаки буде здійснюватися відповідно до закону й для запобігання можливих порушень конфіденційності і прав громадян США буде охоплювати тільки діяльність, пов'язану із забезпеченням внутрішньої безпеки, розвідкою та обороною.

У січні 2008 року на підставі директив №54 та №23 директорів Департаментів національної і внутрішньої безпеки США (відповідно) була утворена надзвичайна ініціатива з питань національної кібернетичної безпеки (*Comprehensive National Cybersecurity Initiative, CNCI*), яка формалізувала серію постійних кроків для подальшого захисту федеральних урядових систем США від кібернетичних нападів і загроз. На національному рівні ініціатива була сфокусована на:

встановленні лінії захисту для зменшення наявних уразливостей та попередження можливих вторгнень і нападів;

захисті від усього спектру загроз із використанням розвідки та посилення безпеки системи постачання;

формуванні майбутнього середовища шляхом удосконалення наукових досліджень і розробок, освіти та інвестицій у передові технології.

Не менш активною стала політика США у сфері кібербезпеки й за Адміністрації Б.Обами. Наприкінці травня 2009 року президент США заявив про свій намір розглядати безпеку кіберпростору як одну з пріоритетних проблем його Адміністрації. До низки найефективніших кроків останньої у цьому напрямку доцільно віднести такі головні заходи:

1) збільшення держзамовлення на розробку нових засобів ведення війни та нових, більш захищених, військових мереж;

2) оприлюднення 29.05.2009 року "Огляду політики кібербезпеки" (*Cyberspace Policy Review*) – комплексного документу, що визначив основні пріоритети нової команди у сфері кібербезпеки та окреслив контури майбутньої "Стратегії національної безпеки" США в цьому напрямку [184]. У проекті стратегії кіберзагрозам було вперше відведено окреме місце у загальній структурі загроз Сполученим Штатам й визначені основні принципи побудови комплексної системи кібербезпеки держави, що мають базуватися на: створенні умов для подальшого розвитку кіберпростору; розподілі відповідальності за кібербезпеку; створенні ефективної зкоординованої системи розподілу інформації та реагування на інциденти; впровадженні нових інноваційних розробок; вдосконаленні підготовки фахівців з кібербезпеки тощо. На підставі "Огляду політики кібербезпеки" (підготовлена апаратом Білого дому в кооперації з комісією з питань кібербезпеки Центру стратегічних і міжнародних досліджень) Президентом США було прийняте рішення про створення у Білому домі Відділу з кібербезпеки та про формування в МО США спеціального військового підрозділу – Кіберкомандування, головними завданнями якого мали стати захист від *Internet*-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].

Довідково: У структурі Стратегічного командування США (*USSTRATCOM*) Об'єднане Кіберкомандування підпорядковується директору АНБ генералу К. Александеру й має власну штаб-квартиру у Форт-Міді, штат Меріленд. Приблизна чисельність структури – 30 000 військових. Її основне призначення – захист військової частини кіберпростору, тобто домену *.mil* й одночасна підтримка доменів "*.gov*" та "*.com*". Початок повномасштабного функціонування нового підрозділу планується на жовтень 2010 року.

У безпосереднє підпорядкування *USCYBERCOM* увійшли:

а) кіберкомандування військово-морських сил США *Fleet Cyber Command* (*FLTCYBERCOM*), створене на базі Військово-морської розвідки й Управління по зв'язку та комп'ютерним мережам, у яке були передані 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* покладене здійснення мережних та інформаційних операцій, радіотехнічної розвідки (*SIGINT*), радіоелектронної боротьби (*Electronic Warfare*), а також забезпечення працездатності сегменту комп'ютерної мережі МО США *Global Information Grid* (*GIG*), що знаходиться у сфері відповідальності военно-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 в складі Управління по операціях, боєздатності й мобілізації (*Directorate of Operations, Readiness and Mobilization, DORM*). На *ACTF* покладені завдання з об'єднання зусиль штабу СВ щодо управління інформаційними системами, розробки політики здійснення операцій у кіберпросторі, а також затвердження вимог та 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, який включений до складу Ради національної та внутрішньої безпеки країни, а також проектів нормативних документів, що спрямовані на покращення взаємодії в сфері кібербезпеки союзниками США та убезпечення власного *Internet* простору в разі виникнення ситуацій, що загрожують національній безпеці. Так, наприклад, з метою законодавчого забезпечення зазначеної діяльності Конгресом США був розроблений новий законопроект "Кібернетична безпека 2009", який встановлював стандарти кібернетичної безпеки та визначив завдання і обов'язки урядових та приватних організацій, що мають здійснювати контроль за функціонуванням об'єктів критично важливої інфраструктури;

6) оголошення про додаткові заходи із посилення внутрішньої кібербезпеки. Так, наприклад, з 1 жовтня 2009 року адміністрація Б.Обами дала старт програмі з укомплектування Департаменту національної безпеки новими співробітниками, які займатимуться забезпеченням безпеки високотехнологічних систем у США. За офіційним даними, протягом майбутніх трьох років у кібервійська при спеціальному кібербезпековому Департаменті управління національної безпеки (*Department of Homeland Security*) буде прийнято близько 1 000 чоловік. При цьому майже всі вакансії планується укомплектувати професійними програмістами, IT аналітиками та інженерами, що мають досвід розслідування зломів і відстеження хакерських атак та які займатимуться виключно безпекою високотехнологічних систем США. Разом з тим адміністрація Б.Обами схильна визнати, що навіть 1000 нових співробітників не повністю відповідає потребам США у фахівцях з кібербезпеки. Враховуючи таке у супровідному документі до спеціально організованих урядом США змагань "Кіберзмагання США" (*U.S. Cyber Challenge*) наводиться думка одного з експертів, що реальна потреба уряду в таких фахівцях становить на сьогодні приблизно від 10 000 до 30 000 співробітників;

7) завершення, відповідно до затвердженої концепції *Air Force Mission Statement*, формування у структурі 8-ї повітряної армії ВПС США у жовтні 2009 року нового командування - *Air Force Cyber Operations Command* (*AFCOC*). Основними цілями підрозділу є забезпечення безпеки військових мереж зв'язку та автоматизованих інформаційних систем підприємств національного військово-промислового комплексу і організацій, що працюють за контрактом з МО США, а також керівництво інформаційними операціями в кіберпросторі.

Довідково: На *AFCOC* покладені такі головні функції:

розпізнавання й запобігання кібератакам, спрямованим на військові та цивільні інформаційні мережі, що відносяться до критично важливих елементів інформаційної інфраструктури США;

здійснення з метою здобуття переваги над супротивником інформаційних операцій під час бойових дій у глобальному масштабі й на конкретних театрах воєнних дій (ТВД);

своєчасне вживання відповідних заходів і відновлення нормального функціонування власних інформаційних мереж;

безперервне відстеження ситуації в кіберпросторі та виконання 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 міжмережевого захисту; шифрування інформації, що зберігається в базах даних; оснащення автоматизованих інформаційних систем електронікою, стійкої до електромагнітних імпульсів) операцій;

забезпечення цілісності мережної інфраструктури (залучення мереж, що самоорганізуються та бездротової передачі даних; проведення перевірок електронних компонентів радіоапаратури; застосування захищених комп'ютерних мереж);

8) початок реалізації у січні 2010 року управлінням перспективних досліджень Пентагона (ДАРПА) програми "Національний кіберполігон" [183]. Її метою є створення до 2015 року центра щодо запобігання кібератак, устаткування й програмне забезпечення якого мають дозволити моделювати масштабні акції проти американських інформаційних і телекомунікаційних мереж, навчати співробітників діям по їхній нейтралізації, а також проектувати системи захисту інформаційних ресурсів. До роботи над даним проектом залучені компанія "Локхід-Мартін" та університет Дж.Хопкінса. Одночасно в інтересах МО США активізована діяльність корпорації *SAIC*, яка здійснює створення методик і програмних засобів ведення наступальних (атакуючих) дій у кіберпросторі, а також корпорації *Boeing*, яка проводить наукові та науково-дослідні роботи із створення в інтересах ВПС США систем моніторингу. Останньою розробляється дослідний варіант системи, що матиме сервісно-орієнтовану архітектуру та буде здатна оптимізувати управління кібернетичними ресурсами шляхом автоматизації попередження про загрозу кібератак та прийняття заходів щодо їх нейтралізації;

9) початок створення у середині 2010 року на авіабазі Лакленд (штат Техас) першого спеціалізованого кібернетичного розвідувального центру на 400 осіб. Структурною частиною кіброзвідцентру стали 68-а ескадрилья мережних операцій (68-th *Network Warfare Squadron*) та 710-а ланка інформаційних операцій (710-th *Information Operations Flight*). Поряд з ним розташоване також 67-е мережне крило космічного командування ВПС, розвідуправління ВПС, техаський крипто логічний центр АНБ, об'єднане командування інформаційних операцій, група криптологічної підтримки ВПС тощо;

10) оприлюднення нової "Стратегії національної безпеки" (2010), в якій вперше у загальній структурі загроз США окреме місце відведене саме кіберзагрозам, а також "Міжнародної стратегії для кіберпростору" ("*International Strategy for Cyberspace*") як цілісне бачення урядом США найближчого майбутнього у розвитку кіберпростору;

11) прийняття нової доктрини кібербезпеки. Про її спрямованість можна судити з опублікованої у вересні 2010 року програмної статті заступника глави Пентагона Вільяма Лінна III із символічною назвою "Захищаючи новий простір". Головна думка статті: відтепер США будуть вважати кіберпростір таким же потенційним полем бою, як сушу, море й повітря [187]. Підтвердженням цьому стало публічне оголошення Вільямом Лінном III на конференції *Virus Bulletin* 2010, що проходила у Ванкувері (Канада), п'яти принципів на яких базуватиметься нова стратегія кібербезпеки США у перспективі, а саме:

визнання кіберпростору новою зоною воєнних дій;

захист цивільної інфраструктури;

застосування заходів колективної оборони;

переформатування пасивної оборонної концепції в активну (використання та своєчасне оновлення антивірусних програм, вдосконалення засобів захисту, застосовування детекторів вторгнення та програм моніторингу безпеки дасть можливість відбити біля 80% кібернападів. Для відбиття інших 20% необхідні інструменти, здатні не тільки виявляти, а й блокувати злоякісні коди);

розробка нових програмних продуктів безпекового спрямування.

Нині, за свідченням *New York Times* адміністрація президента США працює над створенням, по-перше, незалежних і автономних систем мобільного зв'язку в інших країнах світу й, по-друге, тіньових схем *Internet* – так званого компактного *Internet* у валізі, який можна було б без зайвих зусиль розгорнути на території іншої країни, швидко налагодити й установити безпровідний зв'язок на достатньо великій за площиною території.

У питаннях забезпечення загальної безпеки та оборони НАТО керується Стратегічною концепцією, прийнятою на Вашингтонському, ювілейному саміті у квітні 1999 року [188, 189]. Її головні принципи полягають у забезпеченні:

стабільності середовища безпеки Євроатлантичного регіону;

розвитку демократичних інститутів;

мирного улагодження конфліктів;

створення трансатлантичного форуму консультацій щодо життєвих спільних інтересів та мобільності у прийнятті рішень;

спрямування політики безпеки на стримування і оборону;

партнерства та розвитку відповідних широкомасштабних програм;

посилення прозорості взаємної довіри і спроможності діяти спільно.

У системі забезпечення кіберзахисту, в тому числі й захисту від тероризму Альянс керується рішеннями відповідної технічної Програми (так званого "Празького пакету"), прийнятої 21–22 листопада 2002 року главами держав і урядів

НАТО на зустрічі у верхах в Празі. Нею передбачено три етапи практичної діяльності країн-членів. Перший етап містив у собі створення нині функціонуючого Координаційного центра НАТО по реагуванню на комп'ютерні інциденти (КЦНРКІ) і забезпечення його тимчасової робочої конфігурації. Другий етап полягав у забезпеченні повної готовності КЦНРКІ. Третій етап передбачав проведення низки заходів з інтеграції досвіду, засвоєного на першому і другому етапах та використанні новітніх методів кіберзахисту для зміцнення потенціалу НАТО у цій царині. У 2006 році голови урядів та держав під час Ризького саміту (Латвія) на додачу до вже існуючих документів дали завдання Раді НАТО впровадити захист інформаційних систем Альянсу проти кібератак. Ухвалюючи Комплексні політичні настанови вони визнали, що "... тероризм, а також розповсюдження зброї масового знищення, вірогідно будуть головними загрозами Альянсу протягом наступних 10 – 15 років ...". У січні 2008 року Радою НАТО було ухвалено стратегію кіберзахисту, спрямовану на забезпечення ефективного і результативного протистояння Альянсу кіберагресії. Вона містить вказівки цивільним і військовим установам НАТО, спрямовані на вироблення спільного і узгодженого підходу, а також рекомендації країнам-членам щодо захисту їх національних систем. У квітні того ж року (на Бухарестському саміті НАТО) керівництвом Альянсу були схвалені концептуальні документи "Політика Північноатлантичного Союзу в сфері кібернетичного захисту", який передбачає об'єднання національних та колективних зусиль і ресурсів у згаданій сфері та "Настанова Північноатлантичної Ради щодо співробітництва у сфері кібернетичного захисту з державами-партнерами та міжнародними організаціями", а також створене Керівне відомство з кіберзахисту, яке уповноважене приймати певні рішення з цих питань. На листопадовому саміті Альянсу було вирішено розробити "План дій в області кібероборони". Документ повинен бути підготовлений до квітня, а підписаний у червні поточного 2011 року. Важливе місце в ньому буде відведено створенню центра НАТО по реагуванню на кіберінциденти. В рамках практичної реалізації наведеного підходу був створений підрозділ НАТО Швидкого кіберреагування, а також спільними зусиллями семи країн-членів НАТО (Естонії, Німеччини, Італії, Латвії, Литви, Словаччини та Іспанії – країн-донорів) та командування об'єднаних збройних сил НАТО з питань трансформації (в особі керівника групи трансформації генерала Кофмана), у травні 2008 року був підписаний документ про формальне заснування Центру координації зусиль з питань кіберзахисту (далі – Центр або інакше К-5) зі штаб-квартирою у м. Таллінн (Естонія). У цей час штат співробітників Центру складається з 30 фахівців (як військовослужбовців, так і цивільних осіб) – представників країн-донорів. Керує Центром організаційний комітет учасників, на який покладені завдання щодо:

оцінки та затвердження програми роботи Центру;

залучення країн-членів НАТО до боротьби з кібертероризмом;

організації взаємодії з іншими країнами;

збору, аналізу та збереження даних про кібератаки;

інформування про кібератаки та методи захисту від них тощо.

Центр проводить дослідження та тренінги з питань захисту інформації і протидії кібертероризму. В кожній з країн-донорів для забезпечення цих потреб розгорнуті власні центри комп'ютерного реагування. Центр не є структурою НАТО й не фінансується за рахунок країн Альянсу. Потенціальними спонсорами Центру є Турція, Сполучені Штати Америки (з 2007 року надають допомогу спеціалістами в галузі ВМС) та Угорщина. Центр складається з трьох відділів: адміністративного та двох спеціалізованих. Адміністративний відділ займається забезпеченням життєдіяльності Центру.

Один із спеціалізованих відділів займається правовими питаннями та питаннями організації і стандартизації діяльності Центру у сфері боротьби з кібертероризмом. Робота цього відділу спрямована на вирішення таких завдань: розробку концепції та стратегії кіберзахисту (без права затвердження); проведення аналізу кібероперацій (включаючи наступальні, оборонні та повсякденні); розробку аналітичних засад кіберзахисту; розповсюдження інформації; правове регулювання взаємовідносин; розробку словників спеціалізованих термінів. Другий спеціалізований відділ займається вирішенням суто технічних проблем. Його діяльність спрямована на: моніторинг можливих кібератак; виявлення кібернападів та пом'якшення їх впливів; моделювання можливих ситуацій; проведення тренувань з питань захисту від кібернападів. На сьогодні фахівці Центру із залученням представників від інших зацікавлених сторін займаються:

створенням за замовленням НАТО концепції кібервійни (концепція розглядає інформаційний простір як "паралельне поле бойових дій" у майбутніх конфліктах – як політичних, так і військових);

створенням словника термінів, що стосуються кібероборони;

розробкою доктрини та стратегії кіберзахисту;

моделюванням певних ситуацій та розробкою методик по оцінці рівнів безпеки і кіберзагроз, а також моделюванням можливих відповідей на кібератаки;

розробкою юридичних питань зазначеної діяльності.

Центр фактично виконує роль модератора (координатора) цієї роботи.

Наступним важливим кроком стало створення у структурі НАТО Управління кібернетичного захисту, на яке покладені функції по забезпеченню координації правових, політичних та оперативно-технічних заходів окремих країн-членів

Північноатлантичного Союзу та Альянсу в цілому у сфері захисту від кібернетичних загроз. З цією ж метою 22 січня 2009 у м. Обераммергау (Германія) пройшов симпозіум на тему "НАТО і його партнери: Обличчями разом до загроз від Мережі" за результатами якого було скоректовано напрями кіберзахисту. Окрім цього розпочалась підготовка до розробки нової Стратегічної концепції Альянсу та саміту НАТО у 2010 році. Серед основних викликів, на які має відповісти нова концепція, можна виділити такі:

1) захист інформаційної складової системи безпеки та оборони країн-членів;

2) співвідношення інтересів країн-членів до загальної системи життєдіяльності Альянсу, та відповідне співвідношення двосторонніх відносин країн-членів з країнами не членами НАТО;

3) реагування на підвищення небезпеки з боку загроз нової генерації: тероризм, та як прояв розвитку цього явища кібертероризм, піратство тощо;

4) подальше розширення НАТО, проблема глобального партнерства за межами Євроатлантичного регіону;

5) перспективи відносин між НАТО та Росією, між НАТО та Європейським Союзом;

6) проблематика систем протиракетної оборони та енергетичної безпеки;

7) проблема вирішення довгострокових операцій під проводом НАТО, зокрема місії в Афганістані та Іраку тощо.

Враховуючи, що у цей час ймовірність "асиметричних атак" з використанням кіберзброї значно зросла, власні дієві заходи щодо захисту національного кіберпростору здійснюються також і **Великобританією**. Цьому не в останню чергу сприяє суспільна думка, яку фактично освітив директор лондонського Міжнародного інституту стратегічних досліджень Джон Чіпмен. За його словами [190] перед світовою спільнотою на порядку денному перш за все стоїть завдання усвідомити, що є "кібернетичним конфліктом", що вважати "кібернападом" і як оцінити момент, коли вони відбуваються, а "... з погляду кібервоєн, перед нами зараз взагалі стоїть інтелектуальний виклик на зразок ..." загрози ядерної війни.

З метою моніторингу інформаційного простору та своєчасного реагування на кіберзагрози, що стосуються головним чином виведення з ладу комп'ютерних систем та полювання за коштовною інформацією (фішинг), у складі Кабінету міністрів Великобританії останнім часом створено Центральне управління з кібербезпеки (ЦУКБ) [183, 190]. Управління є основним органом, відповідальним за формування національної стратегії у сфері інформаційної безпеки країни. Наряду з цим на території країни вступив у дію закон про тероризм, що ставить комп'ютерних хакерів в один ряд з бойовиками Ірландської республіканської армії.

Даний нормативний акт покликаний посилити боротьбу з різними угрупованнями, які використовують територію Об'єднаного Королівства для своєї діяльності. Відповідно до нього, у випадку злому хакерами комп'ютерної системи, що забезпечує національну безпеку країни, а також спроб з їх боку будь-яким чином вплинути на державні структури або загрожувати суспільству, вони можуть бути обвинувачені в тероризмі з усіма наслідками, що 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*), який поки що налічує лише 20 співробітників. Його метою є координація зусиль вже існуючих різноманітних центрів із кібербезпеки різних відомств щодо захисту критичної інфраструктури у сфері IT технологій та створення майданчику для співпраці між урядом та приватним сектором із проблем кібербезпеки [190, 191]. Крім 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.

В країнах континентальної Європи - Франції, Італії, ФРН та інших йдуть аналогічні процеси. До розряду пріоритетних ними висуваються питання правових і організаційних механізмів регулювання використання комп'ютерних мереж. Першою міжнародною угодою по юридичних і процедурних аспектах розслідування та кримінального переслідування кіберзлочинів стала Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 року [192, 193]. Конвенцією передбачаються скоординовані на національному і міждержавному рівнях дії, спрямовані на недопущення несанкціонованого втручання в роботу комп'ютерних систем. З цією метою у **Франції** для забезпечення безпеки урядових інформаційних систем від кібератак був створений Центр інформаційних систем Служби безпеки (*Central Information Systems Security Service*), підпорядкований Генеральному секретаріату з оборони та національної безпеки. У кінці 2009 – на початку 2010 року при даному центрі створено Національну агенцію безпеки інформаційних систем, яка перебуває у безпосередньому підпорядкуванні прем'єр-міністра Франції. Основними завданнями агенції визначені: узгодження, розробка та реалізація міжвідомчих заходів із забезпечення інформаційної безпеки національних інформаційних систем; виявлення кіберзагроз, їх оцінка, а також координація заходів протидії. Очікується, що чисельність персоналу агенції до кінця 2011 року становитиме понад 200 осіб. Безпосередня реалізація заходів щодо

планування й здійснення використання ІТ технологій в інтересах впливу на інформаційні й телекомунікаційні об'єкти іноземних держав покладена на головне управління безпеки інформаційних систем (ГУ БІС) - міжвідомчу структуру, створену й функціонуючу також при кабінеті міністрів країни.

Нормативно-правовою основою їх діяльності має стати нова концепція інформаційного протиборства в комп'ютерних мережах (*Lutte Informatique - LI*), розробку якої, взявши за основу американський підхід, здійснює загальновійськовий центр 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 по забезпеченню безпеки військових об'єктів, Генеральною делегацією по озброєннях, Національною жандармерією й зовнішньою розвідкою. Фахівці *CICDE* розглядають кіберпростір в якості реального фізичного поля, що охоплює соціальну, технічну (інформаційні системи й мережі) та інтелектуальну (процеси обробки інформації) сфери. При цьому вони виділяють дві групи наступальних заходів *LI*, а саме:

1) розвідувального характеру:

акції, спрямовані на збір відомостей про ІТС противника;

проникнення до автоматизованих ІТС противника для добування розвідданих і виявлення його намірів;

2) деструктивного характеру:

перекручування, підміни або знищення інформації з метою зниження ефективності прийняття управлінських рішень;

акції, спрямовані на порушення цілісності, погіршення функціонування або руйнування ІТС противника.

Французькі експерти виділяють три фази проведення операцій у кіберпросторі: підготовчий етап, у ході якого основні зусилля зосереджуються на зборі інформації про противника; другий етап - власне вплив на противника; третій етап - забезпечення безпеки власного інформаційного простору.

В **Італії** головним координуючим органом з питань інформаційної безпеки країни став Національний центр інформатики у сфері державного управління, створений при Президії ради міністрів Італії. Крім того, у Генеральному штабі ЗС Італії створено структурний підрозділ –Управління інформації та безпеки, який відповідає за інформаційну безпеку систем і ресурсів збройних сил держави.

У **ФРН** підходи до проблем інформаційної і кібервоєн та захисту власної ІТ інфраструктури від кіберзагроз збігаються з американськими та британськими. Вони включають ведення наступальних та оборонних операцій для досягнення

національних цілей. Певна особливість полягає у створенні спеціалізованих поліцейських та військових підрозділів для боротьби зі злочинами у сфері високих технологій, які проводять моніторинг інформаційних систем, в першу чергу мережі *Internet*, з метою виявлення кіберзлочинів та здійснення оперативно-розшукових заходів. Так, одна з останніх інформацій [194], що пройшла у європейській пресі, стосувалась створення командуванням Збройних Сил Німеччини у лютому 2009 року в структурі бундесверу управління мережних операцій. Одною з головних причин такого рішення стали масовані атаки на обчислювальні мережі ЗС Німеччини з 14 по 16 лютого 2009 року, у результаті якого декілька сот ПЕОМ та сервер головного інформаційного сайта МО були тимчасово виведені з ладу.

Діяльність управління спрямована на здійснення впливу на комп'ютерні мережі супротивника шляхом використання, перекручування, підміни або знищення інформації, що міститься в базах даних комп'ютерів та інформаційних мереж, а також зниження ефективності їхнього функціонування або виведення з ладу. Завданнями підрозділу на даному етапі є вивчення можливості та наслідків застосування кіберзброї, вироблення основ ведення кібервоєн, що регламентують умови проведення атак на комп'ютерні мережі, права й обов'язки виконавців і осіб, що віддають відповідні розпорядження, а також визначення методик захисту власних мереж та протидії сторонньому кібернетичному впливу. Передбачається, що управління мережних операцій повинно бути повністю готовим до застосування наприкінці 2010 року. Окрім цього у країні створено центр забезпечення безпеки інформаційної техніки зі штатом близько 500 співробітників та річним бюджетом понад 50 мільйонів євро. Передбачається, що наприкінці 2010 – початку 2011 року в рамках реалізації концепції з кіберзахисту у ФРН в структурі командування бундесверу буде завершене формування підрозділу інформаційних і комп'ютерних мережних операцій (*Abteilung der Informations und Computernetzwerkoperationen*). До його головних задач належатиме: створення нових методів кібератак, проникнення до комп'ютерних мереж інших держав, проведення операцій деструктивного впливу на мережі та управляючі системи цих держав й блокування їх роботи. Вже сьогодні штат підрозділу налічує 100 експертів у галузі інформаційних технологій, що практикують хакерські методи віддаленого проникнення до комп'ютерних систем стратегічного призначення протилежної сторони з метою несанкціонованого копіювання або знищення інформації, а також виведення з ладу їх інформаційних систем та мереж. До перспективних завдань підрозділу на сьогодні віднесено проведення диверсійних дій та дезінформаційних заходів у кіберпросторі.

У найближчий час уряд ФРН збирається відкрити Національний центр захисту від кібератак. У задачі Центра буде входити також боротьба з електронним

шпигунством і створення системи забезпечення електронної безпеки. Також планується відкрити дослідний центр інформаційних технологій міністерства оборони ФРН. Для ведення інформаційно-психологічних операцій у збройних силах будуть сформовані відповідні батальйони.

В **Ізраїлі** завдання з планування і реалізації заходів щодо порушення функціонування об'єктів інформаційної й телекомунікаційної інфраструктури інших держав покладені на розвідувальне управління та управління зв'язку і комп'ютерних систем ГШ національних ЗС. Для захисту національного кіберпростору при Міністерстві фінансів Ізраїля створений спеціальний підрозділ *Tehila*. На нього покладені наступні завдання [183, 191]:

забезпечення захищеного обміну даними через *Internet* між державними відомствами;

створення безпечних програмно-апаратних платформ для *Web*-сайтів і ресурсів урядових організацій;

припинення поширення через *Internet* протиправної інформації;

координація зусиль зацікавлених відомств по протидії кібератакам.

Оперативне відбиття нападу на національні комп'ютерні мережі, якщо алгоритм комп'ютерної атаки відомий, в *Tehila* забезпечує чергова група. У випадку виявлення нестандартної схеми дій супротивника до роботи підключається група експертів, що проводить всебічний аналіз ситуації й виробляє інструкції для чергового персоналу.

На початку 2010 року Тель-Авівом прийнята концепція, що допускає кібератаки на сервери й електронні адреси, через які потенціальні супротивники вживають спроби руйнування інформаційного простору, комп'ютерних систем і електронних баз даних Ізраїлю. У зв'язку із цим група *Tehila* наділена додатковими повноваженнями, що передбачають можливість проведення нею наступальних акцій на закордонні комп'ютерні системи без узгодження їх з міжнародними організаціями та іноземними державами. Такий підхід до вирішення проблемних питань пов'язаний з відсутністю відповідних міжнародних правових механізмів, які б обмежували використання програмно-апаратних засобів для поразки інформаційно-телекомунікаційних систем.

У зв'язку зі зростанням кількості кібератак з боку ісламських екстремістів в Інтернеті у червні 2010 року Тель-Авів ухвалив рішення щодо створення підрозділу, який буде спеціалізуватися на протиборстві кібертероризму та проведенні спеціальних операцій у мережі *Internet*, а також в інформаційних мережах урядових, силових, фінансових і інших структур потенційного супротивника. Його формування здійснюється в складі спеціального підрозділу

радіоелектронної розвідки розвідувального управління ГШ. Разом з цим Ізраїль здійснює підбір найбільш обдарованих фахівців у галузі ІТ технологій для армії й цивільних структур. Організовано взаємодію з неурядовою хакерською групою "Гілад тім" (створена у 2009 р.), що має досвід "злому" урядових сайтів Туреччини, Лівану й ряду ісламських організацій.

Загалом про рівень занепокоєності провідних держав світу у сфері кібербезпеки свідчить їх бажання врегулювати на міжнародному рівні можливість визнання кібератаки "актом війни". Так, 30 січня 2010 року, під час Всесвітнього економічного форуму у Давосі, сенатор США від Республіканської партії С. Колінз зазначила, що США всерйоз розглядають питання щодо ставлення до кібератак як до оголошення війни. 12 травня цього ж року помічник заступника міністра оборони США з політичних питань Дж. Мілер взагалі заявив, що США готові нанести військовий удар у відповідь на кібератаки на свої комп'ютерні мережі. Така позиція США щодо трактування кібератак та потенційних кібервійн набуває свого продовження і в межах НАТО: група експертів під керівництвом М. Олбрайт у червні 2010 року запропонувала трактувати масштабні кібератаки як такі, що підпадають під п'яту статтю Північноатлантичного договору і вважаються атаками на всіх членів Альянсу. Швидше за все така позиція НАТО буде відображена і у новій "Стратегічній концепції НАТО" [191] із пропозицією розширення організаційних та військових можливостей НАТО у протидії кібернападам та створення єдиного інформаційного (кібернетичного) простору блоку.

Основний вміст концепції полягатиме в об'єднанні коаліційних і національних органів управління, військових формувань, засобів розвідки та передавання інформації, а також впровадження у військах єдиних процедур планування і прийняття рішень. З урахуванням організаційної і технічної складності реалізації згаданого проекту очікується, що його технічне проектування буде завершене у 2010-2011 роках, необхідна інфраструктура буде створена до 2015 року, а повна оперативна готовність досягнута приблизно в період з 2020 по 2025 роки.

Тобто, як видно з викладеного, провідні держави світу все більше уваги приділяють розвитку та захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що в цілісному вигляді описується проблемою забезпечення їх власної кібербезпеки.

Додаток Б
Навчання Cyber Storm та Cyber Europe: мета, хід і результати

Зважаючи, що послуги з виявлення й запобігання несанкціонованих проникнень в інформаційні системи (мережі) державних установ, а також підготовка останніх до захисту від внутрішніх і зовнішніх кібернетичних втручань і загроз стануть у найближчій коротко й середньостроковій перспективах чи не найбільш пріоритетними послугами в сфері кібербезпеки [168], а навчання з цих питань – практично єдиною формою перевірки здатності державних установ протистояти кібератакам як національного, так і світового масштабу, провідні країни світу приділяють цим питанням найпильнішу увагу. Одним із беззаперечних лідерів серед них на сьогодні визнані Сполучені Штати Америки, де заходи подібного плану під кодовою назвою "Cyber Storm" проводяться починаючи з 2006 року.

За результатами першої операції Cyber Storm I, що завершилась у лютому 2006 року, керівництво США виявило надзвичайно низький рівень підготовки співробітників об'єктів критично важливої інфраструктури до протидії сторонньому кібернетичному впливу. Як з'ясувалось, при кібератаках люди здебільшого просто не розуміли, що відбувається й до кого вони у певних умовах можуть звернутись за допомогою. Результати операції Cyber Storm II, проведеної у березні 2008 року, виявились не набагато кращими. У своїй більшості співробітники об'єктів критично важливої інфраструктури також не змогли правильно зорієнтуватися в ситуації, для того щоб 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 й були присвячені випробуванню нової системи протистояння кібератакам, що покликана захистити в першу чергу системи енерго- і водопостачання, а також банки країни. Приводом для проведення навчань стали хакерські напади на Internet-сайти державних установ і найбільших компаній США у день незалежності 4 липня 2009 року. Їх результатом стали збої в роботі сайтів Організації об'єднаних націй, штаб-квартира якої перебуває в Нью-Йорку. Разом з тим до числа потерпілих від кібервзломів потрапили: Держдепартамент, Пентагон й інші відомства. В навчаннях прийняли участь тисячі фахівців з 11 американських штатів, 60 приватних компаній та 12 закордонних країн. Серед іноземних партнерів були представники від Австрії, Великобританії, Канади, Франції, Японії, Німеччини, Угорщини, Італії,

Голландії, Нової Зеландії, Швеції та Швейцарії. Росія в навчаннях участі не приймала. З урядових структур не рахуючи Білого Дому, розвідки та правоохоронних органів до навчань підключилися сім американських міністерств: торгівлі, оборони, енергетики, національної безпеки, юстиції, транспорту та фінансів.

Метою навчань було підвищення готовності фахівців до кібератак шляхом імітування дій зловмисників, а також дослідження існуючих процесів обміну інформацією між федеральними службами, державною владою й приватними особами. В офіційному повідомленні DHS говориться про те, що "... у своїй основі ці навчання є перевіркою на міцність ..." об'єктів критично важливої інфраструктури та їх "... спроможності справлятися з втратами у найбільш важливих аспектах сучасного життя ...". Серед імітуємих наслідків нападу – "... завдання збитків важливим державним і приватним системам: комунікаційним мережам, енергосистемам тощо ...".

В ході навчань його учасниками, без нанесення реального збитку телекомунікаційним системам і мережам, було перевірено понад півтори тисяч різновидів кіберзагроз, починаючи від масового розсилання спама з вірусами, атак через USB-пристрої, цілеспрямованих атак ботнетів, атак типу "відмова в обслуговуванні" (DDoS атак на окремі сервери державних установ), фішингових атак, міжсайтового скриптінгу, атак мобільних пристроїв і бездротових мереж й закінчуючи спробами підмінити DNS-сервери та замінити сертифікати, що використовуються для автентифікації у державних автоматизованих інформаційних системах.

Як результат було підтверджено спроможність потужних державних установ та об'єктів критично важливої інфраструктури витримувати та протистояти кібератакам національного масштабу.

На підтвердження тому, що питання захисту інформаційного та кіберпросторів останнім часом є надто актуальним, країнами Європейського союзу (ЄС) 4 листопада 2010 року були проведені перші кібернавчання – Cyber Europe-2010. У них взяли участь всі 27 країн, що входять у ЄС, а також Ісландія, Норвегія та Швейцарія. При цьому безпосередньо задіяними у навчаннях були представники від 22 країн ЄС, інші 8 направили на навчання лише своїх спостерігачів. Навчання були організовані при сприянні Європейського агентства по мережевій та інформаційній безпеці (European Network and Information Security Agency – ENISA, Греція, о.Крит, м. Іракліон), а також Об'єднаного наукового центра Європейської комісії (Joint Research Centre – JRC, Бельгія, м. Брюссель) [172–178]. Штаб Cyber Europe-2010 був розташований в Афінах (Греція) й координував роботу більш ніж 150 експертів

з 70 суспільних організації по усій Європі. За словами Вангеліса Узуніса, старшого консультанта агентства ENISA, у рамках навчань планувалося виробити найкращі способи захисту від масштабних вірусних інфекцій та атак ботнетів, а саме: "...виробити єдиний підхід до захисту, створити єдиний кіберпростір і налагодити контакти між країнами-учасниками проекту ...". На його думку "... подібні заходи вкрай важливі для відпрацьовування реальних відповідних дій на загрози, які можуть відбутися ... ". В. Узуніс також відзначив, що зазначені заходи є особливо актуальними в умовах сьогодення, коли кожна із країн ЄС має власний механізм забезпечення ІТ безпеки, який у більшості випадків нажаль не передбачає взаємодії навіть із найближчими сусідами. У ході навчань моделювалась глобальна DDoS атака на критично важливі елементи системи управління, результатом якої в реальних умовах мало б стати поступове відключення зв'язку між різними країнами Євросоюзу (за час навчань було проведено приблизно 320 подібних симуляцій). Атаці точно такого ж типу навесні 2007 року була піддана Естонія. При цьому, за повідомленням прес-служби Європейської комісії, головне завдання держав-учасниць ЄС полягало в тому, щоб перевірити свої можливості по спільному функціонуванню в умовах "загального відключення мережі" і, як результат, втрати зв'язку між критичними об'єктами їхньої інфраструктури, що позбавляє громадян, компанії та державні структури доступу до Web-сервісів. Представникам відповідальних міністерств і відомств у державах ЄС потрібно було продемонструвати свою здатність до пошуку обхідних шляхів і вміння відновлювати сильно ускладнений зв'язок за умов, коли комунікації з колегами порушені, а їх відновлення взагалі неможливе. За висновком представників Європейської Комісії якби не дії фахівців, спрямовані на зміну маршрутів трафіку в обхід ушкоджених з'єднань, доступність основних Web-послуг для населення й бізнесу навіть у ході симуляції можливих атак могла б виявитися під загрозою. 10 листопада 2010 року за повідомленням BBC News фахівцями від ENISA був підготовлений попередній звіт про хід та наслідки проведених навчань. В ньому наголос був зроблений на те, що сценарій навчань як у технічній, так і у комунікаційних сферах виявився добре збалансованим, а мета навчань – досягнутою. Разом з тим ними були відмічені й певні недоліки, що супроводжували хід навчань. У першу чергу це стосувалось забезпечення рівня підготовки до навчань на загально європейському рівні (більшість країн-членів ЄС на сьогодні в сфері інформаційної безпеки потребують переопрацювання власної національної політики). Особливий наголос фахівцями від ENISA був зроблений на те, що Cyber Europe-2010 – це лише перший крок у справі вироблення стратегії забезпечення комплексної безпеки на території об'єднаної

Європи. Зазначені навчання повинні надати старт програмі широкої кооперації в сфері захисту комп'ютерних мереж країн Європи, першими кроками якої має бути: вироблення єдиного підходу до захисту; створення єдиного інформаційного та кіберпросторів; налагодження контактів між країнами-учасниками проекту.

4 жовтня 2012 року під егідою Європейської комісії за участю фахівців з понад 25 країн ЄС та чотирьох країн спостерігачів були проведені чергові кібернавчання типу "стрес-тест " під назвою Cyber Europe-2012. За інформацією, наданою прес-службою Європейського агентства по мережевій та інформаційній безпеці, під час начань була змодельована широкомасштабна DDoS-атака на сайти і сервери державних органів влади країн ЄС, Internet-провайдерів, великих фінансових установ та телекомунікаційних компаній. Сценарій атаки, яка здійснювалась декількома кримінальними угрупованнями, передбачав біля 1200 окремих інцидентів та 30 000 спам-листів. Її метою було з'ясувати наскільки продуктивно структури, задіяні у навчаннях, зможуть взаємодіяти та реагувати на постійні атаки на власні Web-сайти та державні ІС банківської сфери.

Навчання 2012 року мали надто більший масштаб та межі застосування порівняно з навчаннями 2010 року. Віце президент Європейської комісії, Нелі Крус заявила: "Це перший раз, коли банки і Internet-провайдери приймають участь у навчаннях з протидії кібератакам по усій території ЄС. ... Навчання є предметом співробітництва на європейському рівні для підтримування функціональної інфраструктури Internet". У ході проведення навчань використовувалась автономна система, яка відбивала основні характеристики та продуктивність критично важливих інформаційних (кібер) інфраструктур. Жодна з реальних інфраструктур задіяною не була.

Загальний висновок, зроблений за результатами навчань Cyber Europe-2010 та Cyber Europe-2012, говорить сам за себе: "Європі необхідно вжити додаткових заходів, щоб підготуватися до захисту від кібератак майбутнього". Подібні заходи, за думкою учасників кібернавчань, є вкрай важливими для відпрацьовування реальних відповідних дій на загрози, які можуть статися у перспективі. Враховуючи таке європейськими інститутами вже нині створена система комп'ютерного реагування на надзвичайні ситуації (CERT-EU) з метою захисту власних інформаційних і кіберінфраструктур від кібератак та інцидентів у сфері високих технологій. До кінця 2012 року Європейська комісія має за мету розробити Стратегію інформаційної безпеки, одним із ключових елементів якої будуть законодавчі пропозиції, спрямовані на покращення мережевої та інформаційної безпеки на усій території ЄС.

Додаток В
Організація малозатратної timing атаки.

Термін «малозатратна атака» означає що для успіху нападаючому достатньо мати можливість спостерігати тільки за частиною мережі, наприклад бути одним з Tor-Вузлів. **Основна ідея** – використовувати здавалося б неминуче обмеження всіх анонімізуючих систем з малими затримками. Виходячи з того, що системи з малими затримками не можуть дозволити собі вносити в потік які-небудь затримки, часові характеристики (timing паттерн) пакетів зберігаються на всьому протязі ланцюга. Атака матиме місце зважаючи на те, що розроблювачі Tor порахували неймовірним появу в мережі глобального пасивного спостерігача. Така ситуація не розглядалася й не входила в модель загроз.

Мета атаки визначити які саме вузли зараз використовуються для організації Tor-ланцюжків. У випадку успіху, це сильно вдарить по анонімізуючим властивостях Tor (сокр. 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). Дійсно, той хто нападає не бачить всіх зв'язків у мережі. Але ні що не заважає йому виступити в якості одного з вузлів Tor і замірити затримки між собою й усіма іншими вузлами. За допомогою знання цих затримок можна побічно оцінити обсяг трафіка який передає кожний вузол у кожний момент часу. Далі, знаючи картину розподілу обсягу трафіка від часу для всіх улов мережі, можна, використовуючи техніку (Danezis 2004), будувати досить гарні прогнози про те які вузли передають трафік з однаковими характеристиками. Іншими словами виявити анонімізуючі ланцюжки.

Реалізація атаки. Архітектура Tor сприяє атаці. Tor-вузол виділяє кожному з'єднанню окремий буфер, обробка буферів іде в режимі round robin fashion. Якщо в буфері немає потоку - він ігнорується, починається обробка наступного буфера. Відзначимо, що з міркувань продуктивності змішування було вилучено. Таким чином, коли встановлюється нове з'єднання або віддаляється існуюче з'єднання, або ж коли міняється трафік у поточному з'єднанні змінюється навантаження на Tor-вузол. Це відбивається на швидкості відповідей іншим вузлам які вже мають або тільки хочуть установити з'єднання з поточним. З таких саме причин міняється навантаження й на інших Tor-вузлах. Виходить, що зміна навантаження трафіка на Tor-вузлі відбивається на навантаженні з'єднаних з ним вузлів. Отже, вузли в одному ланцюжку будуть мати схожі картини розподілу навантаження від часу. Відзначимо, зміна навантаження трафіка може виникати не тільки вищеописаним образом, але й через внутрішні причини Tor-вузла, наприклад навантаження на CPU - такі затримки

не враховуються й можуть знизити ефективність атаки. Для успішної атаки, особі яка нападає досить бути одним із клієнтів мережі Tor. Такий вузол називається шкідливим (corrupt node) або зондом (probe node). Модель атаки показана на рис. Б.1.

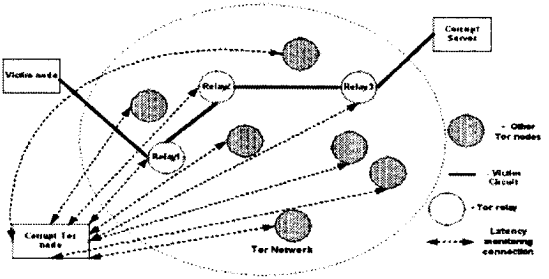


Рис. Б.1. Модель малозатратної timing-атаки на Tor

Основні етапи атаки (рис. Б.2). Шкідливий Tor-Вузол установлює з'єднання з іншими Tor-Вузлами для виміру затримок цих зв'язків. Протягом деякого часу він спостерігає за затримками у всіх цих з'єднаннях. Виміри затримок використовуються для оцінки обсягів трафіків переданих кожним Tor- вузлом (навантажень трафіка на Tor-вузли), з якими шкідливий вузол має з'єднання. На основі знання обсягів трафіків, виводяться паттерни трафіків. Коли нападаючий знає паттерни трафиков всіх вузлів, він може виконати атаку (Danezis 2004, Levine et al. 2004). Атака буде ще більш ефективною якщо нападаючий контролює сервер до якого підключається користувач Tor. Це пояснюється тим, що в цьому випадку не потрібно виявляти паттерн трафіка - нападаючий сам може видозмінювати трафік так, щоб його легко було виявити. Мета атаки: виявити шлях між клієнтським вузлом жертви й захопленим сервером. Це знизить анонімізуючу здатність системи до рівня звичайної proxy. У підсумку, автори роблять висновок про те, що атака буде ефективна для всіх анонімізуючих систем з малими затримками, включаючи Tarzan і MorphMix.

At a corrupt node	At a corrupt server
Preparation	
Find a list of all other nodes ($\{1, 2, \ldots, N\}$)	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, $node_1 \rightarrow node_3 \rightarrow node_8$	

Рис.Б.2. Алгоритм малозатратної атаки.

Додаток Г

Віруси в соціальних мережах

Якщо при вході на сайти такі як, наприклад «Одноклассники» (рис. В.1) або «ВКонтакте» (рис. В.2), Вам пропонується відправити sms-повідомлення з кодом підтвердження про валідацію аккаунта – це значить, що у вашому комп'ютері оселився вірус. Треба пам'ятати, що в процесі справжньої валідації жодних смс-ок користувачеві відправляти не потрібно.

Подібні повідомлення мають такий вигляд:

«Одноклассники»:

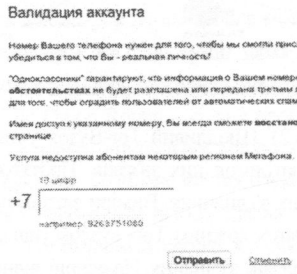


Рис. В.1. Валідація аккаунта «Одноклассники»

«Вконтакте»:

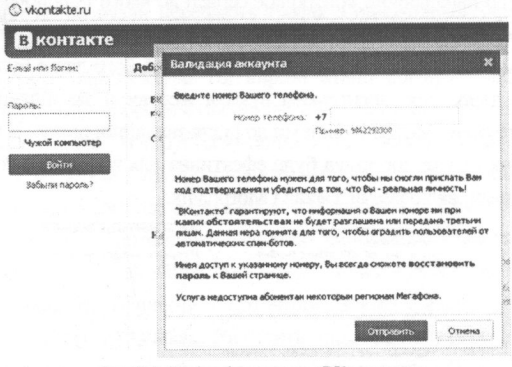


Рис. В.2. Валідація аккаунта «ВКонтакте»

Яким же чином позбутися від подібного шкідника?

Для цього необхідно видалити 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 нього перенапрямок на свій сайт-клон. Виходить, що в адресному рядку ви бачите адресу потрібного вам сайту, але в дійсності відкритий зовсім інший ресурс, що зроблений таким чином, щоб зовні бути в точності схожим на оригінал.

Існує кілька способів рішення даної проблеми.

Спосіб 1. Скористатися безкоштовною програмою CureIt! Звичайно, їй не важко буде не тільки знешкодити сам вірус, але й виправити заподіяні вірусом наслідки. А саме, з донедавна CureIt! здатна виявляти зміни у файлі hosts.

Спосіб 2. Вручну. Для цього спочатку необхідно скачати Process Explorer і запустити його. У списку процесів знайти файл lsass.exe і визначити до нього шлях доступу (рис. В.3). Якщо файл lsass.exe перебуває НЕ в папці WindowsSystem32, необхідно запам'ятати цей шлях, виділити процес лівою кнопкою миші й нажати червоний хрестик зверху (ще можна виділити процес правою кнопкою миші й вибрати з меню, що випадає, пункт "Kill process"). Тим самим процес роботи вірусу буде вилучений 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 лежить у папці C:WindowsSystem32DriversEtc, цим файлом. Для цього в 64-розрядній системі Windows файл варто скопіювати по такій адресі: C:WindowsSysWOW64DriversEtc. Після виправлення файлу 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").

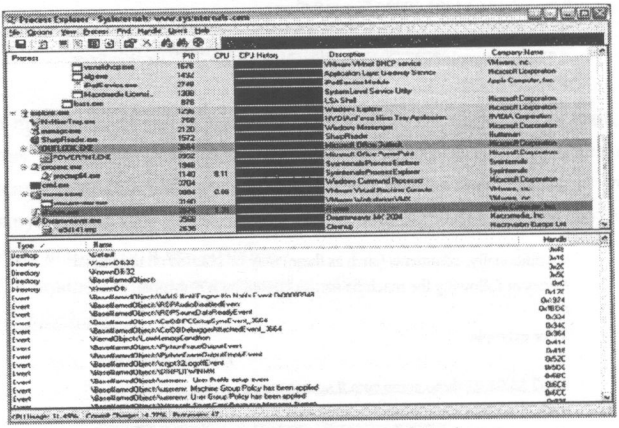


Рис. В.3. Визначення шляху доступу до файлу lsass.exe

Для завершення роботи комп'ютер необхідно перезавантажити.

Спосіб 3. Деякі антивіруси здатні знешкодити тіло вірусу, але не:

виправити файл hosts, як це робить утиліта CureIt!,

очистити маршрути й кэш, як це робиться командами в другому способі.

У цьому випадку досить тільки виконати наведені вище команди й виправити файл hosts - закачавши його по посиланню вище, відредагувавши вручну в Блокноті або скориставшись спеціальною програмою від Microsoft. Однак, якщо після цього файл буде знову ушкоджений, значить вірус усе ще не видалений і вам таки прийде скористатися одним із двох способів, описаних вище.

Додаток Д
Тест на проникнення та рекомендації щодо 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 атакуючими методів соціального інжинірингу(СІ) за допомогою яких без особливих труднощів і пояснень вони виконали пошук в Internet та сформували для себе уявлення про досліджувану організацію. Вивчення баз даних організації дозволило встановити імена великої кількості її співробітників та її керівництва. Пошук у телефонному довіднику дав телефонний номер офісу компанії поблизу від атакуючих. Дзвінок в офіс дозволив одержати копію щорічного звіту компанії, а також безкоштовний телефонний номер компанії. Об'єднавши дані щорічного звіту з даними, отриманими з Internet, атакуючі одержали відомості про імена й посади багатьох осіб з керівництва разом з інформацією про проекти, над якими вони працюють.

Наступним кроком було одержання телефонного довідника компанії. Це дозволило встановити імена ще ряду співробітників і одержати повне уявлення про організаційну структуру компанії. З безкоштовного телефонного номера був зроблений дзвінок по основному номеру компанії для контакту зі службою розсилання. Телефонуючий, представившись новим співробітником, намагався довідатися, яку інформацію потрібно вказати для пересилання поштою в США й за кордон. З отриманої відповіді стало зрозуміло, що для цього потрібно лише два числа – особистий номер співробітника й номер торгового центра. Дзвінок у відділ графіки підтвердив важливість цих двох чисел. Використовуючи телефонний довідник, атакуючі почали дзвонити десяткам службовців у різних відділах для одержання особистих номерів службовців, які могли бути використані для наступних атак. Номери отримували таким чином: телефонуючий видавав себе за співробітника відділу кадрів, який помилково подзвонив не тому співробітникові й запитував номер для того, щоб зрозуміти, що він помилився. Потім атакуючі визначили, що вони можуть спробувати одержати імена нових співробітників, які, скоріш за все менш інформовані про можливі загрози для компанії.

Таким чином, використовуючи інформацію першої фази атаки, були встановлені імена декількох керівників компанії. Телефонний довідник дозволив установити ім'я тієї особи, яка швидше за все і є керівником. На цей момент часу було констатовано, що найкращим методом одержання імен нових службовців

буде заява керівника про те, що він особисто хоче познайомитися з новими службовцями компанії. Для цього атакуючі планували спочатку заявити, що вони виконують доручення керівника, а потім, що керівник розстроєний через якість отриманої інформації. Тим не менш чисто технічна вдача супроводжувала їм, і на дзвінок у відділ по роботі з новими співробітниками відповів автосекретар. Повідомлення дозволило атакуючим встановити таке: 1) відділ переїхав; 2) ім'я людини, за якою закріплений телефонний номер; 3) новий телефонний номер. Особливо цінною виявилась інформація про ім'я людини, за якою закріплений телефонний номер оскільки його знання збільшує правдоподібність питань того, хто дзвонив. Як результат, атакуючими були отримані імена всіх співробітників, що почали працювати протягом цього тижня, і відносно багатьох стали відомими відділи, у яких вони працюють.

Разом з цим було встановлено, що атакуючим варто уникати контакту зі співробітниками відділу ІС оскільки вони, скоріш за все, знають про важливість захисту паролів. Враховуючи таке при дзвінках новим співробітникам атакуючі видавали себе саме за співробітників відділу ІС і проводили з ними короткий інструктаж з комп'ютерної безпеки. У ході цього інструктажу атакуючий одержував базову інформацію, включаючи типи використовуваних комп'ютерних систем, використовувані додатки, номер співробітника, ідентифікатор користувача й пароль.

Аналізуючи результати, отримані в ході експерименту, І. Вінклер запропонував комплекс заходів щодо розробки й впровадження політики безпеки які дозволять захиститися від СІ. Основні з них рекомендують:

1) *не покладатися на систему внутрішньої ідентифікації*. Атакуючих іноді просять аутентифікуватися за допомогою вказівки їхнього особистого номера. На радість зломщиків, такі номери часто використовуються й можуть бути легко отримані від реальних співробітників.

Враховуючи таке компаніям варто мати власні ідентифікатори для робіт, пов'язаних з підтримкою ІС. Наявність такого ідентифікатора дозволить відокремити функції технічного супроводу від інших і забезпечить додаткову безпеку як для робіт із супроводу, так і для взаємодії співробітників в організації;

2) *реалізовувати систему перевірки за допомогою зустрічного дзвінка, коли повідомляєте захищену інформацію.* Від багатьох атак можна було б захиститися, якби працівники компанії перевіряли особистість того, хто дзвонить набравши його телефонний номер, зазначений у телефонному довіднику компанії.

Ця процедура не дуже зручна в повсякденній роботі, однак при зіставленні з можливими втратами незручності будуть виправдані. Якщо від співробітників

зажадати робити зустрічні дзвінки кожному, хто просить повідомити персональну або конфіденційну інформацію, ризик витоку інформації буде зведений до мінімуму. Використання АОН також може стати у пригоді для досягнення цієї мети;

3) *реалізовувати програму навчання користувачів в області безпеки*. Як не парадоксально, але багато комп'ютерних користувачів у наданні свого пароля сторонньому не вбачать нічого поганого. Компанії витрачають величезні суми, закуповуючи найсучасніше встаткування й програми, але необхідність навчати користувачів ігнорується.

Комп'ютерні професіонали повинні розуміти: те, що для них природно, може бути невідомо іншим. Гарна 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 винятково до нього. При цьому на 60 користувачів досить одного відповідального.

Користувачі повинні негайно зв'язуватися з аналітиком, якщо до них звертається особи, які представляються співробітниками служби технічної підтримки;

5) *створити систему оповіщення про загрози*. Атакуючі знають, що, навіть якщо їх виявлять, у працівників компанії немає можливості попередити один одного про атаки. У результаті атака може бути продовжена з мінімальними змінами й після компрометації. По суті, компрометація тільки поліпшить атаку, тому що атакуючі довідаються, що саме не спрацьовує.

Додаток Е

Стратегія оцінювання рівня кіберпотужності об'єкту інформаційної діяльності в умовах стороннього кібернетичного впливу та реагування на його прояви

Під забезпеченням інформаційної і кібербезпеки об'єкту інформаційної діяльності (ОІД) розумітимемо виконання низки заходів, щодо застереження відповідної АС ОІД від випадкового або навмисного втручання у штатні режими її функціонування, а також захисту інформації, яка циркулює у такій АС від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз.

Нині існує декілька принципових підходів, що сприяють реалізації цих заходів. Серед них, по-перше, фрагментарний й, по-друге, комплексний, що поєднує різнорідні заходи протидії загрозам ОІД і традиційно розглядається у вигляді трьох взаємодоповнюючих напрямків, а саме правового, організаційного та інженерно-технічного. Вони, як відомо, належать до класу багатокритеріальних, для колегіального рішення яких в умовах невизначеності і конфлікту серед існуючих методів математичного моделювання, методів формування та дослідження узагальнених показників якості з використанням графоаналітичного і ним подібних підходів, експертних методів вирішення складних завдань оцінювання та вибору будь-яких об'єктів, в тому числі спеціального призначення, а також аналізу та прогнозування ситуацій з великою кількістю значимих факторів, найбільш раціональними і визначальними є саме експертні методи.

Нині саме експертні методи дають можливість більш глибоко вивчити явища, які істотно впливають на рівень захищеності як держави в цілому, так і окремих об'єктів її інформаційної та кіберінфраструктури від впливу внутрішніх і зовнішніх кібернетичних втручань та загроз, виявити найбільш важливе та істотне у цих процесах, не опускаючи тих деталей і взаємозв'язків, без яких не може бути побудована модель досліджуваної проблеми. Метою такої моделі є оцінювання готовності об'єктів інформаційної і кіберінфраструктури до безпечного функціонування в умовах стороннього кібервпливу та встановлення на підставі так званого "індексу кіберпотужності" $G_{захист}^{рівень}$ вимог до власних систем кібербезпеки. Його значення залежить від виявлених відхилень від штатного режиму функціонування IP, IT систем і мереж, а також програмно-апаратних засобів шляхом аналізу чотирьох основних категорій, а саме:

1) наявної нормативно-правової бази;

2) стану соціально-економічного розвитку держави;

3) наявності розгалуженої технологічної інфраструктури;

4) ступеня використання ІКТ та ІТС у розвитку інформаційного суспільства.

Кожна з цих категорій включає ряд узагальнених індикаторів таких, як:

1.1) ставлення керівництва держави до питань забезпечення кібербезпеки: наявність національної стратегії (доктрини тощо) з кібербезпеки; наявність нормативно-законодавчого забезпечення сфери кібербезпеки; наявність міжнародних зобов'язань країни у сфері кібербезпеки; наявність співробітництва державних і приватних структур у сфері кібербезпеки;

1.2) стан розвитку політики кіберзахисту: рівень діяльності керівництва держави у питаннях кіберзахисту; рівень діяльності суб'єктів інформаційної і кіберінфраструктури у питаннях кіберзахисту;

2.1) рівень освіти, науки та техніки: частка населення з вищою освітою; частка населення, що володіє іноземною й передусім англійською мовою; частка НДР та ДКР з 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 Інтернет (у т.ч. поширення Wi-Fi – точок доступу); рівень використання засобів мобільного зв'язку та соціальних мереж;

3.2) рівень впровадження технологічної інфраструктури: рівень фінансування заходів з впровадження ІКТ (у відношенні 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 вище індикаторів, що характеризують здатність ОІД забезпечити кібербезпеку і підтримувати безпечне функціонування власних об'єктів інформаційної і кіберінфраструктури, розробимо ієрархічну схему їх показників (табл. Е.1) в якій значення попереднього i-го рівня визначаються значенням відповідних показників $(i+1)$-го рівня [195]. При цьому категоріям поставлена у відповідність сукупність специфічних індикаторів, що в свою чергу описані елементарними характеристиками, які отримали назву показників.

Таблиця Е.1

Ієрархічна схема рівня критичності кібербезпеки

Рівень критичності кібербезпеки								1-й рівень
Наявність нормативно-правової бази		Стан соціально-економічного розвитку держави		Наявність розгалуженої технологічної інфраструктури		Ступінь використання ікт та ітс		2-й рівень (категорії)
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 впровадження технологічної інфраструктури	Використання інформаційно-комунікаційних технологій у ЛОМ	Використання ресурсів мережі Інтернет у комерційній діяльності	3-й рівень (індикатори)
$A1_1$, $A1_2$, $A1_3$, $A1_4$	$A2_1, A2_2$	$B1_1, B1_2$, $B1_3, B1_4$	$B2_1, B2_2$, $B2_3$	$C1_1, C1_2$	$C2_1, C2_2$	$D1_1, D1_2$	$D2_1, D2_2$	4-й рівень (показники)

Кожній категорії 2-го рівня, кожному індикатору 3-го рівня та кожному показнику 4-го рівня ієрархії за певним правилом, наприклад шляхом експертного опитування [195], може бути поставлене у відповідність деяке число (табл. Е.2, табл. Е.3). Обов'язковою умовою при цьому є наступне: сума ваг категорій, індикаторів та показників одного рівня завжди має дорівнювати одиниці.

Таблиця Е.2

Значення вагових коефіцієнтів категорій і 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 впровадження 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	

При цьому значення категорій та індикаторів якості визначаються в такий спосіб (табл. Е.3) [195]:

Таблиця Е.3

Процедури визначення категорій та індикаторів рівня критичності кібербезпеки

$<$ **НАЯВН. НОРМАТ. – ПРАВОВ. БАЗИ** $>= a1 <$ *ставлення керівництва до кібербезпеки* $> + a2 <$ *стан розвитку політики кіберзахисту* $>$ де $a1$, $a2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $a1 + a2 = 1$;	(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 $A1_1$, $A1_2$, $A1_3$ та $A1_4$; $a1_1 + a1_2 + a1_3 + a1_4 = \sum_i a1_i = 1$;	(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 $A2_1$ та $A2_2$; $a2_1 + a2_2 = \sum_i a2_i = 1$.	(Е.3)
$<$ **СТАН СОЦІАЛ. – ЕКОНОМ. РОЗВИТКУ** $>= b1 <$ *рівень освіти, науки, техніки* $> + b2 <$ *рівень розвитку інновац. середовища* $>$ де $b1$, $b2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $b1 + b2 = 1$;	(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 $B1_1$, $B1_2$, $B1_3$ та $B1_4$; $b1_1 + b1_2 + b1_3 + b1_4 = \sum_i b1_i = 1$;	(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 $B2_1$, $B2_2$ та $B2_3$; $b2_1 + b2_2 + b2_3 = \sum_i b2_i = 1$.	(Е.6)
$<$ **НАЯВН. РОЗГАЛУЖ. ТЕХНОЛ. ІНФРАСТР.** $>= c1 <$ *якісний стан технологіч. інфрастр.* $> + c2 <$ *рівень впроваджж. технологіч. інфрастр.* $>$, де $c1$, $c2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $c1 + c2 = 1$;	(Е.7)
$<$ *Якісний стан технологіч. інфрастр.* $>= c1_1 \cdot C1_1 + c1_2 \cdot C1_2 = \sum_i c1_i \cdot C1_i$; $i = \overline{1,2}$, де $c1_1$, $c1_2$ – вагові коефіцієнти відповідних показників 4-го рівня для $C1_1$ та $C1_2$; $c1_1 + c1_2 = \sum_i c1_i = 1$;	(Е.8)
$<$ *Рівень впроваджж. технологіч. інфрастр.* $>= c2_1 \cdot C2_1 + c2_2 \cdot C2_2 = \sum_i c2_i \cdot C2_i$, $i = \overline{1,2}$ де $c2_1$, $c2_2$ – вагові коефіцієнти відповідних показників 4-го рівня для $C2_1$ та $C2_2$; $c2_1 + c2_2 = \sum_i c2_i = 1$	(Е.9)
$<$ **СТУПІНЬ ВИКОРИСТ. ІКТ та ІТС** $>= d1 <$ *використання ІКТ* $> + d2 <$ *Використання мережі Інтернет* $>$ де $d1$, $d2$ – вагові коефіцієнти відповідних індикаторів 3-го рівня, причому $c1 + c2 = 1$;	(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 $D1_1$ та $D1_2$; $d1_1 + d1_2 = \sum_i d1_i = 1$;	(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 $D2_1$ та $D2_2$; $d2_1 + d2_2 = \sum_i d2_i = 1$.	(Е.12)

Примітка: вираження $<$ x $>$ позначає числове значення показника властивості x.

За формулами (Е.2), (Е.3), (Е.5), (Е.6), (Е.8), (Е.9), (Е.11) та (Е.12), що приведені у таблиці Е.3, з використанням даних анкети експерта (табл. Е.4), що регламентує значення показників та їхніх вагових коефіцієнтів обчислюються значення індикаторів 3-го рівня таких, як:

- <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 Е.4

Анкета експерта для оцінювання рівня критичності кібербезпеки

Позначення показника	Питання, на які повинен відповісти експерт для визначення значення показника	Відповіді на питання	Знач. показника	Позначення вагового коефіцієнта показника	Знач. вагового коеф-та показника
$A1_1$	Чи існує в державі національна стратегія (доктрина, концепція тощо) з кібербезпеки?	1) Стратегія зрозуміла з чітко визначеними цілями та термінами реалізації. 2) Стратегія нечітка, незрозуміла або формальна. 3) Стратегія тільки розробляється. 4) Стратегія відсутня.	1,0 0,4 0,2 0	$a1_1$	0,4
$A1_2$	Чи функціонує у державі система нормативно-законодавчого забезпечення сфери кібербезпеки?	1) Законодавство охоплює усі аспекти кібербезпеки. 2) Є певні закони, проте виконуються лише окремі з них. 3) Є певні закони, проте жоден з 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 має місце співробітництво державних і приватних структур у сфері кібербезпеки?	1) Держава прикладає значні зусилля для розвитку державно-приватного співробітництва. 2) Держава прикладає активні, проте недосконалі зусилля для розвитку державно-приватного співробітництва. 3) Державно-приватне співробітництво не здійснюється.	1,0 0,5 0	$a1_4$	0,1
$A2_1$	Який рівень діяльності керівництва держави у питаннях кіберзахисту?	1) У державі створено орган виконавчої влади, відповідальний за кіберзахист, діяльність якого визнана 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. Е.4

Позначення показника	Питання, на які повинен відповісти експерт для визначення значення показника	Відповіді на питання	Знач. показника	Позначення вагового коефіцієнта показника	Знач. вагового коеф-та показника
$A2_2$	Який рівень діяльності суб'єктів інформаційної і кіберінфраструктури у питаннях кіберзахисту?	1) Рівень реагування суб'єктами інформаційної і кіберінфраструктури на прояви стороннього кібервпливу вищне середнього. 2) Рівень реагування суб'єктами інформаційної і кіберінфраструктури на прояви стороннього кібернетичного впливу періодичний і спонтанний. 3) Суб'єкти інформаційної і кіберінфраструктури питаннями реагування на прояви стороннього кібервпливу не займаються.	1,0 0.5 0	$a2_2$	0,5
$B1_1$	Яка частка населення у державі має вищу освіту?	1) Висока. 2) Середня. 3) Низька. Визначається як відсоткове відношення молоді віком від 18 до 22 років, яка отримує освіту за денною формою навчання, до загальної кількості студентів зазначеного віку в країні.	1,0 0,5 0	$b1_1$	0,2
$B1_2$	Яка частка населення у державі володіє іноземною й передусім англійською мовою?	1) Висока. 2) Середня. 3) Низька. Визначається на основі інформації державного центру з вивчення англійської мови.	1,0 0,5 0	$b1_2$	0,2
$B1_3$	Яка частка НДДКР у державі присвячена дослідженню питань кібербезпеки?	1) Висока. 2) Середня. 3) Низька. Визначається на основі інформації органу держреєстрації НДДКР.	1,0 0,5 0	$b1_3$	0,3
$B1_4$	Який рівень залучення до виконання НДДКР за напрямом кібербезпеки інженерно-технічного персоналу?	1) Достатній. 2) Середній. 3) Недостатній. Визначається як кількість фахівців, залучених до виконання НДДКР на 1 млн. чоловік населення країни.	1,0 0,5 0	$b1_4$	0,3
$B2_1$	Який стан витрат у державі на проведення НДДКР в сфері кібербезпеки?	1) Достатній. 2) Середній. 3) Недостатній. Визначається як відношення поточних і капітальних витрат на проведення НДДКР до рівня ВВП.	1,0 0.5 0	$b2_1$	0,3
$B2_2$	Який стан у державі патентно-раціоналізаторської роботи в сфері кібербезпеки?	1) Достатній. 2) Середній. 3) Недостатній. Визначається як кількість заявок на отримання патентів на 1 млн. чоловік населення країни.	1,0 0,5 0	$b2_2$	0,4
$B2_3$	Який стан залучення приватного та венчурного капіталу до сфери кібербезпеки?	1) Достатній. 2) Середній. 3) Недостатній. Визначається у відсотковому відношенні приватного та венчурного капіталу до рівня ВВП країни.	1,0 0,5 0	$b2_3$	0,3
$C1_1$	Який рівень використання мережі Інтернет?	1) Високий. 2) Середній. 3) Низький. Свідчить про кількість Інтернет-користувачів на 100 чоловік та розраховується на основі інформації JiWire (бази даних щодо Wi-Fi – точок доступу у 142 країнах).	1,0 0,5 0	$c1_1$	0,5

Продовження табл. Е.4

Позначення показника	Питання, на які повинен відповісти експерт для визначення значення показника	Відповіді на питання	Знач. показника	Позначення вагового коефіцієнта показника	Знач. вагового коеф-та показника
$C1_2$	Який рівень використання засобів мобільного зв'язку та соціальних мереж?	1) Високий. 2) Середній. 3) Низький. Свідчить про кількість користувачів мобільного зв'язку на 100 чоловік та відсоткове відношення кількості користувачів до загальної кількості Інтернет-користувачів.	1,0 0,5 0	$c1_2$	0,5
$C2_1$	Який рівень фінансування заходів з впровадження ІКТ?	1) Достатній. 2) Середній. 3) Недостатній. Визначається у відсотковому відношенні загальних витрат на програмне забезпечення, апаратні засоби та IT-послуги до рівня ВВП.	1,0 0,5 0	$c2_1$	0,5
$C2_2$	Який рівень безпеки сервісів?	1) Достатній. 2) Середній. 3) Недостатній. Свідчить про кількість серверів, що використовують технології шифрування даних для безпечного обміну даними.	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 у інтелектуальних транспортних системах?	1) Рівень використання ІТС для вирішення важливих функцій високий. 2) Рівень використання ІТС для вирішення важливих функцій нижче 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) Більше 55 відсотків. 2) Від 25 до 54 відсотків. 3) Від 0 до 24 відсотків.	1,0 0,5 0	$d2_1$	0,5
$D2_2$	Яка частка користувачів використовує Інтернет для замовлення товарів і послуг?	1) Більше 80 відсотків. 2) Від 40 до 79 відсотків. 3) Від 0 до 39 відсотків.	1,0 0,5 0	$d2_2$	0,5

За формулами (Е.1), (Е.4), (Е.7) та (Е.10) табл. Е.3 з використанням даних табл. Е.4 та значень отриманих попередньо показників 3-го рівня обчислюються значення комплексних показників (категорій) 2-го рівня, таких як:

а) наявність нормативно-правової бази ($G_1^{факт}$);

б) стан соціально-економічного розвитку держави ($G_2^{факт}$);

в) наявність розгалуженої технологічної інфраструктури ($G_3^{факт}$);

г) ступінь використання ІКТ та ІТС($G_4^{факт}$).

Індекс кіберпотужності ($G_{захищ}^{рівень}$) з точки зору одного експерту може бути обчислений за такою формулою [195]:

$$G_{захищ}^{рівень} = \left(\sum_{i=1}^{n} \left(g_i \cdot G_i^{факт} \right) \right) \cdot 100\%, \qquad (Д.13)$$

де g_i – вагові коефіцієнти категорій другого рівня ієрархії $G_i^{факт}$;

n – число категорій (в даному випадку $n = 4$).

Прийняття рішення щодо здатності держави протистояти кібератакам у буде здійснюватися за 100-бальною шкалою на підставі такого правила:

якщо $90 \le G_{захищ}^{рівень} \le 100$, то рівень захищеності держави від ризику стороннього кібервпливу вважається достатньо високим для підтримки безпечного функціонування об'єктів її інформаційної і кіберінфраструктури;

якщо $45 \le G_{захищ}^{рівень} < 90$, то рівень захищеності держави від ризику стороннього кібервпливу вважається допустимим для підтримки безпечного функціонування об'єктів її інформаційної і кіберінфраструктури;

якщо $G_{захищ}^{рівень} < 45$, то рівень захищеності держави від ризику стороннього кібервпливу вважається недостатнім.

Таким чином, запропонована стратегія дасть можливість одержати кількісну оцінку рівня захищеності ОІД від ризику стороннього кібернетичного впливу, встановити вимоги до формування ними власних систем кібернетичної безпеки та розробити заходи спрямовані на підвищення їх результативності. Підставою таким діям може слугувати виявлення відхилень від штатного режиму функціонування державних ІР, ІТ систем і мереж, а також відповідних програмних і апаратних засобів, а саме, наприклад, виявлення ознак:

виведення з ладу окремих компонентів радіоелектронних систем;

змінювання алгоритмів функціонування ПЗ систем управління в ІТ системах і мережах;

несанкціонованих змін у файлах (їх розмірів та останньої дати модифікації);

порушення безпеки інформаційного обміну, протоколів передачі даних вхідного або вихідного трафіка, а також прав доступу користувачів до ІР;

уповільнення завантаження та роботи ПЕОМ;

зменшення обсягів вільної оперативної пам'яті;

виконання неконтрольованих процесів тощо.

Окрім всього цьому може сприяти виявлення чисельних помилок при завантаженні ОС, неможливості збереження файлів у необхідних каталогах, а також незрозумілих системних повідомлень, музикальних і візуальних ефектів.

НАВЧАЛЬНЕ ВИДАННЯ

Володимир Леонідович БУРЯЧОК
Володимир Борисович ТОЛУБКО
Володимир Олексійович ХОРОШКО
Сергій Васильович ТОЛЮПА

ІНФОРМАЦІЙНА І КІБЕРБЕЗПЕКА:
соціотехнічний аспект

підручник
(українською мовою)

Підписано до друку 01.09.2018 р.
Формат 60x84/16. Папір друк. №2. Гарнітура Times New Roman
Умовн. друк. арк. 20

ПП «Магнолія 2006»
а/с 431, м. Львів-53, 79053, Україна, тел./факс 240-54-84; 245-63-70 e-mail: magnol@lviv.farlep.net
Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції: серія ДК № 2534 від 21.06.2006 року,
видане Державним комітетом інформаційної політики, телебачення та радіомовлення України

Надруковано у друкарні видавництва «Магнолія 2006»